
Hackers zijn geen tovenaars

“War stories” over digitale
inbraak & risicobeheersing

Mark Koek

m.koek@hackdefense.nl

15-Nov-2017

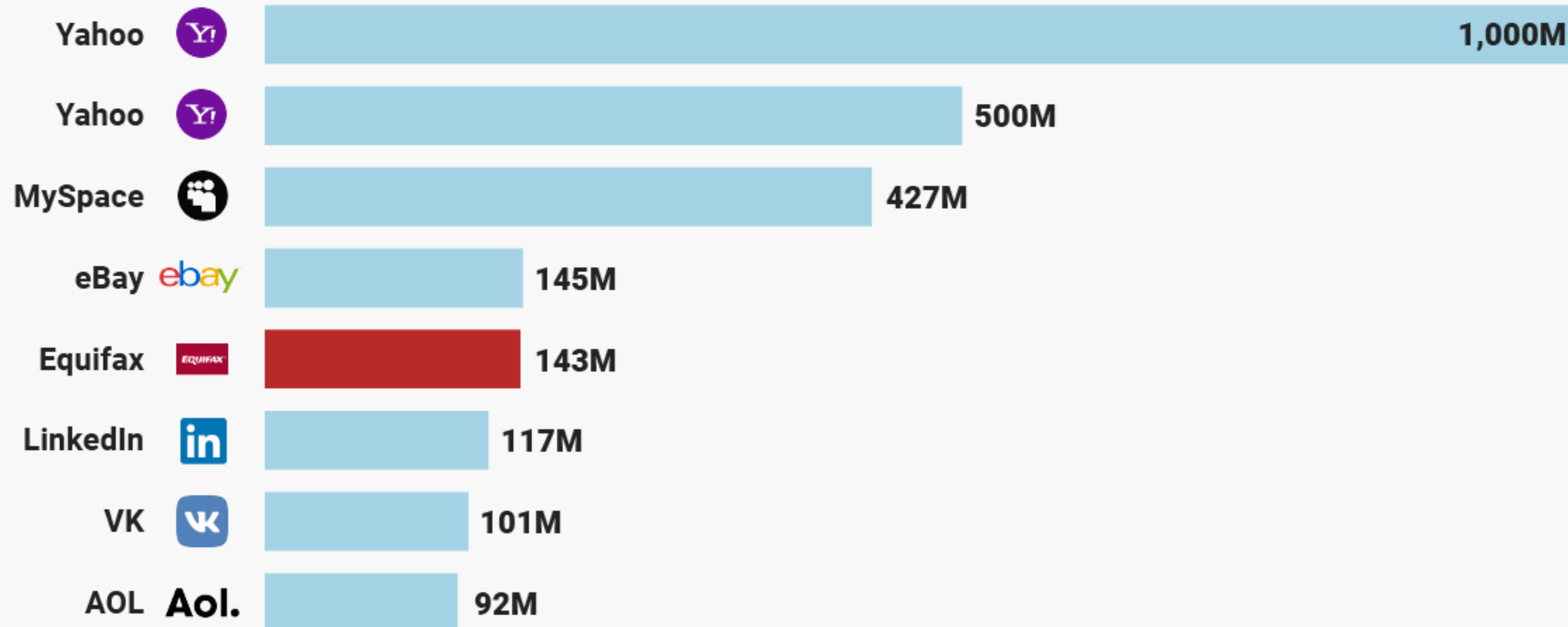
Datalekken aan de orde van de dag

SPAMMERS CAN STEAL ENTIRE IDENTITIES

SPEAR phishing takes place when a spammer has a name and email address for a target they know has ties to a particular website or brand. They will send out phishing emails

identity and access shopping and bank accounts. Often the spam will come with an attachment. Clicking on it will automatically download some malicious software

LATEST EQUIFAX HACK COULD BE THE WORST TO DATE



dinsdag 12 april 2016

Verontrusting na gelekte info

'Moet de he' stad zich zorgen maken of maar een gedeelte?'

Amersfoort

donderdag 13 april 2016

Datalek lang toegedekt

ambtenaren verzwegen blunder voor wethouder

Meerda
Jeruzal
verbouw

van 15000 mensen op straat

Internetbedrijf failliet

Einde e-tuinmeubelen door boete datalek

Liebedrijf failliet door boete CBP

€450.000 voor datalek

Boete CBP betekent
einde tuinmeubelgigant

Overtreding meldplicht datalekken
kost internetonderneming de kop

DEN HAAG, 18 november 2015
Voor de datalek die enkele weken geleden aan het licht kwam
heeft het bedrijf e-tuinmeubelen.nl een boete gekregen van



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

[pwned?](#)


251
pwned websites

4,818,883,599
pwned accounts

57,148
pastes

54,792,698
paste accounts

Top 10 breaches

 711,477,622 [Onliner Spambot accounts](#)







Wie zijn die hackers dan?

- Kwaadaardige hackers zijn:
 - 4% vandalen
 - 1% activisten
 - 0,01% “state actors”
 - 95% handelaren op een wereldwijde zwarte markt
- En er zijn natuurlijk *ethische* of *white hat* hackers

THE GLOBAL BLACK MARKET PRICES
These are some of your personal data and their corresponding prices:



BRAZILIAN UNDERGROUND

Set of business application account credentials	US\$155-193
Set of credit card credentials	US\$35-135
Set of online service account credentials	US\$19
List of mobile phone numbers	US\$290-1,236
List of landline phone numbers	US\$317-1,931

Naar een volwassen benadering

- Risicobeheersing
 - Begint met kennen van de risico's
- *Preventie*
- *Detectie*
- *Response*
- *Recovery*

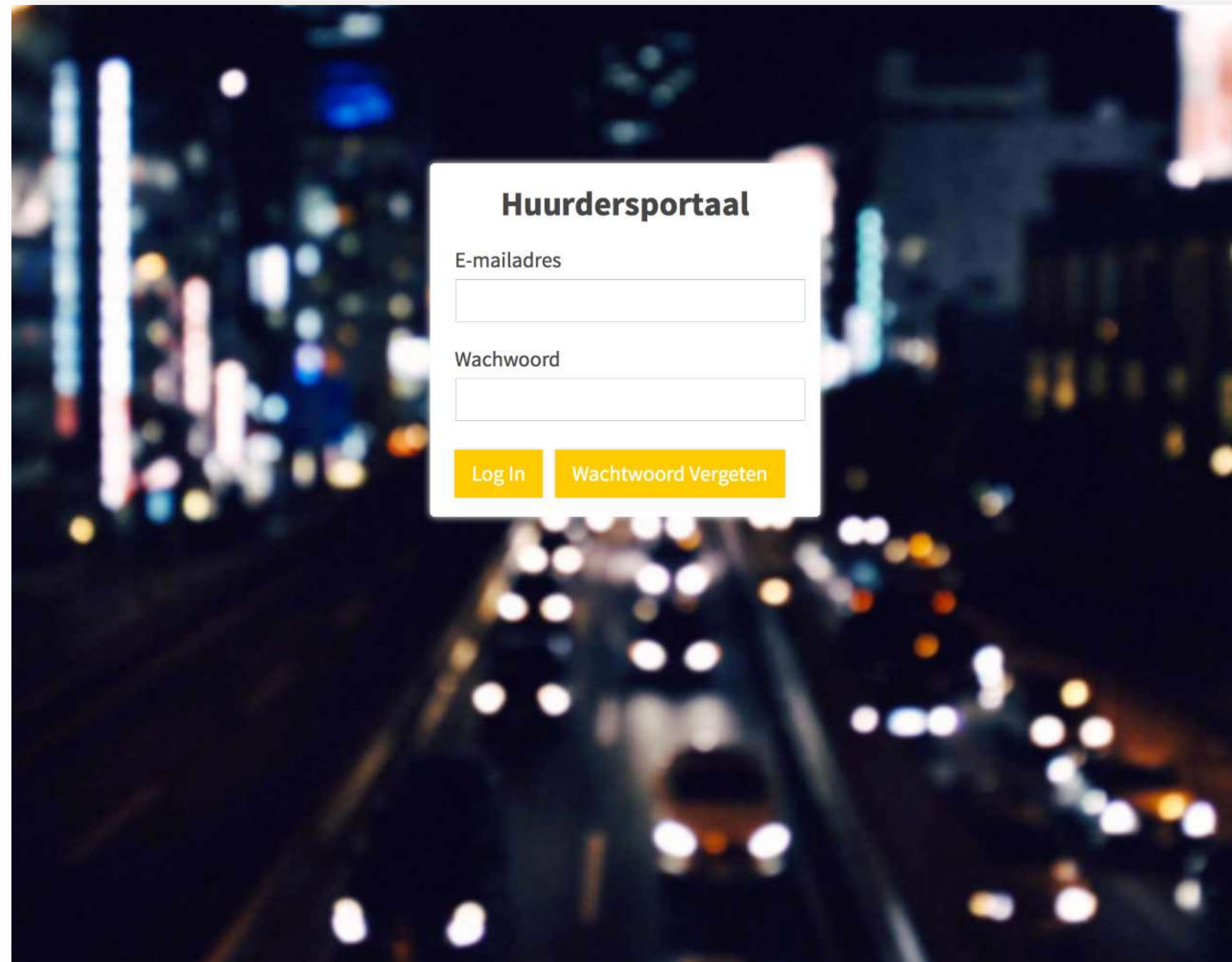


Preventie

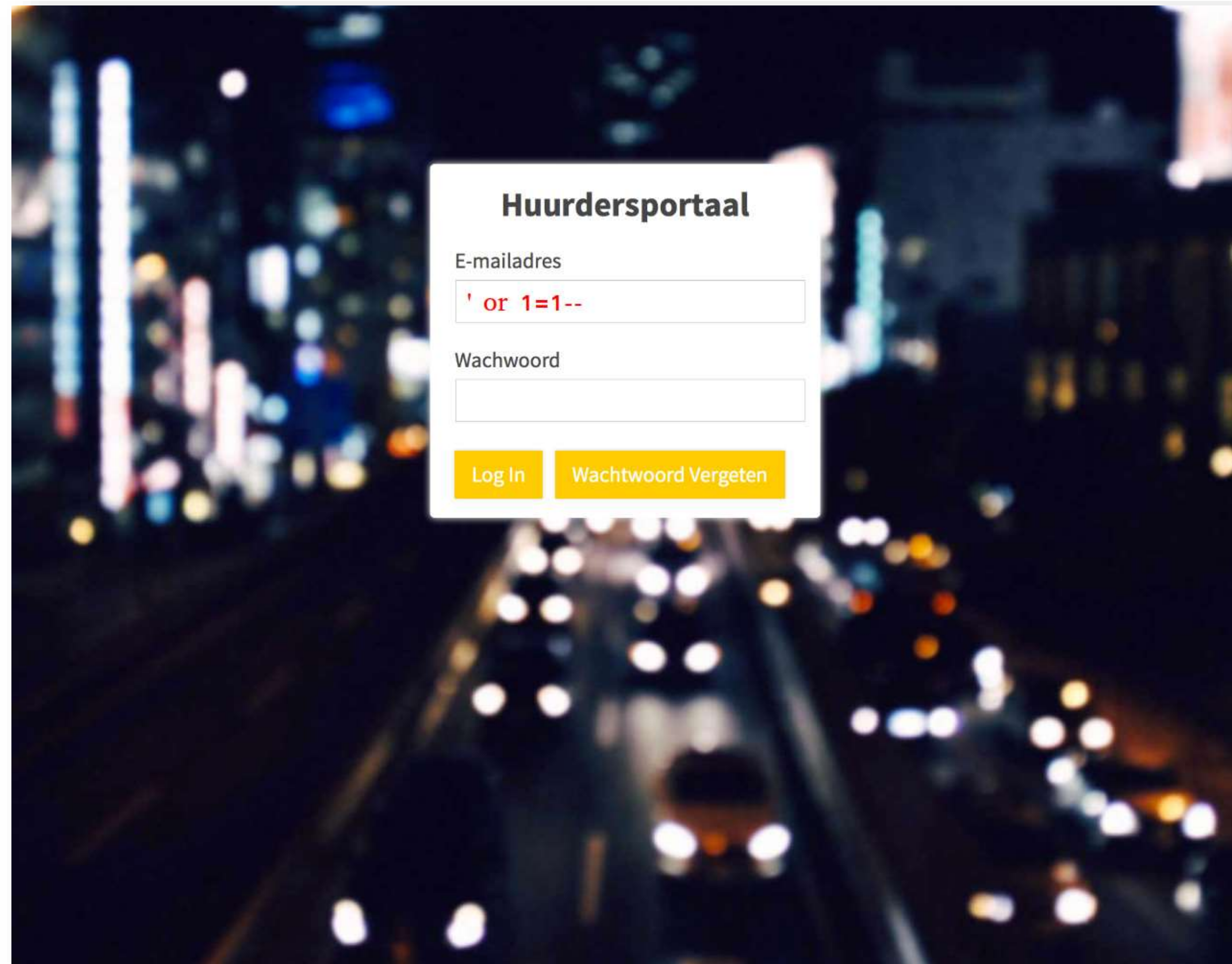
- Wat zijn de oorzaken van digitale inbraken?
 - Fouten in software
 - Misplaatst vertrouwen
 - Fouten in IT-infrastructuur
 - Fouten in technisch beheer
 - Fouten in functioneel beheer
- Niet: BLUNDERS!!!!1!



Ingang 1: uw software aan het internet



Ingang 1: uw software aan het internet



Is het echt zo eenvoudig?

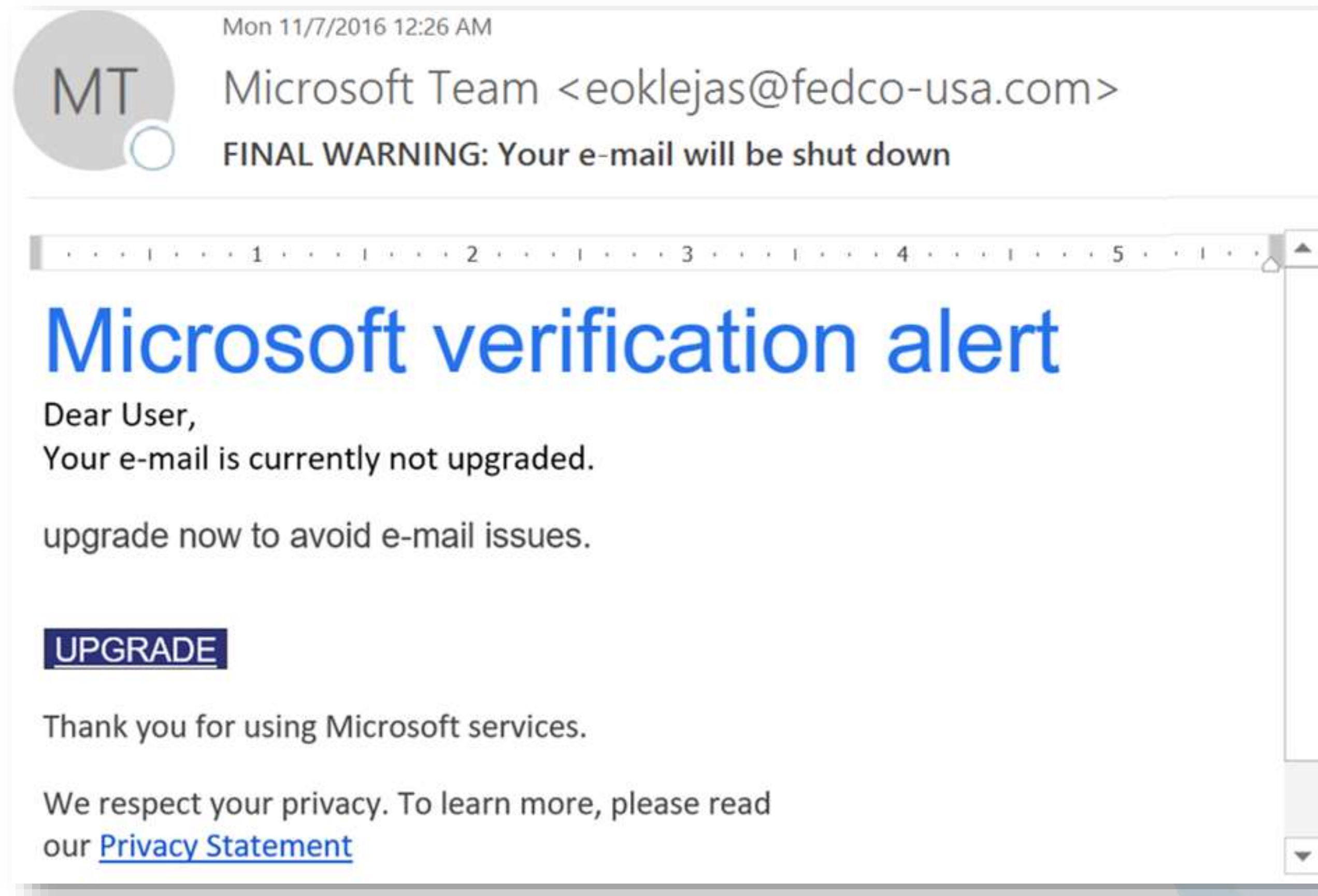
- Vaak wel...
- Kwaliteit van software is evenredig aan
 - Financiën
 - Tijdsdruk
 - Specificaties
- **Opdrachtgeverschap!**
 - Software wordt geleverd zoals gevraagd
 - Vaak worden alleen functionele eisen gesteld
 - Of onmeetbaar: “*de software moet veilig zijn*”

Meer software security war stories

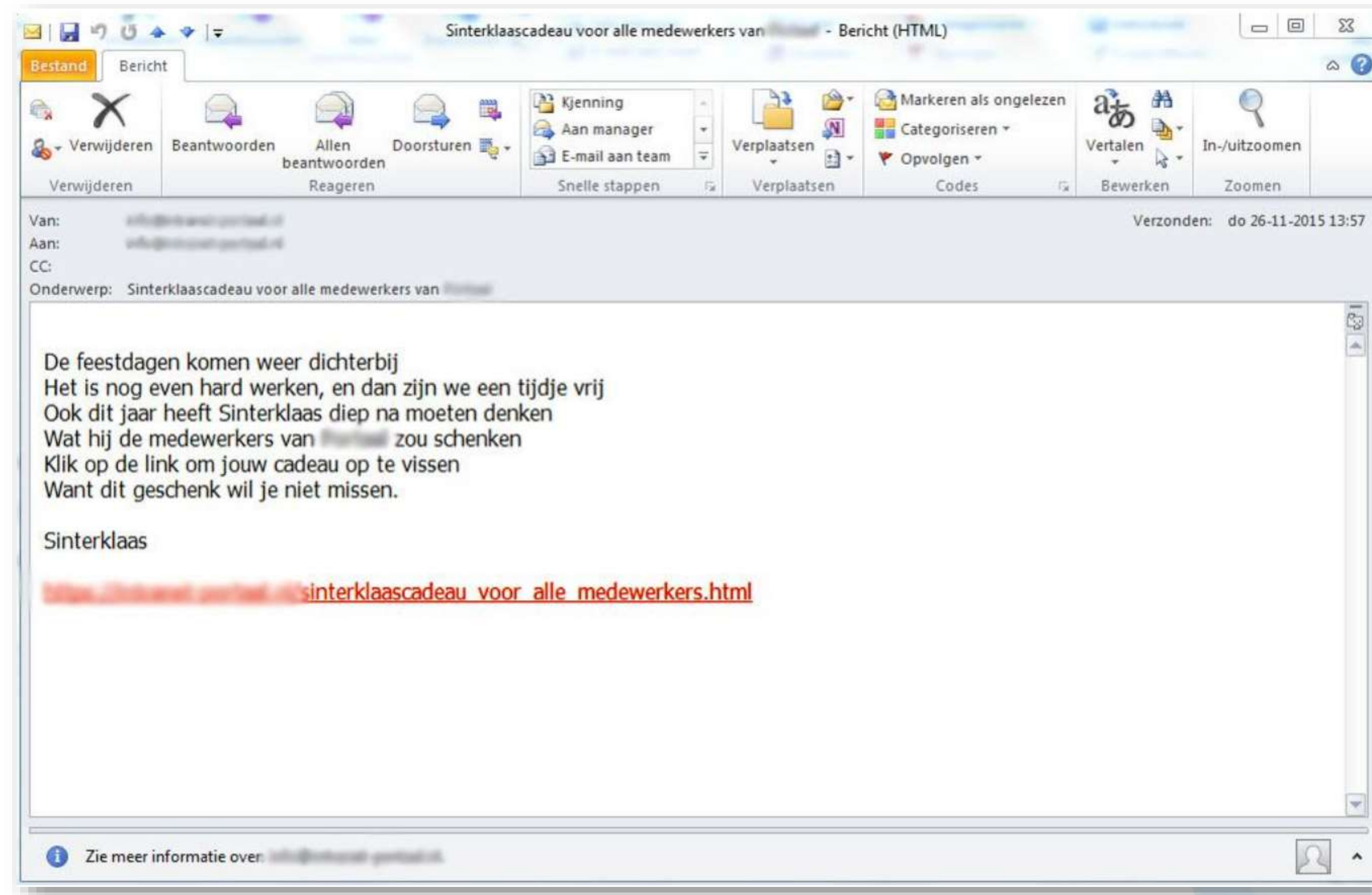
- €-100.00
- Android-app die medische gegevens op SD-kaart schrijft
- Subtiel

```
if ( (options == (__WCLONE | __WALL) ) &&  
    (current->uid = 0) )  
    retval = -EINVAL;
```


Ingang 2: Misplaatst vertrouwen



Ingang 2: Misplaatst vertrouwen

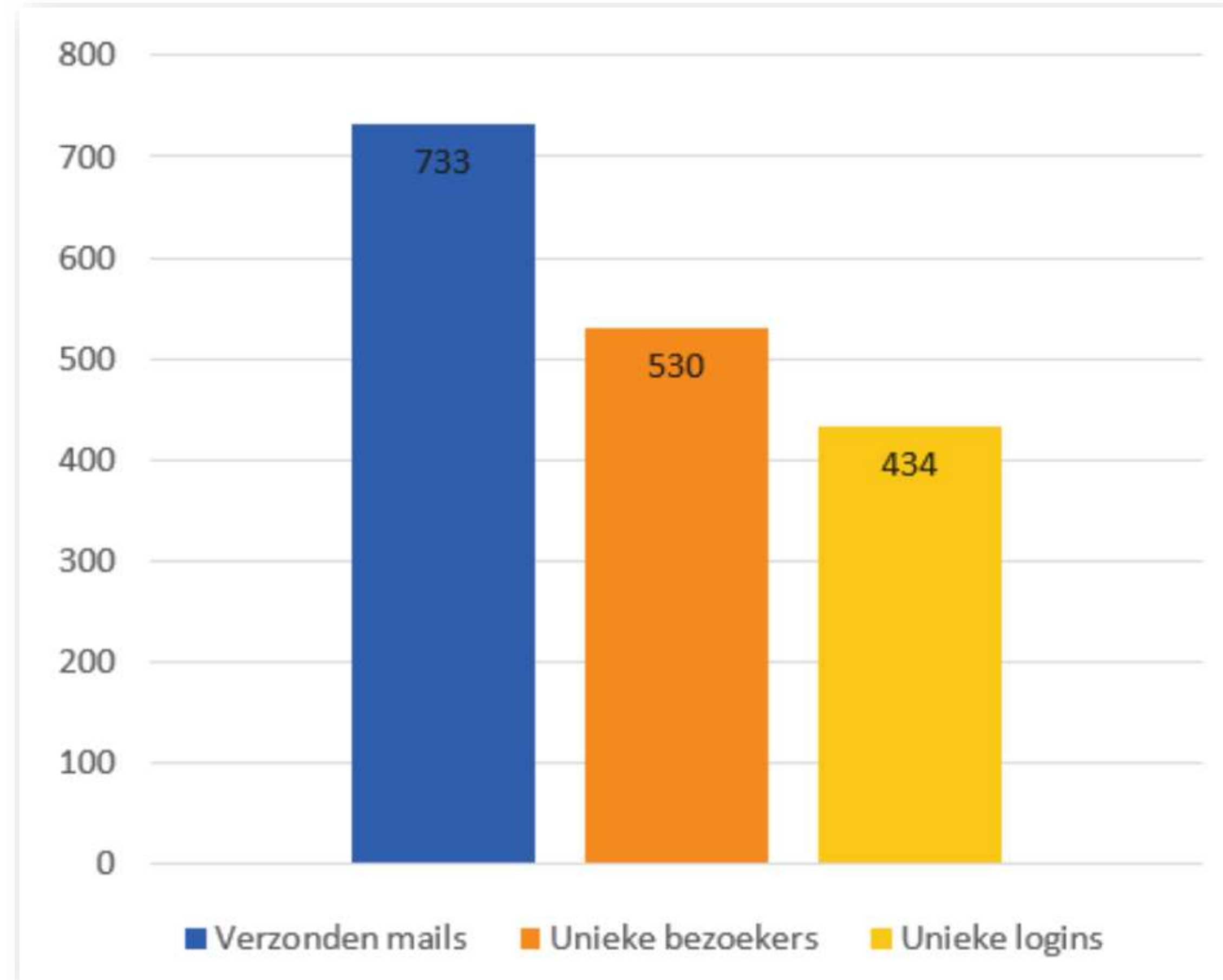


Bron:



PHISHINGTEST.NL

Ingang 2: Misplaatst vertrouwen



Bron:



PHISHINGTEST.NL

Ingang 2: Misplaatst vertrouwen

- Hoge percentages:
 - Klikken
 - Geven hun wachtwoord af
 - Installeren software van het internet op de werkplek
- De verzender van de nepmail kan nu wat de medewerker kan
 - En medewerkers kunnen vaak veel teveel in een netwerk

Ingang 3: fouten in IT-infrastructuur

- Beheerschermen van UPS benaderbaar via het internet
- Toegang tot bestandssysteem van de firewall
- Meerdere vertrouwensdomeinen binnen hetzelfde Windows domain

Ingang 4/5: fouten in beheer

- Klassieker: niet patchen, of 2x per jaar
- Autorisatiebeheer
- Rechten voor iedereen



Detectie



Response

- iets doen met de output van detectie-systemen
- We hebben een inbraak. Wat nu?



Oplossingen - preventie

- PLAN
 - In kaart brengen assets, risico's en maatregelen
- ACT
 - Maatregelen laten aansluiten op risico's
- CHECK
 - Auditing & *penetration testing*
- ACT
 - Opvolgen aanbevelingen

Oplossingen - detectie

- Security Monitoring
- Meer dan SIEM / log watching
- Intrusion Detection
- Zeer specialistisch werk
- Niet goedkoop maar heel belangrijk
- 100% preventie is onmogelijk, er zullen incidenten zijn
- Er snel bij zijn redt levens

Oplossingen - response

- Plannen & procedures
- Contacten & netwerken
- Technische voorbereiding
 - *Forensic readiness*
- Organisatorische voorbereiding
 - Wie mag wat

The logo for CERT (Computer Emergency Response Team) features a blue arc above the word "CERT" in bold black capital letters.

CERT

The logo for FIRST (Forum of Incident Response and Team Leaders) features a black swoosh above the word "FIRST" in bold green capital letters, with a small orange square above the "I". Below "FIRST" is the tagline "Improving Security Together" in orange. A trademark symbol (TM) is at the end of "FIRST".

FIRSTTM
Improving Security Together

Oplossingen - recovery

- Herstel na een incident
- Leer lessen om herhaling te voorkomen
- “Never waste a good crisis”

De meeste beveiligingsmaatregelen komen tot stand naar aanleiding van beveiligingsincidenten

Famous last words

- “We hebben toch een firewall? Die houdt toch hackers tegen?”
- Idem: virusscanner
- “IT moet gewoon zorgen dat het veilig is”
 - Problemen daarmee:
 - Medewerkers voelen zich niet medeverantwoordelijk
 - IT wil van nature graag snel & tegen lage kosten opleveren
 - Beveiliging kost tijd en geld en is onzichtbaar als het goed gebeurt

Tot slot (1)

- Er is een financieel motief om data te stelen
- Er is gelegenheid
 - Mensen maken fouten
 - Budgetten zijn beperkt
- Pakkans is klein
- Dus er zijn duizenden mensen op de wereld bereid en in staat om het beperkte risico te nemen

Tot slot (2)

- Hackers zijn geen tovenaars
- Met slimme maatregelen is het risico beheersbaar
- Een lek of inbraak is ook geen “blunder”
- Waar gewerkt wordt, worden fouten gemaakt
- Neem slimme maatregelen op basis van *risk management*
 - Wat zijn de grootste risico's qua kans en qua impact?
- Wees erop voorbereid dat het toch kan misgaan

Vragen / opmerkingen / ...

Mark Koek

m.koek@hackdefense.nl

(071) 204 01 01

