
internet fraude
databreach
gijzelen gegevens
DDoS aanval
hacking acount
social engineering
digitale afpersing
spam
waterholing
defacement
phishing
CYBERCRIME
organised crime
state sponsored
digitale fraude
cybersabotage
cyberspionage
APT
malware
overname systeem
exploit
online banking fraude
phreaking
infiltratie systeem
blokkeren systeem

# ACTUEEL?


Bedreiging/smaad/laster
Burgeropsporing Cybercrime
Discriminatie/racisme Fraude
internetoplichting illegale
handel Internetgokken
Kinderporno/zeden
/grooming Open bronnen
Politie op het web
profielsites Terrorisme/jihadisme
Tweepuntnul Uncategorized

http://copsincyberspace.wordpress.com/

# ACTUEEL?


Politie
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.
Prepaid4me
Prepaid4me - Acheter Ukash avec Bancontact / Mr. Cash.
Également disponible auprès de votre revendeur:
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.
OK

# ACTUEEL?

## Bedrijven beseffen ernst van cybercriminaliteit


do 28/08/2014 - 17:24 Thomas Cruysberghs (redacteur StampMedia)

De ernst van cybercriminaliteit lijkt langzaam door te sijpelen bij Belgische bedrijven en organisaties. Nu er steeds meer gevallen van hacking bij belangrijke bedrijven aan het licht komen, dringt de veiligheidskwestie zich op. Ook de Belgische overheid heeft haar inspanningen opgedreven.

Bron: deredactie.be

# ACTUEEL?

## Gerecht onderzoekt cyberspionage bij Belgische topbedrijven


**Het federaal parket onderzoekt na de grote computerhacking bij Belgacom nog andere gevallen van cyberspionage bij Belgische topbedrijven. 'Deze vakantie hebben we nog een vijftal andere dossiers geopend over grootschalige hackings bij belangrijke bedrijven in België', bevestigt de woordvoerder van het federaal parket, Eric Van Der Sypt, aan De Tijd. 'Ook in deze dossiers zijn er vermoedens van 'staatsspionage'.'**

Bron: De Tijd – 26/08/2014

# Actueel?

EDWARD SNOWDEN

13/09/2014

## NSA en GCHQ hebben toegang tot netwerk Deutsche Telekom

NIEUWS > BEDRIJVEN

De Amerikaanse veiligheidsdienst NSA en haar Britse tegenhanger GCHQ beschikken over geheime toegang tot het netwerk van verschillende Duitse telefoonoperatoren. Dat schrijft het weekb...


06/07/2014

## Negen op tien door NSA geviseerde internetgebruikers zijn gewone mensen

NIEUWS > BUITENLAND

Negen op tien mensen in wiens intercommunicatie de Amerikaanse geheime dienst NSA heeft geneusd, zijn gewone onschuldige burgers, zo heeft de krant Washington Post bericht op basis van...


02/07/2014

## 'Prism-spionageprogramma van NSA is wettelijk'

NIEUWS > BUITENLAND

Het Amerikaanse spionageprogramma "Prism", waarmee de e-mails en internetactiviteiten van buitenlandse terreurverdachten worden onderschept, is legaal en nuttig in de strijd tegen het ...

Bron: De Standaard

# ACTUEEL?

01/09/14, 06u30 – Bron: Belga

© thinkstock.

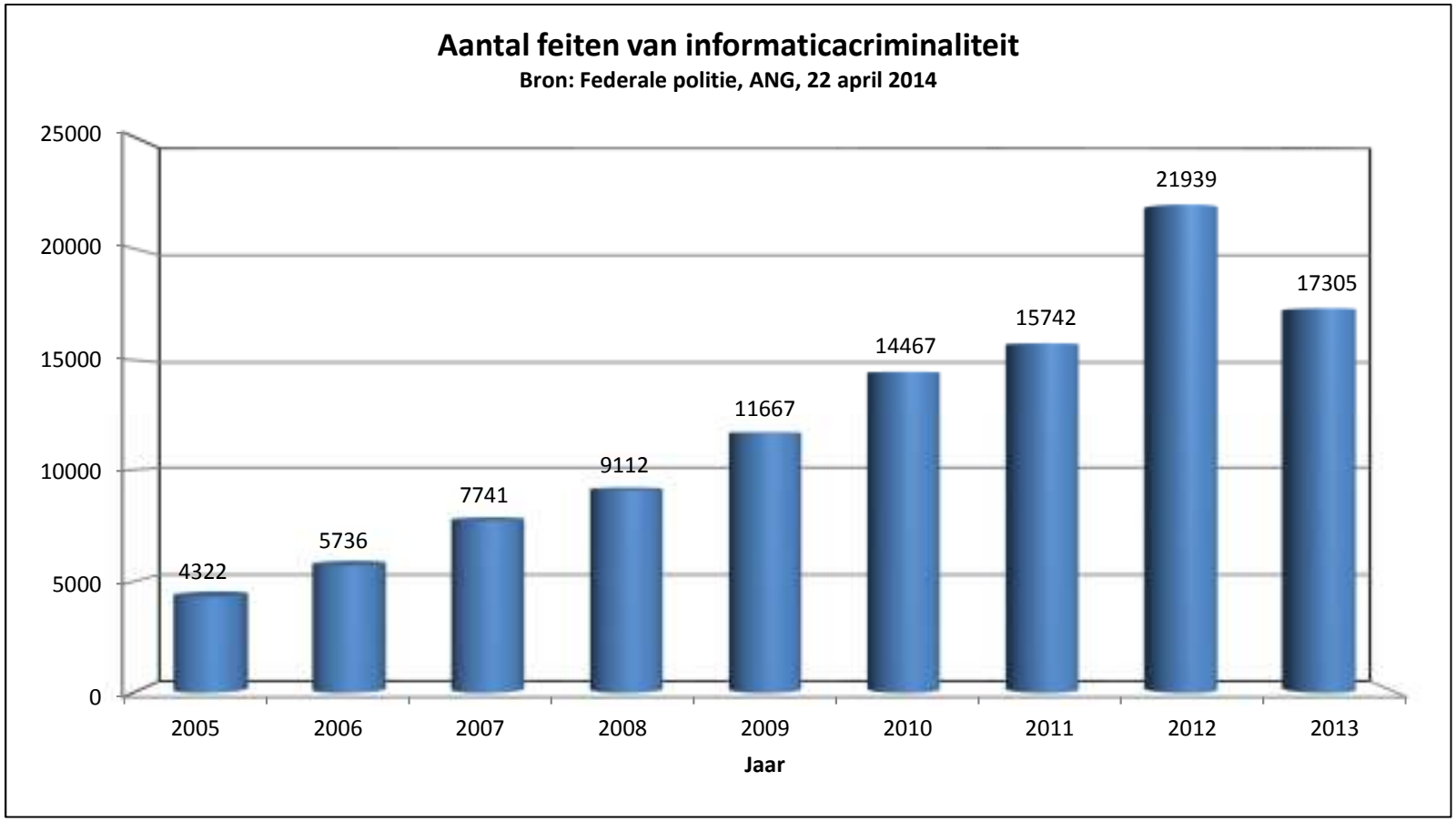
## Netwerk van sensoren tegen cyberspionage

**Er komt een centraal netwerk van sensoren dat de internettrafiek bij de overheid scant om cyberspionage te voorkomen. Dat schrijft De Standaard vandaag.**

Een strengere beveiliging van het internetverkeer van de overheid drong zich op na verschillende hackings. Zo konden Russische spionnen het netwerk van de federale overheidsdienst Buitenlandse Zaken hacken. De zaak kwam bovendien pas aan het licht na een tip van de Amerikaanse inlichtingendienst CIA.

Bron: Dmorgen,be – 01/09/2014

# Cijfers informaticacriminaliteit



# DARK NUMBER

## Hacking: zeer groot Dark Number
## → 8 op 10 slachtoffer doet geen aangifte!

- Bedrijven: 94% (2012) →85 % (2014)
- Particulieren: 98 % (2014)

## Fenomeen Cybercrime steeds meer zichtbaar

- Pers: bijna dagelijks over slachtoffers cybercrime
- Criminelen: naast financiële, steeds meer gedreven door politieke en ideologische motieven

# TRENDS

## Trend in cybercrime

- Meer gerichte aanvallen waarbij targets steeds belangrijker worden
- Meer gevallen van cyberspionage met infiltratie in verschillende overheidsdiensten en –bedrijven
- cybercriminaliteit op hoog niveau, die een gecoördineerde en efficiënte aanpak vereist.

## Algemene trend → Evolutie naar e-maatschappij meer risico's!

- stijging ICT-afhankelijkheid: personen vervangen door e-applicaties –
- interconnectiviteit tussen systemen - Internet of Things
- mobiele systemen – cloud
- sociale netwerken

# MOTIEVEN

## Financiële motieven

- Digitale afpersing en fraude
- Ransomwarevirus, hacking Rex Mundi, online banking fraude..

## Politieke, ideologische motieven

- Vooral spionage en sabotage om hun doel te bereiken.
- Hacktivisme: vooral in defacements.
- Cyberspionage door overheidsinstanties of state sponsored cybercrime
  - Kan enorme proporties aannemen
  - Vereist inspanning van verschillende specialisten
  - Is op maat gemaakt

# MOTIEVEN

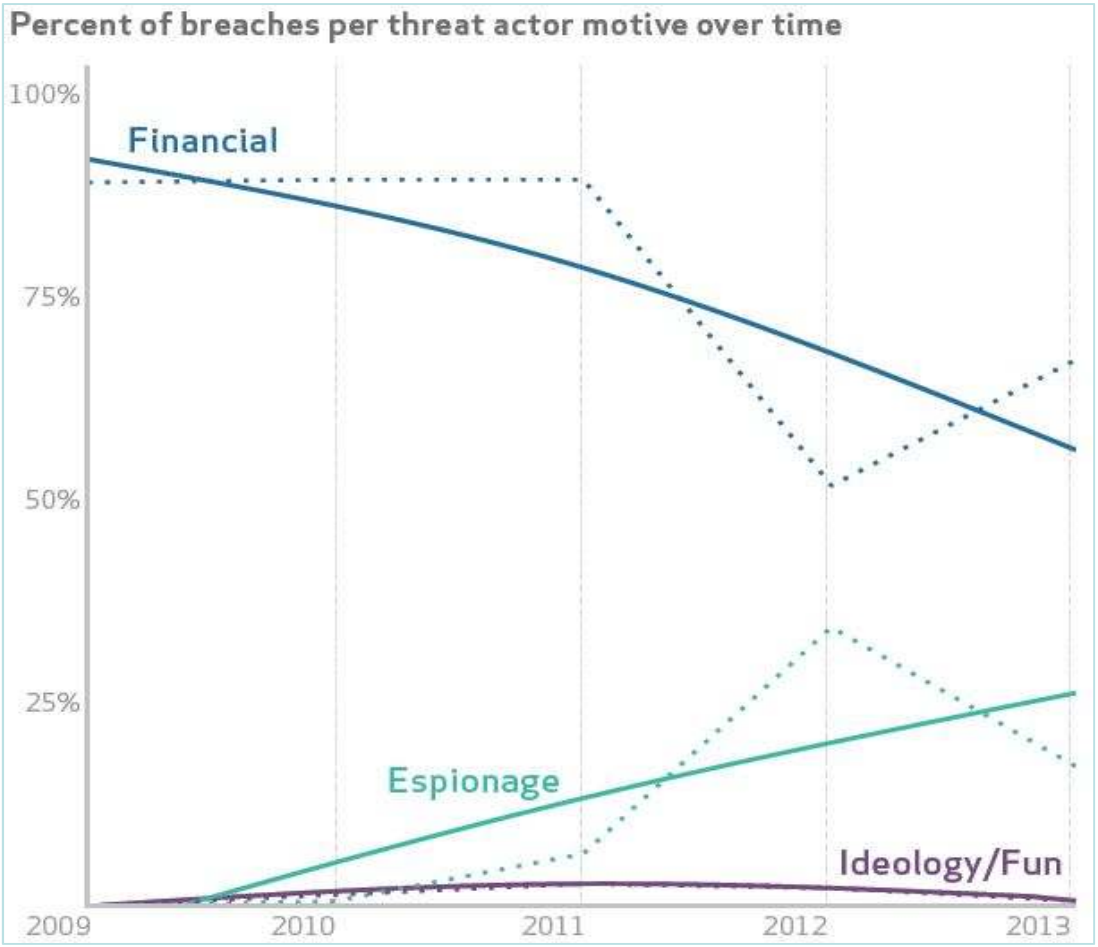
## Persoonlijke motieven

- vaak gelegenheidshackers die een hacking plegen
- Schade toebrengen, uitdaging, plezier, interne hacking

## Gevaarlijke evolutie

- Toename APT door organised crime (ipv state sponsored)
- Gevaarlijker! → evolutie van spionage naar sabotage

# MOTIEVEN




Verizon, *2014 Data Breach Investigations Report*, 2014, 9, http://www.verizonenterprise.com/DBIR/2014/ (22 augustus 2014).

# BEWUSTWORDING

## Bewustwording aan de gang maar nog niet voldoende!



# PREVENTIEVE TIPS

## Stel algemene ICT gebruiksrichtlijn op

- ICT beveiligingsbeleid als onderdeel globaal veiligheidsbeleid

## Stel ICT veiligheidsverantwoordelijke aan

- Bewustmaking & controle van de toepassing

## Bereid ICT-incidentendossier voor met :

- plan van architectuur/ toepassingen/ databanken/ interconnecties
- Namen / tel / gsm van verantwoordelijke systeem /DB/toep
- Namen+ tel / gsm leveranciers HW / SW / Maintenance/BU
- Tel Cert.be
- Tel + permanentienummer FCCU

# PREVENTIEVE TIPS

- Wees duidelijk in outsourcing van maintenance
  → rapportering van alle interventies op afstand
- Scherm bedrijfskritische systemen/ toepassingen / data af van op Internet aangesloten netwerken !
- Installeer recente Antivirus ; Firewall en actualiseer
- Synchroniseer de systeemklokregelmatig
- Activeer en controleer loggings IN en OUT
- Voer audits uit op loggings
- Maak en test backups en bewaar ze veilig !

# VERMOEDEN VAN FRAUDE

**Wettelijk werken – respect wetten & CAO 81**

- Finaliteit (misdrijven, econ & fin belang, ICT veiligheid, gebruikersregels)
- Proportionaliteit (minimale inbreuk op privacy, in fases)
- Transparantie (op basis van duidelijke policy)

**Diagnose stellen / oorzaak & sporen vinden**

**Bewijsmateriaal integer bewaren**

- Integraal, ongewijzigd met garantie

**Noodzaak om specialisten in te schakelen**

- Zeker van klacht → politie
- Zo niet → Cert.be / forensisch ICT auditor

# SLACHTOFFER ICT-CRIME

## Bij ontvangst dreigingen

- reageer snel… maar niet naar afperser
- bewaar berichten in originele (digitale vorm)
  → contact politie

## Bij effectieve incidenten:

- Verbreek verbinding (indien niet door aanvaller veroorzaakt)
- Log max. info inzake laatste ICT activiteit/tijdstip
- Vermijd actie op het systeem (sporen aanvaller)
- beveilig fysiek het systeem
- beperk de interne communicatie tot noodzakelijke
- Dien klacht in bij politie of parket …

# SLACHTOFFER ICT-CRIME

## Voor incidentafhandeling

- Bereken schade : direct en indirecte
- Evalueer: schade belangrijker dan heropstart?
  - Heropstart belangrijk
    - ✓ Plaats reserve systeem online
    - ✓ Of minimaal : maak full backup vóór herinstallatie
  - Schade belangrijker : laat situatie onaangeroerd

## Bij heropstarten

- Wijzig alle paswoorden en liefst ook gebruikersnamen
- Pas opnieuw verbinden als alle oorzaken verholpen

# POLITIE?

| Geïntegreerde politie | | | | | |
|---|---|---|---|---|---|
| **Federale politie**<br>Nationaal<br><br>31 personen | **Federal Computer Crime Unit**<br>24/7 (inter)nationaal contactpunt<br>autonome onderzoeken kritieke ICT-infrastructuur | | | | |
| | Management Team | Intelligence Team | Tactical Team | Technical Team | Support Team (o.a. logistiek, training) |
| **Federale politie**<br>Regionaal<br><br>212 personen | **13 Regionale Computer Crime Units** | | | | |
| | Bijstand bij huiszoekingen, forensische analyse van ICT-materiaal, internetrecherche | | Onderzoek van cybercrime cases (met bijstand van FCCU) | | |
| **Lokale politie** | **Eerstelijnspolitie** | | | | |
| | 'Bevriezen van de situatie'<br>Selecteren en bewaren van digitaal bewijs<br>Netwerk First responders | | | | |

# Waar klacht indienen?

- **Lokale politie**
  - → Niet juiste plaats voor ICT-crime (hacking/sabotage/spionage)
  - → Wel geschikt voor klachten internetoplichting/-fraude

- **Federale gerechtelijke politie (FGP)**
  - → beter, maar…→ Regional CCU: juiste plaats voor ICT crime

- **Federale Computer Crime Unit**
  - → 24/7 contact
  - → Bij gevaar voor vitale of kritieke infrastructuur => dringend!

- **Magistraten ?**
  - →Lokaal parket (Procureur): zendt het naar de politie / kan beslissen niet te vervolgen
  - → Onderzoeksrechter : klacht met burgerlijke partijstelling (borg) verplichting om te onderzoeken

# VRAGEN?