854/1

# RAADGEVENDE INTERPARLEMENTAIRE BENELUXRAAD

2 september 2012

## CONFERENTIE

**"De bewustmaking van de burger van de risico's van cybercrime"**

**Luxemburg, vrijdag 26 april 2013[1]**

## VERSLAG

[1] Deze conferentie vond plaats in de *Chambre des Députés* van het Groothertogdom Luxemburg.

VAST SECRETARIAAT
VAN DE INTERPARLEMENTAIRE BENELUXRAAD
PALEIS DER NATIE — BRUSSEL

# CONSEIL INTERPARLEMENTAIRE CONSULTATIF DE BENELUX

2 septembre 2012

## CONFÉRENCE

**"La sensibilisation du public aux risques de la cybercriminalité"**

**Luxembourg, vendredi 26 avril 2013 [1]**

## RAPPORT

[1] Cette conférence a eu lieu à la Chambre des Députés du Grand-Duché de Luxembourg.

SECRETARIAT PERMANENT
DU CONSEIL INTERPARLEMENTAIRE DE BENELUX
PALAIS DE LA NATION — BRUXELLES

## PROGRAMMA

## DE BEWUSTMAKING VAN DE BURGER VAN DE RISICO'S VAN CYBERCRIME

**Voorzitters**: mevrouw Ingrid de Caluwé, voorzitter van de commissie Justitie en Binnenlandse Zaken, en de heer Xavier Bettel, voorzitter van de commissie Economische Aangelegenheden, Landbouw en Visserij

Voormiddag: Welkomstwoord door mevrouw Ingrid de Caluwé en de heer Xavier Bettel

Uiteenzettingen door:

— de heer Luc Beirens, hoofd van de Federal Computer Crime Unit (FCCU), Federale Politie, België;
— de heer Patrick Houtsch, directie CERT (*Computer Emergency Response Team*) gouvernemental, Luxemburg;
— de heer Karlis Engelis, *member of the Legal Affairs and Security Committee* van de Baltische Assemblee.

Namiddag: Uiteenzettingen door:

— de heer Fred Streefland, *director Education, Training & Knowledge Center, European Network for Cybersecurity* (ENCS), Nederland;
— de heer Gérard Hoffmann, CEO Telindus, Luxemburg.

Paneldebat

Besluit

Afkortingen
(B): België – (L): Luxemburg – (NL): Nederland
(BA): Baltic Assembly
N.: in het Nederlands – F.: in het Frans – E.: in het Engels

## PROGRAMME

## LA SENSIBILISATION DU PUBLIC AUX RISQUES DE LA CYBERCRIMINALITÉ

**Présidents**: Mme Ingrid de Caluwé, présidente de la commission de la Justice et des Affaires intérieures, et M. Xavier Bettel, président de la commission des Affaires économiques, de l'Agriculture et de la Pêche

Matin: Paroles de bienvenue de Mme Ingrid de Caluwé et M. Xavier Bettel

Exposés de:

— M. Beirens, chef de la Federal Computer Crime Unit (FCCU), Police fédérale, Belgique;

— M. Patrick Houtsch, chargé de la direction CERT (*Computer Emergency Response Team*) gouvernemental, Luxembourg;
— M. Karlis Engelis, *member of the Legal Affairs and Security Committee* de l'Assemblée balte.

Après-midi: Exposés de:

— M. Fred Streefland, *director Education, Training & Knowledge Center, European Network for Cybersecurity* (ENCS), Pays-Bas;
— M. Gérard Hoffmann, CEO Telindus, Luxembourg.

Table ronde

Conclusions

Abbréviations
(B): Belgique – (L): Luxembourg – (NL): Pays-Bas
(BA): Baltic Assembly
F.: en français – N.: en néerlandais – E.: en anglais

## PROGRAMME

## MAKING THE PUBLIC AWARE OF THE RISKS OF CYBERCRIME

Chairs: Mrs Ingrid de Caluwé, chairwoman of the Justice and Home Affairs Committee, and Mr Xavier Bettel, chairman of the Economic Affairs, Agriculture and Fishery Committee

A.M.: Welcome address by Mrs Ingrid de Caluwé and Mr Xavier Bettel

Presentations by:

— Mr Luc Beirens, head of the Federal Computer Crime Unit (FCCU), Federal Police, Belgium;

— Mr Patrick Houtsch, in charge of the government direction CERT (Computer Emergency Response Team), Luxemburg;

— Mr Karlis Engelis, member of the Legal Affairs and Security Committee of the Baltic Assembly

P.M.: Presentations by:

— Mr Fred Streefland, director Education, Training & Knowledge Center, European Network for Cybersecurity (ENCS), the Netherlands;

Mr Gérard Hoffmann, CEO Telindus, Luxemburg.

Debate

Closing remarks

## INHOUD

Welkomstwoord door mevrouw Ingrid de Caluwé en de heer Xavier Bettel ..... 6

Uiteenzetting door de heer Luc Beirens, hoofd van de *Federal Computer Crime Unit* (FCCU), Federale Politie, België..... 8

Uiteenzetting door de heer Patrick Houtsch, directie CERT (*Computer Emergency Response Team*) gouvernemental, Luxemburg ..... 18

Uiteenzetting door de heer Karlis Engelis, *member of the Legal Affairs and Security Committee* van de Baltische Assemblee 28

Uiteenzetting door de heer Fred Streefland, *director Education, Training & Knowledge Center, European Network for Cybersecurity* (ENCS), Nederland..... 32

Uiteenzetting door de heer Gérard Hoffmann, CEO Telindus, Luxemburg .... 41

Paneldebat ..... 50

Besluit..... 61

Bijlagen:

1. Presentatie van de heer Beirens..... 65

2. Presentatie van de heer Streefland .... 95

3. Presentatie van de heer Hoffman..... 123

## INHOUD

Paroles de bienvenue par Mme Ingrid de Caluwé et M. Xavier Bettel ..... 6

Présentation par M. Beirens, chef de la *Federal Computer Crime Unit* (FCCU), Police fédérale, Belgique..... 8

Présentation par M. Patrick Houtsch, chargé de la direction CERT (*Computer Emergency Response Team*) gouvernemental, Luxembourg..... 18

Présentation par M. Karlis Engelis, *member of the Legal Affairs and Security Committee* de l'Assemblée balte..... 28

Présentation par M. Fred Streefland, *director Education, Training & Knowledge Center, European Network for Cybersecurity* (ENCS), Pays-Bas ..... 32

Présentation par M. Gérard Hoffmann, CEO Telindus, Luxembourg..... 41

Table ronde..... 50

Conclusions..... 61

Annexes:

1. Présentation de M. Beirens ..... 65

2. Présentation de M. Streefland ..... 95

3. Présentation de M. Hoffman..... 123

## DEELNEMERS

*Sprekers*

Luc Beirens, Patrick Houtsch, Karlis Engelis, Fred Streefland, Gérard Hoffmann

*Leden van het Beneluxparlement*

Xavier Bettel, Philippe Collard, Patricia Creutz, Ingrid de Caluwé, Michel Lebrun, Roger Negri, Marcel Oberweis, Nanneke Quik-Schuijt, Daniel Senesael, Louis Siquet, Sabine Vermeulen, Veerle Wouters

*Andere personen*

Gilles Herrmann, substitut principal, Parquet de Luxembourg, section économique et financière

*Benelux Unie*

Luc Willems, Alain De Muyser, Sonja Van Rossem, Thierry Charlier

## PARTICIPANTS

*Orateurs*

Luc Beirens, Patrick Houtsch, Karlis Engelis, Fred Streefland, Gérard Hoffmann

*Membres du Parlement Benelux*

Xavier Bettel, Philippe Collard, Patricia Creutz, Ingrid de Caluwé, Michel Lebrun, Roger Negri, Marcel Oberweis, Nanneke Quik-Schuijt, Daniel Senesael, Louis Siquet, Sabine Vermeulen, Veerle Wouters

*Autre personnes*

Gilles Herrmann, substitut principal, Parquet de Luxembourg, section économique et financière

*Union Benelux*

Luc Willems, Alain De Muyser, Sonja Van Rossem, Thierry Charlier

De vergadering wordt om 11 uur geopend

**Verwelkoming door de voorzitters van de conferentie**

*De heer Bettel (L) F.-* Dames en heren, ik heet u van harte welkom op deze vergadering die door mevrouw de Caluwé zal worden voorgezeten. Het verheugt mij ten zeerste u in het Luxemburgs parlement te mogen verwelkomen, het onderwerp dat zal worden besproken is immers zeer interessant en belangt ons allen aan.

Twee weken geleden zijn we in de Senaat te Brussel bijeengekomen om de organisatie van deze dag te bespreken. De zeer interessante en zeer levendige discussie dreigde ons zelfs ietwat mee te slepen en we hebben op de rem moeten gaan staan, anders was het debat voortijdig van start gegaan.

We hebben het geluk te worden toegesproken door sprekers uit België, Luxemburg en Nederland over een onderwerp dat uitermate interessant en actueel is. Mevrouw de Caluwé heeft me gezegd dat Nederland door een IDOS-aanval werd getroffen. Ik ben, zoals anderen veronderstel ik, benieuwd naar wat dat betekent.

Ook Luxemburg werd onlangs aangevallen. Het onderwerp werd trouwens uitgebreid om de commissieleden en degenen die niet aanwezig waren op de vergadering te Brussel, in te lichten. We hebben beslist ook de beveiliging van aankopen online door internetgebruikers te behandelen. Uiteraard komen er nog andere onderwerpen aan bod, maar ik zal ze hier niet onthullen aangezien ze onze commissie aanbelangen. Ik dank u voor uw aandacht en ik geeft het woord aan mevrouw de Caluwé die het debat zal openen.

*Mevrouw de Caluwé (NL) N.* — Goedemorgen en welkom bij deze conferentie over cybersecurity in het Beneluxparlement. Welkom ook aan de hier reeds aanwezige sprekers, de heren Beirens, Houtsch, Engelis en Streefland.

Wat kunnen we zeggen over cybersecurity? Het is een ontzettend breed onderwerp dat over vele dingen gaat. Men kan het hebben over aankopen

La séance est ouverte à 11 heures

**Paroles de bienvenue par les présidents de la conférence**

*M. Bettel (L) F.-* Mesdames et messieurs, je vous souhaite la bienvenue à cette réunion, sous la présidence de Mme de Caluwé. Je suis d'autant plus heureux de vous accueillir au sein du parlement luxembourgeois, qu'il s'agit d'un sujet très intéressant qui nous concerne tous.

Il y a quinze jours, nous nous sommes rencontrés à Bruxelles, au Sénat, pour discuter de l'organisation de cette journée. Les débats, très intéressants, et fort animés, ont d'ailleurs failli nous emporter un peu trop loin et nous avons nous freiner afin de ne pas lancer le débat prématurément.

Nous avons la chance de bénéficier d'intervenants venant de Belgique, du Luxembourg et des Pays-Bas, sur un sujet on ne peut plus intéressant et d'actualité. Mme de Caluwé m'a fait part d'une attaque d'IDOS aux Pays-Bas. Comme d'autres j'imagine, je suis impatient de savoir ce que cela signifie.

Des attaques sont également survenues au Luxembourg récemment. Ce sujet sera d'ailleurs élargi afin d'informer les membres des commissions et ceux qui n'étaient pas présents lors de la réunion à Bruxelles. Nous avons décidé aussi de l'étendre à la sécurisation des achats on-line par des usagers. D'autres thèmes seront évidemment abordés mais je ne les dévoilerai pas ici car ils concernent notre commission. En vous remerciant de votre attention, je cède la parole à Mme de Caluwé, qui lancera les débats.

*Mme de Caluwé (NL) N.* — Bonjour et bienvenue à cette conférence sur la cybersécurité. Bienvenue aussi aux orateurs déjà présents, MM. Beirens, Houtsch, Engelis en Streefland.

Que pouvons-nous dire de la cybersecurité? C'est un très vaste sujet qui touche à bien des domaines. Nous pourrions parler des achats en

via internet, over kinderporno, over aanvallen op vitale infrastructuur, alles is mogelijk.

We hebben beslist het onderwerp toch iets te beperken zodat we niet tot een heel breed debat komen, maar wel tot concrete aanbevelingen aan onze ministers, wat toch uiteindelijk de bedoeling is, en ook tot een concreet actieplan voor de Benelux.

Daarom is ervoor gekozen om vandaag te praten over de bewustwording. De bewustwording bij burgers, bij bedrijven en organisaties over wat er kan gebeuren. Waar kan men last van hebben bij een cyberattack? Hoe ver kan dit gaan?

Van daaruit kunnen we verder gaan en uitzoeken hoe we die bewustwording kunnen vergroten.

De sprekers kunnen daarover ook suggesties doen.

De heer Oberweis heeft reeds gesproken over een eventuele *follow-up* van deze conferentie, over specifieke acties die dan op Beneluxniveau zouden kunnen worden uitgevoerd.

Deze ochtend krijgen we dus drie presentaties, daarna na de middag volgen nog twee presentaties en een paneldebat waarvoor ik u hartelijk uitnodig.

Ik geef nu graag het woord aan de heer Beirens van de Belgische Federale Politie.

*De heer Bettel (L) F.* — Dames en heren, u hebt gemerkt dat op deze vergadering de heer Engelis van de Baltische Assemblee aanwezig is die de situatie en de realisaties in de Baltische landen zal toelichten, alsook de heer Herrmann, eerste substituut van Luxemburg die te uwer beschikking staat om te antwoorden op uw vragen met betrekking tot de strafrechtelijke, repressieve aspecten en de middelen waarover de parketten beschikken. Ik dank hem voor zijn bereidheid de leden van onze assemblee over dat belangrijk onderwerp in te lichten.

ligne, de la pédopornographie, des attaques contre des infrastructures vitales, tout est possible.

Nous avons néanmoins choisi de circonscrire quelque peu le sujet afin de ne tomber dans un vaste débat mais d'en arriver à des recommandations claires à l'intention de nos ministres, ce qui est en définitive l'objectif poursuivi, et de déboucher aussi sur un plan d'action concret pour le Benelux.

C'est pourquoi nous avons décidé de parler aujourd'hui de la sensibilisation. La sensibilisation de nos concitoyens, des entreprises et des organisations à ce qui peut survenir. Que risque-t-on en cas de cyberattaque? Jusqu'où cela peut-il aller?

Nous pourrons partir de là et voir comment la accroître sensibilisation.

Les orateurs pourront formuler des suggestions à ce propos.

M. Oberweis a déjà évoqué un éventuel suivi de cette conférence, ainsi que des actions spécifiques qui pourraient être menées au niveau du Benelux.

Nous allons donc entendre ce matin trois présentations. Il y aura ensuite dans le courant de l'après-midi deux autres présentations et un débat auquel je vous convie de tout cœur.

Je cède à présent la parole à M. Beirens, de la police fédérale belge.

*M. Bettel (L) F.* — Mesdames et messieurs, vous remarquerez la présence à cette séance de M. Engelis du Parlement balte, qui exposera la situation et les réalisations au niveau des pays baltes, ainsi que celle de M. Herrmann, Premier substitut du procureur d'État du Luxembourg. Il s'occupe de la cybercriminalité et se tiendra à votre disposition pour répondre à vos questions relatives au volet pénal, donc répressif, des arsenaux dont les parquets se sont pourvus. Je le remercie d'avoir bien voulu donner de son temps afin d'éclairer les membres de notre Assemblée sur ce sujet si important.

**Uiteenzetting door de heer Luc Beirens, hoofd van de *Federal Computer Crime Unit* (FCCU), Federale Politie, België**

*De heer Beirens (B) N.-* Goedemorgen iedereen. Ik ben diensthoofd van de *Federal Computer Crime Unit*, de centrale cybercrime eenheid in België, die deel uitmaakt van de Federale gerechtelijke politie.

Vorig jaar, in de plenaire zitting van het Beneluxparlement in Den Haag, heb ik een volledige uiteenzetting gegeven over de dreigingen van cybercrime en geschetst wat op ons afkwam op het gebied van cybercriminaliteit. Sindsdien hebben we een aantal nieuwe fenomenen gezien, onder andere police ransomware. Bij police ransomware wordt je computersysteem plots geblokkeerd door kwaadaardige software die zich op je computer installeert en die zegt: de politie blokkeert je computersysteem en nu moet je honderd of tweehonderd euro betalen om je systeem te deblokkeren. Alleen al dit jaar zijn in België tienduizenden mensen daar het slachtoffer van geworden. Verschillende duizenden mensen hebben daar een klacht over neergelegd bij de politie.

Toch krijgen we elke dag opnieuw nog mensen aan de telefoon die ons meedelen dat “er iets nieuws is”. Wij merken dus dat men niet op de hoogte is van dit fenomeen ondanks de verschillende campagnes die we al gevoerd hebben.

Een soortgelijk fenomeen dat recent heel actueel is geworden, is phishing. Ook sinds vorig jaar zien we dat er, zowel in Nederland als in België, e-mails toekomen die zeggen: u moet uw banktoepassingen online bijwerken, want de security moet geüpdatet worden. Men verwijst naar financiële fraude en misbruik van banktoepassingen. De mensen worden ertoe aangezet om te klikken op de link in de e-mail, waarna ze op een valse website terechtkomen waar ze gegevens moeten invullen, onder andere hun telefoonnummer. Vervolgens wordt ze gemeld dat het niet lukt online en dat ze telefonisch gecontacteerd zullen worden, waarna ze ertoe gebracht worden om een toestel te gebruiken om transacties te bevestigen.

**Présentation par M. Beirens, chef de la *Federal Computer Crime Unit (*FCCU), Police fédérale, Belgique**

*M. Beirens (B) N.-* Bonjour à tous. Je dirige la *Federal Computer Crime Unit*, l’unité de lutte contre la cybercriminalité qui, en Belgique, fait partie de la policie judiciaire fédérale.

L’an dernier lors de la session pléniaire du Parlement Benelux àLa Haye, j’avais fait un exposé complet sur les menaces de la cybercriminalité et j’avais indiqué ce à quoi nous devions nous attendre en matière de cybercriminalité. Depuis, un certain nombre de phénomènes nouveaux sont apparus, dont le police ransomware. Dans le cas du police ransomware, le système informatique est subitement bloqué par des logiciels malveillants qui s’installent sur votre système et qui vous disent: la police bloque votre système informatique et vous devez payer cent ou deux cents euros pour le débloquer. Rien que cette année, des dizaines de milliers de personnes en ont été victimes. Plusieurs milliers de citoyens ont porté plaite à ce sujet auprès de la police.

Pourtant, des gens nous téléphonent encore quotidiennement pour nous annoncer “quelque chose de nouveau”. Nous observons donc qu’en dépit des campagnes que nous avons déjà menées, l’on ignore que le phénomène est déjà en cours.

Un phénomène analogue devenu tout récemment très actuel est le phishing. Depuis l’an dernier également, nous voyons, aux Pays-Bas comme en Belgique, que des e-mails sont envoyés pour signaler que la sécurisation d’applications bancaires en ligne doit être mise à jour. Il est fait référence à la fraude financière et à l’utilisation abusive d’applications bancaires. Les gens sont invités à cliquer sur le lien contenu dans le courriel, ce qui les mène vers un faux site internet où il leur est demandé de fournir des renseignements, dont leur numéro de téléphone. Il leur est dit que l’opération a échoué en ligne et qu’ils seront recontactés par téléphone, après quoi ils sont amenés à utiliser un appareil pour confirmer des transactions.

Dat is met betrekking tot de eindgebruiker. Bij de bedrijven zien we iets helemaal anders. Zowel in havenbedrijven als in grote transportmaatschappijen dringen de criminelen binnen in de netwerken om door spionage codes te ontfutselen zodat ze kunnen tussenkomen in de transporten en containers kunnen afhalen.

Wanneer we dan gaan kijken naar de infrastructuur, zien we dat de telecomoperatoren eigenlijk nooit echt zeer betrokken zijn geweest in de strijd tegen botnets.

U vroeg daarnet wat een DDOS is, een distributed denial of service – wij gebruiken graag Engelse termen, al is het niet de bedoeling u daarmee plat te slaan. Een distributed denial of service attack is een aanval waarbij men, vanaf geïnfecteerde personal computers van eindgebruikers, (pc's dus die zijn overgenomen door kwaadaardige software), een grote hoeveelheid aanvragen lanceert naar een en hetzelfde punt, waardoor die computer overbelast raakt of waardoor de capaciteit van de internetverbinding geblokkeerd wordt. Op de Nederlandse banken zijn er een aantal van die aanvallen geweest, maar we zien het fenomeen in verschillende landen opduiken.

Vroeger waren de operatoren eigenlijk niet geïnteresseerd in de botnets, dus in al die geïnfecteerde pc's die onder controle staan van de hackers. Vandaag zien we ook bij die mensen een interesse ontstaan, want een distributed denial of service neemt een bandbreedte af en neemt dus capaciteit van een internetconnectie af, waardoor ze plots ook zelf slachtoffer worden.

Ik geef u die nieuwe update om u erop attent te maken dat de dreigingen van vorig jaar er nog steeds zijn, maar vandaag zijn er nieuwe dreigingen. Niettegenstaande de bewustmakingscampagnes al een hele tijd lopen, bellen mensen ons dagelijks en zien we dat ze vaak nog uit de lucht vallen, dat ze niet weten wat er aan de hand is. Daarom zijn die campagnes zo noodzakelijk.

Wat zien we wanneer we websites opzetten, wanneer we informatiesessies houden? Wie komt

Voilà pour ce qui concerne l'utilisateur final. Au niveau des entreprises, nous assistons à quelque chose de très différent. Qu'il s'agisse d'entreprises portuaires ou de grandes sociétés de transport, des criminels s'introduisent dans les réseaux pour mettre la main, par des pratiques d'espionnage, sur des codes qui leur premettent d'intervenir dans les transports et de s'approprier des conteneurs.

En ce qui concerne l'infrastructure, nous observons que les opérateurs de télécoms ne se sont en fait jamais sentis très concernés par la lutte contre les botnets.

Vous avez demandé il y a un instant ce qu'est un DDOS, un distributed denial of service – nous utilisons volontiers des termes anglais mais sans aucunement vouloir vous impressionner. Un distributed denial of service attack est une attaque par laquelle on lance – à partir de PC infectés d'utilisateurs finaux des PC dont des logiciels malveillants ont pris les commandes donc – un grand nombre de demandes à destination d'un même point, ce qui a pour conséquence de saturer l'ordinateur ou de bloquer la capacité de la liaison internet. Des banques néerlandaises ont subi un certain nombre d'attaques de ce type mais le phénomène a fait son apparition dans différents pays.

Par le passé, les opérateurs ne se sont en fait pas souciés de ces botnets, c'est-à-dire de tous ces PC infectés contrôlés par des hackers. On observe aujourd'hui chez eux de l'intérêt pour la question dans la mesure où un distributed denial of service réduit la largeur de bande et donc la capacité d'une interconnection, ce dont ils deviennent soudain eux-mêmes les victimes.

Si je fais cette mise au point, c'est pour souligner que les menaces de l'an passé existent toujours mais que d'autres sont apparues depuis. Malgré les campagnes de sensibilisation en cours depuis un certain temps déjà, des gens nous téléphonent tous les jours et nous constatons qu'ils tombent des nues parce qu'ils ignorent de quoi il retourne. D'où la nécessité de mener ces campagnes.

Que constatons-nous lorsque nous créons des sites internet, que nous organisons des sessions

er naartoe? Wie is er op de hoogte? Dat zijn de slachtoffers. Wie slachtoffer geworden is, gaat zich informeren over wat er aan de hand is. Als je niet weet wat de dreiging is, kan je je ook niet gaan beveiligen.

Als we dus gaan kijken naar wie de partners zijn die allemaal in die campagne betrokken moeten worden, dan gaat het niet alleen over politie en justitie. Ik zal eerlijk zijn: de strijd tegen cybercriminelen ga je niet met de politie oplossen. Wij pakken af en toe eens een crimineel op, maar er zijn er zoveel dat de bescherming van de infrastructuur veel belangrijker is dan de strijd waar politie en justitie zich mee bezighouden.

We moeten dus gaan naar een versterking van de infrastructuur, naar het veilig maken zowel bij de operatoren als bij die eindgebruiker. Daarom moet die boodschap bij de eindgebruiker terechtkomen.

Politie en justitie hebben natuurlijk een rol, maar ook de CERT *Community*, de *Computer Emergency Response Teams*, waarvan u straks een presentatie zal zien.

De antivirusmaatschappijen zien enorm veel dreigingen. Zij maken ook rapporten, maar dat is zoals een jaarrapport van alle organisaties. Dat wordt gemaakt, mooi uitgeprint, maar dan is de vraag: wie leest dat? Juist daar moeten we toe komen, dat die boodschap niet op papier blijft staan, maar bij de mensen gebracht wordt. Die maatschappijen hebben dus ook een rol te spelen.

We zien in enkele landen cyberexpertisecentra ontstaan, die ook een rol willen spelen. Uiteindelijk zien we een grote verspreiding van expertise, waardoor niemand eigenlijk de zaak globaal bekijkt. We verspillen dus enorm veel capaciteit, zonder dat de boodschap effectief wordt overgebracht.

Een grote rol is voorbehouden voor de bedrijven zelf. Zij groeperen alle eindgebruikers. Bij u thuis bent u een gewone eindgebruiker, maar als u deel uitmaakt van een organisatie, moet die organisatie er ook voor zorgen dat de boodschap overgebracht wordt, dat de veiligheid van die organisatie ge-

d'information? Qui s'y rend? Qui est informé? Ce sont les victimes. Les victimes s'informent sur ce qui se passe. Car lorsqu'on ignore en quoi consiste une menace, on ne peut pas prémunir contre elle.

Lorsque nous essayons de déterminer qui est concerné, quels partenaires doivent être associés à la campagne, nous voyons qu'il ne s'agit pas seulement de la police et de la justice. Je vais être honnête: ce n'est pas la police qui va régler la lutte contre la cybercriminalité. Il nous arrive d'appréhender un criminel mais il y en a tellement que la protection de l'infrastructure est beaucoup plus importante que la lutte que mènent la police et la justice.

Nous devons donc aller vers un renforcement de l'infrastructure, vers une sécurisation au niveau des opérateurs comme des utilisateurs finaux. Et c'est pourquoi le message doit être délivré à l'utilisateur final.

La police et la justice ont certes un rôle à jouer mais il en va de même de la CERT *Community*, les *Computer Emergency Response Teams*, dont une présentation vous sera faite ultérieurement.

Les sociétés qui proposent des antivirus décèlent de très nombreuses menaces. Elle rédigent aussi des rapports mais il en va de ces rapports comme des rapports annuels de toutes les organisations. Il est réalisé, joliment imprimé. Reste la question: qui le lit? C'est précisément à cela qu'il faut arriver: il ne suffit pas que ce message soit inscrit sur papier, il doit aussi être délivré. Ces sociétés ont donc aussi un rôle à jouer.

Nous voyons se créer dans un certain nombre de pays des centres de cyberexpertise qui veulent également jouer un rôle. On assiste en définitive à une large diffusion de l'expertise qui a pour conséquence qu'il n'y a en fait jamais de globalisation. Nous gaspillons donc beaucoup de capacité, sans que le message ne soit effectivement délivré.

Un rôle important est réservé aux entreprises elles-mêmes. Elles regroupent tous les utilisateurs finaux. Chacun est un utilisateur final. Chez vous, à la maison, vous êtes un simple utilisateur final mais si vous faites partie d'une organisation, celle-ci doit faire en sorte que le message soit transmis,

garandeerd wordt door de juiste houding van de mensen die in de maatschappij zelf werken. Als organisatie kunnen we er dus ook voor zorgen dat de men de dreigingen beter leert kennen.

Naast de eindgebruikersorganisaties zijn er, last en zeker not least, de media: televisie, radio, de kranten. Dat zijn de kanalen waarmee je de meeste mensen bereikt. Als we het niet via televisie en radio kunnen spelen, dan komen we niet tot bewustmaking over de dreigingen van cybercrime.

Wat we niet mogen doen, is één boodschap brengen en denken dat we maar één boodschap te brengen hebben. Er zijn verschillende types van publiek. Je hebt de gewone eindgebruikers, in hun verschillende leeftijdsklasses. Aan jongeren die op school zitten, moet je niet dezelfde boodschap brengen als aan mensen van de derde leeftijd, die net met de computer leren werken. Die zitten in een andere leefwereld. Bij de jongeren gaan we spreken over sociale netwerken en de dreigingen die daarmee te maken hebben. Oudere mensen vragen zich af wat ze met al die gegevens moeten doen en zijn al tevreden als ze veilig kunnen bankieren online en op een veilige manier een reis boeken.

We moeten ons specifiek richten naar de dreigingen afhankelijk van de leeftijd.

Ook bedrijven kunnen we niet zomaar beschouwen als één groot geheel. Er zijn de kleine bedrijven, die soms maar één of zelfs geen informaticus hebben die kan instaan voor de veiligheid. Nochtans hebben zij wel een website. Het zijn die websites die gehackt worden om bijvoorbeeld phishing websites op te plaatsen. Het zijn websites van kleine bedrijven die gehackt worden en waar cybercriminelen dan een valse website van om het even welke bank op plaatsen. Die bedrijven moeten op hun verantwoordelijkheid worden gewezen omtrent de veiligheid die zij moeten bieden met hun website, niet alleen omdat er phishing websites op gezet kunnen worden, maar ook omdat er scripts in geïntegreerd kunnen worden.

Een paar weken geleden zijn in Nederland op een zaterdagmorgen, wanneer iedereen de tijd heeft om zijn krant te lezen, alle bezoekers van de

que la sécurité soit garantie par un comportement approprié des gens qui y travaillent. En tant qu'organisation, nous pouvons donc contribuer à mieux faire connaître les menaces.

Outres les organisations de consommateurs finaux, il y a, last but not least, très certainement pas, les médias: la télévision, la radio, les journaux – les gens lisent encore les journaux. Ce sont les canaux qui permettent d'atteindre la majorité des gens. Si nous ne pouvons pas agir par le biais de la télévision et de la radio, nous n'arriverons pas à sensibiliser les gens à la menace du cybercrime.

Ce que nous devons nous garder de faire, c'est délivrer un message en pensant qu'il n'y en a qu'un. Il y a plusieurs types de public. Il y a le simple utilisateur final, dans les différentes catégories d'âge. Or on n'apporte pas le même message aux jeunes qui vont à l'école qu'aux personnes du troisième âge qui aprennent à se servir d'un ordinateur. Ils vivent dans des mondes différents. Aux jeunes, on parlera de réseaux sociaux et des menaces qui y ont trait. Les personnes plus âgées se demandent quoi faire de toutes ces informations et sont déjà très heureuses de pouvoir faire du selfbanking en ligne ou réserver un voyage en toute sécurité.

Nous devons l'axer sur les menaces en fonction de l'âge.

Les entreprises non plus ne peuvent pas être tout bonnement considérées comme un seul vaste ensemble. Il y a les petites entreprises qui ne comptent parfois qu'un informaticien voire même aucun pour assurer leur sécurité. Elles ont pourtant un site internet. Ce sont ces sites qui sont hackés pour y installer, par exemple,des sites de phishing. Il s'agit de sites internet de petites entreprises qui sont hackés et où des cybercriminels installent un faux site internet de l'une ou l'autre banque. Ces entreprises doivent être sensibilisées à la nécessité de sécuriser leur site internet, non seulement parce que des sites de phishing peuvent y être installés mais aussi parce que des scripts peuvent y être intégrés.

Il y a quelques semaines, aux Pays-Bas, un samedi matin, à un moment où chacun a le temps de lire le journal, tous les visiteurs du site internet

website van NRC Handelsblad, een vrij populaire krant, vier uur aan een stuk geïnfecteerd met een kwaadaardige software. Dat is kunnen gebeuren omdat die bedrijven onvoldoende bezig zijn met hun website en zich onvoldoende bewust zijn van het risico dat bezoekers van hun website lopen.

We moeten aan bedrijven dus de boodschap brengen, niet alleen dat ze gehackt kunnen worden, maar ook dat als ze gehackt zijn, hun website misschien misbruikt zal worden en ze misschien mee burgerrechtelijk aansprakelijk zullen worden gesteld voor de schade die ze veroorzaken door nalatigheid in hun security.

Wanneer we dan gaan kijken naar de grotere bedrijven, zien we op dit moment dat spionage zeer intensief is, met zeer gerichte aanvallen: e-mails die gezonden worden met kwaadaardige software die specifiek geschreven wordt voor een paar personen en die dus niet door de antivirusmaatschappijen gedetecteerd wordt. Bij de grote maatschappijen, de kritieke infrastructuren, zien we dus allerlei andere dreigingen.

Een bijzonder publiek waaraan we aandacht moeten besteden, zijn de mensen die producten ontwikkelen inzake security: software, hardware. Als we die mensen niet bewust maken van wat de dreigingen zijn en van de noodzaak om verdere stappen te ondernemen, zijn we niet goed bezig. Maar vaak zien we dat die mensen in hun eigen wereldje, in hun eigen cocon blijven zitten en niet op de hoogte zijn van de echte dreigingen.

Ik wil nog kort vertellen wat de Federale politie in België daarrond doet. Wij hebben een vrij gediversifieerd programma met betrekking tot bewustmaking. We hebben de website van de Federale politie en onze website e-cops, waar men kinderpornografie online kan melden.

Op zich zijn dat statische websites. Wie komt daarnaartoe of hoe kom je op die website? Slechts weinig mensen in het grote publiek zijn geïnteresseerd in de politie en waarmee deze bezig is. Ze komen op die website als ze op google een aantal trefwoorden ingevuld hebben omdat ze slachtoffer geworden zijn. Wij krijgen enorm veel telefoontjes in de unit omdat op de police randsomware, de afpersingssoftware, onze naam staat. De mensen

du très populaire quotidien NRC Handelsblad ont été infectés quatre heures durant par un logiciel malveillant. Cela a été rendu possible parce que ces entreprises se soucient insuffisamment de leur site internet et ne sont pas assez conscientes des risques que courent les visiteurs de leur site.

Nous devons donc dire aux entreprises que non seulement elles peuvent être hackées mais aussi que lorsqu'elles l'on été, leur site internet sera peut-être utilisé abusivement et qu'elles pourront être rendues civilement coresponsables des dommages qu'elles causent par la négligence dont elles font preuve concernant leur sécurisation.

Si nous nous tournons à présent vers les grandes entreprises, nous voyons que l'espionnage est actuellement très intense, avec des attaques très ciblées: e-mails comportant des logiciels malveillants écrits spécifiquement pour un certain nombre de personnes et que ne détectent donc pas les sociétés qui produisent des antivirus. On observe donc au niveau des grandes entreprises, des infrastructures critiques, toutes sortes d'autres menaces.

Un public particulier auquel il faut être attentif est celui des personnes qui développent des produits dans le domaine de la sécurité: software, hardware. Nous commettrions une erreur en ne les sensibilisant pas aux menaces et à la nécessité d'effectuer des démarches plus avant. Mais nous constatons souvent que ces gens se complaisent dans leur monde, dans leur cocon et ne sont pas informés des véritables menaces.

Je voudrais vous dire brièvement ce que fait à ce propos la police fédérale belge. En matière de sensibilisation, nous avons un programme très diversifié. Nous avons le site internet de la police fédérale et notre propre site e-cops, où l'on peut signaler les faits de pédopornographie.

Il s'agit de sites internet statiques. Qui les visite et comment y accède-t-on? Peu de gens parmi le grand public se soucient de la police et de ce qu'elle fait. Elles visitent le site après avoir tapé sur google un certain nombre de mots clés parce que'elles ont été victimes d'un abus. Nous recevons énormément d'appels téléphoniques à l'unité parce que notre nom est mentionné sur le police randsomware, un logiciel de racket comme je l'ai dit. Les gens

willen af van die blokkade, vullen onze naam in, zien ons telefoonnummer en op dat moment komen ze eventueel op de website terecht, maar anders niet.

We moeten ze daar dus effectief naartoe brengen. Er zijn een aantal collega's die bloggen over *security* – zelf doe ik dat ook af en toe. Dan is er het tweeten, we vinden onszelf daar zo belangrijk in, maar hoeveel mensen bereiken we daar uiteindelijk mee? Is het effectief dat publiek dat dan slachtoffer wordt? Neen, wie ons al volgt is natuurlijk een stuk wijzer; het zijn de anderen die in de val van de cybercriminelen lopen.

Er zijn informatiesessies, zeer specifiek gericht op de IT-afdelingen van hogescholen en universiteiten, om daar de boodschap te brengen in het laatste jaar. Als de afgestudeerden in de bedrijven komen, kunnen ze die boodschap daar overbrengen. In de scholen zelf gaan we niet zo dikwijls uiteenzettingen geven, want de vraag is te groot. We gaan wel naar de scholen waar zich al problemen voorgedaan hebben. Dan doen we zeer ruime presentaties waardoor de mensen bewust worden dat ook cyberpesten en misbruik van die cyberinfrastructuur in hun school een belangrijke rol kan spelen.

Voor kleine bedrijven werken wij samen met de federatie van kmo's in België. Er zijn verschillende federaties. We geven in de verschillende regio's informatie over de dreigingen en tegelijkertijd komen we – dat is dan iemand anders – met een stuk oplossing. Je moet de mensen niet alleen bang maken, je moet ze ook oplossingen aanreiken. Dat is het stuk dat in de bewustmaking vaak ontbreekt. Dat zien we ook in de pers. De pers brengt de sensatie, maar vergeet de oplossingen te brengen. Daar moeten we ons in onze bewustmakingsacties absoluut mee bezighouden.

Als we radio en televisie meekrijgen, zijn we goed bezig. In België hebben we sinds de jaren zeventig op televisie "Kijk Uit" – voordien was het "Veilig Verkeer". "Kijk Uit" gaat over de dreigingen van het verkeer in het reële leven. Wat is daar zo bijzonder aan en waarom blijft dat sinds de jaren zeventig actueel? Dat is omdat er een politieman in

veulent résoudre ce problème de blocage, tapent notre nom, voient notre numéro de téléphone et se retrouvent éventuellement sur le site internet. Sinon, ils ne le consultent pas.

Nous devons donc les y amener. Un certain nombre de collègues participent à des blogs dédiés à la sécurité, ce que je fais parfois moi-même. Il y a aussi les tweets – et nous nous y trouvons très importants – mais combien de gens touchons-nous en définitive? S'agit-il bien du public de victimes potentielles? Non car ceux qui nous suivent sont mieux informés. Ce sont les autres qui tombent dans les pièges des cybercriminels.

Nous avons les sessions d'information axées très spécifiquement sur les sections IT des hautes écoles et des universités où nous délivrons le message à l'intention des étudiants de dernière année qui le transmettront à leur tour lorsqu'ils arriveront dans les entreprises. Nous n'allons pas souvent dans les écoles proprement dites car la demande est trop importante. Mais nous allons dans les écoles où des problèmes se sont déjà posés. Nous y faisons alors des présentations détaillées pour sensibiliser au rôle important que peuvent jouer le cyber-harcèlement ou l'utilisation abusive de la cyberinfrastructure dans l'école.

Concernant les petites entreprises, nous travaillons avec les fédérations de PME de Belgique. Elles sont plusieurs. Nous nous rendons dans les différentes régions pour y informer sur les menaces. Par la même occasion, nous – il s'agit alors d'une autre personne – proposons une partie de solution. Car il ne faut pas seulement faire peur, il faut aussi apporter des solutions. C'est un élément qui fait souvent défaut dans la démarche de sensibilisation. Nous le voyons aussi dans la presse. La presse apporte le sensationnel mais oublie de proposer des solutions. C'est un aspect dont nous devons absolument nous préoccuper dans nos actions de sensibilisation.

Si nous bénéficions du concours de la radio et de la télévision, ce serait une bonne chose. En Belgique, nous avons depuis les années septante à la télévision l'émission "*Kijk Uit*" – anciennement "*Veilig Verkeer*". "*Kijk Uit*" traite des dangers de la circulation dans la vie réelle. En quoi est-elle pertinente et comment se fait-il qu'elle a conservé son

uniform uitleg komt geven er wordt als het ware een gezicht geplakt op de campagne. Dat zorgt voor interactie, want die uitzending krijgt tegelijkertijd ook vragen van de kijkers.

Als je dus een gezicht kan plakken op een campagne, krijg je een veel grotere respons. Toch is het voor ons zeer moeilijk – ik heb nochtans al een paar keer voorstellen gedaan, zowel aan de VRT als aan de VTM, om iets te brengen. In het Franstalig landsgedeelte hebben we bij de radio "*Surfons Tranquille*". Elke week wordt daar een zeer korte boodschap van één minuut gebracht waarbij ook interactie plaatsvindt. Je krijgt automatisch vragen en je gaat mensen bewust maken, op één bepaald kanaal – niet het meest populaire, maar het is een stap. In Vlaanderen bestaat dat niet.

We zijn dus eigenlijk een insteek aan het zoeken om het grote publiek te bereiken. Vorige week ben ik gaan samenzitten met VTM, met de mensen die de scripts schrijven voor "Familie", een soap. Met die soap bereiken we 700 000 mensen, elke dag opnieuw, dus ben ik daar de uiteenzetting gaan geven over de dreigingen en de meest elementaire tips die de men moet naleven.

Als we steun kunnen krijgen voor dit opzet, gaan we een veel groter publiek hebben en bereiken we ook de personen die niet tot onze websites toetreden, die niet naar die informatiesessies komen. Dat is nochtans het publiek waar we op focussen en waar we mee verder willen gaan.

Ik denk dat de noodzaak van televisie evident als voorstel moet worden geformuleerd. Televisie kost geld en in alle strategieën over cybersecurity, zowel voor Nederland, Luxemburg als voor België, is er het aspect van de noodzaak van informatie van bevolking. Maar, je kan niet koken zonder ingrediënten en ingrediënten kosten nu eenmaal geld.

Dus, als we een boodschap willen brengen via de televisie, dan moeten we dat mee voorzien in het budget. Als er geen budget is – en ik weet dat het moeilijke tijden zijn – dan gaan we nog meer schade lijden. De afweging moet gebeuren: hoeveel

caractère d'actualité depuis les années septante? Parce qu'elle est associée à un visage, celui d'un policier en uniforme qui vient expliquer les choses. Il en résulte une interaction dans la mesure où l'émission reçoit aussi les questions que lui adressent les spcetateurs.

Si l'on peut associer un visage à une campagne, le retour sera beaucoup plus important. Mais il nous est très difficile d'obtenir quelque chose, bien que j'ai déjà fait des propositions à la VRT et à VTM. Dans la partie francophone du pays, il y a l'émission radiophonique "Surfons Tranquille". Chaque semaine, un court message d'une minute y est diffusé et les gens peuvent interagir. Des questions sont automatiquement formulées et les gens sont sensibilisés sur un canal – ce n'est pas le plus populaire mais c'est un premier pas. Nous n'avons rien de tel en Flandre.

Nous sommes donc à la recherche d'un moyen de toucher le grand public. La semaine dernière, j'ai rencontré chez VTM les gens qui écrivent les scénarios de "*Familie*", un soap. L'émission est regardée quotidiennement par 700 000 personnes. J'y ai donc fait un exposé sur les menaces et sur les précautions élémentaires à prendre.

Si nous pouvons recevoir de l'aide pour cela, nous aurons un public beaucoup plus large et nous toucherons aussi les personnes qui ne se rendent pas sur notre site, qui n'assistent pas aux sessions d'information. C'est pourtant le public que nous visons et avec lequel nous voulons aller de l'avant.

Je pense que si des dispositions doivent être formulées, la télévision est une nécessité. La télévision coûte de l'argent et toutes les stratégies en matière de cybersecurité comportent, aux Pays-Bas, en Belgique et au Luxembourg, un élément lié à la nécessité d'informer la population. Mais pour cuisiner, il faut des ingrédients et les ingrédients coûtent de l'argent.

Ainsi donc, si nous voulons délivrer un message par le canal de la télévision, nous devons le prévoir dans le budget. S'il n'y a pas de budget – et je sais que les temps sont difficiles – nous subirons des dommages plus grands encore. Ce choix doit

wil je investeren in preventie of hoeveel schade wil je lijden omdat de mensen onbewust zijn gebleven?

Dat is eigenlijk onze bedoeling. We kunnen met de verschillende landen samenwerken met betrekking tot de content van de verschillende websites, de ideeën rond campagnes samenleggen en hergebruiken. We doen immers al te veel dubbel werk, in elk land apart.

Ik beëindig hier mijn presentatie. Dank u wel.

*Mevrouw de Caluwé (NL) N.-* Heel hartelijk dank, mijnheer Beirens. Ik denk dat we tijd hebben voor een paar vragen. Het woord is aan mevrouw Vermeulen.

*Mevrouw Vermeulen (B) N.-* We bekijken de problematiek hier vanuit twee uitgangspunten: de infrastructuur veilig maken en de eindgebruiker beter beschermen. Ik heb twee vragen daaromtrent.

Ten eerste, wat de infrastructuur betreft. Het internet is in feite gebouwd rond gebruikersvertrouwen. Gebruikersvertrouwen was de ruggengraat van het economisch succes van internet. Moeten wij dan niet van mening zijn dat vooral de private internetproviders zelf het verbruikersvertrouwen moeten herstellen en de bescherming verbeteren? Het is dus in feite ook in hun eigen belang.

Mijn tweede vraag betreft vooral de bescherming van de eindgebruiker. De technologie biedt ons nu firewalls en filters aan, maar eerlijk gezegd, de eindgebruiker ziet volgens mij het bos door de bomen niet meer. Eindgebruikers kunnen moeilijk selecteren, zijn daar meestal niet in onderlegd en vragen zich af wat ze nu moeten gebruiken. Moeten die veiligheidstools dan ook niet als een soort standaarduitrusting aangeboden worden door de internetproviders? Ik denk dan aan auto's, waar de airbag en het ABS-systeem ook als standaarduitrusting aangeboden worden bij de aankoop.

*De heer Beirens (B) N.-* Ik begin met de tweede vraag.

être opéré: combien voulons-nous investir dans la prévention ou quels dommages acceptons-nous de subir parce que les gens n'ont pas été sensibilisé à la question?

Tel est en fait notre objectif. Nous pouvons coopérer avec les différents pays, mettre en commun les contenus des différents sites internet, partager les idées concernant des campagnes et réutiliser le tout. Car trop souvent déjà on constate des doublets dans led différents pays.

J'en terminerai par là en ce qui concerne ma présentation. Je vous remercie.

*Mme de Caluwé (NL) N.-* Merci beaucoup, M. Beirens. Je crois qu'il nous reste du temps pour quelques questions. La parole est à Mme Vermeulen.

*Mme Vermeulen (B) N.-* Nous considérons la question selon deux points de vue: sécuriser l'infrastructure et mieux protéger l'utilisateur final. Je voudrais poser deux questions à ce sujet.

Tout d'abord, concernant l'infrastructure. L'internet repose en fait sur la confiance des utilisateurs. Cette confiance a été la colonne vertébrale du succès économique de l'internet. Ne devons-nous dès lors pas considérer qu'il appartient aux fournisseurs d'internet privé surtout de rétablir la confiance de l'utilisateur et d'améliorer la protection? Ce serait en fait aussi dans leur propre intérêt.

Ma deuxième question a principalement trait à la protection de l'utilisateur final. La technologie nous propose des pare-feu et des filtres mais, honnêtement, c'est un peu pour l'utilisateur l'arbre qui cache la forêt. Les utilisateurs finaux ont du mal à opérer une sélction parce qu'il ne sont pas bien informés et se demandent ce qu'ils doivent utiliser. Ces instruments de sécurité ne doivent-ils pas être proposés par les fournisseurs d'internet comme une sorte d'équipement de base? Et je fais ici un parallèle avec les voitures dont les airbags et le système ABS sont également proposés à l'achat comme faisant partie de l'équipement de base.

*M. Beirens (B) N.-* Je commencerai par la deuxième question.

Het is niet de fabrikant die benzine in de auto doet, maar de eindgebruiker zelf die voor een stuk moet instaan voor het kopen van de juiste tools voor zijn auto, in dit geval de juiste tools als hij op zijn computersysteem op het internet gaat surfen.

Ce n'est pas le fabricant qui remplit le réservoir de la voiture mais c'est l'utilisateur final qui, pour partie, doit veiller à acquérir les outils appropriés à son véhicule. Dans la cas qui nous occupe, c'est lui qui doit se procurer les outils apppropriés pour surfer sur internet au moyen de son ordinateur

Het is inderdaad zo dat de providers een rol moeten spelen om de mensen bewust te maken. Men kon de operatoren echter moeilijk verplichten om de veiligheid op je computersysteem te voorzien, want dan gaan we komen tot een verstoring van de markt, iedereen moet kunnen kiezen uit verschillende tools.

Il est exact que le fournisseur doit jouer un rôle dans la sensibilisation des gens. Mais il est difficile de contraindre les fournisseurs à doter le système informatique des outils de sécurité nécessaires, le marché va être perturbé car chacun doit pouvoir choisir parmi plusieurs outils.

Er zijn verschillende veiligheidsproducten op de markt. Het ene biedt wat meer toeters en bellen dan het andere, sommige zijn specifiek gericht op een bepaalde doelstelling en sommige bedrijven hebben een grotere dreiging op een bepaald punt. Niet iedereen kan dus dezelfde tools gebruiken. Er zijn natuurlijk wel basisniveaus die door de operatoren moeten worden voorzien.

Il existe plusieurs outils de sécurité sur le marché. L'un comportera un peu plus d'éléments qu'un autre, certains seront destinés spécifiquement à un usage donné et certaines entreprises seront exposées à une menace plus grande que d'autres. Chacun ne peut donc utiliser les mêmes outils. Il existe certes des niveaux de base que doivent proposer les opérateurs.

Een van de grootste problemen die we kennen en waarmee de meest kwaadaardige software nog altijd verspreid wordt, is e-mail. Dat is het slechtste protocol op aarde qua veiligheid. Maar het bestaat al zo lang en er zijn zoveel computersystemen die datzelfde protocol gebruiken dat, als we nu een stuk authenticatie zouden gaan inbouwen zodat je verplicht wordt je te identificeren om een e-mail te sturen, er zoveel systemen aangepast moeten worden dat de mensen dit een onverantwoorde kost zullen vinden. En toch zien we dat dagelijks 85 procent van alle e-mails spam is.

L'e-mail constitue l'un des problèmes majeurs auxquels nous sommes confrontés et qui sert toujours de canal de diffusion de logiciels malveillants. En matière de sécurité, c'est le pire protocole qui existe au monde. Mais il existe depuis si longtemps et les systèmes informatiques sont si nombreux à l'utiliser que si l'on imposait une forme d'authentification obligeant à s'identifier pour envoyer un e-mail, il faudrait adapter un tel nombre de systèmes que le coût serait insupportable. Mais il n'empêche que l'on conste quotidiennement que 85 % des e-mails sont des SPAM.

85 procent is een enorm volume. Dat moet kunnen gefilterd worden. Als de volgende generatie er dus rekening mee wil houden dat, bij het uitwisselen van berichten, sterke authenticatie een zeer belangrijk element is in security, dan gaan we veel problemen oplossen – vóórdat er een probleem ontstaat. Want als je verplicht wordt om je te identificeren om een bericht te verzenden, wordt het natuurlijk een stuk moeilijker.

Imaginez-vous quels volumes énormes peuvent représenter ces 85 %. Il faut pouvoir filtrer tout cela. Si, dans le cadre de l'échange de messages, la prochaine génération voulait une authentification sérieuse comme un élément très important au regard de la sécurité, de nombreux problèmes seraient résolus avant même qu'ils surgissent. Car l'obligation de s'identifier pour pouvoir envoyer un message rendrait les choses déjà beaucoup plus compliquées

Dat is wat de banken al lang begrepen hebben. Zij maken gebruik van die moeilijke authenticatie. Moesten ze dat niet doen, dan zouden we toestan-

Les banques l'ont compris depuis bien longtemps, elles qui recourent à cette difficile authentification. Si elles ne le faisiaient pas, nous connaîtrions des

den hebben zoals in Amerika en Brazilië, waar men nog altijd met gebruikersnaam en paswoord werkt, wat zo gemakkelijk te onderscheppen en te misbruiken is, dat je inderdaad komt tot veel grotere schade dan hier in België en in Nederland. Over Luxemburg ken ik de juiste cijfers niet.

*Mevrouw de Caluwé (NL) N.-* Dank u wel. De heer Angel wenst nog een vraag te stellen.

*De heer Angel (L) F.-* Ik dank u. Ik denk dat u als vertegenwoordiger van de Belgische federale politie het best geplaatst bent om op mijn vraag over het nieuwe centrum EC3 te antwoorden. Dat European Cybercrime Center dat de Europese Commissie bij Europol heeft opgericht, is in januari 2013 met zijn werkzaamheden gestart.

We weten hier allen dat de cybercrimebestrijding vaak zeer versnipperd is. Samenwerking is des te belangrijker. Hebt u als Belgisch vertegenwoordiger de voordelen van dat nieuw centrum al opgemerkt en bent u dagelijks in contact met dat centrum? Wat zijn uw relaties met het centrum en gaat het hier om een goed initiatief?

*De heer Beirens (B) F.-* Het is zeker een goed initiatief. Cybercrime is grotendeels internationaal. Afgezien van een of twee dossiers behandelen we elk jaar tientallen, zelfs honderden internationale dossiers.

Er wordt inderdaad vooruitgang geboekt . Maar dat veronderstelt dat de lidstaten bereid zijn hun gegevens uit te wisselen. Europol dat geen onderzoeksbevoegdheid heeft, kan immers enkel inlichtingen inwinnen, analyses verrichten, de dreigingen aanwijzen en de links tussen de onderscheiden dossiers blootleggen.

Europol kan enkel optreden wanneer de gegevens worden overgezonden, maar velen doen dat niet en zonder die gegevens kan Europol niets ondernemen.

Mijn ervaring met het European Cybercrime Center is inderdaad positief en aangezien het hier om

situations comme en Amérique et au Brésil, où l'on utilise encore le nom d'utilisateur et le mot de passe qui sont tellement faciles à intercepter et à utiliser frauduleusement que les dommages subis sont beaucoup plus élevés qu'en Belgique et aux Pays-Bas. Je ne connais pas les chiffres exacts en ce qui concerne le Luxembourg.

*Mme de Caluwé (NL) N.-* Je vous remercie. M. Angel souhaite encore poser une question.

*M. Angel (L) F.-* Je vous remercie. Comme représentant de la police fédérale belge, je vous crois le plus apte à répondre à ma question qui concerne le nouveau centre EC3. Cet European Cybercrime Center, annoncé au sein d'Europol par la Commission européenne, a commencé ses travaux en janvier 2013.

Nous savons tous ici qu'il y a souvent une très grande fragmentation de la lutte contre la cybercriminalité; la coopération en est d'autant plus importante. En tant que représentant belge, avez-vous déjà perçu les bénéfices de ce nouveau centre et entretenez-vous des contacts avec celui-ci dans votre vie quotidienne? Comment sont vos relations avec lui et peut-on dire qu'il s'agit d'une bonne initiative?

*M. Beirens (B) F.-* C'est certainement une bonne initiative. La cybercriminalité est internationale dans sa grande majorité. A part un ou deux dossiers, nous traitons chaque année des dizaines voire des centaines de dossiers internationaux.

En effet, cela avance, mais, pour ce faire, il faut une volonté des États membres d'échanger leurs données car Europol n'a pas de compétence de recherche et peut seulement récolter des informations, faire des analyses et indiquer les menaces et les liens entre les différents dossiers.

Europol ne peut intervenir que si les données sont transmises, mais beaucoup de pays ne le font pas et, sans information, Europol est dans l'impossibilité de faire quoi que ce soit.

Effectivement, j'ai déjà eu de bonnes expériences de la mise en place du European Cybercrime Cen-

een noodzaak gaat hoop ik dat men in de toekomst nog verder zal gaan.

*Mevrouw de Caluwé (NL) N.-* Dank u wel. Dan geef ik nu graag het woord aan de heer Houtsch van het Luxemburgse CERT.

**Uiteenzetting door de heer Patrick Houtsch, directie CERT (*Computer Emergency Response Team*) gouvernemental, Luxemburg**

*De heer Houtsch (L) F.-* Dames en heren, zoals u weet sta ik aan het hoofd van het CERT (Computer Emergency Response Team) van de regering in Luxemburg. Ik zou hier vandaag de kwestie cybercrime willen overlopen en eventueel de onderscheiden aspecten aanstippen die verband houden met de bewustmaking, de informatie en de opvoeding om aldus de mogelijke reële gevolgen van die maatregelen, in het licht van de incidenten die zich voordoen, te schetsen.

Ik neem de gelegenheid te baat om de acties van het CERT toe te lichten. Hoeveel CERT zijn er in Europa actief en wat vertegenwoordigen ze? Maar voor alles, wat zijn onze doelstellingen en wat willen we beschermen? Om de zaken te vereenvoudigen zou ik het onderwerp in drie punten willen onderverdelen.

De eerste doelstelling heeft betrekking op de werking van onze maatschappij, die vandaag nauw verbonden is met de goede werking van de infrastructuur van de communicatiesystemen. Die goede werking kan van vitaal belang zijn voor de burgers aangezien ze betrekking heeft op uiteenlopende sectoren zoals energie, communicatie, vervoer, gezondheid enz. Het hoofddoel is dus de bescherming van de landen tegen ernstige informaticadreigingen die de vitale systemen kunnen aantasten.

De tweede doelstelling is een gevolg van het feit dat de economische groei vandaag in zeer grote mate beïnvloed wordt door de ontwikkelingen in de sector van de informatie- en communicatietechnologie. Die groei leidt tot banen en we weten allemaal dat dat essentieel is. De groei berust op een infrastructuur die operationeel, betrouwbaar

ter et, parce que c'est absolument nécessaire, j'espère que l'on ira plus loin dans le futur.

*Mme de Caluwé (NL) N.-* Je vous remercie. Je cède à présent la parole à M. Houtsch, du CERT luxembourgeois.

**Présentation par M. Patrick Houtsch, chargé de la direction CERT *(Computer Emergency Response Team*) gouvernemental, Luxembourg**

*M. Houtsch (L) F.-* Mesdames et messieurs, comme vous le savez, je suis en charge du CERT (Computer Emergency Response Team) gouvernemental au Luxembourg. Aujourd'hui, mon objectif est de passer en revue le sujet de la cybercriminalité et éventuellement d'en pointer les différents aspects liés à la sensibilisation, l'information et l'éducation. Ceci en vue de percevoir quel impact ces mesures peuvent avoir dans la réalité, par rapport aux incidents discernés.

Je profite donc de l'occasion qui m'est donnée ici pour illustrer les actions des CERT, combien de CERT agissent en Europe et ce qu'ils représentent. Avant tout, quels sont nos objectifs et que voulons-nous protéger? Pour simplifier, ce sujet peut être scindé en trois points.

Le premier objectif concerne le fonctionnement de notre société, aujourd'hui étroitement lié à la bonne marche des infrastructures des systèmes de communication. Ce bon fonctionnement peut représenter des besoins vitaux pour les citoyens, dans la mesure où il concerne des secteurs aussi variés que l'énergie, la communication, le transport, la santé ou d'autres encore. L'objectif principal consiste en la protection des pays contre des menaces informatiques majeures dirigées vers leurs systèmes vitaux.

Le deuxième résulte du fait qu'aujourd'hui la croissance économique est très fortement stimulée par les développements dans le secteur des technologies de l'information et de la communication. Cette croissance génère des emplois, ce qui est essentiel, nous en sommes tous conscients. Elle repose sur des infrastructures qui doivent être

en beveiligd moet zijn, vandaar dat de plaatselijke bedrijven over een aantrekkelijke communicatieomgeving moeten beschikken.

De derde en laatste doelstelling strekt ertoe de persoonlijke levenssfeer van de burgers te beschermen en hun grondrechten veilig te stellen. Steeds meer burgers doen een beroep op nieuwe technologieën, zowel in hun sociaal leven, als in hun betrekkingen met de besturen of in hun economisch leven.

Nu wat de cybercrime betreft: wat betekent dat? De heer Beirens heeft goed toegelicht wat er vandaag gebeurt. Ik zal het onderwerp uitvoeriger behandelen. Een cybercrime is een misdrijf dat een cybercompenent heeft. In principe gaat het steeds om dezelfde misdrijven, maar er wordt gebruik gemaakt van nieuwe middelen en technologieën alsook van een cybercomponent.

Bepaalde nieuwe misdaden kunnen enkel met een cybercomponent worden gepleegd. Vergelijken we, bijvoorbeeld, een inbraak in de woning van een privépersoon, wat een misdrijf is, met een frauduleuze toegang tot een informaticasysteem. Er werd geen schade aangericht, niemand werd benadeeld, maar die daad kan al worden bestraft.

De wet is duidelijk: "*Iedereen die zich frauduleus toegang verschaft of die zich in het geheel van het systeem dan wel in een deel ervan ophoudt…*". Alleen al een informaticasysteem binnendringen kan volgens mij al een nieuw soort misdrijf zijn. Het zijn geen klassieke misdaden, begaan met behulp van een cybercomponent, maar misdrijven die eigen zijn aan de cyberwereld. Sommige van die strafbare feiten zijn daden die de systemen wijzigen of de goede werking ervan belemmeren.

De tenuitvoerlegging van de overeenkomst over cybercrime heeft tot nieuwe wetsartikelen met betrekking tot het onderscheppen van communicatie geleid. De ontwikkeling van tools zoals virussen die tot doel hebben schade aan te brengen, zullen worden bestraft. Vandaag kunnen ze nog niet worden bestraft, hoewel ze als nieuwe misdaden kunnen worden beschouwd.

opérationnelles, fiables et sécurisées, d'où son importance pour la fourniture d'un environnement de communication attrayant, sûr et fiable pour des entreprises locales.

Le troisième et dernier objectif s'attache à protéger la vie privée des citoyens et à préserver leurs droits fondamentaux. De plus en plus les citoyens ont recours aux nouvelles technologies, que ce soit dans leur vie sociale, leurs relations avec les administrations ou dans leur vie économique.

J'en viens brièvement à la cybercriminalité. Que représente-t-elle? M. Beirens a fort bien illustré ce qui se passe actuellement. J'aborderai ce sujet sous un angle plus exhaustif. Un cybercrime est un crime qui a une composante cyber. En principe, ce sont les mêmes délits, mais en utilisant des moyens, des technologies nouvelles et une composante cyber pour les perpétrer.

Certains nouveaux crimes ne peuvent être commis qu'avec seulement une composante cyber. Comparons, par exemple une intrusion dans la maison d'une personne privée, ce qui représente un délit, avec un accès frauduleux à un système informatique. On n'a pas commis de dégâts, ni encore nui à une personne, mais cette action peut déjà être pénalisée.

La loi dit d'ailleurs: "*Quiconque aura accédé frauduleusement ou se maintiendra dans tout ou partie du système...*". Rien que le fait de s'introduire simplement dans un système informatique peut déjà constituer, à mon sens, un nouveau type de délits. Ces ne sont pas des crimes classiques, commis à l'aide d'une composante cyber, mais des crimes particuliers au domaine cyber. Parmi ces faits pénalisables, on trouve des actions qui modifient les systèmes ou en entravent le bon fonctionnement.

De nouveaux articles de loi relatifs à l'interception des communications sont introduits par la mise en oeuvre de la convention sur la cybercriminalité. On sanctionnera le développement d'outils comme les virus dont l'objectif est de nuire, ce qui n'est pas encore puni actuellement, alors qu'ils peuvent être considérés comme nouveaux crimes.

Maar laten we het hebben over de klassieke overtredingen, met andere woorden met behulp van een cybercomponent: eerroof, aantasten van het imago, gebruik van valse documenten, valse naam, allerhande pesterijen… Uit de media weten we dat dergelijke praktijken die tot het uiterste worden doorgedreven, zelfmoord tot gevolg kunnen hebben.

Er zijn tal van andere voorbeelden, zoals oplichting en misbruik van vertrouwen. Een spam uit Nigeria: een gewezen dictator neemt contact met u op omdat hij uw hulp nodig heeft om aan zijn geld te geraken. Natuurlijk is dat verzonnen, maar sommige mensen geloven die mails helaas en verliezen aldus veel geld.

Vervolgens vervalsing, het gebruik van valse documenten en alles wat verband houdt met kredietkaarten, carding met andere woorden. Gespecialiseerde criminelen verzamelen die kaarten om ze te verkopen of voor eigen gebruik.

Er is ook afpersing, *phishing*. De heer Beirens heeft het voorbeeld – een mooi schoolvoorbeeldgegeven van ransomware, het politievirus genaamd. De pc van de gebruikers wordt vercijferd en de toegang geblokkeerd. De pc kan pas opnieuw worden gebruikt wanneer een bepaald bedrag wordt betaald. Vandaag worden ook maatschappijen met dat misdrijf geconfronteerd. Onlangs werd een server met bestanden van een maatschappij volledig vercijferd zodat ze geen toegang maar had tot haar data. Om toegang te bekomen zou ze losgeld moeten betalen. Indien ze geen kopie van haar saveboards had gemaakt, had ze al haar data verloren, tenzij ze het losgeld had betaald, wat ze waarschijnlijk zou gedaan hebben.

En wat kunnen we zeggen van die hele categorie van auteursrechten, intellectuele eigendom, privacy en, ten slotte, de ietwat bijzondere misdaden, zoals industriële of gouvernementele spionage of nog sabotage? Privépersonen merken daar niet veel van, in tegenstelling tot de maatschappijen en de regeringen die vaak worden getroffen.

Wat zijn de gebruikte procedés en de cybercomponenten bij het plegen van die misdaden? Ik zal niet te technisch worden, maar indien u in dat verband vragen heeft, zal ik ze graag beantwoorden.

Revenons-en aux infractions classiques, c'est-à-dire à composante cyber: diffamation, atteinte à l'image, usage de faux, faux noms, harcèlements divers... Par les médias, nous savons tous que ce genre de pratique, poussé à l'extrême, peut conduire des gens au suicide.

D'autres exemples abondent, comme l'escroquerie et l'abus de confiance. Ainsi, un spam nigérien: un ancien dictateur vous contacte car il a besoin de votre aide pour pouvoir libérer son argent. C'est faux évidemment mais, malheureusement, certaines personnes croient à la véracité de ces mails et sont victimes d'importantes pertes financières.

Ensuite le faux, l'usage de faux et tout ce qui tourne autour des cartes de crédit, le carding. Des criminels spécialisés les collectionnent pour les revendre ou les utiliser personnellement.

Il y a aussi l'extorsion, le *phishing*. M. Beirens a cité l'exemple du ransomware, un beau cas d'école, qu'on appelle le virus police. Le PC des utilisateurs est chiffré et l'accès bloqué. Le PC n'est réutilisable qu'en échange d'une somme d'argent. Aujourd'hui, les sociétés sont également confrontées à ce délit. Récemment, un serveur de fichiers d'une société a été chiffré complètement au point qu'elle n'a pu accéder à ses données. Pour y arriver, une rançon a été demandée. Si cette société n'a pas pris la précaution de réaliser des copies de ses saveboards, elle perd toutes ses données, à moins de payer la rançon, ce qu'elle fera probablement.

Et que dire de toute la catégorie des droits d'auteur, propriété intellectuelle, vie privée et, pour finir, les crimes un peu plus spéciaux que sont l'espionnage industriel ou gouvernemental ou encore le sabotage. Ils sont moins perceptibles auprès des particuliers mais fréquents auprès des sociétés et des gouvernements.

Quels sont les procédés utilisés et la composante cyber par rapport à ces crimes? J'éviterai ici d'être trop technique mais, si vous avez des questions à ce sujet, je vous y répondrai volontiers.

Over het algemeen spreekt men van kwaadaardige codes, het gebruik van virussen, wormen, Trojaanse paarden, malware. Men spreekt ook van denial of service die tot een overbelasting van de systemen leidt waardoor ze niet langer operationeel zij, het misbruik van functionaliteiten voor oneigenlijke doeleinden, intellectuele injectie, crosssite scripting, enz.

Met *spoofing*, bijvoorbeeld, wordt een adres afkomstig van een email gewijzigd: men geeft een valse naam. Met brute force attacks kunnen paswoorden worden bemachtigd. Vergeten we ook niet de cryptografie op het stuk van het politievirus voor het vercijferen van de pc, de middelen om berichten te onderscheppen, en eenvoudiger, het stelen van materieel, een laptop om het misdrijf voor te bereiden. Ten slotte is er nog social engineering, een van de meest gebruikte technieken om, samen met andere zaken, cybercrime te plegen. Ik kom daar later op terug.

Aan de hand van enkele statistieken kan ik een idee geven van de incidenten die we vandaag behandelen. 85 % van de gevallen zijn opportunistische aanvallen, met andere woorden, ze zijn gericht op de zwakke schakel in de keten. Ze zijn gericht op de gebruiker die het minst is voorbereid of die het minst bewust is, de *drive-by* aanvallen, bijvoorbeeld.

Zoals de heer Beirens heeft aangegeven gaat het om zeer drukbezochte internetsites. Het materieel van die gebruikers wordt aangetast, eenvoudigweg omdat ze die site bezoeken. Een opportunistische aanval is niet speciaal gericht tegen bepaalde personen, bepaalde sectoren of regeringen, maar enkel tegen degenen die op dat ogenblijk zijn aangesloten  Wie kan daarvan het slachtoffer zijn? Uiteraard zijn de opportunistische aanvallen belangrijker voor particulieren.

Het percentage voor de regeringen en de maatschappijen ligt veel lager: namelijk 15 %. Het gaat in dat geval om zeer gerichte cyberaanvallen tegen bepaalde  bedrijven of regeringen. In 31 % van de aanvallen wordt gebruik gemaakt van social engineering. Interessant is in dat verband dat de zwakheden van de mensen worden benut om nog andere aanvallen op te zetten.

Généralement on parle de codes malveillants, comme l'utilisation de virus, de vers, de "cheval de Troie", de Malware.  On parle aussi de techniques de déni de service qui aboutissent à une surcharge des systèmes afin de les rendre inopérationnels, d'abus de fonctionnalités qui n'étaient pas prévues dans ce sens et d'injection intellectuelle, de crosssite scripting, entre autres.

Le *spoofing*, lui, par exemple, modifie une adresse provenant d'un e-mail: on donne donc un faux nom. Des techniques de brute forcing parviennent à deviner les mots de passe. Pensons aussi à la cryptographie au niveau du virus police qui chiffre les PC, les moyens d'interception des communications et, plus simplement, le vol de matériel, laptop ou portable, pour préparer le crime. Enfin, relevons l'ingénierie sociale, une des techniques les plus utilisées pour commettre des crimes cyber, en combinaison avec d'autres choses. J'y reviendrai.

Quelques statistiques nous indiquent bien les incidents que nous traitons. Aujourd'hui, 85 % d'entre eux sont des attaques opportunistes, c'est-à-dire axées sur le maillon faible de la chaîne. Elles visent l'utilisateur le moins bien préparé ou le moins sensibilisé, par exemple les attaques *drive-by*.

Ainsi que M. Beirens l'a signalé, il s'agit de sites internet très fréquentés. Or, le matériel de ces utilisateurs est compromis simplement par le fait qu'ils visitent ce site. L'attaque opportuniste ne vise pas spécialement des personnes, des secteurs particuliers ou des gouvernements, mais simplement ceux qui sont connectés à ce moment précis. Qui peut en être victime? Il est évident que les attaques opportunistes seront plus importantes pour les particuliers.

Au niveau des gouvernements et des sociétés, le pourcentage est nettement inférieur: quelque 15 %. Il s'agit dans ce cas de cyberattaques spécialement ciblées contre des entreprises ou des gouvernements bien spécifiques. Un autre chiffre montre que 31 % des attaques utilisent des techniques d'ingénierie sociale. À cet égard, il est intéressant de constater qu'elles utilisent les faiblesses de l'être humain pour combiner leurs attaques à d'autres.

Ten slotte dient te worden opgemerkt dat in 40 % van de aanvallen gekende technische mankementen worden benut: met andere woorden slecht onderhouden systemen worden aangevallen Het updaten van een informaticasysteem zal die aanvallen inefficiënt maken.

Wanneer men rekening houdt met die twee factoren, de 31 % aanvallen gebaseerd op social engineering en de 40 % aanvallen die enkel efficiënt zijn omdat ze tegen slecht onderhouden systemen zijn gericht, is het duidelijk dat een groot aantal van de aanvallen kan worden voorkomen door de gebruikers te sensibiliseren, hen in te lichten en hen uit te leggen dat zij niet enkel hun systemen moeten updaten maar ook dat ze over een antivirus moeten beschikken. Daarmee wordt het enorm potentieel van informatie- en bewustmakingscampagnes aangetoond.

Slechts 5 % van de aanvallen zijn “onmerkbaar”, met andere woorden nagenoeg onvermijdbaar. Ze maken gebruik van kwetsbaarheden OD genaamd of die OD benaderen. Die kwetsbaarheden zijn niet gekend ofwel gekend maar kunnen tot op heden niet worden verbeterd. In heel weinig van de aanvallen worden die technieken gebruikt en voor een particulier zijn ze moeilijk te voorkomen.

Een eventuele kwetsbaarheid in de jongste Java-versie, die onlangs werd vastgesteld, kan niet echt worden verholpen, updaten van het systeem zal niet volstaan. Grondiger bewustmakingscampagnes kunnen duidelijk maken dat Java moet worden verwijderd, ofwel een andere browser moet worden gebruikt. Maar die campagnes moeten worden gelanceerd zodra de kwetsbaarheden opduiken, die reflex kan de mensen niet worden bijgebracht. Het heeft geen zin ze te herhalen aangezien het om tijdelijke problemen gaat.

Een laatste woord over de statistieken: deze cijfers zijn afkomstig van het domein van de kritieke infrastructuur van de regering. Wat de particulieren betreft, zijn ze natuurlijk aan veranderingen onderhevig aangezien we ervan uitgaan dat zich op dat gebied veel minder aanvallen zullen voordoen.

Met betrekking tot de preventie van die misdrijven zijn er drie zaken mogelijk. Ten eerste, technische

Ensuite, il faut remarquer que 40 % des attaques utilisent des failles techniques connues, c’est-à-dire qu’elles s’adressent à des systèmes mal entretenus. Mettre à jour un système informatique rendra ces attaques inefficaces.

En combinant les deux facteurs: les 31 % d’attaques basées sur l’ingénierie sociale et les 40 % efficaces uniquement sur des systèmes mal entretenus, on constate que l’on peut éviter un grand nombre d’attaques en sensibilisant les utilisateurs, en les informant et en leur expliquant qu’il est nécessaire, non seulement de mettre à jour les systèmes, mais aussi de les doter d’un antivirus. Cela montre donc le potentiel énorme des campagnes d’information et de sensibilisation.

Seulement 5 % des attaques sont “non voyantes”, c’est-à-dire quasi inévitables. Elles utilisent des vulnérabilités appelées OD ou proche des OD. Ces vulnérabilités sont, soit inconnues, soit connues mais impossibles à corriger à l’heure actuelle. Très peu d’attaques utilisent ce genre de techniques et elles sont difficiles à éviter pour le particulier.

S’il y a une vulnérabilité dans la dernière version “Java”, ce qui a été constaté récemment, il ne pourra pas réellement faire grand chose car mettre son système à jour ne suffira pas. Des campagnes de sensibilisation plus poussées peuvent lui faire comprendre que, soit il enlève son “Java”, soit il utilise un autre browser. Mais ces campagnes doivent être menées dès que des vulnérabilités apparaissent, ce ne sont pas des réflexes qu’on peut apprendre aux gens. Elles n’ont pas lieu d’être répétées dans le temps, puisqu’il s’agit de problèmes momentanés.

Un dernier mot sur les statistiques: ces chiffres proviennent du domaine des infrastructures critiques du gouvernement dans le domaine des particuliers. Ils sont évidemment sujets aux changements étant donné que nous y prévoyons beaucoup moins d’attaques ciblées.

Pour ce qui est de la prévention de ces crimes, trois choses sont possibles. D’abord, mettre en

maatregelen, vervolgens, organisatorische maatregelen en, ten slotte, bewustmaking wat de opleiding en de opvoeding betreft. De eerste twee maatregelen zal ik niet toelichten. ik zal het inzonderheid hebben over de bewustmaking, het onderwerp van deze conferentie.

Wanneer men vaststelt dat een derde van de incidenten verband houdt met social engineering, is het zonder meer duidelijk dat er op dat gebied een enorm potentieel is. Een bewustmaking van de mensen, vanaf zeer jonge leeftijd, is absoluut noodzakelijk.

Een voorbeeld: mijn dochter van negen wil toegang hebben tot het internet. Ik moet haar uitleggen wat er op het internet gebeurt, hoe ze toegang krijgt en hoe het wordt gebruikt. Maar het volstaat niet de jongeren bewust te maken, de bewustmaking mag nooit worden stopgezet waarbij met de evolutie van de technologieën rekening wordt gehouden.

Een enkele actie op school volstaat niet: de actie moet voortdurend worden hernieuwd. Het doel is natuurlijk de gevaren onderkennen, weten welke daden men moet stellen en hoe men in geval van een incident kan optreden, al is het een feit dat dat punt vaak over het hoofd wordt gezien. Men kan het vergelijken met een airbag in een wagen. Men kan er een, twee of tien hebben, men investeert dus in veiligheid.

Op het gebied dat we vandaag bespreken, kunnen we kiezen voor een betere beveiliging, maar dat betekent natuurlijk dat producten worden gekocht die veiligheid bieden.

Het volstaat immers niet een pc up te daten. Een goede beveiliging betekent dat in een antivirus software wordt geïnvesteerd. Over het algemeen is er een licentie wanneer de pc wordt aangekocht, maar de mensen hernieuwen die niet omdat dat 30 euro kost. Dat is niet niks, inderdaad, maar we mogen niet vergeten dat dat antivirus veel werk vertegenwoordigt. De gebruikers moeten beseffen dat ze op een bepaald ogenblik moeten beslissen of ze al dan niet in veiligheid willen investeren.

Ik zal nu kort de rol en de realisaties van de CERT toelichten. Na de preventie is er het incident, na het incident, de reactie. Wat kan men op dat ogenblik

place des mesures techniques, ensuite prendre des mesures organisationnelles et, enfin, sensibiliser à la formation et à l'éducation. Je ne m'éterniserai pas sur les deux premières. Je m'attacherai plus particulièrement à la sensibilisation, sujet de cette conférence.

Si l'on observe qu'un tiers des incidents est lié à l'ingénierie sociale, il est très clair qu'il y a un énorme potentiel dans ce domaine. Il est indispensable d'y sensibiliser les personnes et les sensibiliser très jeunes.

Ainsi, par exemple, ma fille de neuf ans souhaite avoir accès à internet. Il faut donc expliquer ce qui s'y passe, comment y accéder et comment l'utiliser. Mais la sensibilisation des jeunes ne suffit pas, elle doit continuer tout au long de la vie, en tenant compte de l'évolution des technologies.

Ce n'est pas une action que l'on fait une seule fois à l'école; elle doit être constamment renouvelée. Son but est évidemment de connaître les dangers, d'adopter les bons gestes et de savoir comment réagir en cas d'incident, mais il faut admettre que ce point est souvent oublié. Comparons-le aux airbags des voitures. On peut en avoir un, deux, ou dix, on investit donc dans la sécurité.

Dans le domaine qui nous occupe aujourd'hui, nous pouvons choisir d'avoir plus de sécurité mais cela passe évidemment par l'achat de produits capables de l'assurer.

En effet, il ne suffit pas de mettre à jour son PC. Assurer une bonne sécurité mérite d'investir dans un logiciel antivirus. En général celui fourni avec le PC a une licence mais bien souvent les gens ne la renouvellent pas parce qu'elle coûte 30 euros. Ce n'est pas donné, c'est un fait, mais n'oublions pas qu'elle représente beaucoup de travail. Les utilisateurs doivent donc avoir conscience qu'à un moment donné ils doivent décider s'ils veulent investir ou non dans la sécurité.

Je vous parlerai brièvement ici du rôle et des réalisations des CERT. Après la prévention, il y a l'incident; après l'incident, il y a la réaction. Que

doen? Ofwel is men bij machte zelf het probleem op te lossen, ofwel vraagt men hulp van een CERT. Het strafrechtelijk aspect is zaak van de politie, dat is iets totaal anders.

De CERT zijn interventiecentra voor de behandeling van informatica noodtoestanden, dus Computer Emergency Response Teams. Ze kunnen uiteenlopende vormen aannemen. Sommige zijn privé, zo hebben grote maatschappijen hun eigen centrum, gespecialiseerde teams behandelen de beveiligingsincidenten. De commerciële CERT verkopen gewoonweg hun diensten. Er zijn tevens CERT per sector. Ten slotte beschikken ook universiteiten en onderzoek- en ontwikkelingscentra over CERT.

Maar er zijn ook in de privésector CERT: zo is er in Luxemburg een CERT dat KMO's en burgers helpt bij het beheren van beveiligingsincidenten. Ook in de financiële sector kan er een CERT zijn. Ten slotte is er de categorie op regeringsniveau of nationaal niveau. Zoals de andere CERT helpen zij vooral bij het beheer van beveiligingsincidenten.

Ze staan in de eerste plaats in voor de coördinatie. Vaak volstaat het dat de juiste mensen bijeen worden gebracht om de incidenten op een behoorlijke manier te beheren. Ze zorgen voor een analyse van de incidenten en voor steun bij het beheer. Ze kunnen zelfs ter plaatse gaan om mensen of maatschappijen te helpen bij het herstellen van hun systeem. Vaak weten de maatschappijen niet dat ze een beroep kunnen doen op hulp van dat team. De CERT stellen nog andere diensten voor waarover ik het hier, wegens tijdsgebrek, niet zal hebben.

Europa telt 179 CERT die bij *Trust Introduce* – een soort Europees verbond voor de CERT-gemeenschap – zijn geaccrediteerd en 96 CERT zijn in Europa geaccrediteerd bij de JI. Die vele teams bestaan vooral uit mensen die actief zijn op het gebied van het beheer van beveiligingsincidenten, wat gelet op het groot aantal, normaal is.

Wat de Benelux betreft, telt België drie CERT, waarvan er twee zijn geaccrediteerd, Nederland

peut-on faire à ce moment? Soit on est capable de résoudre le problème soit-même, soit on demande l'assistance d'un CERT. Le volet pénal, lui, doit être traité par la police, ce qui est tout à fait autre chose.

Les CERT sont des centres d'intervention pour le traitement des urgences informatiques, donc des Computer Emergency Response Teams. Ils existent en plusieurs variantes. Certains sont privés, ainsi les grandes sociétés ont leur propre centre et des équipes spécialisées prennent en charge les incidents de sécurité. Les CERT commerciaux, eux, vendent simplement leurs services sur le marché. On trouve également des CERT sectoriels. Enfin, d'autres existent au niveau des universités et des centres de recherche et développement.

Mais on en trouve aussi dans le secteur privé, comme au Luxembourg où un CERT assiste les PME et les citoyens à gérer les incidents de sécurité. Le secteur financier peut en avoir un également. Enfin, la dernière catégorie concerne les CERT gouvernementaux ou nationaux. Comme les autres, ils aident principalement à gérer les incidents de sécurité.

En premier lieu, ils se chargent de la coordination. Il suffit souvent de mettre les bonnes personnes ensemble pour que les incidents soient convenablement gérés. Ils s'occupent aussi de l'analyse des incidents et de l'appui à leur gestion. Ils peuvent même se rendre sur le site afin d'aider les personnes ou les sociétés à restaurer leur système. Le fait que les sociétés ont la possibilité de demander de l'aide auprès de cette équipe ne leur est souvent pas connu. Les CERT proposent encore d'autres services dont je ne parlerai pas ici, faute de temps.

L'Europe compte 179 CERT accrédités auprès du *Trust Introduce*, une sorte de fédération européenne pour la communauté des CERT et 96 CERT sont accrédités en Europe auprès des JI. Ces équipes nombreuses sont composées principalement de gens actifs dans le domaine de la gestion des incidents de sécurité, ce qui est normal, vu leur nombre important.

Au niveau du Benelux, la Belgique comprend trois CERT, dont deux, accrédités; les Pays-Bas en

heeft er tien, waarvan er vier zijn geaccrediteerd en Luxemburg vier, waarvan er drie zijn geaccrediteerd.

Interessant lijkt me dat elk Beneluxland over een nationaal regerings-CERT beschikt. Dat is belangrijk, niet alle landen kunnen dat zeggen. Dat CERT dat het hele land bestrijkt en instaat voor een dispatching van de inlichtingen, draagt in grote mate bij tot een efficiënte communicatie en een vruchtbare samenwerking tussen alle teams. Dat is een zeer goede zaak, me dunkt.

Tot slot van mijn betoog wens ik nogmaals te herhalen dat het zaak is de mensen bewust te maken voor de mogelijke gevaren en voor de juiste daden die ze moeten stellen om de incidenten zo goed mogelijk te beheren. Ik dank u voor uw aandacht.

*Mevrouw de Caluwé (NL) N.-* Dank u wel, mijnheer Houtsch. De heer Angel vraagt het woord.

*De heer Angel (L) F.-* Ik dank de heer Houtsch voor zijn interessante uiteenzetting. Hij heeft eraan herinnerd dat de gebruikers de noodzaak moeten beseffen van een investering in hun veiligheid en met dat doel betrouwbare antivirusprogramma's moeten aankopen.

Uit het onderzoek eurobarometer van 2011 over de veiligheid van het internet blijkt dat slechts 26 % van de Europese bedrijven een echt beleid op het gebied van informaticabeveiliging heeft. Dat cijfer doet me versteld staan, cybercrime brengt immers enorm veel geld op.

Het is dus van levensbelang dat deze kwestie wordt aangepakt. Ik herinner er u trouwens aan dat de Europese Commissie op 7 februari van dit jaar een voorstel van richtlijn ter zake heeft ingediend. We zouden misschien kunnen spreken over de wijze waarop de voorstellen van richtlijn in de nationale parlementen werden behandeld.

Het is een stap in de goede richting, maar ik stel vast dat het slechts om een minimale harmonisatie gaat terwijl de sprekers het belang van samenwerking hebben beklemtoond. Natuurlijk, indien dat onderwerp al in een of andere commissie werd be-

ont 10, dont quatre sont accrédités, et le Luxembourg quatre, dont trois accrédités.

Il est intéressant de noter que les pays du Benelux ont chacun un CERT national gouvernemental, cela a son importance puisque tous les pays n'en possèdent pas. Ce CERT, qui chapeaute tout le pays et dispatche les informations, contribue largement à une communication efficace et à une collaboration fructueuse entre toutes les équipes. Il s'agit d'une très bonne chose, me semble-t-il.

Je termine ici mon intervention pour répéter une fois encore à quel point il est important de sensibiliser les gens à la connaissance des risques et à l'adoption des bons gestes afin de pouvoir gérer au mieux les incidents. Je vous remercie de votre attention.

*Mme de Caluwé (NL) N.-* Je vous remercie, M. Houtsch. M. Angel demande la parole.

*M. Angel (L) F.-* Je remercie M. Houtsch pour son intéressant exposé. Il a rappelé que les utilisateurs doivent être conscients de la nécessité d'investir dans leur sécurité en achetant des programmes antivirus fiables.

Si l'on consulte l'enquête eurobaromètre de 2012 sur la sécurité internet, on s'aperçoit que 26 % des entreprises européennes ont une véritable politique de sécurité informatique. Ce chiffre m'a effrayé quand on constate les bénéfices énormes réalisés par la cybercriminalité.

Travailler sur cette matière se révèle donc crucial. Je vous rappelle d'ailleurs que le 7 février dernier, la commission européenne a déposé une proposition de directive concernant ce sujet. On pourrait peut-être discuter de quelle façon les propositions de directive ont été traitées dans les parlements nationaux.

Il s'agit d'un pas dans la bonne direction, mais je constate qu'il ne s'agit encore que d'une harmonisation minimale alors que les orateurs proclament que la coopération est tellement importante. Bien entendu, si ce domaine a déjà été traité dans

sproken, kan een lid van die commissies misschien met mij van gedachten komen wisselen. Ik dank u.

*Mevrouw de Caluwé (NL) N.-* Dank u, mijnheer Angel. Het woord is aan de heer Lebrun.

*De heer Lebrun (B) F.-* Mijnheer Houtsch, u hebt een hele reeks handelingen als misdaden bestempeld. Hoe zou u het gedrag bestempelen van degenen die WikiLeaks en Offshore Leaks mogelijk hebben gemaakt?

*De heer Bettel (L) F.-* Als jurist, een correctie als u me toestaat: het gaat hier om een misdrijf niet om een misdaad.

*De heer Lebrun (B) F.-* Ik zou toch de mening van de cyberspecialisten willen horen.

*De heer Bettel (L) F.-* Mijnheer de procureur, ik heb gelijk, het is een misdrijf maar geen misdaad.

*De heer Houtsch (L) F.-* Ik ben geen jurist, maar ik lees toch de teksten. Wat WikiLeaks, en meer in het algemeen het informatielynchen, betreft weet ik niet of men dat als cybercrime kan bestempelen, want dat kan ook op papier en het gaat dus niet om wat we exfilteren van inlichtingen kunnen noemen.

Informatie stelen is een ding, maar wanneer men over informatie beschikt weet ik niet of het verspreiden ervan een misdrijf is. Zoals ik al heb gezegd, ben ik geen deskundige, maar volgens mij gaat het hier niet echt om een cyberprobleem.

*De heer Bettel (L) F.-* We kunnen misschien het woord geven aan de heer Herrmann.

*De heer Herrmann (L) F.-* Dank u, mijnheer Bettel. Ik ben inderdaad dezelfde mening toegedaan als de heer Houtsch.

Het hoofddoel van WikiLeaks was niet bestraffen en bijgevolg is het geen cybercrime. Het gaat hier gewoonweg om inlichtingen en documenten die men heeft bemachtigd en vervolgens via het internet openbaar heeft gemaakt.

l'une ou l'autre commission, peut-être l'un de ses membres pourrait venir vers moi pour un échange sur ce sujet. Je vous remercie.

*Mme de Caluwé (NL) N.-* Je vous remercie, M. Angel. La parole est à M. Lebrun.

*M. Lebrun (B) F.-* Monsieur Houtsch, vous avez qualifié toute une série de gestes comme criminels. Quelle est votre appréciation quant à la qualification de ceux qui ont permis WikiLeaks et Offshore Leaks?

*M. Bettel (L) F.-* En tant que juriste, je me permets de rectifier: c'est délictuel et non criminel.

*M. Lebrun (B) F.-* J'aimerais quand même avoir l'avis des cyberspécialistes.

*M. Bettel (L) F.-* Monsieur le procureur j'ai raison, ce n'est pas criminel mais délictuel.

*M. Houtsch (L) F.-* Je vous signale que je ne suis pas juriste, mais je lis quand même les textes. En ce qui concerne WikiLeaks, et généralement l'"information lynchage", je ne sais pas si l'on peut qualifier ce fait de cybercrime, car on peut aussi commettre ces crimes sur papier et ce n'est pas, disons, exfiltrer des informations.

Voler des informations est une chose, mais quand on en dispose, je ne sais pas si les divulguer est un délit. Cependant, comme je vous l'ai dit, je ne suis pas un spécialiste, mais pour moi, ce n'est pas réellement un problème de cyber.

*M. Bettel (L) F.-* C'est peut-être l'occasion de donner la parole à M. Herrmann.

*M. Herrmann (L) F.-* Merci, monsieur Bettel. Effectivement, je suis du même avis que M. Houtsch.

Le but principal de WikiLeaks n'était pas de sanctionner, ce n'est donc pas de la cybercriminalité. Dans le cas présent, il s'agit tout simplement d'informations, de documents subtilisés et rendus publics sur internet par la suite.

Aan de basis ligt er geen specifieke cybercrime. Het gaat om feiten die in de onderscheiden Staten een andere kwalificatie kunnen krijgen. Dat is in grote mate afhankelijk van de inlichtingen die werden bemachtigd.

Gaat het om een eenvoudig probleem van auteursrecht, van staatsinformatie of van een misdaad tegen de binnenlandse veiligheid, in casu van de Staat? Het gaat om strafrechtelijke overtredingen die al naar gelang van het land worden gecriminaliseerd. Van cybercrime is echter geen sprake in de strikte zin van het woord want het is pas achteraf dat de inlichtingen via het internet werden verspreid.

*Mevrouw de Caluwé (NL) N.-* Dank u wel. De heer Siquet wil graag nog een korte vraag stellen.

*De heer Siquet (B) F.-* Naar verluidt wijzigt Windows zijn beveiligingssysteem tot in 2014. Waarover gaat het precies? Is het een vorm van handel? Ik wijs erop dat die beveiligingssystemen commercieel zijn. Ados, bijvoorbeeld, is niet langer op dezelfde manier toegankelijk.

*De heer Houtsch (L) F.-* Ik zie niet precies waarover het gaat. Er zullen steeds mankementen zijn, wat men ook doet.

Een van de meest gebruikte technieken is *sandboxing*, waarbij de toepassing die draait in een *sandboxing*-omgeving van de algemene omgeving van de computer wordt geïsoleerd zodat ze geen toegang heeft tot of kan werken met andere applicaties.

Ik kan me voorstellen dat, zoals voor veel OAS, daarover wordt gesproken op voice mobile en de tabletten. Windows gaat ook in die richting. Maar die technieken vertonen ook zwakke plekken omdat die beveiligingsmechanismen kunnen worden omzeild. Dat zal een stap voorwaarts zijn, maar er zullen steeds mankementen zijn en een antivirusoplossing zal het aanzien van de wereld niet veranderen.

*Mevrouw de Caluwé (NL) N.-* Dank u wel, mijnheer Houtsch. Ik geef nu graag het woord aan de heer Engelis, die lid is van de Legal Affairs and Security Committee van de Baltische Assemblee.

À la base, il n'y a pas une infraction spécifique de cybercriminalité. Il s'agit de faits pouvant recevoir, dans des États différents, des qualifications différentes. Cela dépend en grande partie des informations subtilisées.

S'agit-il d'un simple problème de droit d'auteur, d'informations d'État ou d'un crime contre la sûreté intérieure, le cas échéant, de l'État? Ce sont des infractions de droit pénal normal criminalisées d'après la position des différents pays. Mais là, il n'est pas question de cybercriminalité au sens strict car ce n'est qu'ensuite que la distribution de ces informations s'est produite via internet.

*Mme de Caluwé (NL) N.-* Je vous remercie. M. Siquet souhaite encore poser une brève question.

*M. Siquet (B) F.-* Il paraît que Windows modifie son système de sécurité jusqu'en 2014. De quoi s'agit-il exactement? Est-ce une forme de commerce? J'attire l'attention sur le fait que les systèmes de sécurisation sont commerciaux. Ainsi, Ados, par exemple, n'est plus accessible de la même façon.

*M. Houtsch (L) F.-* Je ne vois pas spécifiquement de quoi il s'agit. De toute façon, des failles existeront, indépendamment de ce qui se fera.

L'une des techniques de plus en plus utilisées est le sandboxing, qui sous-entend que l'on isole de l'environnement général de l'ordinateur l'application qui tourne dans un environnement sandboxing afin qu'elle ne puisse pas accéder ou interagir avec d'autres applications.

Je peux imaginer que l'on en parle comme c'est le cas pour beaucoup d'OAS sur les voice mobile et les tablettes. Windows va également dans cette direction. Mais ces techniques révèlent aussi des failles car ces mécanismes de sécurité peuvent être contournés. Ce sera un pas en avant, mais il y aura toujours des failles et mettre en place des solutions antivirus ne changera pas réellement le monde.

*Mme de Caluwé (NL) N.-* Merci, M. Houtsch. Je cède à présent la parole à M. Engelis, qui est membre de la Legal Affairs and Security Committee de l'Assemblée balte. Nous avons beaucoup

Wij kunnen veel leren van wat de Baltische Staten hebben gedaan in verband met cybersecurity.

**Uiteenzetting door de heer Karlis Engelis, member of the *Legal Affairs and Security Committee* van de Baltische Assemblee**

d'enseignements à tirer de ce que les États baltes ont réalisé en matière de cybersécurité.

**Présentation par M. Karlis Engelis, *member of the Legal Affairs and Security Committee* de l'Assemblée balte**

*Mr Engelis (BA) E.-* Thank you very much. Honourable members of parliament, it is truly my pleasure to address this conference on behalf of the Baltic Assembly. This conference deals with the very important topics of raising awareness to the risks of cybercrime and informing the users about possible dangers.

I am not sure that I will be able to provide and relate to the experiences in the Baltic States in a way that would help you advance in these topics domestically. Personnaly, I have the feeling from what I have heard here from the speakers today that the Benelux cooperation is more advanced in this field. I think there is more for the Baltic Assembly to learn from the Benelux Parliament.

Nevertheless, allow me to proceed with my speech. In my speech, I will first give some general background information that will illustrate the way we think about cybercrime in the Baltics. I am rather sure that it will not at all be far from your own approach. Then I will inform you of the actions we have already undertaken and in the end I will highlight some fields that are gaining increasing political will to rein in more cooperation, not only among the Baltic States, but also beyond.

Over the last two decades, the internet has had an immense impact on social life. Today, our social life and economic well being depend on information and communication technology. Open and free cyberspace has contributed to social and political inclusion world wide. It has promoted physical security and human rights; it has broken down barriers between countries, communities and citizens, allowing interaction and information sharing world wide.

Information and communication technology has become the backbone for economic growth and it is a critical resource that the free market relies on. For cyberspace to remain open and free, the same principles, norms and values that are observed offline should also be applied online in the cyberdomain.

Fundamental rights, freedom of expression, personal data protection and privacy, democracy and the rule of law need to be protected in cyberspace as well.

During the recent years we have seen that while the digital world brings great benefits, it is also very vulnerable.

The increased number of accidental and intentional cybersecurity incidents disrupts the supply of essential services that we take for granted, such as water, health care, electricity, mobile services, and so on. These threaths can have different origins including political motivated, criminal, terrorist or state sponsored attacks as well as natural disasters and unintentional mistakes.

We are affected by cybercrime activities against the private sector and individuals on a daily basis. Cybercriminals use ever more sophisticated methods for intruding into information systems, stealing critical data and holding companies to ransom. The increase of economic espionage and state sponsored activities in cyberspace poses a new category of threaths for our governments and companies.

The scale of cybercriminal activity represents a considerable challenge to law enforcement agencies and the total cost of cybercrime to society is significant. A recent report suggests that victims lose around 290 billion euros each year world wide as a result of cybercrime, making it more profitable than the global trade in marihuana, cocaine and heroine combined.

The internet as a major driver of criminal activity enables organized crime groups to access a large pool of victims, obscure their activities and carry out their worst range of criminal acts in a shorter period of time and on a much larger scale than ever before.

Cybercrime affects all countries and is linked primarily to financial fraud offences. According to research by the European Commission, 8 % of the internet users in the European Union have experienced identity theft and 12 % have suffered from some form of online fraud.

Malware affects millions of households and the general volume of banking fraud related to cybercrime is increasing year after year. Only about 30 % of certain cybercrime such as identity theft is actually reported to law enforcement.

It should be noted that certain criminals are no longer focused solely on attacks against users to gain access to personal information, but increasing attention is applied to the service providers. By hacking service providers, these criminals quickly gain access to large volumes of data, which they can retail in the digital underground community.

The volume of cybercrime offences looks to increase in the future. This increase will closely mirror the growth of the attack surface as the internet becomes even more essential to every day life. The growth of mobile devices as the primary means of accessing internet resources will lead to a greater targeting of these devices by criminals as well.

The issue of cybersecurity has been topical on the agenda of the Baltic Assembly. Especially after the first ever coordinated cyberattack against Estonian government agencies, banks, media and telecommunication companies in 2007, that demonstrated that the vulnerability of the information system of the societies is an aspect of national security that needs urgent attention and action.

There have been attacks of similar nature against Lithuania, Georgia and Kazachstan. Government ministries and agencies, often defense related, in the United States, Germany, France and South Korea have also been attacked.

Without doubt, the freedom online requires safety and security. In order to insure the security of a country's cyberspace, a range of activities at different levels needs to be implemented. These include reducing the vulnerability of cyberspace, preventing cyberattacks and in the event of an attack, insuring swift recovery of the fonctioning information systems.

In order to tackle different forms of cyberthreath, there is a need for comprehensive strategy on the cybersecurity, both on the national and on the EU level. We are in favor of the development of a transeuropean cyberstrategy. The European Cybercrime Centre at Europol has commenced its activities on January 1st, 2013 and it will be the focal point in the EU's fight against cybercrime.

On the Baltic level, we have developed and adopted the necessary legislation. For example, Estonia has elaborated and adopted a broad national cybersecurity strategy in 2008; Lithuania adopted the national strategy on cybersecurity in 2011 and in 2012 Latvia adopted the national defense concept which sets out tasks to increase cybersecurity.

At this moment, the government is working on separate policy documents in order to increase cybersecurity for the period of 2013 to 2018. This document is still in preparation. In 2011, Latvia also adopted a law on critical information technology infrastructure which outlines the infrastructure that plays a critical role, sets out obligations for private holders of infrastructure as well as public institutions, and also outlines the procedures that must be carried out in case of cyberbreakdown and cyberattacks.

The main action points covered by the strategies of the Baltic States include the following : responsibilities of the state and private organizations, vulnerability assessment of critical national IT infrastructure, response system, domestic and international legal instruments, international and institutional cooperation, training, research programmes, awareness raising, protection of personal data and privacy.

One of the priority areas in the Baltic cooperation is the establishment of a digital single market. We are well aware that growth in the digital economy will promote crossborder commerce and improve competitiveness. A well fonctioning digital single market opens doors to e-commerce, simplification of procedures for entrepreneurs, offers new digital services as a result of which it will facilitate crossborder cooperation and increase productivity.

In the European Union it has been calculated that building a digital single market is worth 4 % of GDP (gross domestic product) per year.

For example, Estonia has gone further than any other country in the world in investing into digitizing the basic process of society within government, citizens and entreprises. A quarter of the electoral votes in Estonia are casted online. They have implemented the internet voting system. 95 % of tax return applications are also done online. Citizens as legal owners of their own data have access to their digital, medical and dental records.

These issues which are connected with cybersecurity, data protection, e-signature, roll out and web accessibility have to be seriously considered. We should think of cybersecurity not as a cost, but as an enabler. It goes without saying that for the free movement of people, goods, services, capital and information in a globalized economy, cybersecurity is vital.

We carry the responsibility to maintain the digital way of life of our citizens.

Many problems, especially misuse and accidental incidents can be avoided. In order to promote awareness on cybersecurity issues, there are several tasks to be accomplished on a continuous basis.

First, organizing information security, awareness raising for the wider public and cooperation with the private sector, with a particular focus on home users, small and medium enterprises, employees of local governments and state agencies, teachers and students.

Secondly, conducting target and media campaigns on cybersecurity and computer protection

Third, raising the awareness of cyberculture in every agency and company by training executives and officials in the promotion of safe use of the internet.

Fourth, the last but not least, introducing and exchanging experience in cybersecurity at the international level.

Thank you for your attention.

*Mrs de Caluwé (N) E.-* Thank you very much, Mr Engelis. Are there any questions or remarks ? Mr Angel.

*Mr Angel (L) E.-* Thank you very much. We all know that Estonia has a fantastic internet policy and is also the leader in cybersecurity in you area. Within the Baltic Assembly, do you copy laws from Estonia or do the other two countries try to follow the same path, or is Estonia an exception ?

*Mr Engelis (BA) E.-* Estonia does stand out, as you correctly described it. That is logical because the public investment which is given to the relevant sectors is much larger than in the other Baltic States.

In terms of legislation and procedures that they draft, I presume that they do set an example. It is probably not the Baltic Assembly which relates to this example because in the Baltic States, the cooperation on the governmental level is far more active and developed. The Baltic Assembly tries to set the general agenda. The government is more active in decision taking.

We do learn much from the example of Estonia but we also acknowledge that it is not so easy to copy their achievements. It first of all relates to their funding capabilities and it should be pointed out that Estonia has world class programmers and Latvia at the moment has none.

To implement the IT structures that have been achieved in Estonia, is intellectually impossible in Latvia. For instance, Estonia was able to implement the internet voting system which is a system that requires a very high level of security against attacks that would terminate the results of the elections.

Estonia sets an example but we can't always follow in the prioritizing of policies.

*Mrs de Caluwé (N) E.-* Thank you very much, Mr. Engelis. I think you have been far to modest by saying you could not teach us anything.

(vervolgt in het Nederlands)

Dames en heren, de ochtendvergadering eindigt hier.

De conferentie wordt geschorst van 12.30 uur tot 13.30 uur.

(poursuivant en néerlandais)

Mesdames et messieurs, c'est ici que se termine la réunion de ce matin.

La conférence est suspendue de 12 heures 30 à 13 heures 30.

*De heer Bettel (L) F.-* Dames en heren, we hervatten onze werkzaamheden met het betoog van de heer Streefland dat oorspronkelijk voor deze ochtend was gepland.

*Mevrouw de Caluwé (NL) N.-* Ik geef graag het woord aan de heer Fred Streefland van het European Network for Cybersecurity in Den Haag. Hij zal zich zelf aan u voorstellen en zal zijn uiteenzetting inleiden met een filmpje dat illustreert wat je met cybercriminaliteit allemaal kunt doen.

**Uiteenzetting door de heer Fred Streefland, *director Education, Training & Knowledge Center, European Network for Cybersecurity* (ENCS), Nederland**

*De heer Streefland (NL) N.-* Dank u wel, voorzitter.

Ik zal inderdaad een presentatie geven over cybersecurity in de vitale en critical infrastructuur en me daarbij vooral toeleggen op de vraag how to raise public awareness. Hoe kun je de bewustmaking vergroten?

Om te illustreren wat cybercriminaliteit kan doen en u wakker te maken na de goede lunch wil ik u eerst een kort filmpje laten zien.

Ik zal u eerst kort en bondig vertellen wie ik ben en waar ik werk. Vervolgens zal ik u uitleggen wat cybersecurity is en wat dat is in de vitale infrastructuur. Hoe kan ik dan de *awareness*, de publieke bekendheid, hierbij vergroten?

Wie is Fred Streefland? Ik ben 1,95 m. lang en licht kalend en ik heb 20 jaar ervaring binnen de inlichtingen- en veiligheid. Ik ben inlichtingen- en veiligheidofficier geweest bij de luchtmacht. Ik heb gewerkt bij het NAVO-hoofdkwartier voor Jaap de Hoop Scheffer. Ik heb bij de inlichtingendienst gewerkt en ben vervolgens door IBM geheadhunt als luitenant-kolonel om daar cybersecurityexpert te worden. Vervolgens weer weggehaald door

*M. Bettel (L) F.-* Mesdames et Messieurs, nous reprenons notre séance de l'après-midi avec l'intervention de M. Streefland, initialement prévue ce matin.

*Mme de Caluwé (NL) N.-* Je cède la parole à M. Fred Streefland, du European Network for Cybersecurity de La Haye, qui va se présenter et introduire son exposé par la projection d'un petit film qui illustrera tout ce qu'il est possible de faire en matière de cybercriminalité.

**Présentation par M. Fred Streefland, *director Education, Training & Knowledge Center, European Network for Cybersecurity* (ENCS), Pays-Bas**

*M. Streefland (NL) N.-* Je vous remercie, Mme la Présidente.

Je vais en effet vous faire un exposé sur la cybercriminalité dans la cadre de l'infrastructure vitale et critique et traiter essentiellement de la question how to raise public awareness. Comment renforcer la sensibilisation?

Pour illustrer ce à quoi peut conduire la cybercriminalité et un peu aussi pour vous réveiller après l'excellent déjeuner qui nous a été servi, je vais vous projeter un petit film.

Pour commencer, je vais vous dire succinctement qui je suis et où je travaille. Je vous expliquerai ensuite ce qu'est la cybersécurité et ce qu'elle représente dans l'infrastructure vitale. Comment puis-je renforcer la *awareness*, la sensibilisation du public?

Qui est Fred Streefland? Je mesure 1 m 95, ai une calvitie naissante et possède 20 années d'expérience en matière de renseignement et de sécurité. J'ai été officier de renseignement et de sécurité à la force aérienne. J'ai travaillé au quartier général de l'OTAN pour Jaap de Hoop Scheffer. J'ai travaillé au service de renseignement avant d'être recruté par des chasseurs de tête pour IBM en tant que lieutenant colonel, pour y devenir

Accenture en nu werkzaam bij het *European Network for Cybersecurity* (ENCS), waarover ik dadelijk meer zal vertellen.

Ik heb een aantal cursussen gevolgd, o.a. in Engeland, Israel en in Nederland en over twee weken vertrek ik naar Amerika voor een speciale advanced cybersecurity cursus. Ik geef advies zowel in de publieke sector als in de private sector en ik heb ook een aantal maanden gewerkt als projectleider in een slimme-energienetwerk en dan vooral gekeken naar de cybersecurity, namelijk de veiligheid bij het automatiseren van onderstations. Maar ik ben nog steeds geen expert.

Wat is ENCS, de organisatie waarvoor ik werk? Het *European Network for Cybersecurity* is een hele nieuwe organisatie, slechts 8 maanden geleden, in juli 2012, opgericht door onder andere KPN, een telecomprovider, Alliander, een energiebedrijf, de Radboud Universiteit Nijmegen, TNO en KEMA, met het doel om de Europese weerbaarheid van de kritische infrastructuur te vergroten.

Als bedrijven een probleem op dat gebied hadden, dan konden ze nergens naar toe. Daaruit kwam het idee van onze oprichting. Het bedrijf bevindt zich in Den Haag en de organisatie bestaat uit vier elementen:

• *Research & Development* (R & D);

• *Test Bed*: we hebben ons eigen testlab; we kunnen dus inderdaad een stukje van de fabriek of van een energienetwerk in ons lab testen;

• *Education & Training* (E & T): we hebben een training- en educatiegedeelte, waarvoor ik verantwoordelijk ben;

• *Information & Knowledge Sharing* (I & KS): een informatieverspreidingsgedeelte waar ik eveneens verantwoordelijk voor ben.

In de uiteenzettingen van mijn voorgangers werd reeds vermeld dat er meer informatie moet gedeeld worden.

expert en cybersécurité. J'ai ensuite été recruté une nouvelle fois, cette fois par Accenture, et je travaille actuellement au *European Network for Cybersecurity* (ENCS) au sujet sur lequel je vous en dirai plus dans un instant.

J'ai suivi un certain nombre de cours, entre autres en Angleterre, en Israël et aux Pays-Bas, et je me rendrai dans deux semaines aux Etats-Unis pour y suivre un cours spécial de cybersécurité avancée. Je rends des avis dans le secteur privé comme dans le secteur public et j'ai également travaillé un certain nombre de mois comme chef de projet dans un réseau énergétique intelligent en m'y occupant principalement de cybersécurité, à savoir la sécurité de l'automatisation de sous-stations. Mais je ne suis toujours pas un expert en la matière.

Que représente ENCS, l'organisation pour laquelle je travaille? *L'European Network for Cybersecurity* est une toute nouvelle organisation créée il y a seulement 8 mois, en juillet 2012, par, entre autre, KPN, un fournisseur de services de télécoms, Alliander, une entreprises énergétique, la Radboud Universiteit Nijmegen, TNO et KEMA dans le but d'accroître la résistance européenne de l'infrastructure critique.

Les entreprises qui rencontraient un problème dans ce domaine n'avaient personne à qui s'adresser. D'où l'idée de créer l'entreprise dont le siège se trouve à La Haye et qui se compose de 4 éléments :

• *Research & Development* (R & D);

• *Test Bed*: nous possédons notre propre laboratoire de tests; nous pouvons donc y tester une partie d'une usine ou d'un réseau énergétique;

• *Education & Training* (E & T): nous avons un département de formation et d'éducation dont j'assume la responsabilité;

• *Information & Knowledge Sharing* (I & KS) : un département de diffusion de l'information dont je suis également responsable.

Un des orateurs précédents a déjà indiqué qu'il faut davantage de partage de l'information.

Het doel van onze organisatie is om de vitale infrastructuur in Europa, europees te vergroten. Wat is dan de cybersecurity in de kritische infrastructuur? Waarover praten we dan eigenlijk?

Ik geef u hier de definitie van mevrouw Neelie Kroes; deze definitie komt rechtstreeks uit de European Strategy for Cybersecurity. Zij zegt: “Hoe meer mensen er op internet gaan, hoe meer mensen er van uitgaan dat het veilig moet zijn.”

Ik heb dan een volgende spreuk, niet omdat ik mezelf op dezelfde hoogte bevindt als Neelie Kroes, maar wel omdat het mijn eigen mening is: “Hoe meer kritische infrastructuur aan het internet wordt gekoppeld, hoe onveiliger het wordt.”

Wat is cybersecurity? Daar bestaan veel definities van. Cybersecurity is eigenlijk “de beveiliging van een organisatie en haar eenheden, haar elementen tegen een electronische aanval met het doel de schade zo min mogelijk te maken” Dat is eigenlijk cybersecurity; meer is het niet. Belangrijk is vooral “electronische aanval” – *“electronic attack”*, dus vanuit internet. Het moet ergens electronisch aan gekoppeld worden.

Wat zijn kritische infrastructuren? Dat zijn de elementen, de organisaties die essentieel zijn voor onze maatschappij.

• utilities: elektriciteit, olie, gas, water, licht;

• transport: spoorwegen, verkeerslichten, lucht- en zeehavens;

• telecom;

• landbouw: voedselproductie en –verdeling;

• gezondheidsdiensten: ziekenhuizen, …;

• financiële diensten.

Het ENCS focust zich enkel op de eerste drie elementen.

Notre organisation a pour but d’accroître l’infrastructiure vitale en Europe sur le plan européen. Que représente alors la cybersécurité dans l’infrastructure critique? De quoi est-il exactement question?

Je vais vous donner la définition de Mme Neelie Kroes qui est directement extraite de la European Strategy for Cybersecurity: plus les gens qui utilisent l’internet sont nombreux, plus ils pensent que la toile est nécessairement sûre.

J’ai quant à moi mon propre slogan, non pas parce que je me place au même niveau que Mme Neelie Kroes mais parce que c’est ma propre opinion: plus on lie d’infrastructure critique à l’internet, plus il devient risqué de s’y aventurer.

Qu’est-ce que la cybersecurité? Les définitions sont nombreuses. La cybersecurité est en fait la sécurisation d’une organisation et de ses éléments contre une attaque électronique dans le but de limiter les dommages au maximum. C’est cela la cybersecurité, rien de plus. Les termes “attaque électronique” surtout son importants – “attaque électronique”, c’est-à-dire depuis l’internet. Il faut donc un lien avec l’électronique.

Que sont les infrastructures critiques? Ce sont des éléments, des organisations essentiels pour notre société.

• équipements: électricité, pétrole, gaz, eau, lumière;

• transport: chemins de fer, feux de signalisation, ports et aéroports;

• telecom;

• agriculture: production et distribution alimentaires;

• services de soins de santé: hôpitaux, …;

• Services financiers.

L’ENCS ne s’occupe que des trois premiers éléments.

We kennen nu de definities. Wat is nu eigenlijk die kritische infrastructuur?

Kritische infrastructuur bestaat onder andere uit industriële controlesystemen, SCADA systemen. U hebt daar misschien reeds van gehoord. Dat zijn systemen die vooral in die fabrieken van belang zijn. Dat is dus de fabrieks-IT.

U heeft op uw bureau een laptop, dat is de kantoorautomatisering; in de fabriek worden de machines aangestuurd en dat gebeurt door middel van fabrieksautomatisering. Dat zijn de SCADA-systemen. Die systemen geven dus instructies, stuursignalen (klepje open, klepje dicht, temperatuur omhoog of omlaag, enz.). Die geven ook informatie daarover terug aan de operators en het is ook een alarmsysteem. Het is de eigenlijke fabrieks-IT.

Die techniek is eigenlijk heel basaal, heel erg simplistisch. Dat zijn namelijk heel simpele computers, die ongeveer 20 jaar geleden zijn ontwikkeld, en nooit werden ontwikkeld om veilig te zijn. Zij werden ontwikkeld om te werken, om 30 jaar klepje open, klepje dicht te doen. Zij zijn ook ontwikkeld voor operators zodat die heel snel dingen kunnen aanpassen (temperatuur moet iets hoger, klepje moet iets sneller dicht, druk moet hoger of lager, enz.). Daarvoor werden ze ontwikkeld.

In het verleden waren deze systemen eigenlijk niet aan internet gekoppeld en daar zit de crux. In het verleden was de fabrieks-IT open. Er was dus geen behoefte aan security, dat was niet nodig. Ze moesten juist open zijn, vanwege de functionaliteit, en ze waren niet aan internet gekoppeld. Maar nu is dat wel het geval.

Dat is het gevaar. Op het moment dat men vanuit internet die fabriek kan inkomen, dan is men overal bij. Dat is juist zo gevaarlijk.

Nous connaissons à présent les définitions. Mais en quoi consiste précisément l'infrastructure critique?

L'infrastructure critique comprend, entre autres, des systèmes de contrôle industriels, des systèmes SCADA. Vous en avez peut-être déjà entendu parler. Il s'agit de systèmes qui sont surtout important dans les usines. Il s'agit donc des TI industrielles.

L'ordinateur portable que vous avez sur votre bureau, c'est de la bureautique. Dans une usine, les machines sont commandées par le biais de l'automatisation industrielle. Il s'agit des systèmes SCADA qui donnent des instructions, émettent des signaux de commande (ouverture ou fermeture d'une valve, augmentation ou abaissement de la température, *etc.*). Ils transmettent également des informations à ce sujet aux opérateurs et constituent aussi un système d'alerte. Il s'agit des TI industrielles à proprement parler.

Cette technique est en fait très basique et simpliste. Elle repose sur des ordinateurs très simples, qui ont été développés il y a environ 20 ans sans jamais avoir été conçus pour être sûrs. Ils ont été développés pour travailler, pour commander, 30 années durant, l'ouverture ou la fermeture d'une valve. Ils ont également été conçus en fonction des besoins d'opérateurs qui doivent pouvoir apporter des aménagements très rapidement (la température doit être un peu plus élevée, la valve doit se fermer un peu plus rapidement, la pression doit être augmentée ou abaissée, *etc.*). Voilà pourquoi ils ont été développés.

Par le passé, ces systèmes n'étaient pas liés à l'internet et c'est là le problème. A l'époque, les TI industrielles étaient ouvertes. La sécurité ne répondait pas à un besoin. Elles devaient simplement être ouvertes pour des raisons de fonctionnalité et n'étaient pas liées à l'internet. Aujourd'hui, elles le sont.

C'est là que réside le danger. Dès lors que l'on peut pénétrer dans l'usine à partir de l'internet, on est partout. Et c'est ce qui rend la chose si dangereuse.

Dan krijg je berichtgeving in de media dat de industrial control systemen worden gehackt. Dan gaan echt de poppen aan het dansen.

Als we zo'n DDoS aanval krijgen dan is dat lastig want dan kunnen we niet bij de website van onze bank.

Maar als ons energienetwerk wordt gehackt, dan hebben wij pas echt een uitdaging.

Ik geef een paar voorbeelden. Het gebeurde in Australië in 2000. Een persoon die boos was omdat hij niet werd aangenomen bij de watervoorziening heeft als wraakactie met zijn laptop en een radiotransmitter, meer niet, de controle over 142 pompstations gekregen. Hij heeft in drie maanden tijd 100 miljoen liter stortwater in de lokale meren en rivieren doen dumpen.

Ik geef twee andere voorbeelden die hetzelfe effect beogen, namelijk chaos creëren. In 2003 hebben hackers door middel van een virus de treinstoplichten van CSX, een treinorganisatie in het noordoosten van Amerika, verstoord, waardoor het hele treinverkeer stillag.

Iets dergelijks gebeurde in Los Angeles in 2006, waar twee ingenieurs van het stadsbedrijf de hoofdcomputer van het verkeerssysteem hebben gehackt en op slechts vier kruispunten de verkeerslichten verstoorden. Er ontstond complete chaos. Zij deden dat als protest namens de stadswerkers.

Wat misschien bekender is, is het Stuxnet, het verhaal van Iran in 2010. Hackers zijn in staat geweest door middel van een virus de SCADA-systemen binnen die kerncentrale te veranderen waardoor de centrifuges van die verwerking kapot gingen. Zo zijn er in totaal 2 000 van de in totaal 7 000 centrifuges in de soep gedraaid.

Een recenter voorbeeld gebeurde in 2012 in Nederland. Een journalist hackte de waterbeveiliging van sluizen van de buitenkant. Hij heeft twee keer een poging gedaan om het paswoord te raden. De derde keer was het al raak; het paswoord was heel simpel. Hij is in het systeem geraakt en is via de webserver binnengekomen. Het SCADA-systeem

Et l'on apprend alors par la presse que des systèmes de contrôle industriel font l'objet de hacking. Et c'est là que les choses commencent vraiment.

Lorsque nous sommes confrontés à une telle attaque DDOS, le problème est que nous n'avons pas accès au site internet de notre banque.

Mais lorsque notre réseau énergétique est victimes de hackers, alors nous sommes réellement confrontés à un défi.

Permettez-moi de citer quelques exemples. En 2000, en Australie, une personne qu'une société de distribution d'eau avait refusé d'embaucher s'était vengée en prenant, à l'aide de son ordinateur portable et d'un transmetteur radio – rien de plus – le contrôle de 142 stations de pompage. En trois mois, elle a fait rejeter 100 millions de litres d'eau dans les lacs et les rivières locaux.

Voici deux autres exemples d'attaques qui poursuivent le même objectif, à savoir susciter le chaos. En 2003, des hackers ont perturbé au moyen d'un virus le fonctionnement des feux stop ferroviaires de CSX - une organisation ferroviaire du nord-ouest des Etats-Unis – au point de paralyser tout le trafic.

Un cas similaire s'est produit à Los Angeles en 2006, lorsque deux ingénieurs de la ville ont piraté l'ordinateur principal du système de circulation routière en perturbant le fonctionnement des feux de seulement 4 carrefours. Ce fut le chaos total. Les pirates voulaient protester au nom des travailleurs de l'administration de la ville.

Plus connu peut-être, le Stuxnet, qui s'est passé en Iran en 2010. Des hackers ont réussi, au moyen d'un virus, à modifier les systèmes SCADA d'une centrale nucléaire et à y détruire des centrifugeuses. Quelque 2 000 centrifugeuses sur un total de 7 000 ont été touchées.

Un exemple plus récent nous est venu des Pays-Bas en 2012. Un journaliste a piraté la sécurité hydraulique d'écluses. Il a essayé de deviner le mot de passe. La troisième tentative a été la bonne. Le mot de passe était en effet très simple. Il a pu entrer dans le système et a accédé au serveur internet. Le système SCADA était dépourvu de mot de passe.

had geen paswoord. Hij kon vanop zijn thuiscomputer de sluizen open en dicht zetten.

Het laatste voorbeeld is recent, uit 2012. De grootste oliemaatschappij in de wereld, Saudi Aramco-Shamoon is gehackt, waarbij gelukkig enkel de kantoorautomatisering is gehackt, waardoor 30 000 computers zijn gewist. Ze zijn gelukkig niet in de industriële controlesystemen kunnen komen, maar dat had wel een volgende stap kunnen zijn.

Deze voorbeelden illustreerden wat cybersecurity betekent in de kritische infrastructuur.

Hoe kunnen we nu de publieke bewustmaking op dit gebied vergroten?

Ik heb daarover een paar ideeën. Vertel dit! Wees iemand die deze boodschap verkondigt. Vertel het en blijf het vertellen! Dat helpt echt. Blijf mensen bewust maken van het gevaar.

Ik verwijs ook naar de EU-strategie waar voorbeelden staan van hoe we die awareness kunnen vergroten. Ik raad u aan dit te lezen want het is echt een heel goed document.

Gebruik de voorbeelden die heel eenvoudig kunnen worden verteld, zowel door een security expert als door u. Een aantal voorbeelden zijn:

• meer dan 200 vitale infrastructuurorganisaties zijn in 2012 gehackt in Amerika en dat zijn alleen de geregistreerde;

• op een gegeven moment werd door een organisatie een nep-SCADA-systeem op internet geplaatst om te zien wanneer het zou worden aangevallen; reeds na 18 uur na de plaatsing op het internet vond de eerste aanval plaats; in de volgende 28 dagen werd het 39 keer aangevallen door 14 verschillende landen;

• nog schokkender: in 2012 heeft Eurostat een onderzoek gedaan naar de Europese organisaties, bedrijven en daarvan was er slechts 26 % die een daadwerkelijke security policy hadden.

Depuis son ordinateur personnel installé chez lui, il a pu à loisir ouvrir et fermer les écluses.

Le dernier exemple est récent. La plus grande société pétrolière au monde, la Saudi Aramco-Shamoon, a été piratée mais, fort heureusement, seule la bureautique a été hackée et le contenu de 30 000 ordinateurs effacé. Les pirates n'ont pas pu accéder aux systèmes de contrôole industriels, ce qui aurait toutefois pu être l'étape suivante.

Ces exemples montrent ce que la cybersécurité représente pour l'infrastructure critique.

Cela dit, comment pouvons-nous accroître la sensibilisation du public à cet égard?

J'ai quelques idées à formuler en la matière. Diffusez tout cela ! Soyez de ceux qui porteront ce message. Racontez, encore et encore ! Cela marche vraiment. Continuez à sensibiliser les gens aux dangers.

Je me réfèrerai aussi à la stratégie de l'UE où il est indiqué comment l'on peut accroître la conscientisation. Je vous invite à lire ce document qui est vraiment excellent.

Utilsez des exemples qui peuvent être racontés très simplement, par un expert en sécurité comme par vous-même. Voici quelques exemples:

• plus de 200 organisations d'infrastructure vitales ont été piratées en 2012 en Amérique, et encore ne s'agit-il que de celles qui étaient enregistrées;

• à un moment donné, une organisation a mis sur l'internet un faux système SCADA pour voir quand il serait attaqué. La première attaque a eu lieu au bout de 18 heures seulement. Au cours des 28 jours qui ont suivi, le système a été attaqué 39 fois par 14 pays différents;

• plus choquant encore: en 2012, Eurostat a effectué une étude sur les organisations et les entreprises européennes dont il s'est avéré que 26 % seulement étaient dotées d'une véritable politique de sécurité.

Vervolgens, nu je die awareness creëert en die boodschap gaat verkondigen, wat kun je dan nog meer doen?

Hier ligt een taak voor u, als Beneluxparlement. Kom met een announcement; kies iemand als grote verkondiger, de grote verteller, iemand die hiervan het boegbeeld is.

Zoals Barack Obama heeft gezegd in 2012: *"Cybersecurity is one of the most serious economic and national security challenges we face as a nation, bigger than terrorism*!", zo zou dat ook vanuit het Beneluxparlement en vanuit Europa keihard moeten worden verkondigd. Mensen, luister, *this is serious business!*

Zorg ook voor de opvolgactie. Maak iemand probleemeigenaar.

Mijn derde advies is ervoor te zorgen dat ook daadwerkelijk vanuit de Europese context een beleid en standaarden worden ontwikkeld, natuurlijk in lijn met de *EU Cyber Security Strategy*.

Dit is ook een boodschap en een taak voor u, waar u daadwerkelijk iets aan kunt doen. Zorg dat er iemand verantwoordelijk wordt gemaakt en zet de pikketpaaltjes uit! Zeg tegen de mensen dat het erg is, dat het serieus is en dat we er iets moeten aan doen!

Dan kom ik tot de conclusie van mijn verhaal.

Wacht alstublief niet tot het te laat is! Ik vermoed en ik ben bang dat er binnenkort inderdaad in een groot gedeelte van Europa of ergens in een land vitale infrastructuur zal worden aangevallen. Het zijn nu de banken, sommige bedrijfjes of websites die worden aangevallen. Maar er zal eens een energiebedrijf, of een waterbedrijf, of een telecombedrijf of een spoorwegorganisatie aangevallen worden. En dat zal dan een mega-aanval zijn, gewoon omdat het kan. Hackers houden immers van uitdagingen en zullen dat zeker proberen.

Ik zeg het nogmaals, vertel het, verkondig het, begin een mediacampagne, wat een heel goed idee is. Zorg voor een statement en voor follow-on acti-

Après avoir favorisé la conscientisation et propagé le message, que pouvez-vous faire d'autre?

Une tâche vous est réservée, à vous, Parlement Benelux. Faites faire une annonce par un grand communicateur, quelqu'un qui soit une figure de proue:

Comme a dit Barack Obama en 2012 : "*Cybersecurity is one of the most serious economic and national security challenges we face as a nation, bigger than terrorism!*". Il faudrait que le Parlement Benelux, que l'Europe le dise haut et fort. Ecoutez, *this is serious business*!

Veillez également à assurer un suivi. Quelqu'un doit s'approprier le dossier.

Mon troisième avis sera pour vous dire qu'il faut faire en sorte de définir dans le cadre européen une politique et des standards qui soient bien évidemment en phase avec la *EU Cyber Security Strategy*.

C'est aussi un message et une tâche pour vous car vous pouvez réellement faire quelque chose. Faites en sorte que quelqu'un soit responsable et posez les jalons! Dites au gens combien la situation est grave, que c'est du sérieux et qu'il nous faut faire quelque chose!

J'en viens enfin à la conclusion de mon intervention.

S'il vous plait, n'attendez pas qu'il soit trop tard! Je pense, je crains que prochainement, une infrastructure vitale sera attaquée dans un grande partie de l'Europe ou dans un pays. Ce sont aujourd'hui les banques, de petites entreprises ou des sites internet. Mais ce sera un jour une entreprise énergétique, une entreprise de distribution d'eau ou de télécommunications ou encore une organisation ferroviaire. Ce sera alors une méga-attaque, simplement parce que c'est possible. Car les pirates informatiques aiment les défis et ne manqueront pas de les relever.

Je le répète, propagez le message, portez-le, entamez une campagne d'information, ce qui est à mon estime une excellente idee. Faites un point

ons! Ontwikkel een Benelux-policy en standards! Nogmaals, het is nu het ogenblik om er wat aan te doen! Dat is mijn boodschap. Dank u wel.

*Mevrouw de Caluwé (NL)* N.- Dank u wel, mijnheer Streefland. Zijn er vragen of opmerkingen vanuit de zaal? Het woord is aan de heer Beirens.

*De heer Beirens (B) N.-* Ik heb hier een kleine aanvulling op te geven.

Wij denken altijd dat degenen die aanvallen, belangrijke mensen zijn of organisaties. Wij hebben echter aanvallen op datacenters gezien van jongelui die op de websites van *Anonymus* gezien hadden hoe ze de security kunnen testen en die dan op diezelfde websites ook de tools vinden. Die hebben volledige datacenters.

We spreken erover om al die servers in de bedrijven eigenlijk weg te laten en ze samen te zetten in een groot datacenter. Zo'n datacenters zijn in België platgelegd geweest door een knaap van 17 jaar. Die is strafrechtelijk nog niet meerderjarig. Voor zulke feiten komt hij niet voor de strafrechter. Daarvan gaat men niet zeggen dat het een misdrijf is. Dan komt hij terug voor de jeugdrechter.

Het zijn die mensen die onze infrastructuur ook mee bedreigen. Als iemand van 17 jaar dat kan, met zeer elementaire kennis, wat moet het dan zijn als er een criminele organisatie op poten wordt gezet die ons met duidelijke drijfveren gaat aanvallen?

*Mevrouw de Caluwé (NL) N.-* Het woord is aan mevrouw Quik.

*Mevrouw Quik-Schuijt (NL) N.-* U zegt dat iemand eigenaar van het probleem moet worden. In Nederland is het in ieder geval niet duidelijk wie dat zal worden. Ik denk dat het waarschijnlijk het ministerie van Veiligheid en Justitie zal zijn. Hoe is dat in andere landen? Ik vraag ook aan mijn collega's of iemand in België of Luxemburg eigenaar is van dat probleem. Wie is daar verantwoordelijk voor de cybersecurity?

de la situation et assurez un suivi! Développez une politique et des standards pour le Benelux. Une fois encore, le moment est venu de faire quelque chose. Tel est mon message. Je vous remercie.

*Mme de Caluwé (NL) N.-* Merci, M. Streefland. Quelqu'un souhaite-t-il poser une question ou formuler une observation ? La parole est à M. Beirens.

*De heer Beirens (B) N.-* Je voudrais ajouter quelque chose.

L'on croit toujours que les pirates sont des gens ou des organisations importants. Mais nous avons connu des attaques contre des centres prepétrées par des jeunes gens qui avaient vu sur le site internet d'*Anonymus* comment ils pouvaient tester la sécurité et avaient trouvé sur le même site les outils nécessaires. Car des centres de données complets sont à disposition.

L'on évoque l'idée d'évacuer tous les serveurs des entreprises et de les regrouper dans un grand centre. Or de tels centres ont été paralysés par un gamin de 17 ans qui, pénalement, n'est même pas majeur. Il ne comparaîtra donc pas devant le juge pénal pour ces faits. On ne parlera donc pas de crime et il sera renvoyé devant le juge de la jeunesse.

Ces gens aussi constituent une menace pour notre infrastructure. Si un garçon de 17 ans, qui possède sans doute des connaissances limitée, est capable de faire cela, que dire alors d'une organisation criminelle mise sur pied pour nous attaquer avec des objectifs précis ?

*Mme de Caluwé (NL) N.-* Je donne la parole à Mme Quik.

*Mme Quik-Schuijt (NL) N.-* Vous dites que quelqu'un doit se saisir du problème. Aux Pays-Bas en tout cas, on ne voit pas clairement de qui il s'agira Sans doute sera-ce le ministère de la Sécurité et de la Justice. Qu'en est-il dans les autres pays ? Je pose la questions à nos collègues. Quelqu'un est-il en charge de cette question en Belgique et au Luxembourg ? Qui y est responsable de la cybersécurité ?

*De heer Beirens (B) N.-* Krediet moet gegeven worden aan wie krediet moet krijgen. Nederland is wat dat betreft een stuk verder dan België.

In België hebben we een cybersecuritystrategie die door de ministerraad is aangenomen in december van vorig jaar. Daar is nauwelijks publiciteit rond geweest.

Een van de eerste punten in het uitwerken van die cybersecuritystrategie is het aanduiden van een nationale overheid. Maar zover zijn we nog niet gekomen. We zitten dus met een verspreiding van politieke bevoegdheden over verschillende departementen en er is niemand die dat coördineert. Dat leidt tot een situatie waarbij niemand de taakhouder is en de verantwoordelijkheid voor een bepaald probleem gaat opnemen.

*Mevrouw de Caluwé (NL) N.-* Ik denk dat er in Nederland ook nog een uitdaging op dat vlak bestaat.

*Mevrouw Quik-Schuijt (NL) N.-* U zegt dat Nederland verder staat dan België. Hoe dan?

*De heer Beirens (B) N.-* Jullie hebben al een nationaal cybersecuritycenter.

Om even de vergelijking te maken: wij hebben CERT.be, dat opgericht is in 2009. Daar zitten 7 mensen in. Zeven mensen om alle incidenten van én de overheid én de grote bedrijven op te vangen. Dat is veel te weinig!

Als het maar een doekje voor het bloeden is, dan hoeft het eigenlijk niet, want dan geef je de mensen een verkeerd of een vals gevoel van veiligheid. Je moet er echt in investeren en iemand aanwijzen die duidelijke verantwoordelijkheid moet opnemen.

*Mevrouw de Caluwé (NL) N.-* Misschien kan de heer Houtsch dit hier aanvullen voor Luxemburg?

*De heer Houtsch (L) F.-* Het "*Haut Commissariat à la protection nationale*" ressorteert onder het "*ministère d'État*".

*De heer Beirens (B) N.-* Il faut donner du crédit à qui doit en recevoir.Sur ce point, les Pays-Bas sont plus avancés que la Belgique.

Il existe en Belgique une stratégie de cybersécurité qui a été adoptée en décembre de l'an dernier par le conseil des ministres. On n'en a guère fait état.

L'un des premiers éléments dans le cadre de la mise au point d'une stratégie de cybersécurité est la désignation d'une autorité nationale. Mais nous n'en sommes pas encore là. Les compétences politiques sont donc éparpillées entre plusieurs départements, sans aucune coordination. Il en résulte donc qu'il n'y a personne qui soit en charge du dossier et assume la responsabilité d'un problème donné.

*Mme de Caluwé (NL) N.-* Je crois qu'aux Pays-Bas aussi, il reste un défi à relever dans ce domaine.

*Mme Quik-Schuijt (NL) N.-* Vous dites que les Pays-Bas sont plus avancés que la Belgique. Qu'est-ce à dire?

*De heer Beirens (B) N.-* Vous êtes déjà dotés d'un centre national de cybersécurité.

Pour opérer une comparaison: nous avons CERT.be, qui a été créé en 2009, et qui comprend 7 personnes. Sept personnes pour faire face à tous les incidents qui pourraient affecter tous les pouvoirs publics et les grandes entreprises. C'est largement insuffisant !

Si ce n'est qu'un emplâtre sur une jambre de bois, ce n'est pas utile car on suscite ainsi à tort un sentiment de sécurité. Il faut vouloir investir et désigner quelqu'un qui soit amené à réellement assumer les responsabilités.

*Mme de Caluwé (NL) N.-* M. Houtsch pourrait-il compléter le tableau en ce qui concerne le Luxembourg?

*M. Houtsch (L) F.-* Le Haut-commissariat à la protection nationale dépend du ministère d'État.

*Mevrouw Quik-Schuijt (NL) N.-* Is dat dan een organisatie buiten de ministeries of valt ze onder een ministerie

*De heer Houtsch (L) F.-* Het HCPN ressorteert onder het “ministère d’État”

*Mevrouw de Caluwé (NL) N.-* Zijn er nog andere vragen? De heer Streefland wil nog iets zeggen.

*De heer Streefland (NL) N.-* Ik heb misschien nog wel een aanvulling. Ik ben zelf drie weken geleden in Estland geweest en heb daar gesproken met de Estonian Information Security Authority en ook met het NAVO Centre of Excellence.

De Estse regering heeft bepaald dat energiebedrijven elk jaar een cyber security assessment moeten ondergaan. Dat is een hele simpele maatregel, maar volgens mij wel effectief.

De regering zet hier de pikketpaaltjes uit, maar de bedrijven zijn zelf verantwoordelijk voor de uitvoering ervan. Dat is een idee dat ik ook graag in Nederland en misschien ook in België en Luxemburg zou willen verwezenlijkt zien.

Dit zijn concrete ideeën over hoe dit vorm kan worden gegeven. Ik ben het eens met de heer Houtsch dat het maar een gedeelte is. Maar het is wel een begin. Het is nodig er nu aan te beginnen want anders gaan we achter de feiten aanlopen.

*Mevrouw de Caluwé (NL) N.-* Dank u wel, mijnheer Streefland. Zijn er nog opmerkingen of vragen? Dan geef ik nu het woord aan de heer Gérard Hoffmann, CEO van Telindus.

**Uiteenzetting door de heer Gérard Hoffmann, CEO Telindus, Luxemburg**

*De heer Hoffmann (L) F.-* Dag, dames en heren. Ik dank u voor uw uitnodiging.

Alvorens mijn uiteenzetting te beginnen, zal ik enkele woorden zeggen over Telindus, dochter van de Belgacomgroep, de Belgische historische

*Mme Quik-Schuijt (NL) N.-* S’agit-il d’une organisation extérieure aux ministères ou relève-t-elle d’un ministère ?

*M. Houtsch (L) F.-* Le HCPN dépend du ministère d’Etat.

*Mme de Caluwé (NL) N.-* Y a-t-il d’autres questions ? M. Streefland demande la parole.

*M. Streefland (NL) N.-* Je puis peut-être apporter un complément d’information. Je me suis rendu il y a trois semaines en Estonie et j’y ai eu des contacts avec la Estonian Information Security Authority ainsi qu’avec le NAVO Centre of Excellence.

Le gouvernement estonien a décidé que les entreprises énergétiques devraient chaque année faire l’objety d’un cyber security assessment. C’est une mesure très simple mais elle ne m’en semble pas moins efficace.

Le gouvernement pose là les jalons mais les entreprises sont responsables de la mise en oeuvre. C’est une mesure que j’aimerais voir appliquer aux Pays-Bas et peut-être aussi en Belgique et au Luxembourg.

Il s’agit là d’idées quant à la manière de donner concrètement forme aux choses. Je pense comme M. Houtsch qu’il ne s’agit que d’une partie de la solution. Mais c’est un début. Il nous faut nous mettre au travail maintenant sous peine de devoir courir derrière les faits.

*Mme de Caluwé (NL) N.-* Merci, M. Streefland. D’autres questions ou observations? Dans ce cas, je donne la parole à M. Gérard Hoffmann, CEO de Telindus.

**Présentation par M. Gérard Hoffmann, CEO Telindus, Luxembourg**

*M. Hoffmann (L) F.-* Bonjour mesdames et messieurs. Je vous remercie de m’avoir invité aujourd’hui.

Avant de commencer la présentation, je parlerai très rapidement de Telindus, filiale du groupe Belgacom, opérateur historique belge, présent

operator die aanwezig is in onze drie landen. In België stellen we zowat 17 000 mensen te werk, in Luxemburg 500 en in Nederland ongeveer 250.

In Luxemburg, waar we de tweede operator van het land zijn, beschikken we over twee maatschappijen. De eerste, Telindus, die ik leid, is actief in de bedrijfswereld. Onze competenties zijn beveiliging, bescherming of *consultancy*. De tweede maatschappij, Tango, is een mobiele operator. We zorgen eveneens voor beschermingsinfrastructuur, niet enkel voor bedrijven, maar ook voor openbare instellingen.

Mijn uiteenzetting van vandaag is tamelijk algemeen aangezien veel zaken al werden gezegd. Er zullen ongetwijfeld overlappingen zijn, maar nuances, die met voorbeelden kunnen worden toegelicht, zijn steeds mogelijk. Vorige sprekers hebben al beklemtoond dat het aantal cyberaanvallen steeds maar toeneemt.

Wanneer men bijvoorbeeld de Verenigde Staten neemt, blijkt dat de jongste zes jaar de aanvallen elk jaar toenemen. Het is een echte plaag geworden die niet enkel grote firma's treft, maar in de helft van de gevallen, de kleine en middelgrote ondernemingen, wat begrijpelijk is aangezien ze het slechtst zijn uitgerust. De kleine ondernemingen met minder dan 250 werknemers vertegenwoordigen inderdaad 18 % van het totaal.

Met uitzondering van een of twee grote groepen, maakt Luxemburg eerder deel uit van de groep *"small and medium business*". Hier kan dezelfde tendens andere vormen aannemen. Zonder in detail te treden, geef ik u een overzicht van de soorten aanvallen die zich op de onderscheiden gebieden kunnen voordoen.

Als we het voorbeeld nemen van de wormen in mobile computing stellen we vast dat, afgezien van een of andere uitzondering, alle soorten aanvallen en activiteiten overal blijven toenemen. De spam is vandaag ietwat afgenomen, maar de toestand wordt toch steeds erger.

dans nos trois pays. En Belgique, nous occupons quelque 17 000 employés, au Luxembourg 500 et aux Pays-Bas 250 environ.

Au Luxembourg, où nous représentons le deuxième opérateur du pays, deux sociétés sont présentes. La première, Telindus, que je dirige, est active dans le monde des entreprises. Nous y avons une compétence de sécurité, de protection ou de consultance. La deuxième société, Tango, est, elle, l'opérateur mobile. Nous mettons également en place des infrastructures pour la protection, non seulement des entreprises, mais également des institutions publiques dans ce domaine.

Ma présentation d'aujourd'hui est assez générale car beaucoup de choses ont déjà été dites précédemment. Sans doute y aura-t-il des recoupements mais, dans ce monde, des nuances existent que l'on peut illustrer. Il a déjà été souligné ici que le nombre de cyberattaques est en pleine expansion.

Si l'on s'attache aux États-Unis, par exemple, l'évolution des six dernières années montre bien que les attaques augmentent d'année en année. Il s'agit d'un véritable fléau, qui n'affecte pas seulement les grandes firmes mais aussi, pour la moitié des cas, les petites et moyennes entreprises, ce qui peut se comprendre puisqu'elles sont souvent les moins bien outillées. Ainsi, les petites entreprises de moins de 250 employés représentent 18 % du total.

À l'exception d'un, deux ou trois grands groupes, le Luxembourg se situe plutôt du côté des *"small and medium businesses*". Ici, la même tendance peut s'exprimer différemment. Sans entrer dans les détails, je vous donne un aperçu des différents types d'attaques qui peuvent se produire dans des domaines divers.

Si nous prenons l'exemple des Worms dans Mobile computing, on constate qu'en fait, à part l'une ou l'autre exception, tous les types d'attaque et d'activité témoignent d'une croissance partout. Si l'on remarque un peu moins de spam aujourd'hui, pour le reste la tendance est quand même à l'aggravation.

Met welke uitdagingen worden de onderscheiden landen geconfronteerd? Voor de Staten zijn de uitdagingen strategisch, politiek, economisch, diplomatiek en militair. Ze bestrijken alle werkingsgebieden van een Staat. Als voorbeeld geef ik de "*tacturret*" van oktober die een beetje beter is gekend. Het ging om een aanval gericht tegen de diplomatieke vertegenwoordigingen en bepaalde staatsdiensten. In Luxemburg was de aanval gelukkig minder erg, maar we werden toch getroffen.

Wat de bedrijven betreft, dient te worden vermeld dat de site van ArcelorMital onlangs door Anonymous werd aangevallen; de media hebben daar veel aandacht aan besteed.

De gevolgen voor de bedrijven zijn niet enkel financieel en juridisch, maar tasten ook het imago aan. Wanneer de site van ArcelorMital wordt gehackt, is dat niet alleen zichtbaar maar kan dat, in zekere mate, politieke gevolgen hebben.

Deze plaag is alomtegenwoordig en de media geven aan dat steeds meer privépersonen worden aangevallen. Zo zijn er de phone scams die zijn opgedoken op microsoft Phone, een tamelijk recent verschijnsel: gebruikers stellen vast dat hun telefoon door virussen is aangetast waarmee getracht wordt de nummers van hun kredietkaarten te bemachtigen. Die gegevens worden achteraf natuurlijk misbruikt. Ik zal later nog andere voorbeelden geven.

De meeste incidenten doen zich voor op het gebied van phishing en malware.

Onlangs hebben we cliënten geholpen die boodschappen ontvingen, zogezegd afkomstig van een bedrijf, waarin hun gevraagd werd het nummer van hun kredietkaart mee te delen, anders zou hun kaart worden geblokkeerd. De personen die die inlichtingen doorspeelden werden natuurlijk het slachtoffer van een financiële aanval.

Een andere aanval had betrekking op Laurenson. Het gaat hier om een virus waarbij het insigne van de politie van het Groothertogdom werd gebruikt. De politie had er natuurlijk niets mee te maken, maar dat virus blokkeerde uw computer zogezegd

Quels sont les enjeux pour les différents pays? En fait, pour les États, ils sont stratégiques, politiques, économiques, diplomatiques et militaires. Ils couvrent tous les domaines d'activité d'un État. À titre d'exemple, je vous cite le tacturret d'octobre, un peu plus connu. Il s'agissait d'une attaque visant les représentations diplomatiques et certains services de l'État. Heureusement, au Luxembourg, l'attaque a été moins grave, mais nous en avons malgré tout été victime.

En ce qui concerne les entreprises, il faut signaler que le site web ArcelorMittal par Anonymous a été touché récemment par une attaque qui a été très médiatisée.

Les impacts pour les entreprises ne sont pas seulement financiers et juridiques mais représentent aussi une altération de l'image que l'on en a. Lorsque ArcelorMittal se fait hacker son site web, c'est non seulement très visible mais cela peut avoir, dans une certaine mesure, un impact politique.

Ce fléau est omniprésent et les médias font observer que privés et particuliers subissent de plus en plus d'attaques. Ainsi le Phone Scams, apparu sur le Microsoft Phone, où les utilisateurs retrouvent sur leur téléphone, c'est assez nouveau, des virus destinés à sortir leurs numéros de cartes de crédit afin d'utiliser ensuite ces données à des fins abusives. Je reviendrai avec d'autres exemples plus tard.

Les incidents les plus répandus se situent dans le domaine du phishing et dans le Malware.

Récemment, nous avons aidé des clients recevant des messages provenant soi-disant d'une entreprise, leur demandant d'indiquer leur numéro de carte de crédit, sous prétexte que, sans message de leur part, cette carte serait suspendue. Les personnes fournissant ces informations subissent évidemment par après des attaques financières.

Une autre attaque a concerné le Laurenson. Il s'agit d'un virus répandu sous l'insigne de la police grand-ducale. Bien entendu la police n'était pas impliquée mais ce virus bloquait votre ordinateur sous prétexte que vous aviez consulté certains

omdat u sites had bezocht die door de politie waren verboden. Om opnieuw toegang te krijgen tot uw computer werd u gevraagd 100 euro te betalen met een kredietkaart of via PayPal. Om dergelijke incidenten te voorkomen, moet men zich organiseren!

Drie definities dienen zich hier aan: een beschrijving van de soorten misdadigers die op de netwerken actief zijn, de dreigingen waarmee we eventueel geconfronteerd worden en de maatregelen die de Staat en de bedrijven kunnen nemen. We geven in dit verband ons standpunt en trekken er de nodige besluiten uit.

In die specifieke wereld zijn er tal van definities en voor niet gespecialiseerde mensen is het soms moeilijk om er zijn weg te vinden. Dat geldt ook voor mij want ik ben ter zake geen specialist. We werken met beveiligingsteams en toch blijft het voor mij moeilijk om al die voortdurend veranderende definities uit elkaar te houden, die wereld evolueert immers zeer snel en er komt steeds nieuwe informatie op ons af.

In de eerste plaats dient de beveiliging van de informaticasystemen de discussiebasis te zijn. Wil een bedrijf of de Staat zich voorzien van de organisatorische, juridische en menselijke middelen die noodzakelijk zijn om die veiligheid te garanderen en de integriteit van het informaticasysteem veilig te stellen? Dat is de kern van de discussies.

De bedoeling is steeds de beschikbaarheid van de systemen in hun integraliteit en ook de confidentialiteit ervan te waarborgen. Bepaalde aanvallen kunnen die beschikbaarheid opheffen, andere aanvallen veranderen de data zonder dat de gebruikers er zich rekenschap van geven. De meeste aanvallen tasten de vertrouwelijkheid aan en verspreiden informatie.

Cybercrime betekent: het internet en de netwerken gebruiken om geld af te troggelen of misdaden te plegen. De misdaad wordt met andere woorden geëxtrapoleerd op het internet.

Cyberaanvallen zijn specifieke aanvallen met een specifiek doel. Cyberbeveiliging staat uiteindelijk voor alle informaticaprocédés die erop gericht zijn de gegevens die via internet circuleren te bescher-

sites interdits par la police. Pour pouvoir accéder à nouveau à votre ordinateur une somme de 100 euros vous était réclamée, payable par carte de crédit ou Paypal. Pour éviter si possible ce genre d'attaque, il faut s'organiser!

Nous aborderons ici trois définitions: la description des types de criminels actifs sur les réseaux, les menaces auxquelles nous risquons d'être confrontés et les mesures qui peuvent être mises en oeuvre par les États et les entreprises. Dans ce domaine, nous donnerons notre point de vue et en tirerons la conclusion.

Dans ce monde spécifique, il y a beaucoup de définitions et, pour les personnes non spécialisées, il est parfois difficile de s'y retrouver. Cela vaut également pour moi car je ne suis pas un expert dans cette matière. Même si des équipes de sécurité travaillent avec nous, j'ai de la peine à me retrouver dans des définitions qui changent constamment, puisque c'est un monde qui évolue très vite avec sans cesse de nouvelles informations.

En premier lieu, la sécurité des systèmes d'information doit former la base de la discussion. Veut-on se donner des moyens organisationnels, juridiques et humains dans une entreprise ou auprès de l'État pour garantir cette sécurité et conserver l'intégrité du système d'information? C'est autour de cela que gravitent les discussions.

L'objectif est toujours d'assurer la disponibilité de l'intégralité et de la confidentialité d'un système. Certaines attaques peuvent enlever cette disponibilité, d'autres sont capables de changer les données sans que les utilisateurs s'en rendent compte. Finalement, les attaques les plus courantes sont celles qui violent la confidentialité et divulguent les informations.

La cybercriminalité, c'est l'utilisation de l'internet et des réseaux pour détourner des sommes d'argent ou accomplir des crimes. En d'autres termes, il s'agit de l'extrapolation de la criminalité sur le réseau internet.

Les cyberattaques sont des attaques particulières visant une cible spécifique. Finalement, la cybersécurité regroupe l'ensemble des procédés informatiques visant à protéger les données tran-

men. Er zijn vele definities en de juiste betekenis ervan is niet altijd gekend.

Voor ons professionelen komt het erop aan eerst het type aanval precies te kwalificeren. En dat is niet altijd gemakkelijk: waarover spreekt men precies en wat zijn de bedoelingen van de aanvallers? We hebben trouwens voorbeelden gegeven van enkele specifieke dreigingen en het type misdadigers waarmee we kunnen worden geconfronteerd.

Zoals in de echte wereld beogen de misdadigers financieel gewin door fraude. Spionnen zoeken naar vertrouwelijke informatie in bedrijven of van de Staat om de concurrentie voor te zijn of zijn op zoek naar militaire informatie om strategische inlichtingen, bijvoorbeeld over een ander land, te bekomen.

Er is ook alles wat te maken heeft met hacking: destabilisatie, propaganda, ideologie en uiteindelijk acties van terroristen die uit wraakzucht installaties of informatie zonder meer saboteren of vernietigen.

Alle soorten virussen worden als wapen gebruikt: *malware*, paard van Troje, wormen, enz. De cybercriminelen maken gebruik van de zwakke plekken van onze systemen. Het is precies dat wat moet worden verholpen, al weten we dat er steeds misdadigers zullen zijn die ze zullen gebruiken. U mag ervan op aan: als er een zwakke plek is, dan zal iemand die plek vinden en er misbruik van maken.

Er worden beheerssystemen op afstand gebruikt om toegang te krijgen tot de systemen. Een klassieke aanval die al lang is gekend, bestaat in een denial of service waardoor de informatiesystemen worden geblokkeerd.

Met social engineering wordt naar inlichtingen over personen gezocht om met die informatie, bijvoorbeeld, een paswoord, enz. te bemachtigen. De aanvallen, die tien of vijftien jaar geleden marginaal waren en ook weinig aandacht kregen in de media, worden steeds ernstiger en nemen ook in aantal toe.

sitant par internet. Les définitions sont multiples et on n'en connaît pas toujours exactement leur signification.

Pour les professionnels que nous sommes, l'un des problèmes consiste à qualifier d'abord le type d'attaque, à déceler exactement de quoi on parle et quels sont les objectifs des attaquants. Nous en avons d'ailleurs illustré quelques menaces spécifiques et le genre de criminels que nous pouvons rencontrer.

Comme dans le monde réel, des criminels cherchent à obtenir un gain financier par de la fraude. Des espions veulent trouver des informations confidentielles au sein d'entreprises ou d'États, pour en tirer des avantages compétitifs ou, dans le domaine militaire, obtenir des informations stratégiques, par exemple sur un autre pays.

Nous y trouvons également tout ce qui est *hacking*, donc déstabilisation, propagande, idéologie et, finalement, les actions des terroristes qui essaient simplement de détruire par vengeance, sabotage ou destruction, des installations ou des informations.

Les armes sont constituées de tous les types de virus: *Malware*, "cheval de Troie", vers, *etc*. Les cybercriminels exploitent évidemment les failles de nos systèmes. C'est exactement à cela que nous devons remédier, tout en sachant qu'il existera toujours des criminels qui les utiliseront. Vous pouvez être sûrs que s'il y a une faille, quelqu'un la trouvera et l'exploitera.

Des outils d'administration à distance sont employés pour accéder à des systèmes. L'attaque classique, connue depuis bien longtemps, procède par déni de service (denial of service attack), qui bloque les systèmes d'information.

L'ingénierie sociale, elle, essaie d'obtenir des informations sur des personnes afin de les utiliser par exemple pour trouver leurs mots de passe, *etc.* Les attaques, de plus en plus graves deviennent aussi de plus en plus nombreuses, alors qu'il y a dix ou quinze ans elles représentaient des phénomènes marginaux et peu médiatisés.

We leven in een maatschappij waar informatica en telecommunicatie alomtegenwoordig zijn. Nagenoeg al onze economische activiteiten zijn op een of andere manier afhankelijk van de informatica, wat ons zeer kwetsbaar maakt. De gevolgen van de aanvallen zijn veel ernstiger en worden steeds professioneler.

We leven in een wereld van cybercrime en cyberwar waarvan de omvang totaal verschillend is. Maar de bedrijven en de overheidsinstellingen hebben die tendens nog niet echt begrepen. Men dient echter te beseffen dat het hier om een ernstig en belangrijk feit gaat, terwijl tal van bedrijven, en zelfs Staten, geen middelen nemen om zich te beschermen.

Het is in die geest van bewustmaking, denk ik, dat u dit seminar hebt willen organiseren en u hebt volkomen gelijk want, ik herhaal het, die tendens wordt door de maatschappij onvoldoende onderkend. Waarom? Gewoonweg omdat veiligheid geld kost en niet een rechtstreekse waarde heeft. Bescherming kan niet als een product verkocht worden en betekent geen echte rechtstreekse toegevoegde waarde voor de bedrijven.

De aanvallen zijn niet intenser in de zomer of in de winter. Neen, het hele jaar door worden aanvallen gepleegd en de soort varieert. In 2012 werden de meeste aanvallen veroorzaakt door cybercrime, met andere woorden criminele activiteiten om geld te winnen, vooral op een frauduleuze manier en door hacktivisme, met andere woorden alle activiteiten die de website in een slecht daglicht stellen of de reputatie schade berokkenen.

Twee belangrijke doelwitten: in de eerste plaats de financiële sector, wat geen verrassing is, en vervolgens de regering. Daar bevindt zich over het algemeen de meeste informatica en dat weerspiegelt in zekere zin het gewicht ervan in de onderscheiden instellingen. Een derde doelwit: de media en een vierde: de fabrieksnijverheid waar van een uitbarsting kan worden gewaagd. Olie en gas komen op de eerste plaats en, nog minder verrassend, op de tweede plaats, entertainment wat de industrie betreft.

Actuellement nous vivons dans une société où l'informatique et les télécoms sont omniprésents. Presque toutes nos activités économiques dépendent d'une manière ou d'une autre de l'informatique, ce qui nous rend très vulnérables. Les attaques ont un impact beaucoup plus important et deviennent de plus en plus professionnelles.

Nous nous trouvons aujourd'hui dans un monde de cybercrime, de cyberwar dont l'ampleur est tout à fait différente. Mais cette tendance n'est pas encore réellement comprise par les entreprises et les institutions publiques. Il faut pourtant se rendre compte que ce fait devient grave et important alors que beaucoup d'entreprises, et même d'États, ne prennent pas de mesures pour se protéger.

C'est dans cet esprit de sensibilisation, je pense, que vous avez voulu organiser ce séminaire et vous avez complètement raison car, je le répète, cette tendance est mal perçue au sein de la société. Pourquoi ? Simplement parce que la sécurité représente toujours un coût et n'a pas de valeur directe. La protection ne peut se vendre comme produit et ne constitue pas une réelle valeur ajoutée directe pour les entreprises.

Les attaques ne sont pas particulièrement denses en été ou en hiver. Non, on les constate durant toute l'année et leur type varie. En 2012, les attaques les plus importantes ont été causées par le cybercrime, c'est-à-dire les activités criminelles en vue de gagner de l'argent, surtout de manière frauduleuse, et le hacktivisme, c'est-à-dire toutes les activités de dénigration du site web ou qui touchent à la réputation.

Deux cibles principales : d'abord le secteur financier, ce qui ne constitue pas une surprise, ensuite le gouvernement. C'est là que l'on trouve en général le plus d'informatique et cela reflète d'une certaine façon son poids dans les différentes institutions. Nous y ajoutons la troisième cible : les médias et la quatrième: l'industrie manufacturière, dont nous remarquons un éclatement. Oil and Gas vient en première position et, moins étonnant encore, l'entertainement en deuxième lieu dans l'industrie.

Ook in de overheidsinstellingen, vijfde doelwit, kan van een uitbarsting worden gesproken: politieke partijen, niet-gouvernementele organisaties, enz. De doelwitten lopen zeer uiteen al worden vooral de financiële sector en de Staat getroffen.

Andere soorten dreigingen tonen aan dat er aanvallen zijn met een grote weerslag en veel innovatie en andere aanvallen met een kleine weerslag en een eenvoudige innovatie.

Ik geef u enkele voorbeelden. Zo was de aanval Stuxnet in grote mate innoverend en waren de gevolgen ook groot. Men kan ervan uitgaan dat het ging om een worm die de Verenigde Staten en Israël samen hebben ontwikkeld om de systemen van Iran aan te vallen. Het betrof dus een aanval van Staten tegen een andere Staat, die deel uitmaakte van de operatie "*Olympic games*" tegen Iran en die in juni 2010 werd ontdekt door een informaticamaatschappij in Wit-Rusland. De zeer gesofistikeerde worm of *malware* drong binnen in industriële systemen.

Met die worm die gericht is op standaardsystemen geproduceerd door Siemens, die in de industriële wereld bekend staat om zijn automaten, kan worden gespioneerd. De worm herprogrammeert automaten waardoor het mogelijk wordt waterkrachtcentrales, kerncentrales, oliepijpleidingen, enz. binnen te dringen. Met die worm werd heel wat informatie bemachtigd.

De *malware* heeft 45 000 informaticasystemen besmet, waarvan ongeveer 30 000 in Iran. Er was tevens collateral damage in de computers van de centrales in Duitsland, Frankrijk, India en Indonesië, kortom, overal waar de technologie van Siemens wordt gebruikt. Die zeer gesofistikeerde aanval die een grote weerslag had, is alom gekend en kreeg veel aandacht in de media.

De aanval van LulzSec van 2011, bestond uit een inbraak en een diefstal van gegevens op een netwerk beheerd door Sony. Dat virus heeft meer dan een miljoen accounts aangetast en Sony was verplicht die accounts te sluiten en de gebruikers

Enfin, pour les organisations publiques, qui constituent la cinquième cible, on constate à nouveau un éclatement: partis politiques, organisations non gouvernementales, *etc*. Les cibles sont tout à fait variées même si quelques accents sont mis sur les secteurs financiers et de l'État.

D'autres types de menace montrent que l'on peut trouver des attaques à impact élevé et grande innovation contre d'autres avec un impact faible, avec simple innovation.

Je vous donne ici quelques exemples. Ainsi, l'attaque Stuxnet, elle, a un degré élevé d'innovation avec un impact important. On peut supposer qu'il s'agissait d'un ver informatique développé conjointement par les États-Unis et Israël pour s'attaquer aux systèmes iraniens. C'est donc une attaque publique d'États vers un autre État. Il faisait partie de l'opération "*Olympic games*" sur l'Iran et a été découvert en juin 2010 par une société de sécurité informatique en Biélorussie. On parle ici d'un ver ou d'un *Malware* très sophistiqué qui s'introduit dans les systèmes industriels.

Ce ver permet de les espionner en ciblant des systèmes standards, produits par Siemens, très reconnu dans le monde industriel pour ses automates. Il reprogramme des automates de manière à pouvoir entrer dans des centrales hydroélectriques, dans des centrales nucléaires, dans des oléoducs, *etc*. Beaucoup d'informations sont sorties via ce ver.

Le *Malware*, lui, a infesté 45 000 systèmes informatiques, dont 30 000 rien qu'en Iran. On a déploré également du collegial damage dans des ordinateurs des centrales en Allemagne, en France, en Inde, en Indonésie, bref, partout où les technologies de Siemens sont utilisées. Cette attaque très sophistiquée, avec un impact élevé, est très connue et a été largement médiatisée.

L'attaque du LulzSec, qui date de 2011, consistait en une intrusion et un vol de données sur un réseau maintenu par Sony. Ce virus a compromis plus d'un million de comptes et Sony s'est vu dans l'obligation de les fermer et d'en informer les utilisateurs.

daarover in te lichten, De groep mensen rond die hackers is ook verantwoordelijk voor het blokkeren van de site van de CIA en daardoor berucht.

We weten ook dat politieke partijen in de Verenigde Staten werden aangevallen, iets wat veel aandacht heeft getrokken.

Een laatste eenvoudiger aanval met een veel kleinere weerslag waaraan de media veel aandacht besteedden, trof mevrouw Palin, die kandidaat was voor het Amerikaanse presidentschap in 2008. Haar e-mail account Yahoo werd gehackt via social engineering. Aan de hand van persoonlijke gegevens die op het internet stonden kon haar paswoord worden ontcijferd.

Kortom, we hebben te maken met gekende en minder gekende aanvallen. Maar hoe kunnen we aanvallen voorkomen? In de organisaties, de bedrijven en de instellingen moeten we ons organiseren rond beheerssystemen op het gebied van informatiebeveiliging. Hier raken we aan de kern van de zaak.

De bedrijven maken een risicoanalyse die het mogelijk maakt de aanvallen te identificeren, te analyseren, bij voorrang aan te pakken en de risico's te beheren. Dankzij die systematische aanpak waarbij in de bedrijven geregeld een inventaris wordt opgemaakt, worden de zwakke plekken in de organisatie opgespoord. De IT van een maatschappij of een instelling is uiteindelijk daarvan een weerspiegeling. Dat is de reden waarom men niet enkel het IT-systeem zelf, maar ook de hele organisatie van het bedrijf aanvalt. De norm ISO 27000 is een goede praktijk om dergelijke zaken te beheren.

In bepaalde landen, en meer bepaald in Luxemburg, is dat beleid, dat steunt op beheerssystemen op het gebied van informatiebeveiliging, zelfs opgenomen in de vereisten van de regulators. In het Groothertogdom zijn alle leden van de financiële sector, met inbegrip van de toeleveranciers van de banken en de hele gemeenschap rondom die sector, verplicht hun risico's te beheren aan de hand van een formele aanpak gebaseerd op de risicoanalyse die door de regulator wordt geauditeerd.

Le groupe de personnes gravitant autour de ces hackers est également responsable d'une indisponibilité du site web de la CIA et donc renommé à la suite de ce fait.

On sait aussi qu'il existe des attaques sur des partis politiques aux États-Unis, c'est d'ailleurs quelque chose qui a précédemment retenu beaucoup l'attention.

Une dernière attaque, elle aussi médiatisée, plus simple et avec un impact beaucoup plus limité, concernait Mme Palin, candidate dans la course finale lors des présidentielles américaines en 2008. Son compte e-mail Yahoo a été piraté au moyen d'un engineering social. On a pu déchiffrer son mot de passe grâce à des informations personnelles publiées sur internet.

Bref, nous avons affaire à des attaques connues et d'autres qui le sont moins. Mais comment nous prémunir ? Au sein des organisations, des entreprises et des institutions, nous devons nous organiser autour de systèmes de management de la sécurité de l'information. Nous nous trouvons là au coeur du débat.

Les entreprises se munissent d'une analyse de risques qui permet de les identifier, de les analyser, de les prioriser et d'en gérer les risques. Cette approche systématique, qui fait des inventaires à étapes régulières dans les entreprises, détecte ainsi les failles d'organisation. Finalement, l'IT d'une société ou d'une institution en est son reflet. C'est pour cela que l'on s'attaque, non seulement au système IT lui-même, mais également à l'organisation complète de l'entreprise. La norme ISO 27000, elle, constitue une bonne pratique pour gérer ce genre de chose.

Dans certains pays, et notamment au Luxembourg, cette gestion par des systèmes de management de la sécurité de l'information est même entrée dans les exigences des régulateurs. En effet, au Grand-Duché, il existe l'obligation pour tous les membres du secteur financier, y compris les sous-traitants des banques et toute la communauté qui gravite autour de lui, de gérer leurs risques avec une approche formelle basée sur l'analyse de risque auditée par le régulateur.

De middelen die het bedrijf voor zijn beveiligingsbeleid gebruikt, vormen daarbij de basis. Vervolgens wordt voor de risicoanalyses gebruik gemaakt van methodes zoals Ebios, Melisa, Mehari die wereldwijd de "*best practices*" zijn.

Operationele procedures en technische maatregelen, bewustmaking en proactiviteit moeten worden ontwikkeld en daar knelt het schoentje. De bedrijven en de instellingen geven zich daar onvoldoende rekenschap van en stellen de aanvallen pas vast wanneer ze hebben plaatsgehad.

Dat is een punt waarvoor ik uw aandacht vraag. De privésector en de openbare sector moeten samenwerken om een maximale bewustwording te bewerkstelligen. Daarvoor zijn natuurlijk deskundigen nodig. Luxemburg heeft enkele initiatieven genomen om de bewustwording rond cyberbeveiliging te verbeteren.

Zo was er de *"Journée professionnelle*" in 2008 over cybercrime en de Conferentie over cyberbeveiliging die verleden jaar werd georganiseerd door de business community van Luxemburg maar die, helaas, bij de bedrijven niet veel belangstelling heeft gewekt.

Om echt impact te hebben moet men veel dieper doordringen in de bedrijven zodat ze mensen met een goed niveau afvaardigen. Er werden nog andere conferenties georganiseerd, ik denk hier bijvoorbeeld aan de conferentie van de *American Chambre of commerce* wat de privé IT-organisaties betreft.

In 2011 heeft Luxemburg werk gemaakt van een omvattende strategie op het gebeid van cyberbeveiliging door de oprichting van een Cyber Security Board die de voorbije jaren al verscheidene keren is bijeengekomen. Op de vergadering van november 2012 werd de strategie nader uitgewerkt aan de hand van vijf krachtlijnen.

In januari van dit jaar heeft de Board zijn eerste aanbevelingen geformuleerd, onder meer met betrekking tot de kritieke infrastructuur. Op de vergaderingen van juni 2012 en januari 2013 werden acties uitgewerkt, met betrekking tot, bijvoorbeeld, de e-Telco regulator. Die maatregel waardoor het

Les outils de la politique de l'entreprise sur la sécurité en constituent la base. Ensuite, on utilise des méthodes d'analyse de risque comme Ebios, Melisa, Mehari qui sont des "*best practice*" dans ce monde.

Des procédures opérationnelles et des mesures techniques, comme la sensibilisation et la proactivité, doivent se développer et c'est là où le bât blesse. Les entreprises et les institutions n'y sont pas encore sensibilisées et ne découvrent les attaques qu'une fois le fait accompli.

C'est un point sur lequel je souhaite attirer votre attention. Secteur privé et secteur public doivent travailler ensemble pour une sensibilisation maximale, mais il faut évidemment des spécialistes pour cela. Le Luxembourg a, pour sa part, pris quelques initiatives de sensibilisation autour de la cybersécurité.

Ainsi, on peut citer la Journée professionnelle en juin 2008 sur le thème de la cybercriminalité et la Conférence sur la cybersécurité, organisée l'année dernière par la Fédération des industriels ou business community Luxembourg mais qui, malheureusement, n'a pas suscité énormément d'intérêt des entreprises.

Pour avoir un impact réel, il faudra s'introduire beaucoup plus au sein des entreprises afin qu'elles envoient des personnes de bon niveau. D'autres conférences encore ont été organisées comme, par exemple, celle de l'*American Chambre of commerce* des organisations privées en IT.

En 2011, le Luxembourg a mis en place une stratégie globale en matière de cybersécurité par la création d'un Cyber Security Board qui a déjà tenu plusieurs réunions au fil des années. Au cours de celle de novembre 2012, la stratégie a été définie sur cinq axes.

En janvier de l'année dernière, ce Board a sorti ses premières recommandations, y compris celle sur les infrastructures critiques. En juin 2012 et janvier 2013, des réunions ont défini des actions concernant, par exemple, le régulateur d'e-Telco. Cette mesure, par laquelle l'Institut luxembourgeois

Luxemburgs Reguleringsinstituut van e-Telco een beveiligingsinvestering eist, wordt tamelijk goed toegepast.

Luxemburg keurt bovendien de overeenkomst over cybercrime goed.

Tot besluit zou ik willen zeggen dat de uitdagingen waarvoor de bedrijven staan zeer moeilijk te definiëren zijn aangezien het hier om een wereld gaat die voortdurend evolueert en het probleem helaas wordt onderschat. Ten slotte rekenen de bedrijven op een begeleiding van de openbare sector wat de cyberbeveiliging betreft. Si vis pacem para bellum.

Ik dank u voor uw aandacht.

**Paneldebat**

*Mevrouw de Caluwé (NL) N.-* Dank u wel, mijnheer Hoffmann. Ik stel voor dat we beginnen met het panel en het gesprek aangaan met elkaar en met de zaal. Er kunnen ook nog vragen worden gesteld.

We hebben vandaag heel veel gehoord. Er is de verwevenheid van de systemen. De kansen die het internet biedt maar ook de gevaren en de risiso's van het internet.

De heer Beirens gaf reeds aan dat er niet voldoende politie is om achter al die cybercriminelen aan te gaan en dat we dus maar beter op voorhand kunnen zorgen dat onze bescherming in orde is.

We hebben ook vernomen dat kleine bedrijven en particulieren een hele makkelijke prooi zijn voor hackers en andere cybercriminelen, dat de bewustwording omhoog moet. Niet alleen de bewustwording over de gevaren moet omhoog, maar ook de informatie over de oplossingen.

Tijdens de lucnch hebben we gepraat over onze eigen computerproblemen. We weten soms wel waar het probleem ligt, of soms weten we het ook niet. We weten niet waar we mogen op klikken of wie we moeten bellen of mailen voor een oplossing voor het probleem.

de régulation exige d'e-Telco un investissement pour la sécurité, est relativement bien appliquée.

Le Luxembourg approuve en outre la convention sur la cybercriminalité.

Pour conclure, je dirai que les enjeux pour les entreprises sont très difficiles à déterminer car il s'agit d'un monde en constante évolution et ce problème est malheureusement sous-estimé. Enfin, les entreprises attendent un accompagnement du secteur public dans cette sensibilisation. Si vis pacem para bellum.

Je vous remercie pour votre attention.

**Table ronde**

*Mme de Caluwé (NL) N.-* Merci, M. Hoffmann. Je propose de passer au panel et d'ouvrir le débat entre nous et avec la salle. Des questions peuvent également être posées.

Nous avons reçu aujourd'hui quantité d'informations. On observe une imbrication des systèmes. Si l'internet offre de nombreuses possibilités, il y a aussi les dangers et les risques qui lui sont inhérents.

M. Beirens a déjà indiqué que la police manque d'effectifs pour pister tous ces cybercriminels et qu'il vaut donc mieux veiller à être paré en ce qui concerne notre protection.

Nous avons appris aussi que les petites entreprises et les particuliers constituent des proies très faciles pour les hackers et autres cybercriminels et qu'il faut renforcer la sensibilisation à la question. La sensibilisation aux dangers mais aussi l'information relative aux solutions.

Pendant le déjeuner, nous avons discuté de nos propres problèmes d'ordinateurs. Nous savons parfois où se situe le problème mais pas toujours. Nous ne savons pas sur quoi nous pouvons cliquer, à qui nous devons téléphoner ou envoyer un courriel pour trouver la solution.

Er is een *EU Strategy* voorgesteld op hoofdlijnen waarin wordt aangeraden om met een eigen policy te komen en de bewustwording te verhogen (de bewustwording is inderdaad een hele bladzijde). De heer Streefland suggereerde ook om daarvoor een verantwoordelijke aan te wijzen. We zijn het erover eens dat er helemaal niets gebeurt, zolang er geen verantwoordelijke is aangewezen.

Dat is precies wat we hier in het Beneluxparlement wilden doen. Daarom hebben we hier vandaag deze conferentie over bewustwording en willen we wellicht in november nog een conferentie organiseren om te bekijken welke acties we gezamenlijk kunnen ondernemen. Dat is dan meer een actie voor het voorkomen en het tegengaan van aanvallen.

Waar we het vandaag dus vooral over hebben, is de bewustwording en de oplossing ervan. Hoe kunnen we mensen, kleine bedrijven en organisaties en soms ook hele grote bedrijven ervan bewustmaken wat de gevaren zijn en hoe kunnen we met oplossingen komen?

De heer Beirens heeft bij voorbeeld al gesuggereerd om iets te verwerken in een soapserie, of een twitterende politieagent aan te stellen. Hoe kunnen we ervoor zorgen dat er informatie komt? Ik heb daarnet gekeken of ik het Nederlands Cyber Security Centre kon vinden op twitter. Ik heb het niet direct gevonden, maar zoiets zou ook al een idee zijn.

Ik zou nu heel graag met de sprekers van vandaag en met de zaal discussiëren over hoe en wat voor advies wij binnen de Benelux kunnen geven aan onze ministers, aan onze kabinetten, zodat wij gezamenlijk die bewustwording omhoog kunnen krijgen en oplossingen kunnen aanbieden voor die bedreigingen. Welke acties kunnen wij van hieruit ondernemen? Wie vraagt het woord voor een suggestie, of voor nog een vraag of voor een aanvulling? Het woord is aan de heer Oberweis.

*De heer Oberweis (L) F.-* Dank u, mevrouw de Caluwé.

Mijnheer Hoffmann, ik stel mij een vraag bij het niveau van innovatie en van bescherming. Bedrij-

Il est proposé une *EU Strategy* reposant sur de grands principes, où il est recommandé de définir sa propre politique et d'accroître la sensibilisation (une pleine page est consacrée à la question). M. Streefland a également suggéré de désigner pour cela un responsable. Nous nous accordons pour dire que rien ne se fera tant qu'on n'aura pas désigné un responsable.

C'est précisément ce que nous voulons faire ici, au Parlement Benelux. C'est pourquoi nous avons organisé la conférence d'aujourd'hui sur la sensibilisation, laquelle sera sans doute suivie d'une autre en novembre et qui traitera des actions que nous pouvons mener en commun. Il s'agira plus exactement d'actions destinées à prévenir et à contrer des attaques.

Nous voulons donc traiter principalement aujourd'hui de la sensibilisation et des solutions aux problèmes. Comment pouvons-nous faire prendre conscience des dangers aux individus, aux petites entreprises et aux organisations, voire même à des très grandes entreprises, et quelles solutions peuvent leur être apportées ?

M. Beirens a par exemple déjà suggéré de travailler sur la base d'un soap ou de désigner un fonctionnaire de police qui recourrait aux tweets. Comment susciter l'information ? J'ai regardé il y a un instant si je pouvais trouver le Cyber Security Centre nerlandais sur twitter. Je n'ai pas trouvé tout de suite mais ce pourrait être une idee.

Je voudrais à présent ouvrir la discussion avec les orateurs et avec la salle à propos des avis que nous pourrions adresser à nos ministres, à nos cabinets afin d'accroître ensemble la sensibilisation et proposer des solutions aux menaces. Quelles actions pourrions-nous entreprendre? Qui demande la parole pour une suggestion, une question ou un complément d'information? La parole est à M. Oberweis.

*M. Oberweis (L) F.-* Merci, madame la présidente de me donner la parole.

Monsieur Hoffmann, je me pose une question sur le degré d'innovation et le niveau de protection. Des

ven kunnen zich beschermen door in gesofistikeerde middelen te investeren, maar andere bedrijven kunnen dat niet omdat die middelen te duur zijn.

Er werd hier gesproken over cybercrime, cyberbeveiliging en cybertechnologie. Maar hoe kunnen die structuren ter beschikking gesteld worden van de andere ondernemingen, de kmo's, de ngo's en de regeringen zodat ze de problemen onderkennen en zich bijgevolg verdedigen? Ik heb daarover trouwens gesproken met een collega uit de Baltische landen.

Ik meen gelezen te hebben dat China ingenieurs en gespecialiseerde wetenschapsmensen opleidt in cybercrime. Hoe kunnen we daarop reageren? Worden er cursussen gegeven aan de universiteiten of in gespecialiseerde scholen? Hoe kunnen we de jongeren opvoeden om die aanvallen af te slaan?

*De heer Hoffmann (L) F.-* Ik denk dat op verschillende niveaus iets moet worden gedaan. De opvoeding is natuurlijk een basis om de mensen in de scholen en aan de universiteiten bewust te maken.

Er is vervolgens de productie. Wanneer u het hebt over de kleine ondernemingen, is het zo dat vandaag de IT-infrastructuur opnieuw in de datacentra wordt geconcentreerd.

De bedrijven besteden hun activiteiten meer en meer uit aan dienstverleners, zoals onze maatschappij, die over de vereiste schaalgrootte beschikt om beschermingsmechanismen, standaardisatie en een kostenbesparing mogelijk te maken. Dat is het commercieel antwoord dat we de bedrijven geven. We zeggen hun: geef ons uw IT en wij zorgen voor alles.

Een derde krachtlijn heeft betrekking op de regulering en de wetgeving. Op dat gebied blijft er natuurlijk enorm veel te doen. Luxemburg kan in dat verband beschouwd worden als een voorloper wat de financiële sector betreft.

We beschikken immers over een zeer goede wetgeving met betrekking tot de professionele

entreprises peuvent se protéger en investissant dans des moyens sophistiqués, mais d'autres ne le peuvent pas car ils représentent pour elles un coût important.

On a discuté de la cybercriminalité, de la cybersécurité, la cybertechnologie. Mais comment peut-on mettre ces différentes structures à disposition des autres entreprises, des PME, des ONG et des gouvernements afin qu'ils perçoivent ce problème et se protègent en conséquence ? J'en ai d'ailleurs parlé avec un collègue des pays baltes.

Je me rappelle avoir lu que la Chine forme des ingénieurs et des scientifiques spécialisés en cybercriminalité. Ils sont instruits à cette fin et ils nous tracassent. Comment peut-on réagir ? Donne-t-on des cours dans des universités ou des écoles spécialisées ? Comment peut-on éduquer les jeunes afin de parer à ces attaques ?

*M. Hoffmann (L) F.-* Je pense qu'il faut agir sur plusieurs fronts. L'éducation est évidemment un axe de base pour sensibiliser les gens dans les universités et les écoles.

Il faut agir ensuite au niveau de la production. Quand vous parlez de petites entreprises, nous constatons aujourd'hui une tendance à une concentration nouvelle des infrastructures IT dans les centres de données.

Les entreprises sous-traitent de plus en plus leurs activités à des prestataires, comme notre société, qui dispose d'une économie d'échelle à disposition permettant la création de mécanismes de protection, de réduction des coûts et de standardisation. C'est la réponse commerciale que nous offrons aux entreprises en leur disant : donnez-nous votre IT et nous nous occuperons de tout.

Un troisième axe, important, concerne la régulation et la législation. Dans ce domaine, il reste énormément à faire. C'est là que le Luxembourg peut-être un peu considéré comme le précurseur dans le secteur financier.

En effet, nous avons mis en place une très bonne législation autour des shortcodes professionnels de

shortcodes van die sector die, gewoonweg krachtens een openbare interventie, de toepassing van een aantal mechanismen in de bedrijven oplegt.

Ik denk dat de drie krachtlijnen, regulering, infrastructuur en competentie steeds de sleutelelementen van zo'n bespreking zijn.

*Mevrouw de Caluwé (NL) N.-* Dank u wel. Het woord is aan mevrouw Vermeulen.

*Mevrouw Vermeulen (B) N.-* Ik blijf nog een beetje op mijn honger zitten wat de particulieren betreft. Particulieren kennen die "beestjes" allemaal niet – ik spreek dan over "wormen" en "virussen" en "Trojaanse paarden" – en zien dat waarschijnlijk ook niet passeren op hun computer.

Maar, als je een computer koopt en je moet die installeren, dan moet je op een bepaald moment ergens klikken op "ik ga akkoord met de gebruiksovereenkomst". Iedereen klikt dat aan, want anders kan je niet verder, maar niemand leest dat.

Ik heb dat zelf ook nooit gelezen, maar ik veronderstel dat de experten dat wel al eens gedaan hebben. Ik stel mij dan de vraag: staat daar ergens een soort van clausule in waarbij de aanbieder garandeert dat het veilig is?

Volgens mij gaat een koper er wel van uit dat het product dat hij koopt, veilig is. Als dat niet zo is, kan dan niet op één of andere manier verwacht worden dat die providers gratis freeware aanbieden als encryption tools, zodat die bepaalde "beestjes" toch ergens gedetecteerd worden zonder dat mensen echt antivirussoftware moeten aankopen? Want private gebruikers kunnen die antivirussoftware toch niet installeren. Ik spreek dan niet over bedrijven maar over privépersonen.

Wij kunnen het niet verplichten aan de aanbieders, maar is het dan ook niet de taak van het beleid om dat aan te moedigen, om dat te voorzien en om vooral de samenwerking met de private sector daarin te versterken?

*Mevrouw de Caluwé (NL) N.-* Dat is een heel interessante vraag. Inderdaad, op welk niveau ga je dat neerleggen? De heer Streefland wil daarop antwoorden.

ce secteur qui oblige, simplement par intervention publique, l'application d'un certain nombre de méthodes des mécanismes au sein des entreprises.

En fait, je pense que ces trois actes : régulation, infrastructure et compétence représentent toujours les points clés d'une telle discussion.

*Mme de Caluwé (NL) N.-* Je vous remercie. La parole est à Mme Vermeulen.

*Mevrouw Vermeulen (B) N.-* Je reste un peu sur ma faim en ce qui concerne les particuliers qui ne connaissent pas ces petites "bêtes " – je veux parler des "vers", des "virus" et des "chevaux de Troie" – et ne les voient sans doute pas passer non plus sur leur ordinateur.

Mais lorsque vous achetez un ordinateur et que vous devez l'installer, il faut à un moment donné cliquer pour marquer son accord sur la convention d'utilisation. Tout le monde le fait parce qu'il faut bien mais personne ne lit le texte.

Je ne l'ai jamais lu non plus mais j'imagine que les experts l'on fait. Et je me demande si la convention comporte une clause grantissant que l'ordinateur est sûr.

Je pense que l'acheteur part du principe que le produit dont il fait l'acquisition est sûr. Si tel n'est pas le cas, on peut d'une manière ou d'une autre attendre des fournisseurs offrent des logiciels gratuits, des outils de cryptage permettant de détecter ces petites "bêtes" sans qu'il faille acheter des véritables logiciels antivirus que les utilisateurs privés ne savent de toute façon pas installer. Et je ne parle pas ici d'entreprises mais de personnes privées.

Nous ne pouvons pas imposer une telle obligation mais n'appartient-ils pas aux autorités d'encourager un comportement en ce sens, de le prévoir et, surtout, d'accentuer en cette matière la coopération avec le secteur privé?

*Mme de Caluwé (NL) N.-* La question est très intéressante. À quel niveau va-t-on agir, effet? M. Streefland souhaite répondre.

*De heer Streefland (NL) N.-* Dat is inderdaad een hele goede en terechte vraag. Er worden wel antivirus, firewalls en andere zaken aangeboden via software pakketten. Als je dat tegelijk met de aanschaf van de computer doet, dan is dat prima, maar reeds na een maand is het outdated. Dat is het probleem.

De ontwikkeling van malware, van virussen en wormen is zo ontzettend snel dat het gewoon niet bij te houden is. Dat is één van de redenen waarom altijd tegen eenieder wordt gezegd dat de virusscanner up to date moet zijn. Dat betekent toch een eigen verantwoordelijkheid, enerzijds.

Ik ben het wel met u eens dat we er wat meer druk zouden moeten op leggen, want op dit ogenblik kun je nog steeds een computer kopen zonder dat er uberhaubt enige antivirus in zit. Er is dus gedeeltelijk wel een mogelijkheid om daarop wat meer nadruk te leggen en dus de verplichting bij de fabrikant leggen om hieraan wat te doen.

Aan de andere kant, moeten de mensen, ongeacht hoe expert ze zijn wel, het zelf verder blijven updaten, want de ontwikkelingen gaan razendsnel. Dat is hoe ikzelf het zie. Beide verhalen zijn waar, maar ik denk dat de heer Beirens daarop nog wat kan aanvullen.

*Mevrouw de Caluwé (NL) N.-* Ik wil nog even iets zeggen vooraleer de heer Beirens kan aanvullen.

Ik heb zelf een *online* virusscanner van KPN genomen. Ik dacht dat als ik adobe zou kopen er ik niet veel aan zou hebben. Dat zou dan maar voor een jaar geldig zijn wat kan er in dat jaar allemaal niet gebeuren.

Soms kun je wel *online updates* krijgen, maar als je een online scanner hebt, dan heb je gewoon een abonnement voor een heel jaar. Moet je aanbieders niet gaan verplichten om ook die updates aan te bieden? Misschien kan de heer Beirens hier ook op ingaan.

*De heer Beirens (B) N.-* Antivirusproducten zijn per definitie maar goed voor de virussen die tot gisteren gekend zijn. Vandaag komen er tienduizend nieuwe virussen uit.

*M. Streefland (NL) N.-* C'est en effet une très bonne question qui, en même temps, est très pertinente. Des antivirus, des pare-feu et d'autres outils sont proposés sous la forme d'ensembles de logiciels. Si on les acquiert en même temps que l'ordinateur, c'est très bien mais il faut savoir qu'ils sont déjà obsolètes après un mois. Voilà le problème.

Le développement de malware, virus et vers est tellement rapide qu'il n'est pas possible de suivre. C'est une des raisons pour lesquelles ont dit à chacun que l'antivirus doit toujours être à jour. Cela suppose tout de même une responsabilité propre. C'est une chose.

Je suis d'accord avec vous pour considérer qu'il faudrait mettre davantage l'accent sur cette question car l'on peut toujours acheter aujourd'hui un ordinateur dépourvu du moindre antivirus. Il est donc possible d'insister davantage et d'imposer au fabricant de prendre des mesures pour y remédier.

D'autre part, l'utilisateur, quel que soit son degré d'expertise, doit continuer à mettre son antivirus à jour car les développements sont extrêmement rapides. C'est mon point de vue. Les deux aspects sont confirmés mais je crois que M. Beirens voudrait ajouter quelque chose.

*Mme de Caluwé (NL) N.-* Je voudrais dire un mot avant de céder la parole à M. Beirens.

J'ai moi-même opté pour un antivirus de KPN. Je pensais que si j'achetais adobe, il ne me serait pas très utile Il n'aurait été valable qu'un an et il peut s'en passer des choses dans cet intervalle.

On peut trouver des mises à jour en ligne mais l'abonnement ne court alors qu'un an. Ne faudrait-il pas obliger les fournisseurs de logiciels à offrir ces mises à jour ? M. Beirens peut-il répondre ?

*M. Beirens (B) N.-* Par définition, les antivirus ne sont valables que pour les virus connus jusqu'à hier. Aujourd'hui, il y en a déjà dix mille nouveaux.

Wij zien dat in de malware industrie, de mensen die kwaadaardige software schrijven ervoor zorgen dat als die virussen zich een paar keer verspreid hebben, ze automatisch een andere vorm aannemen waardoor ze opnieuw niet meer herkend worden door die antivirusproducten.

Dus, zelfs als je een antivirusproduct op je personal computer geïnstalleerd hebt, ben je niet zeker dat je niet geïnfecteerd wordt. We zien de dag van vandaag dat men heel precies, als men een bedrijf wil binnendringen, een aantal sleutelfiguren uitkiest, daar heel specifiek kwaadaardige software voor laat schrijven en dat maar op drie, vier exemplaren laat verspreiden naar die sleutelfiguren.

Die virussen worden niet gedetecteerd door het antivirusprogramma en die gaan ook nooit in een antivirusprogramma terechtkomen omdat niemand gaat zeggen: er is hier iets vreemd, ik ga hier een staal van overmaken aan die antivirusproducenten. Nochtans komen zij zo bepaalde zaken op het spoor.

Je zal dus nooit 100 procent zekerheid hebben en we moeten er meer en meer rekening mee houden dat die producten eigenlijk voor een stuk voorbijgestreefd zijn. Bijkomend zien we dat er voortdurend nieuwe systemen ontstaan om mensen te gaan infecteren. Deze morgen vertelde ik over de *Drive-By*, het gewoon bezoeken van een website is soms al voldoende om geïnfecteerd te worden.

Het wordt dus heel moeilijk en het is voor iedereen een strijd om zijn product up-to-date te houden. De meeste antivirusproducten checken alle dagen of er geen nieuwe versie is van een databank waardoor ze de signaturen gaan herkennen. Op bedrijfsservers gaat de databank gepusht worden naar de server: dat wil zeggen dat de producent, als hij een nieuwe databank heeft, het zendt naar alle servers die die virusscanning doen.

Dat is beter, tijdiger en dan ga je ook de nieuwste virussen detecteren, maar er blijft altijd nog een opening.

Nous voyons que, dans l'industrie des logiciels malveillants, les gens qui écrivent ces logiciels font en sorte que lorsqu'ils se sont diffusés un certain nombre de fois, les virus adoptent automatiquement une autre forme qui les rendent méconnaissables pour les nouveaux produits antivirus.

Par conséquent, même si vous avez installé un antivirus sur votre ordinateur, vous n'êtes pas certain de ne pas être infecté. Nous constatons aujourd'hui que celui qui veut pénétrer dans une entreprises choisit méticuleusement un certain nombre de figures clés pour lesquelles il fait écrire un logiciel malveillant spécifique et ne le diffuse qu'à trois ou quatre exemplaires à destination de ces figures clés.

Ces virus ne sont pas détectés par le programme antivirus et ne se retrouveront d'ailleurs jamais dans un tel programme parce que personne ne dira jamais: voilà qui me paraît bizarre, je vais informer les producteurs d'antivirus. C'est pourtant une manière de détecter certains problèmes.

Vous ne serez donc jamais certain à 100 % et nous devons de plus en plus tenir compte de ce que ces produits sont en réalité en partie déjà obsolètes. Accessoirement, on constate l'apparition de nouveaux systèmes de plus en plus nombreux pour infecter les gens. Je vous ai parlé ce matin du *Drive-By* et du risque d'être contaminé uniquement pour avoir visité un site internet.

La situation devient donc très délicate et c'est pour chacun de nous une lutte à mener pour maintenir son produit à jour. La plupart des antivirus vérifient quotidiennement l'existence d'une nouvelle version d'une banque de données leur permettant de reconnaître les signatures. Sur les serveurs des entreprises, les banques de données vont être envoyées vers le serveur: cela veut dire que le producteur, s'il possède une nouvelle banque de données, l'envoie à tous les serveurs qui assurent le scannage de virus.

C'est mieux, c'est plus prompt et cela permet de détecter les virus les plus récents mais il reste toujours une ouverture.

Bijkomend, het zijn niet alleen de virussen, het zijn ook de producten. Microsoft is al x aantal keren veroordeeld omdat ze te veel producten integreren in het besturingssysteem, zodat ze dan de markt geen opening laten om alternatieve producten aan te bieden.

Microsoft biedt dus wel producten aan. Die zijn heel simpel van functionaliteit, maar die bieden wel garantie. Toch zijn er mensen die dat niet activeren.

Dus, daar zit je dan met de verantwoordelijkheid van de eindgebruiker. Dat kon ik een stuk volgen in de regulering die men voorstelt: men moet inderdaad een aantal basisproducten voorzien en die ook standaard activeren, zodat de eindgebruiker niet meer verantwoordelijk is.

*Mevrouw de Caluwé (NL) N.-* Dat klinkt wel vrij hopeloos. Niet de oplossing die u aandraagt, maar wel wanneer u zegt dat de bescherming slechts gaat tot virussen die gisteren werden ontdekt en dat men nu heel specifieke virussen ontwikkelt, die nooit worden gedetecteerd, dan ziet het er slecht uit voor de vitale infrastructuur.

Er wordt hier wel al een suggestie gedaan. Men moet zorgen voor basisproducten die aangeboden moeten worden en die in ieder geval geleverd moeten worden samen met de computer zelf.

Mevrouw Quik vraagt het woord.

*Mevrouw Quik-Schuijt (NL) N.-* Ik dacht ook al: laat het ons dan allemaal maar opgeven.

Maar daarbij aansluitend, wie moet daar dan voor zorgen? Is het de wetgever of moeten we inderdaad iemand aanwijzen die dan verantwoordelijk gaat zijn om zowel de awareness te verhogen als voor het aandragen van wetgeving. Dat zal immers nodig zijn voor het invoeren van de verplichting om er al die producten op te zetten.

Iemand moet dat aangeven. Iemand moet permanent gefocust blijven op wat er op dat gebied moet gebeuren, zowel in verband met wetgeving als op het vlak van wat er in de praktijk moet worden opgezet. Wie moet dat dan worden?

Accessoirement, il n'y a pas que les virus, il y a aussi les produits. Microsoft a déjà été condamné plusieurs fois pour avoir intégré trop de produits dans le système de gestion de sorte qu'il ne laisse pas d'ouverture permettant d'offrir des produits alternatifs.

Microsoft propose donc bien des produits. Ils sont fonctionnellement très simples mais offrent une garantie. Il y a pourtant des gens qui ne les activent pas.

Ici se pose donc la question de la responsabilité de l'utilisateur final. J'ai suivi cela pas à pas dans la régulation qui est proposée: il faut en effet prévoir un certain nombre de produits de base et les activer de manière standard afin que l'ulisateur final n'en porte plus la responsabilité.

*Mme de Caluwé (NL) N.-* Tout cela semble bien désepérant. Je ne parle pas de la solution que vous suggérez mais de vos propos lorsque vous dites que la protection ne concerne que les virus découverts hier et que l'on développe aujourd'hui des virus très spécifiques qui ne sont jamais détectés. Dans ces conditions, l'avenir s'annonce sombre pour l'infrastructure vitale.

Mais une suggestion a déjà été formulée ici. Il faut offrir des produits de base qui, en tout cas, doivent être livrés avec l'ordinateur.

Mme Quick demande la parole.

*Mme Quik-Schuijt (NL) N.-* Je me disais déjà: il n'y a plus qu'à se résigner.

Mais pour faire suite à ce qui vient d'être dit, qui doit s'oocuper cela? Est-ce le législateur ou faut-il désigner quelqu'un qui assumera la responsabilité d'accroître la sensibilisation et de proposer des législations? Car cela sera nécessaire pour instaurer l'obligation d'intégrer tous ces produits.

Quelqu'un doit s'en charger. Quelqu'un doit être attentif en permanence à ce qu'il y a lieu de faire en cette matière, en ce qui concerne tant la législation que ce qu'il faut mettre en place dans la pratique. De qui s'agira-t-il?

*De heer Streefland (NL) N.-* Ik heb daarover wel een idee. Ik kom terug op wat ik reeds tevoren zei. Ik denk dat er vanuit de regeringen een centraal punt moet zijn dat het boegbeeld is en zich ook hiermee bezig houdt en richting kan aangeven. Of er dan vervolgens wetgeving uit voortvloeit, dat is een zaak voor de politiek.

In principe denk ik wel dat het een hoge ambtenaar moet zijn die verantwoordelijk is voor cyber security. Die is er trouwens al in Nederland. Die persoon zou zich daar mee bezig moeten houden. Dat is mijn mening daarover. Ik denk dat het ook de snelste en meest efficiënte manier is.

*Mevrouw Quik-Schuijt (NL) N.-* Ik wist zelfs niet dat iemand daarvoor verantwoordelijk is. Dat moet dan toch anders. Daar moeten we dan nationaal aan werken.

*Mevrouw de Caluwé (NL) N.-* Ik spreek dan voor Nederland. Wij zouden ook vanuit de Tweede Kamer in eerste instantie aan de minister van Veiligheid en Justitie kunnen aangeven dat hierop aansturing moet komen, dat we verwachten dat er iets wordt gedaan vóór de zomer, begin van de herfst, dat er een plan komt om met een bepaald systeem te komen waardoor bij voorbeeld aan de consument meer bescherming kan worden geboden.

De heer Engelis vraagt het woord.

*M. Streefland (NL) N.-* J'ai bien une idee. Je reviens sur ce que j'ai dit précédemment. Je crois qu'il faut créer au niveau des gouvernements un point central qui soit la figure clé, qui s'occupe de la question et qui puisse donner une orientation. Quant à savoir si cela débouchera ensuite sur des législations, c'est l'affaire du politique.

En principe, je dirais qu'il doit s'agir d'un haut fonctionnaire responsable de la cybersecurité. Ce fonctionnaire existe d'ailleurs déjà aux Pays-Bas. Cette personne devrait s'occuper de ces questions. Voilà ce que j'en pense. Je crois aussi que c'est la formule la plus rapide et la plus efficace.

*Mme Quik-Schuijt (NL) N.-* Je ne savais même pas que quelqu'un assume cette responsabilité. Dans ce cas, il faut travailler autrement, au plan national.

*Mme de Caluwé (NL) N.-* Je vais m'exprimer à propos des Pays-Bas. La Deuxième Chambre pourrait faire savoir au ministre de la Sécurité et de la Justice qu'il faut définir une orientation en la matière, que nous attendons que quelque chose soit fait avant l'été ou au début de l'automne, qu'il faut arrêter un plan prévoyant un système donné permettant par exemple d'offrir davantage de sécurité au consommateur

M. Engelis demande la parole.

*Mr Engelis (BA) E.-* We used to have a separate ministry that was tasked to deal with the wide range of policies concerning information technology. This ministry was one of the first institutions that was terminated when the first budget cuts had to be made after the crisis set in.

This decision taken in 2008 was quite shortsighted and today these responsibilities are divided between some internal affairs institutions, regional development institutions and the ministry for transport and communication. So it is very fragmented. I agree that we will have to meet the necessity that it all will have to be concentrated in some point which assumes ownership.

I would also like to relate to something the president said when he opened the discussion about cyber thugs in China. One initiative that is being implemented in Latvia is related to a voluntary counter cyber attack team. It is a part of the so called land guards. Land guards are a kind of paramilitary defence organization, which is organized by the ministry of Defence. But the land guards are also voluntary; they

are not full time; they are trained but they do it outside their every day job. They are also getting paid for their services.

The cyber division of these land guards would also meet the same principles. It would be voluntary. They would need high specialization in information technology, they would have to be patriots of Latvia to find the wish in themselves to enter this division. They would also need access to state secrets, so they will have to be screened.

The plan was to set it up by the autumn of this year, but I cannot say yet that it will be a success story. We will see and follow up this initiative. Thank you.

*Mevrouw de Caluwé (NL) N.-* Dank u wel. Het woord is aan mevrouw Wouters.

*Mevrouw Wouters (B) N.-* Dank u wel, mevrouw de voorzitter.

Een punt wat ik hier een beetje gemist heb en wat we ook in de vorige vergaderingen aangehaald hebben, is het gevaar dat je nu hebt met je mobiele telefoon, met je iPad, dat je dat eigenlijk gebruikt op hotspots die compleet niet beschermd zijn, waardoor je heel snel, zonder dat je het weet, informatie aan het delen bent met anderen.

Ik heb vaak de indruk dat mensen niet beseffen waarmee ze bezig zijn. Dan heb ik het ook over sociale media: Facebook, LinkedIn, … ,al die media waar men zoveel informatie opzet. Veel mensen gebruiken geboortedata en dergelijke nog altijd als paswoord. Hoe meer informatie je deelt, hoe gevoeliger je bent om het slachtoffer van hackers te worden.

Ik heb zelf les gegeven aan informaticastudenten en ik zie daar zelfs dat dat bij jongeren nog niet leeft, dat die ook niet beseffen wat ze doen.

Zeker naar ouders toe denk ik ook dat je moet mobiliseren, want tegenwoordig zitten de kinderen allemaal op de i-pad. Ze downloaden spelletjes. Hoe veilig is dat allemaal?

Hetzelfde met de banksector. Nu kan je je bankverrichtingen ook via de telefoon doen, maar mijn vraag is: hoe veilig is dat? Volgens mij is het niet

*Mme de Caluwé (NL) N.-* Je vous remercie. La parole est à Mme Wouters.

*Mme Wouters (B) N.-* Merci, Mme la présidente..

Il y a un aspect que j'aurais voulu voir développer et dont nous avons traité lors des précédentes réunions. Il s'agit des risques que génèrent les téléphones mobiles, les iPad que l'on utilise en fait dans des hotspots qui ne sont absolument pas sécurisés. Très vite, on peut partager sans le savoir des informations avec autrui.

J'ai souvent le sentiment que les gens ne savent pas de quoi il retourne. Il y a également les médias sociaux comme Facebook, LinkedIn, etc., sur lesquels on poste énormément d'informations. De nombreuses personnes persistent à utiliser leur date de naissance ou d'autres éléments de ce type comme mot de passe. Plus on partage d'informations, plus on risque d'être victime de pirates informatiques.

J'ai moi-même donné cours à des étudiants en informatique et je constate que même les jeunes ne sont pas sensibilisés, qu'ils ne réalisent pas ce qu'ils font.

Je suis véritablement convaincue qu'il faut mobiliser les gens, et je songe tout particulièrement aux parents car, actuellement, tous les enfants utilisent un i-pad. Ils téléchargent des jeux. Dans quelle mesure tout cela est-il sûr?

Il en va de même pour le secteur bancaire. On peut désormais effectuer des opérations par téléphone mais je me demande quel en est le degré

veilig. Er is hier een hele resem specialisten aan wie ik die vraag kan stellen. Ik denk dat we als overheid de mensen meer moeten waarschuwen.

*Mevrouw de Caluwé (NL) N.-* Enerzijds hebben we het natuurlijk gehad over de basisproducten om de computers te beveiligen. Anderzijds is er de bewustwording. Hoe kunnen we mensen bereiken om ze te informeren.

Ik weet zelf ook wel dat die hot spots niet beveiligd zijn. Toch, als ik ergens in een café zit en ik wil mijn e-mails downloaden, dan ben ik snel geneigd om op de wifi te gaan, want het gaat snel en dan kan ik ook nog even twitteren en wat nog allemaal. We doen het dus allemaal.

De vraag is of we tot een geïntegreerde aanpak kunnen komen via twitter, social media, maar ook door nationale ideeën zoals bij voorbeeld via soapseries. Veel jongeren kijken ernaar. Als er dan bij voorbeeld een van de populaire hoofdrolspelers een probleem krijgt omdat hij via facebook onbeveiligd allerlei informatie heeft rondgestrooid, dan landt dat toch gemakkelijker dan door een artikel in de krant dat toch niet wordt gelezen.

Ik denk dat dit echt een tweede punt van zorg is. Misschien kan iemand hier nog iets zeggen over hoe we dit geïntegreerd kunnen aanpakken. Wat voor opdracht kunnen we meegeven aan onze ministers? Of is dat iets wat op nationaal niveau moet gebeuren ?

*De heer Streefland (NL) N.-* U maakt hier een terecht punt. Ik meen dat, vanaf het ogenblik dat je op internet zit, je niet veilig bent; als je op internet zit, kun je gehackt worden. Zo kijk ik er zelf ook naar.

Aan de andere kant kom ik uit de inlichtingenwereld en weet ik ook dat we nog alles over u kunnen vinden, ook al zit je niet op internet. De soep is niet zo heet als ze gegeten wordt.

de sécurité. À mon avis, ces opérations ne sont pas sûres. Il y a ici tout un panel de spécialistes à qui je peux adresser la question. Je crois qu'il est de notre devoir, en tant qu'autorité, de mettre les gens en garde.

*Mme de Caluwé (NL) N.-* Nous avons d'une part parlé bien évidemment des produits de base qui permettent de sécuriser les ordinateurs. Et, d'autre part, il y a la conscientisation. Comment pouvons-nous toucher les gens et les informer?

Je sais bien sûr que les hotspots ne sont pas sécurisés. Mais lorsque je vais dans un café et que je souhaite télécharger mes courriels, j'ai facilement tendance à utiliser le wifi parce que c'est rapide, que je peux twitter, *etc*. Nous le faisons tous.

La question est de savoir si nous pouvons en arriver à une approche intégrée par le biais de twitter et des médias sociaux mais aussi par celui d'initiatives à portée nationale comme, par exemple, des soaps qui sont abondamment regardés par les jeunes. Si un des protagonistes, une figure populaire, est aux prises avec un problème pour avoir diffusé toutes sortes d'informations sur facebook, le message passera plus facilement qu'au-travers d'un article dans un journal que personne ne lira de toute façon.

Je crois que c'est un deuxième souci. Peut-être quelqu'un pourrait-il dire en quelques mots en quoi pourrait consister une apporche intégtégrée. Que pouvons-nous recommander à nos ministres? Ou cela doit-il se faire au niveau national?

*M. Streefland (NL) N.-* Vous avez raison de soulever ce point. Je crois que dès que vous surfez sur l'internet, vous n'êtes pas en sécurité et que vous risquez d'être piraté. C'est ce que je crois.

Mais je suis issu du monde du renseignement et je sais bien que l'on peut trouver sur vous toutes sortes de choses, même en dehors de l'internet. Toutefois, la foudre ne tombe pas chaque fois qu'il tonne.

Het is wel zo dat het heel belangrijk is dat je ervan bewust moet zijn dat, op het moment dat je op facebook of twitter of linkedin bent, je jezelf verbindt met de buitenwereld en dat je aangevallen kan worden. Dat is een gegeven.

Dat betekent dat je eigenlijk ook geen zaken op het internet wil zetten die gevoelig zijn, die confidentieel zijn.

Ik heb wel een facebook account en ook een twitter account, maar alles wat daarop staat mag iedereen weten. Daarvan ben ik me bewust. Ik zal nooit geheime zaken op internet zetten.

Ik denk dat het toch een stuk bewustwording is dat je daarvan op de hoogte moet zijn. Als je ziet wat mensen op facebook zetten, dat is echt belachelijk. Dat geldt zeker voor kinderen met i-pads, levensgevaarlijk, al is het dan alleen maar voor de rekeningen die de ouders kunnen krijgen. Dat is een feit.

Ik zit op internet, ook met *hot spots*. Ik weet dat het niet veilig is, vandaar dat ik ook alleen maar zaken op internet zet die ook echt open zijn, die bekeken mogen worden, waar de mensen ook wat mee mogen doen.

Maar het is een feit dat wanneer je op internet zit, je gewoon kwetsbaar bent. Zo kijk ik er tegenaan.

De bewustwordingcampagnes moet je gewoon blijven doen. Daarom zeg ik ook: *tell the story, tell the story, tell the story*. Dat geldt ook voor de mediacampagnes waar ik me wel bij aansluit.

*Mevrouw de Caluwé (NL) N.-* Dat kan dus simpel een stuk van de opdracht zijn, namelijk te zorgen voor die mediacampagnes en onderling af te stemmen binnen de Benelux als we bij elkaar kunnen zitten, om het maar even heel kort door de bocht, heel praktisch aan te pakken.

Mevrouw Vermeulen vraagt het woord.

*Mevrouw Vermeulen (B) N.-* Ik heb nog één vraagje over de presentatie van de heer Streefland.

Il est très important de réaliser, lorsqu'on se trouve sur facebook, twitter ou linkedin, que l'on se connecte avec le monde extérieur et que l'on peut être attaqué. C'est une donnée.

Cela signifie qu'il vaut mieux ne pas mettre sur l'internet des données sensibles, confidentielles.

J'ai certes un compte facebook et un compte twitter mais ce qui s'y trouve peut être vu de tous. J'en suis conscient. Je ne posterai jamais sur l'internet des choses confidentielles.

Je crois qu'en être informé participe de la conscientisation. Lorsqu'on voit ce que les gens mettent sur facebook, c'est véritablement ridicule. Il en va de même pour les enfants et leur i-pad. C'est une pratique très dangereuse, ne fût-ce qu'en regard des factures que reçoivent les parents. C'est une réalité.

Je surfe aussi sur l'internet, également dans des *hotspots*. Je sais que ce n'est pas sûr et c'est pourquoi je n'y mets que des choses qui peuvent être vues et dont les gens font ce qu'ils veulent.

Mais il est un fait que, sur l'internet, on est vulnérable. C'est mon point de vue.

Il faut poursuivre les campagnes se densibilisation. C'est pourquoi je dis: *tell the story, tell the story, tell the story.* Et cela vaut aussi pour les campagnes dans les medias, que je soutiens.

*Mme de Caluwé (NL) N.-* Tel pourrait donc être un élément de la mission, contribuer à ces campagnes dans les médias et voir dans le cadre du Benelux ce que nous pouvons faire, pour dire les choses de manière simple et pratique.

Mme Vermeulen demande la parole.

*Mme Vermeulen (B) N.-* Une dernière question concernant la présentation de M. Streefland.

De aanvallen kwamen vooral uit specifieke landen. Wij mochten u vragen welke landen.

Ik ga een gok doen; ik denk dat dat vooral Amerika en Azië zijn. Zou ik daaruit kunnen besluiten dat Europa achterloopt, dat wij niet dezelfde kennis hebben als Aziatische landen ? Moeten wij dan niet in de leer gaan bij die landen ? Of ben ik verkeerd en zijn het niet die 14 landen ?

*De heer Streefland (NL) N.-* Ik ken die veertien landen ook niet uit mijn hoofd, maar de top drie waren Rusland, China en Laos. U heeft het wel redelijk goed ingezien. Laos is redelijk verrassend. Nederland, Frankrijk en Engeland zijn ook bij die landen. Dit onderzoek werd gedaan door een bedrijf en is open te vinden op internet. Ik kan u de link doorsturen.

Wat uw tweede opmerking betreft, denk ik niet dat wij achterlopen qua technologie, qua kennis. Ik denk wel dat wij achterlopen in het besef van urgentie.

Ik weet dat China daadwerkelijk een cyberleger heeft. Ik weet dat er nog andere landen zijn die daarin daadwerkelijk investeren en hier in Europa is de urgentie wat minder. Zo zie ik het. Beantwoordt dat uw vraag ?

*Mevrouw Vermeulen (B) N.-* Ja, dank u wel.

**Besluit**

*Mevrouw de Caluwé (NL) N.-* Dank u wel. Ik zou deze conferentie dan nu willen besluiten.

We zijn uiteindelijk, na vele interessante presentaties waarvoor dank, en na een discussie in ieder geval tot twee zaken gekomen die moeten geregeld worden. Dat is dat er een centrale aanpak moet zijn om te zorgen voor veilige basisproducten bij de aankoop. Er moet onderzocht worden of daarvoor wetgeving nodig is.

We moeten dan kijken wat we gezamenlijk kunnen doen; dat kan ook een goede input zijn voor

Les attaques sont venues essentiellement de pays bien spécifiques. Pouvez-vous nous dire lesquels?

Je vais faire un pari: je crois qu'il s'agit principalement de l'Amérique et de l'Asie. Puis-je conclure que l'Europe est à la traîne, que nous ne possédons pas les mêmes connaissances que les pays asiatiques? Ne devons-nous pas, dès lors, nous en inspirer ? Ou suis-je dans l'erreur et ne s'agit-il pas de ces 14 pays?

*M. Streefland (NL) N.-* Je ne connais pas non plus le nom de ces 14 pays par coeur mais les trois premiers étaient la Russie, la Chine et le Laos. Vous aviez plutôt raison. Le Laos constitue une surprise. Les Pays-Bas, la France et l'Angleterre font également partie de ces pays. Cette étude a été réalisée par une entreprise et est disponible sur l'internet. Je puis vous envoyer le lien.

Concernant votre deuxième observation, je ne pense pas que sommes en retard sur le plan de la technologie et des connaissances. Mais je crois que nous le sommes pour ce qui est de la prise de conscience de l'urgence.

Je sais que la Chine possède réellement un cyberarmée. Je sais aussi que d'autres pays investisselent dans ce domaine. Ici, en Europe, l'urgence est un peu moindre. C'est comme cela que je vois les choses. Ai-je répondu à votre question?

*Mme Vermeulen (B) N.-* Oui, je vous remercie.

**Conclusions**

*Mme de Caluwé (NL) N.-* Je vous remercie. Je voudrais à présent clôturer cette conférence.

Après de nombreuses présentations dont je vous sais gré, et à l'issue de la discussion, nous sommes arrivés au constat qu'il y a deux aspects à régler. Il faut une approche centrale pour faire en sorte que des produits de base sûrs soient proposés dès l'achat. Il faudra voir s'il faut légiférer à cet effet.

Nous devons voir ensuite ce que nous pouvons faire en commun; cela peut également constituer

de strategie op Europees niveau. Je kunt daar dan met een voorbeeld komen waar de rest van Europa ook iets aan heeft en dat kan vorden overgenomen door andere landen.

Vervolgens, voor de sociale media en andere gevaren van hackers en cybercriminelen, moet gezorgd worden voor een bewustwordingscampagne en moet worden onderzocht op welke manier zo'n campagne kan worden gevoerd.

Dat hoeven helemaal geen grote, kostbare campagnes te zijn; het kan inderdaad via een soapserie gebeuren, of via tweets, of via een eigen facebookpagina, waarop je allerlei informatie zet en ervoor zorgt dat ze heel gemakkelijk toegankelijk is en dat mensen ook weten waar ze heen moeten.

Ik wil in ieder geval heel hartelijk alle sprekers bedanken die hun hele dag hebben opgeofferd en een lange reis hebben gemaakt om hier te komen en ons op de hoogte te brengen van hun kennis en hun expertise.

Zij hebben al heel wat expertise vergaard en het mooie van hun baan is dat ze iedere dag bijleren, want ze lopen ook iedere dag een dag achter. Ik hoop dat het voor hen niet zo hopeloos is als de indruk die we hier af en toe hebben gekregen wat de problematiek betreft.

Ikzelf sluit hier af. De heer Oberweis vraagt nog even het woord.

*De heer Oberweis (L) F.-* Beste collega's, ik dank mevrouw de Caluwé en de heer Bettel die het initiatief voor deze conferentie, de eerste in een rij, hebben genomen.

Dank zij deze bespreking die velen onder ons na aan het hart ligt, hebben we kennis genomen van de problemen die op dat gebied rijzen. Die problemen ontgaan ons soms, maar nu nemen ze in onze debatten een centrale plaats in.

un élément de la stratégie au niveau européen. On pourrait ainsi avancer un exemple qui servirait à l'ensemble de l'Europe et que d'autres pays pourraient reprendre à leur compte.

Concernant les médias sociaux et autres risques de piratage et de cybercriminalité, il faut mener une campagne de sensibilisation et en définir les modalités.

Il ne doit nullement s'agir d'une campagne à vaste échelle et onéreuse; elle pourrait en effet prendre la forme d'un soap ou de tweets, ou encore d'une page facebook propre où l'on pourrait diffuser toutes sortes d'informations en veillant à ce qu'elle soit aisément consultable et que les gens sachent où aller.

Je tiens en tout cas à remercier chaleureusement tous les orateurs qui nous ont consacré toute cette journée et ont effectué un long voyage pour venir ici et nous faire partager leurs connaissances et leur expertise.

Ils possèdent une vaste expertise et l'attrait de leur fonction est qu'ils continuent d'apprendre tous les jours dans la mesure où ils comptent chaque jour un jour de retard. J'espère que, pour autant, la situation ne leur paraît pas désespérée, un sentiment que nous avons eu ici à certains moments concernant cette problématique.

Je vais rester sur cette conclusion en ce qui me concerne. M. Oberweis souhaite encore intervenir brièvement.

*M. Oberweis (L) F.-* Chers collègues, je tiens à remercier Mme de Caluwé et M. Bettel pour avoir pris l'initiative d'organiser cette conférence, la première d'une série.

Par cette discussion, qui tient au coeur de pas mal d'entre nous, nous avons pris connaissance des différents problèmes qui se posent dans ce domaine, problèmes qui nous échappaient à un certain moment mais qui se trouvent maintenant au centre de nos débats.

Ik stel voor dat mevrouw de Caluwé de taak van rapporteur van deze zitting op zich neemt zodat ze op de plenaire vergadering te Luxemburg de bespreking over cybercrime, cyberbeveiliging en cybertechnologie kan verdiepen.

Een andere conferentie die voor de maand november in het vooruitzicht wordt gesteld, zal het ons mogelijk maken op onze zitting van december in Luxemburg, een voorstel van aanbeveling voor onze ministers te doen waardoor de schijnwerpers op de Benelux worden gericht. Iedereen weet hoe moeilijk het voor ons is om een win-win-win situatie voor onze drie landen te bewerkstelligen.

We moeten onze kennis bundelen zodat de 27 miljoen inwoners van Nederland, België en Luxemburg "hun" Benelux duidelijk zien! We zullen hun op die manier het bewijs leveren dat de Benelux geen instelling is die in een hoekje en in het duister werkt, maar aan hun zijde staat.

De cyberaanvallen moeten grondig worden bestudeerd want ze zullen helaas niet snel verdwijnen. Maar zoals mevrouw de Caluwé al heeft gezegd, we zullen het de volgende keer hebben over de maatregelen die ter zake moeten worden genomen.

Ik dank u en ik wens u een behouden thuiskomst.

De vergadering wordt gesloten om 15.30 uur.

Je propose de confier à Mme de Caluwé la tâche de rapporteur de cette séance afin que le 15 juin, durant la seconde réunion plénière au Luxembourg, elle approfondisse la discussion sur la cybercriminalité, la cybersécurité et la cybertechnologie.

Une autre conférence est prévue dans le courant du mois de novembre. Elle permettrait de présenter, lors notre session de décembre au Luxembourg, une proposition de recommandation à nos ministres, afin de mettre le Benelux en lumière. Chacun connaît les difficultés que nous avons à bien nous positionner et à obtenir un "*win-win-win*" pour nos trois pays.

Il me paraît donc impératif de mettre en commun nos connaissances afin que les 27 millions d'habitants des Pays-Bas, de la Belgique et du Luxembourg perçoivent nettement "leur" Benelux! On leur prouvera ainsi qu'il ne s'agit pas une d'institution qui travaille dans son coin et dans le noir, mais qu'elle est à leurs côtés.

Les cyberattaques représentent un sujet à approfondir car elles sont malheureusement destinées à nous accompagner encore longtemps. Mais, ainsi que Mme de Caluwé l'a signalé, nous parlerons la prochaine fois des mesures à prendre dans ce domaine.

Je vous remercie et vous souhaite un bon retour.

La réunion est clôturée à 15 heures 30.

**BIJLAGE 1**

Presentatie van de heer Beirens

**ANNEXE 1**

Présentation de M. Beirens

# Presentation

- **@LucBeirens**

Chief Commissioner
Head of the Federal Computer Crime Unit

Belgian Federal Judicial Police
Direction Economical and financial crime

© Luc Beirens - Belgian Federal Computer Crime Unit

# Topics

- Evolving threats of cybercrime
- The need of awareness
- Different partners
- The public is very divers
- Actual actions by Belgian police
- What hampers awareness campains ?
- Possible harmonized actions in Benelux

© Luc Beirens - Belgian Federal Computer Crime Unit

# Topics

- Evolving threats of cybercrime
- The need of awareness
- Different partners
- The public is very divers
- Actual actions by Belgian police
- What hampers awareness campains ?
- Possible harmonized actions in Benelux

© Luc Beirens - Belgian Federal Computer Crime Unit

# Evolving threats cybercrime

- Last year's overview => still valid but ...
- Since last year
  - Police ransomware => blocking PCs
  - Phishing mails & false websites ebanking
  - Targetted espionage in transport firms => get codes to fetch containers
  - DDOS Distributed Denial of service attacks using botnets and poorly secured DNS servers => on financial firms => impact business

© Luc Beirens - Belgian Federal Computer Crime Unit

Politie

FCCU

# Federal Computer Crime Unit

**Criminaliteit op het internet**

## Activite illicite demelee!

Ce blocage de l'ordinateur sert a la prevention de vos actes illegaux. Le systeme d'exploitation a ete bloque a cause de la derogation de lois de la Royaume de Belgique!

On a releve l'infraction a la loi: de votre IP adresse qui correspond a "[redacted]" on a realise la requete sur le site qui contient la pornographie, la pornographie d'enfant, la sodomie et des actes de violence envers les enfants. Egalement on a recupere un video avec les elements de violence et la pornographie d'enfants. De meme on a retrouve l'envoi cu courriel electronique sous forme de spam avec les dessous terroristes.

Vos coordonnées:

IP: [redacted]
Localisation: France, [redacted]
ISP: [redacted]

### Pour lever le blocage de l'ordinateur vous devez payer le recouvrement de 100 euros.

### Il y a deux possibilites d'effectuer le paiement:

1) Abolition de dettes a l'aides du systeme de paiement Ukash:

Pour le faire vous devez remplir le champs du paiement avec le code donne, puis appuyer sur OK (en cas de deux codes disponibles, remplissez-les successivement l'un apres quoi appuyes sur OK).

Si le systeme informe d'une erreur, vous devez envoyer le code a l'adresse electronique cybercrime@lokalepolitie.be.

2) Paiement a l'aide de Paysafecard:

Pour le faire vous devez remplir le champs du paiement avec le code (ou avec le mot d'ordre) et appuyer sur OK (en cas de deux codes disponibles, remplissez-les successivement l'un apres l'autre apres quoi appuyez sur OK).

En cas d'apparition d'une erreur, vous devez envoyer le code a l'adresse electronique cybercrime@lokalepolitie.be.

### Ukash Ou puis-je acheter un voucher Ukash?

Vous pouvez obtenir Ukash dans des centaines de milliers d'endroits du monde entier, sur Internet, des portefeuilles, kiosques et GAB.

WWW.beCHARGE.BE

**Becharge** - Utilisez Ukash en ligne 24/7 dès maintenant avec Bancontact / Mr. Cash.

Prepaid4.me

**Prepaid4me** - Acheter Ukash avec Bancontact / Mr. Cash.

Également disponible auprès de votre revendeur:

Champion LUKOIL OIL COMPANY Night and Day

OK

### paysafecard Ou puis-je acheter un voucher Paysafecard?

pay cash. pay safe.

Vous trouverez paysafecard près de chez vous, en Belgique chez un grand nombre de stations services, de supermarchés et de bureaux de tabac.

fnac SELEXION OCTA+ Esso TOTAL Q8 RELAY

OK

# Topics

- Evolving threats of cybercrime
- The need of awareness
- Different partners
- The public is very divers
- Actual actions by Belgian police
- What hampers awareness campains ?
- Possible harmonized actions in Benelux

© Luc Beirens - Belgian Federal Computer Crime Unit

# So there is an evolution… But who is aware of that ?

- The **victims** … and eventually the people & parties they contacted to survive
  - Often not police, not even CERT
- Combating cybercrime is NOT most effective way to give solution
- **Cyber security** is key => protection !
- If you do not **know the threat** you do not know how to protect

© Luc Beirens - Belgian Federal Computer Crime Unit

# Topics

- Evolving threats of cybercrime
- The need of awareness
- Different partners
- The public is very divers
- Actual actions by Belgian police
- What hampers awareness campains ?
- Possible harmonized actions in Benelux

© Luc Beirens - Belgian Federal Computer Crime Unit

# Different partners

- Police & justice (Nat, EU, world wide)
- CERT community
- Cyber security industry (AV producers)
- Centres of expertise (like B-CCentre)
- Enterprise organizations (large => small)
- Consumer protection organizations
- Media (Television, radio, paper, online)

© Luc Beirens - Belgian Federal Computer Crime Unit

# Topics

- Evolving threats of cybercrime
- The need of awareness
- Different partners
- The public is very divers
- Actual actions by Belgian police
- What hampers awareness campains ?
- Possible harmonized actions in Benelux

© Luc Beirens - Belgian Federal Computer Crime Unit

# Not ONE public to target

- End user (in different ages)
- Small companies
- Medium & large companies
- Critical infrastructure companies
- Developers
- Telecom operators & Internet service providers

© Luc Beirens - Belgian Federal Computer Crime Unit

# Topics

- Evolving threats of cybercrime
- The need of awareness
- Different partners
- The public is very divers
- Actual actions by Belgian police
- What hampers awareness campains ?
- Possible harmonized actions in Benelux

© Luc Beirens - Belgian Federal Computer Crime Unit

# Actual actions BE police

- Websites Federal police & eCops
- Blogging of some collegues + tweets
- Information sessions to different audiences
  - ICT high schools and universities
  - School (only when problems occured)
  - General public (end users)
  - SME (with federations of SME)
  - ICC & FEB VBO Fed Belgian enterprises
  - Specific in critical infrastructure

© Luc Beirens - Belgian Federal Computer Crime Unit

# Police

Site de la police fédérale belge

- Organisation
- Circulation
- Criminalité
- Avis de recherche
- Moyens matériels
- Personnel
- Documentation
- Point presse
- Publications
- Evénements
- Liens

Liens externes:

- Police locale
- Comité P
- Inspection générale
- Service social
- Secrétariat SSGPI

Numéros d'urgence

chercher

## COMMISSARIAT GÉNÉRAL

Présentation

**Le Service relations publiques et protocole:** ce service a pour missions la coordination et l'appui aux activités de relations publiques de la Police fédérale; la gestion et le développement ... lire plus

Organigramme

Relations avec la police locale

## AVIS DE RECHERCHE

À identifier: [Suspects inconnus]

Tentative de Shoulder Surfing à la Grand-Place de Tournai

Mailing liste: inscrivez-vous

Affaires non classées

telefactsCRIME

## CIRCULATION

Contrôles annoncés [Vitesse]

Flandre occidentale

AM/PM A014 (E17) E17 Waregem - Courtrai

Inforoutes

CONTACTS [27 avril 2013]

« Cavaliers: A cheval sur la sécurité »

## COMMUNIQUÉS DE PRESSE

25-04-2013

9 personnes arrêtées en flagrant délit de vols de métaux

24-04-2013

2600 euros de perception immédiate lors d'un contrôle de camionnettes

## DIVERS

Ransomware (Police) Virus eCops

Message du FCCU

Surfons Tranquille

PODCAST 23/04/2013

## ÉVÉNEMENTS

17-05-2013

Fête de la circulation à la ZP Meetjesland

19-05-2013

Journée portes ouvertes de la ZP Pays de Herve

DES ANIMAUX SOUS LE KEPI

à partir du 10 octobre 2012

## POLICE ADMINISTRATIVE

Présentation

**Service de sécurité auprès du Palais Royal:** il oriente ses services, à savoir garantir la protection des personnes et la surveillance des propriétés, vers une clientèle spécifique : le Roi et la Famille royale. ... lire plus

## POLICE JUDICIAIRE FÉDÉRALE

Présentation

**FAST:** Le Fugitives Active Search Team est chargé de la recherche active et de l'interception entre autres des personnes qui ont été condamnées par les tribunaux belges et qui veulent échapper à l'exécution de leur jugement ou arrêt. ... lire plus

## APPUI ET GESTION

Présentation

**DSE:** La Direction de la formation a pour mission principale de développer, coordonner, harmoniser et organiser, en concertation avec les autorités et partenaires, tous les types de formations au profit de l'ensemble des membres de la police intégrée, conf ... lire plus

© Luc Beirens - Belgian Federal Computer Crime Unit

ecops
Nederlands | Français | Deutsch | English
Welkom op het Belgisch online meldpunt
eCops is een online Belgisch meldpunt waar je als internetgebruiker misdrijven in verband met België op of via het internet kan melden.
Je hoeft je niet te bekommeren over "Wie is er nu juist bevoegd?", eCops zorgt ervoor dat jouw melding door de bevoegde dienst wordt onderzocht.
Kwam je terecht op een verwarrende site met misleidende informatie?
Ontving je via e-mail ongewenste reclame of een frauduleus voorstel?
Zag je kinderporno op een site?
Jouw melding kan de aanleiding zijn voor een verdere actie door de FOD Economie, Politie of Justitie.
Je doet je melding stap voor stap via het online meldingsformulier.
Verdere informatie over internetmisbruik en internetgerelateerde criminaliteit vind je hier.
eCops is geen online-centrale voor noodoproepen aan de Belgische Politie!
Voor niet-internetgerelateerde klachten kan je terecht op E-Loket Politie.
Is uw computer schijnbaar door politie of SABAM geblokkeerd Klik hier
Politie
Melden
economie
FOD Economie, K.M.O., Middenstand en Energie
eCops is een initiatief van :
De Federal Computer Crime Unit van de Federale Gerechtelijke Politie (FCCU)
De Federale Overheidsdienst Economie, KMO, Middenstand en Energie

# Actual actions BE police

- Press releases with warnings
- Interviews
- Radio
  - Inspecteur Decaluwe (from time 2 time)
  - Grootste helpdesk van Vlaanderen (yearly)
  - Surfons Tranquille Radio 21 (weekly)
- TV
  - Panorama

© Luc Beirens - Belgian Federal Computer Crime Unit

# Other initiatives

- Cooperation with organizations : input
  - Childfocus : clicksafe website
  - Febelfin : Veilig internetbankieren
  - CERT
- Documents for incident handling
  - With FEB VBO ICC

© Luc Beirens - Belgian Federal Computer Crime Unit

# b·ccentre

BELGIAN CYBERCRIME CENTRE OF EXCELLENCE
FOR TRAINING, RESEARCH & EDUCATION

Home | News | Activities | Publications | Events | About | Links

« Older Entries

## B-CCENTRE joins EU partners in fighting botnets

March 14th, 2013 | Author: B-CCENTRE

B-CCENTRE and 27 partners from 14 European countries have joined forces to fight one of the most imminent threats in the Internet, the botnets. One out of five computers connected to the Internet is currently part of a botnet, according to expert estimates. Botnets are made up of computers infected and abused by cyber criminals. They can be used to spread malware and distribute spam emails, among other things.

The new coalition against botnets is supported by the European Union in the ACDC project, which started its activities in February. The new project's heart is the Advanced Cyber Defence Centre, ACDC, scheduled to become a full-service programme for additional cyber security ranging from prevention to detecting malware. The partners include public infrastructure providers, software vendors, scientific and academic institutions, criminal prosecutors and authorities, as well as banks and certification providers. The pilot project has an overall budget of 16 million Euros and is initially scheduled for 30 months.

Search this website:

Search

Upcoming Events

| April 2013 | | | | | | |
|---|---|---|---|---|---|---|
| Mon | Tue | Wed | Thu | Fri | Sat | Sun |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | | | | | |



© Luc Beirens - Belgian Federal Computer Crime Unit

click safe

Child Focus

• Français • Nederlands

Welkom op de **Child Focus** – site over veilig internetten

Hier vindt u alle informatie over een veilig en verantwoord internetgebruik voor kinderen en jongeren.

Voor **Kinderen**

Voor **Jongeren**

Voor **Ouders**

Voor **Professionelen**

FCCU

© Luc Beirens - Belgian Federal Computer Crime Unit

febelfin

Home | Over Febelfin | Nieuws | Thema's en dossiers | Cijfers

Home > Veilig internetbankieren? Enkele tips!

# Veilig internetbankieren? Enkele tips!

04-02-2013

Vorig jaar was *phishing* de meest gebruikte fraudetechniek om klanten via internetbankieren geld te ontfutselen. Febelfin herinnert eraan dat klanten nooit mogen ingaan op e-mails of telefonische contacten waarbij hen gevraagd wordt om persoonlijke gegevens en codes voor internetbankieren waaronder de *response code* – zijnde de elektronische handtekening die verschijnt op het scherm van de kaartlezer – mee te delen!

## Aantal fraudegevallen met internetbankieren is toegenomen in 2012

De voorbije maanden is het aantal fraudegevallen met internetbankieren gestegen. Voor het volledige jaar 2012 staat de teller op 1003 fraudegevallen voor een totaalbedrag van bijna 3 miljoen EUR.

© Luc Beirens - Belgian Federal Computer Crime Unit

# Topics

- Evolving threats of cybercrime
- The need of awareness
- Different partners
- The public is very divers
- Actual actions by Belgian police
- What hampers awareness campains ?
- Possible harmonized actions in Benelux

© Luc Beirens - Belgian Federal Computer Crime Unit

# What hampers awareness campains

- Too many websites
  (waste of available capacity)
- Some campaigns not specific enough for public
- People **do not come to websites**
  unless victims or already aware people
- Not enough political attention
- Lack of coordination nat / internat
- Lack of means => **no "air time" on tv**

- *People and entreprises remain unaware*

© Luc Beirens - Belgian Federal Computer Crime Unit

# Not personal enough

- Tweet account of cpni.nl
- Daily reporting
- Only 581 followers
- Not personal

- Tweet account lucbeirens
- Very unregular reporting
- 1229 followers

© Luc Beirens - Belgian Federal Computer Crime Unit

# Timely awareness

- New threats pop up every day
  - Most of them can be mitigated with updates / upgrades
  - Some of them can not be mitigated immediately and pose a serious threat

⇒ need to warn user / companies

⇒ need for immediate access to media

- But the press takes and publishes what they want and not always what you want

⇒ need for legal framework to publish

© Luc Beirens - Belgian Federal Computer Crime Unit

# Topics

- Evolving threats of cybercrime
- The need of awareness
- Different partners
- The public is very divers
- Actual actions by Belgian police
- What hampers awareness campains ?
- Possible harmonized actions in Benelux

© Luc Beirens - Belgian Federal Computer Crime Unit

# Possible harmonized actions in Benelux

- Yes it is in national strategies !
  - But campaigns cost money !
  - Focus on “unaware” public using their channels of information
- Reduce number of websites & focus
- Reusing content of each others websites work together to copy campaigns

© Luc Beirens - Belgian Federal Computer Crime Unit

# Contact information

Federal Judicial Police
Direction for Economical and Financial crime
**Federal Computer Crime Unit**
Notelaarstraat 211 - 1000 Brussels – Belgium

Tel office : +32 2 743 74 74
Fax : +32 2 743 74 19

E-mail : luc.beirens@fccu.be
Twitter : @LucBeirens
Blog : LucBeirens.blogspot.com

© Luc Beirens - Belgian Federal Computer Crime Unit

**BIJLAGE 2**

Presentatie van de heer Streefland

**ANNEXE 2**

Présentation de M. Streefland

hacking traffic signs

# Content

1. Introduction
2. What is Cyber Security in the Critical Infrastructure?
3. How to raise public awareness?
4. Conclusion

ENCS

# Content

1. Introduction
2. What is Cyber Security in the Critical Infrastructure?
3. How to raise public awareness?
4. Conclusion

ENCS

# 1. Introduction (1)

- Who is Fred Streefland?
  - 20+ years of Intelligence & Security experience
  - Air Force/NATO, Intelligence Service, IBM, Accenture, ENCS
  - Specific Cyber Security courses in UK, Israel and The Netherlands
  - Public & Private Cyber Security advisor
  - Projectleader in Smart Grid domain

……and still not an expert at anything!

# 1. Introduction (2)

- What is ENCS?
  - European Network for Cyber Security
  - Not for profit cooperative organisation (founded: July 2012)
  - Located in The Hague, The Netherlands
  - Organisation: R&D, Test Bed, Education & Training (E&T) and Information & Knowledge Sharing (I&KS)
  - Goal: to increase the cyber resilience of the European Critical Infrastructure

# Content

1. Introduction
2. What is Cyber Security in the Critical Infrastructure?
3. How to raise public awareness?
4. Conclusion

ENCS

# 2. What is Cyber Security in the Critical Infrastructure?

- *"The more people rely on the internet, the more people rely on it to be secure"* – Neelie Kroes

- *"The more critical infrastructures rely on the internet, the more critical infrastructures become insecure"* – Fred Streefland

# Cyber Security

***Cyber Security:*** the protection of an organisation and its assets from electronic attack to minimise the risk of business disruption*.

*Wikipedia (slightly adapted)

# Critical Infrastructure (1)

- ***Critical infrastructure***: assets that are essential for the functioning of a society and economy*.
  - Utilities : Power, Oil, Gas, Water Supply
  - Transportation: Rail, Traffic Lights, (air)ports
  - Telecom
  - (Agriculture: (food production & distribution))
  - (Health (e.g. hospitals))
  - (Financial Services)

* Wikipedia

# Critical Infrastructure (2)

- Industrial Control Systems/SCADA
  - “Basic” technology
  - No build-in security from design phase
  - Designed for “open use” by operators/engineers
  - In the past: stand-alone/isolated network, not connected to internet!

## Thousands of SCADA Devices Discovered On the Open Internet

Posted by **Unknown Lamer** on Thursday January 10, @03:57PM
from the easier-that-way dept.

Trailrunner7 writes with news of the continuing poor stat
control systems. From the article:

> "Never underestimate what you can do with a health
> search terms and a beer budget. That's mostly what
> two critical infrastructure protection specialists who
> months trying to paint a picture of the number of Inte
> critical infrastructure in the United States. It's not a
> have with some help from the Department of Homela

TECHNOLOGY | April 8, 2009

## Electricity Grid in U.S. Penetrated By Spies

Article | Video | Comments (139)

Email | Print | Save

Exclusive subscriber content

CCESS. LOGIN OR Subscribe Now For Full Access » AND GET 4 WEEKS FREE!

**KrebsonSecurity**
In-depth security news and investigation

## 26 DHS Warns of 'Hacktivist' Threat Against Industrial Control Systems

OCT 12

176 tweets TOP ★5K retweet

The **U.S. Department of Homeland Security** is warning that a witch
recent events make it increasingly likely that politically or ideologically
hackers may launch digital attacks against industrial control systems. Th
issued the same day that security researchers published information
undocumented software backdoor in industrial control systems sold by hundred
manufacturers and widely used in power plants, military environments and nautical

The information about the backdoor was published by industrial control systems (ICS) security vendor **Digital Bond**, which

## Backdoor in computer controls opens critical infrastructure to hackers

Widely used software used to control machinery in power plants is vulnerable.

by **Dan Goodin** - Oct 25 2012, 8:45pm WE

HACKING | NATIONAL SECURITY | 29

# Example 1: Maroochy Water Services (2000)

# Example 2 & 3: CSX train systems (2003) & traffic lights in Los Angeles (2006)

# Example 4: Stuxnet (2010)

# Example 5: Dutch Floodgate hack (2012)

# Example 6: Saudi Aramco – Shamoon (2012)

Saudi Aramco

Dear Customer,

We have isolated all our electronic systems from outside access as an early precautionary measure that was taken following a sudden disruption which affected some sectors of our network.

The disruption was suspected to be the result of a virus that had infected personnel workstations without affecting the primary components of the network.

The interruption is under control, we are working diligently to restore services to normal as soon as possible in a methodical approach.

We apologies for any inconvenience.
Thank you for your patience.

Copyright © Saudi Aramco, 2012.

# Content


1. Introduction
2. What is Cyber Security in the Critical Infrastructure?
3. How to raise public awareness?
4. Conclusion

ENCS

# How to raise Public Awareness? (1)

- Tell the Cyber Story!
- Tell the Cyber Story!
- Tell the Cyber story!
- …..keep on telling the Cyber Story!

- See the ‘raising awareness’ suggestions, described in the Cyber Security Strategy of the EU (page 8)
- Use some examples, that can be ‘understandable’ explained

# Did you know that:

- …in 2012 more than 200 cyber attacks against US companies were reported by the US ICS-CERT?
- …a ‘honeypot ICS/SCADA system’ was connected to the internet and received the first attack within 18 hours?
- ….the same honeypot ICS/SCADA system was attacked 39 times from 14 different countries within a period of 28 days?
- ….in Jan 2012, only 26% of European enterprises had a formally defined ICT security policy?

# How to raise Public Awareness? (2)

- Develop/announce a clear European/Benelux statement <u>and</u> direct/guide follow-on action.

- *"**Cybersecurity** is one of the most serious economic and national security challenges we face as a nation!"* – Barack Obama

# How to raise Public Awareness? (3)

- Pro-active support the development of European ICS/Smart Grid Cyber Security Policy & Standards in line with the EU Cyber Security Strategy.

=> This can be done by starting the development of a Benelux Cyber Security Policy & Standards for ICS/Smart Grids!

# Content

1. Introduction
2. What is Cyber Security in the Critical Infrastructure?
3. How to raise public awareness?
4. Conclusion

ENCS

# Conclusion

- Don’t wait for the “BIG HACK”, but start a public awareness program TODAY!

  -> Tell the Cyber story!
  -> Announce a European/Benelux Statement and direct/guide follow-on action!
  -> Develop a European (Benelux) Cyber Security Policy & Standards for ICS/Smart Grids!

# Thank you for your attention!

Fred.Streefland@ENCS.eu

ENCS

# Back-up Slides

ENCS

# Did you know that:

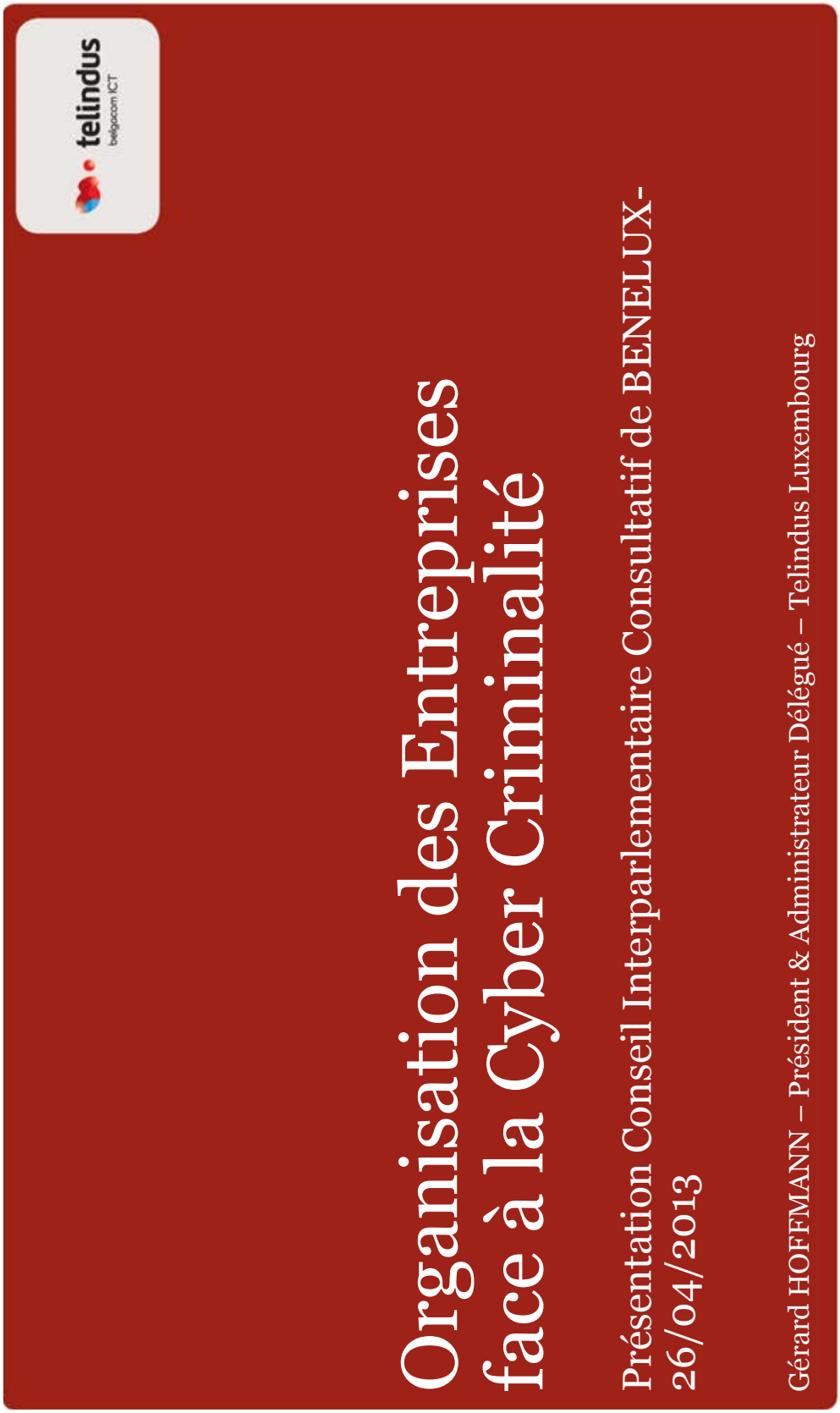
- ….. It is impossible to develop software without bugs?
- …..Every 1000 code strings contains ± 2-3 bugs?
- …..there are more than 120 processors in an average car with more than 10 milion software code strings?
- ….The moonlanding in 1969 needed 7.500 code strings, while an average smart phone contains > 11 million code strings

**BIJLAGE 3**

Presentatie van de heer Hoffman

**ANNEXE 3**

Présentation de M. Hoffman



# Introduction:
# Cyber Attaques - Tendances

- Nombre de Cyber Attaques en pleine expansion

| Top Threats | Current Trends | Top 10 Emerging Trends | | | | | |
|---|---|---|---|---|---|---|---|
| | | Mobile Computing | Social Technology | Critical Infrastr. | Trust Infrastr. | Cloud | Big Data |
| 1. Drive-by exploits | ↑ | ↑ | ↑ | ↑ | | ↑ | ↑ |
| 2. Worms/Trojans | ↑ | ↑ | ↑ | ↑ | | → | ↑ |
| 3. Code Injection | ↑ | → | | ↑ | | ↑ | |
| 4. Exploit Kits | ↑ | ↑ | → | ↑ | | | ↑ |
| 5. Botnets | ↑ | ↑ | | → | | → | |
| 6. Denial of Service | → | | | → | ↑ | → | |
| 7. Phishing | → | ↑ | ↑ | → | | | → |
| 8. Compromising Confidential Information | ↑ | ↑ | | ↑ | → | ↑ | ↑ |
| 9. Rogueware/ Scareware | → | | → | | | | |
| 10. Spam | ↓ | | → | | | | → |
| 11. Targeted Attacks | ↑ | | ↑ | ↑ | → | ↑ | → |
| 12. Physical Theft/Loss/Damage | ↑ | ↑ | ↑ | ↑ | → | → | |
| 13. Identity Theft | ↑ | ↑ | ↑ | | → | ↑ | ↑ |

Legend: ↓ Declining, → Stable, ↑ Increasing

Table 1: Overview of Threats and Trends of the ENISA Landscape[2]

# Introduction:
# Enjeux de la Cyber Sécurité

- **Pour les Etats:**
  - Stratégiques (défense et sécurité natic
  - Politiques
  - Economiques
  - Diplomatiques
  - Militaires
- **Pour les Entreprises:**
  - Financiers (perte de chiffre d'affaire)
  - Juridiques (amendes, non respect de
  - Perte d'image (réputation, confiance
  - Politiques
- **Pour les particuliers:**
  - Financiers (arnaques, vols)
  - Données personnelles - Respect de la

LUXEMBOURG
Publié le 12.04.13 15:00
Ecouter

## Phone Scams, ne vous laissez pas prendre au piège

*Face à la recrudescence des arnaques appelées Microsoft Phone Scam ou Windows Phone Scam, la police grand-ducale lance une nouvelle alerte à la population.*

*En rouge, tous les pays attaqués par le réseau pirate. (photo: kaspersky)*

# Introduction: Cyber Incidents -

- Cyber Incidents les pl
- Le Lux
  - Phis
  - Ran
- Nécess
  - Se p
  - Evit

What typ
experie

Denial of servic

We did not experience any cyber i

Global survey on 387 CEO

CRÉDIT AG

Cher Client(e) .

Votre Carte visa a été
Nous avons détermine
autorisation.
Nous avons envoyé ce
et accéder à votre esp

Note : Si ce n'est pas a
carte indéfiniment ,ca
Cliquez sur le lien et s
Crédit.

La procédure est très sim

1. Cliquez sur le lien
2. Confirmez que vo

Accéder à votre comp

Nous vous remercions de l
espérons que vous compre
protéger votre compte. Nou

Merci,

Crédit agricole

Nous nous excusons de

Bien Cordialement

Police Grand-Ducale Luxembourg

Soutenu et Protégé par

paysafecard Ukash

IP:
Pays: LU Luxembourg
Region: XX
Ville: XX
ISP:
Système d'exploitation: Windows 7 (64-bit)
Nom d'utilisateur:

ATTENTION! Votre ordinateur est bloqué à cause d'un ou de plusieurs motifs, indiqués ci-dessous.

Vous avez violé la loi «Sur le droit d'auteur et les droits contigus» (Vidéo, Musique, Logiciel) et vous avez illégalement servi et/ou diffusé le contenu protégé par le droit d'auteur, de ce fait vous avez violé l'article 128 du Code pénal de la Luxembourg.

L'article 128 du Code pénal prévoit l'amende d'un montant de 200 jusqu'à 500 rémunérations du travail minimales ou la privation de liberté pour de 2 à 8 ans.

Vous avez visionné ou diffusé le contenu pornographique interdit (pornographie impliquant des enfants/Zoophilie and etc), ayant violé l'article 202 du Code pénal de la Luxembourg.

L'article 202 du Code pénal prévoit la privation de liberté pour de 4 à 12 ans.

L'accès inégal aux données informatiques a été effectué de votre ordinateur ou vous...

L'article 208 du Code pénal prévoit l'amende d'un montant de 100.000€ et/ou la privation de liberté pour de 4 à 9 ans.

L'accès illégal a été effectué à votre insu, votre ordinateur est probablement infecté par le logiciel nuisible, de ce fait vous violez la loi «Sur l'utilisation négligente de l'ordinateur».

L'article 210 du Code pénal prévoit l'amende d'un montant de 2000€ jusqu'à 8000€.

La diffusion du spam ou une autre opération publicitaire illégale à but lucratif a été effectué de votre ordinateur, ou à votre insu, votre ordinateur est probablement infecté par le logiciel nuisible.

L'article 212 du Code pénal prévoit l'amende d'un montant jusqu'à 250.000€ et la privation de liberté pour jusqu'à 6 ans. Si cette opération donnée a été produite à votre insu, vous tombez sous le coup de l'article 210 indiqué ci-dessus du Code pénal de la Luxembourg.

Maintenant nous déterminons votre identité et votre location, pendant 72 heures une affaire pénale contre vous est à ouvrir en vertu d'un ou de plusieurs articles indiqués ci-dessus.

Conformément aux amendements au Code pénal de la Luxembourg du 04 février 2013, cette infraction à la loi (en cas de l'absence de la répétition d'un crime) peut être considérée avec sursis en cas du paiement de l'amende au profit de l'État.

Vous ne pouvez payer l'amende que pendant 72 heures après la violation. À l'expiration de 72 heures la possibilité de payer l'amende est annulée, une affaire pénale contre vous sera pendant prochaines 72 heures automatiquement ouverte!

La somme de l'amende fait 100€. Utilisez Ukash ou PaySafeCard.

Au paiement de l'amende et après ce que l'argent est reçu sur le compte de l'Etat votre ordinateur sera débloqué pendant 1 à 72 heures.

Après le déblocage vous avez 7 jours ouvrables pour corriger cette infraction.

Si vous, à l'expiration de 7 jours ouvrables, n'avez pas corrigé tous les délits, votre ordinateur sera bloqué de nouveau, et une affaire pénale contre vous sera automatiquement ouverte en vertu d'un ou de plusieurs articles énumérés ci-dessus.

Code PIN | Montant 100

1 2 3 4 5 6 7 8 9 0

A payer PaySafeCard | A payer Ukash

Dépenser PaySafeCard est facile.

Vous trouverez PaySafeCard près de chez vous, en Luxembourg p.e. chez un grand nombre de kiosques à journaux, de bureaux de tabac et de stations services.

Dépenser Ukash est facile.

Vous pouvez obtenir Ukash dans des centaines de milliers d'endroits du monde entier, sur Internet, des portefeuilles, kiosques et GAB.

Ukash - est disponible dès maintenant à partir de stations-service.

ePay - Ukash à partir de milliers de supermarchés et de magasins d'appels où vous voyez le signe ePay.

Plus Ukash:

www.Faal.co.uk
www.pcGameSupply.com
www.AquadcXchange.com
www.UcashStation.net
www.UkashReselling.com/aurlocator.htm

FAKE

© -Police Grand-Ducale - Luxembourg-

Level of sensitivity : "Pub

# Agenda

Une multitude de Cyber Définitions…

Cyber Criminels et Cyber Menaces

Cyber Sécurité

Conclusion

# Une multitude de Cyber Définitions…

# Une multitude de Cyber Définitions…

- **Sécurité des Systèmes d'Information:**
  - Ensemble de moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour établir, garantir, conserver et rétablir la sécurité d'un Système d'Information.
  - Objectif: prévenir les menaces et assurer la Disponibilité, l'Intégrité et la Confidentialité d'un Système d'Information.
- **Cyber Criminalité:**
  - Utilisation d'Internet et des réseaux informatiques pour détourner des sommes d'argent ou pour accomplir des crimes.
- **Cyber Attaque:**
  - Acte malveillant visant à rendre inopérant ou a utiliser frauduleusement un dispositif informatique, réalisé par l'intermédiaire d'Internet.
- **Cyber Sécurité:**
  - Ensemble des procédés informatiques visant à protéger les données transitant par Internet.

# Une multitude de Cyber Définitions…

- Mais aussi:
  - Cyber Défense
  - Cyber Espace
  - Cyber Espionnage
  - Cyber Conflit
  - Cyber Terrorisme
  - Cyber Magouille
  - Cyber Fraude
  - Cyber Militantisme
  - …

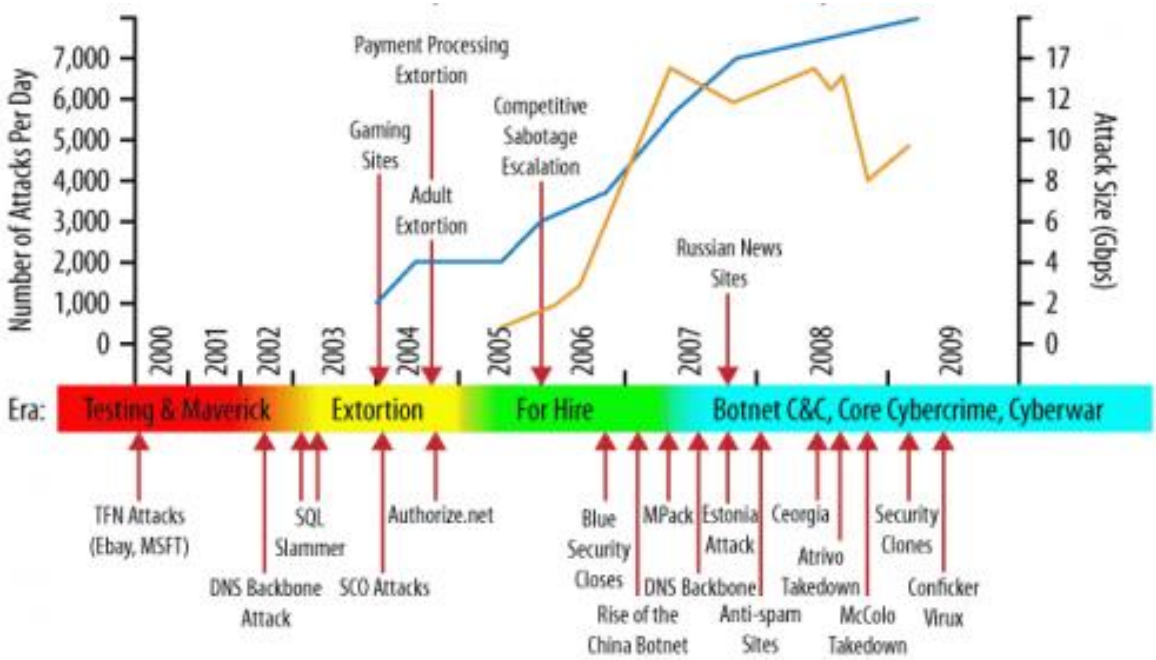
telindus
belgacom ICT

# Cyber Criminels – Cyber Menaces

together with
belgacom
tango

# Cyber Criminels & Cyber Menaces

- **Types**
  - Cybe
  - Cybe
  - Hacl
  - Cybe
- **Les ar**
  - Malv
  - Expl
  - Outi
  - Déni
  - Ingé
  - …




**DDoS Arsenal**

SYN, ICMP, GET/POST, UDP, Bad Protocols, Connection Floods, Applications Back-end, P2P, Browser Malware, DNS Spoofing.

**Motivations**

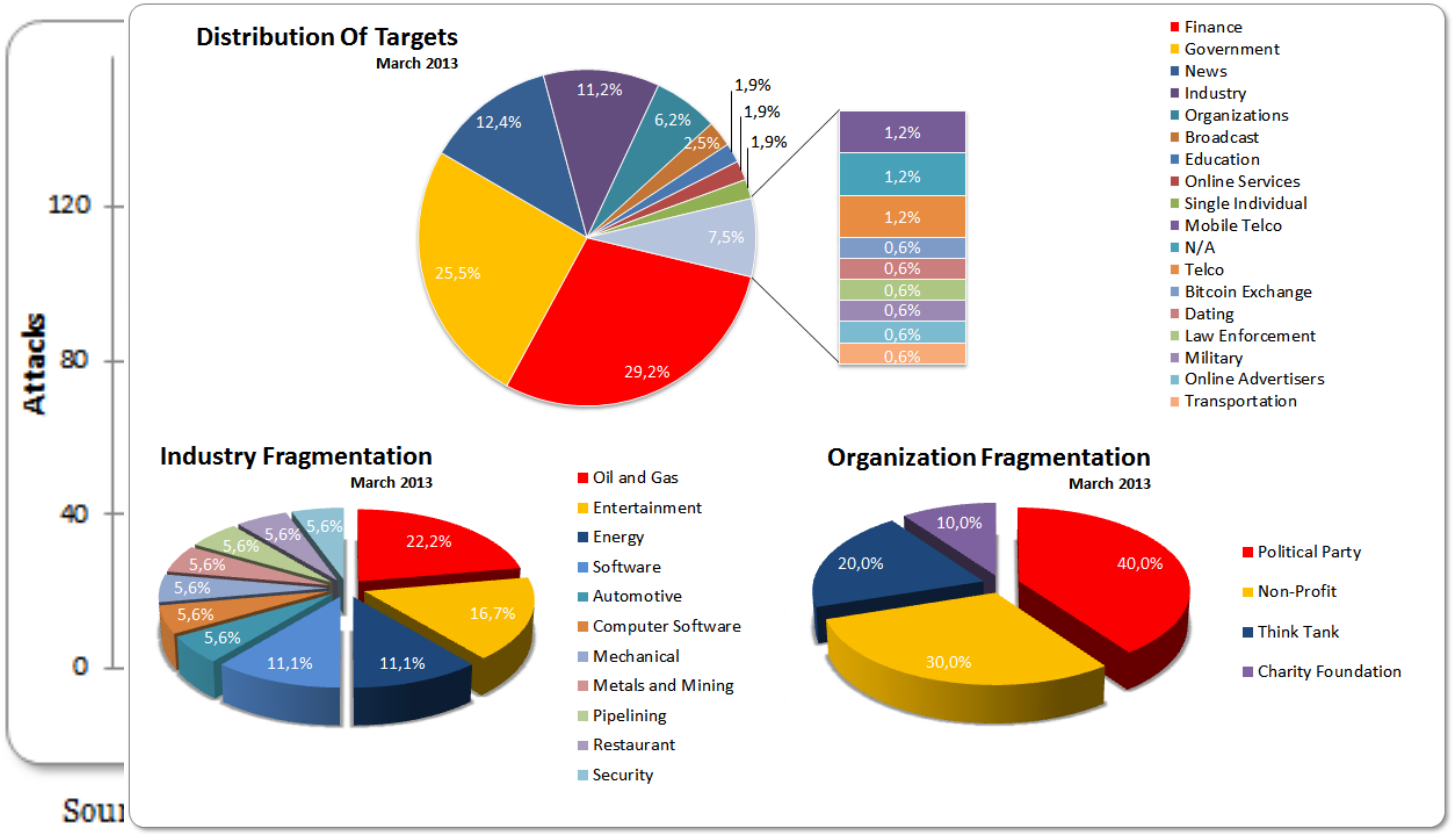
Revenge, Extortion, Industrial/Competitive Sabotage, Political Activism, Terrorism, Theft.

**On the Horizon**

Cloud Attacks, VOIP, IPTV, Defense Immobilization.

# Cyber Criminels & Cyber Menaces

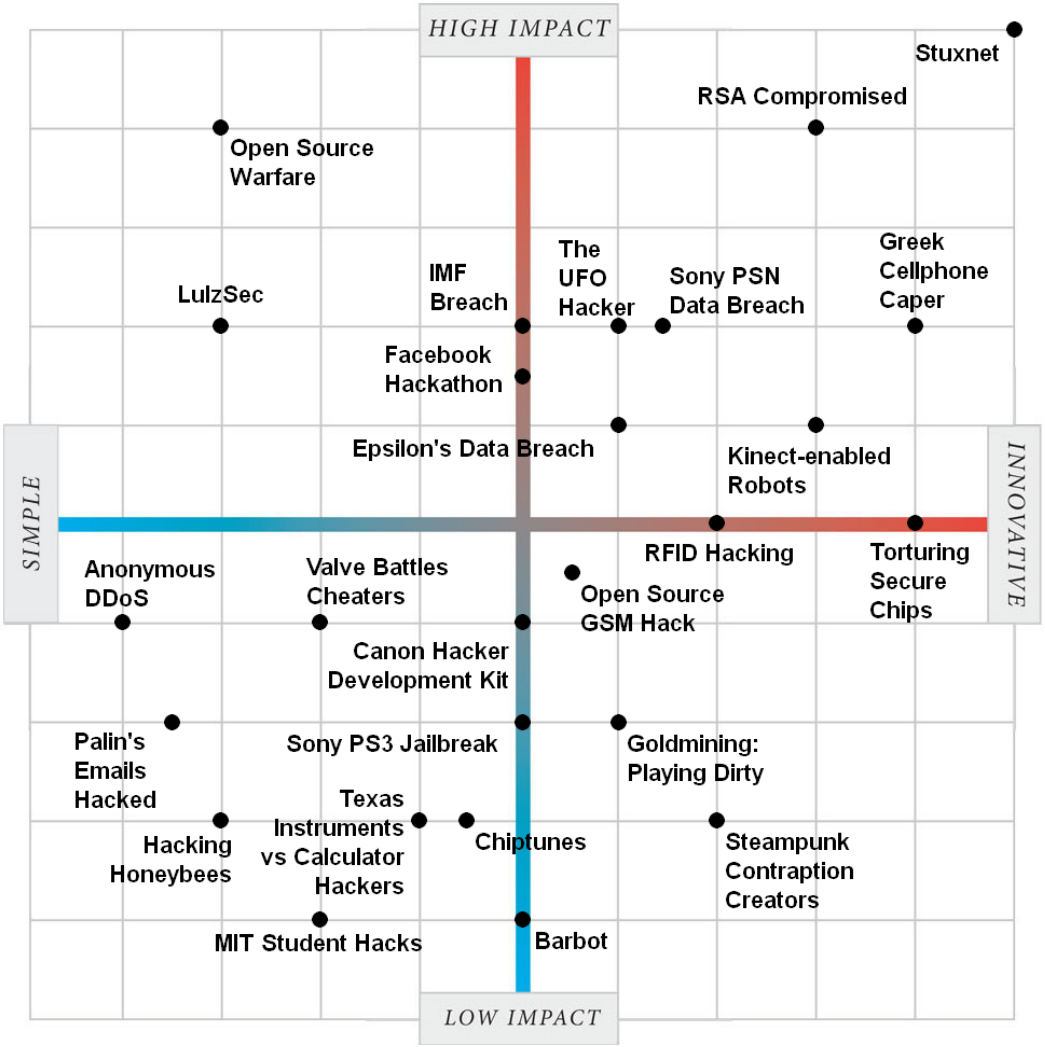
- Types d'Attaquants et motivations sont variés -2012

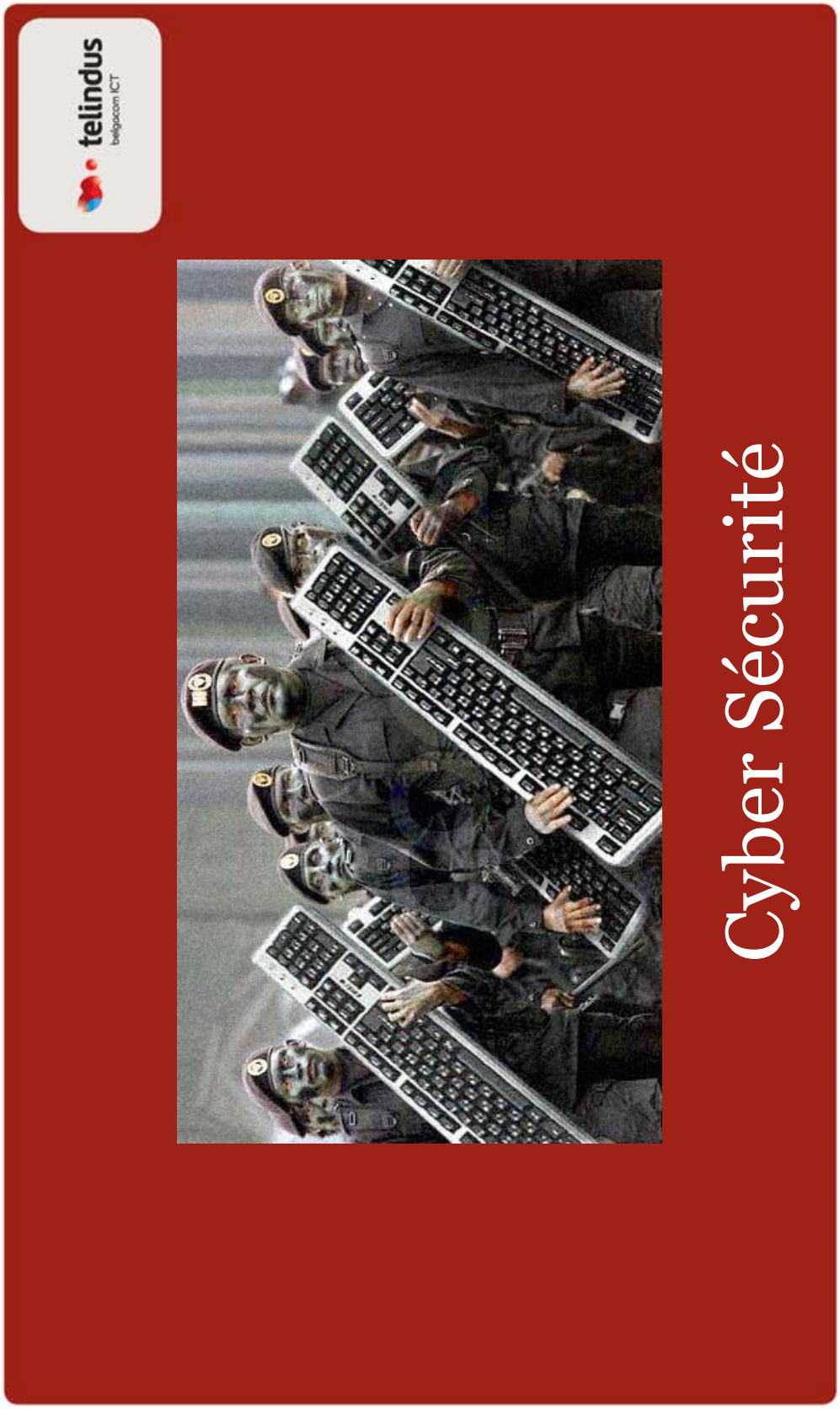



source: http://hackmageddon.com

# Cyber Criminels & Cyber Menaces

- **Impacts:**




telindus
belgacom ICT
Cyber Sécurité

together with
belgacom
tango

# Cyber Sécurité:
# Au niveau des Entreprises

- **Organisation et développement des Systèmes de Management de la Sécurité de l'Information (SMSI):**
  - Démarche d'Entreprise basée sur une Analyse de Risque
    - Identifier – Analyser – Prioriser – Gérer
  - Ensemble de moyens mis en œuvre:
    - Techniques
    - Organisationnels
    - Juridiques
    - Humains
  - Management de la SSI: Normes ISO 2700x
    - ISO 27001 – PDCA - Amélioration Continue, cadre, gouvernance
    - ISO 27002 – Guide de bonnes pratiques
    - ISO 27004 – Indicateurs pour piloter le SMSI
    - ISO 27005 – Méthode d'Analyse de Risque

# Cyber Sécurité:
# Au niveau des Entreprises

- **Les outils de la Cyber Sécurité:**
  - PSSI (définition des orientations stratégiques de la DG)
  - Méthode d'Analyse de Risque (Ebios, Melisa, Mehari, ...)
  - Procédures opérationnelles (résilience, audits, SOC, SIEM, ...)
  - Mesures techniques (IAM, chiffrement, firewalls, antimalware, ...)
  - Sensibilisation à la sécurité (Formations, chartes, ...)
  - Proactivité (Veille sécurité, formations, retour sur expérience, ...)
  - Contre-Attaques

→ appel à des spécialistes externes apportant la connaissance des techniques utilisées par les cybercriminels.

# Initiatives liées à la Cyber Sécurité: Au Luxembourg

- CEPL - Journées Professionnelles en Grande Région sur le thème de la cybercriminalité – Juin 2008
- Conference FEDIL sur la Cybersécurité– mai 2012
- Conférences CLUSIL, AmCham, IT one, …
- Legitech: Cybercriminalité : quelles obligations pour les entreprises ? – juin 2012
- CASES (Cyberworld Awareness Security Enhancement Structure)
- CERT: CIRCL/GOVCERT/Restena CSIRT

# Initiatives liées à la Cyber Sécurité:
## **Gouvernement:** Stratégie nationale en matière de Cybersécurité

- Juillet 2011 – Mise en place d'une stratégie globale en matière de cybersécurité – Création du Cyber Security Board.
- Novembre 2011 – CSB: stratégie sur 5 axes :
  - protection opérationnelle des infrastructures et systèmes de communication et de traitement de l'information;
  - moderniser le cadre légal;
  - développer la coopération nationale et internationale;
  - informer, éduquer et sensibiliser sur les risques encourus;
  - mettre en place des normes et des standards contraignants.
- Janvier 2012 – Recommendations du CSB
  - Sensibilisation – Formation des Agents de l'Etat.
  - Généralisation obligatoire de l'authentification forte pour accès aux données sensibles (Luxtrust)
  - Analyse de risque : identification des DB nécessitant une protection particulière.
  - Protection des infrastructures critiques du pays

# Initiatives liées à la Cyber Sécurité:
## **Gouvernement:** Stratégie nationale en matière de Cybersécurité

- Juin 2012 – Réunion du CSB:
  - Centralisation du signalement des incidents Cyber Sécurité: CERT.lu
  - Mission de l'ILR: obligation pour les TELCOs de prendre des mesures techniques et organisationnelles (gestion de risque sécurité, mesures pour assurer Intégrité et Continuité des services)
- Janvier 2013 - Réunion du CSB:
  - vérification des conditions et modalités d'exploitation ainsi que l'accès aux bases de données de l'État
  - définition des critères de sécurité - Identification des bases de données sensibles
  - définition des consignes obligatoires pour sécurisation et accès aux DB sensibles

# Initiatives liées à la Cyber Sécurité:
## **Gouvernement:** Stratégie nationale en matière de Cybersécurité

- Projet de Loi n° 6514 (approbation de la Convention sur la cybercriminalité) – décembre 2012
  - approbation de la Convention du Conseil de l'Europe sur la cybercriminalité ouverte à la signature à Budapest le 23 novembre 2001
  - approbation du Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, fait à Strasbourg le 28 janvier 2003
  - modification du Code pénal
  - modification du Code d'instruction criminelle
  - modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

# Initiatives liées à la Cyber Sécurité: Au niveau Européen

- Inauguration du Centre européen de lutte contre la cybercriminalité (EC3) – janvier 2013

- Conseil de l'Europe: Convention sur la cybercriminalité … commis par le biais de systèmes informatiques, le Comité de la Convention sur la Cybercriminalité (T-CY) et le projet sur la cybercriminalité. (http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/default_fr.asp)

- ENISA: European Network & Information Security Agency
  - Cyber Europe 2012: Exercice afin d'améliorer la résistance des infrastructures critiques d'Information
  - ENISA Threat Landscape: identify a cyber-security threat landscape – janvier 2013
  - **12/04/2013:** les fournisseurs de services Internet ne parviennent pas à mettre en place des filtres contre les grandes cyber-attaques .

# Quelques Initiatives liées à la Cyber Sécurité: Chez nos voisins

- France: ANSSI (www.ssi.gouv.fr/fr/anssi/) Agence nationale de la sécurité des systèmes d'information
  - Dépend du 1er Ministre – propose des règles pour la SSI et vérifie leur application:
    - guide de l'hygiène Informatique: préconisations techniques très précises
    - La stratégie de la France en matière de cyberdéfense et cybersécurité

- Allemagne : le BSI (www.bsi.bund.de) Bureau Fédéral pour la Sécurité de l'Information
  - Cyber Security Strategy for Germany: focus sur 10 axes stratégiques
    - National Cyber Response Centre
    - Outils pour répondre aux Cyber Attaques

- Royaume-Uni : le CESG (www.cesg.gov.uk) Communications-Electronics Security Group
  - Cyber Incident Response: schéma pilote – octobre 2012
    - Guidance: 10 Steps to Cyber Security.

# Quelques Initiatives liées à la Cyber Sécurité: Chez nos voisins

- Belgique:
  - Belgian Internet Security Conference – décembre 2012
  - B-CCENTRE (Belgian CyberCrime Centre of Excellence for training, research & education)
  - E-cops : Belgian online reporting service for crimes on or through the internet.
- Pays-Bas :
  - NCSC (National Cyber Security Centre)
  - AIVD (Algemene Inlichtingen- en Veiligheidsdienst)
- États-Unis :
  - la NSA (www.nsa.gov/ia/) Information Assurance Program
  - Le DHS (www.dhs.gov/cyber): Electronic Crimes Task Forces (ECTFs)
    - Identification et localisation des Cyber Criminels internationaux (Intrusion, fraude bancaire, vol de données, …)
  - NSC (National Security Council): identification de 10 actions à court terme pour supporter la stratégie des USA en terme de Cyber Sécurité.

telindus
belgacom ICT

# Conclusion

together with
belgacom
tango

# Les défis de demain

telindus

## Enjeux pour les Entreprises:

- Rythme élevé pour l'adoption (obligatoire) de nouvelles technologies (cloud, BYOD, …)
- Croissance des besoins métiers vis-à-vis d'Internet (dépendance).
- Risques par rapport à la Cyber Criminalité connus mais sous-estimés: peu de proactivité !
- Définition d'une Stratégie d'Entreprise: prise en compte des risques associés à la Cyber Criminalité.

## Enormément d'initiatives récentes pour contrer la Cyber Criminalité:

- Actions nationales, européennes et mondiales prises pour aider les Entreprises.
- Quelles sont les attentes des Entreprises ?
  - → Nécessité de prendre en compte le poids de ces mesures pour les Entreprises
  - → Nécessité de cohésion et de consolidation de ces actions / initiatives !
  - → Nécessité d'être proactif – « Si vis pacem, para bellum !!!»

telindus
belgacom ICT

# Merci pour votre attention.

together with
belgacom
tango

telindus
belgacom ICT
Questions /Réponses ?

together with
belgacom
tango