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

';--have i been pwned?

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

email address or username pwned?

251	4,818,883,599	57,148	54,792,698
pwned websites	pwned accounts	pastes	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

Naar een volwassen benadering

- Risicobeheersing
  - Begint met kennen van de risico’s

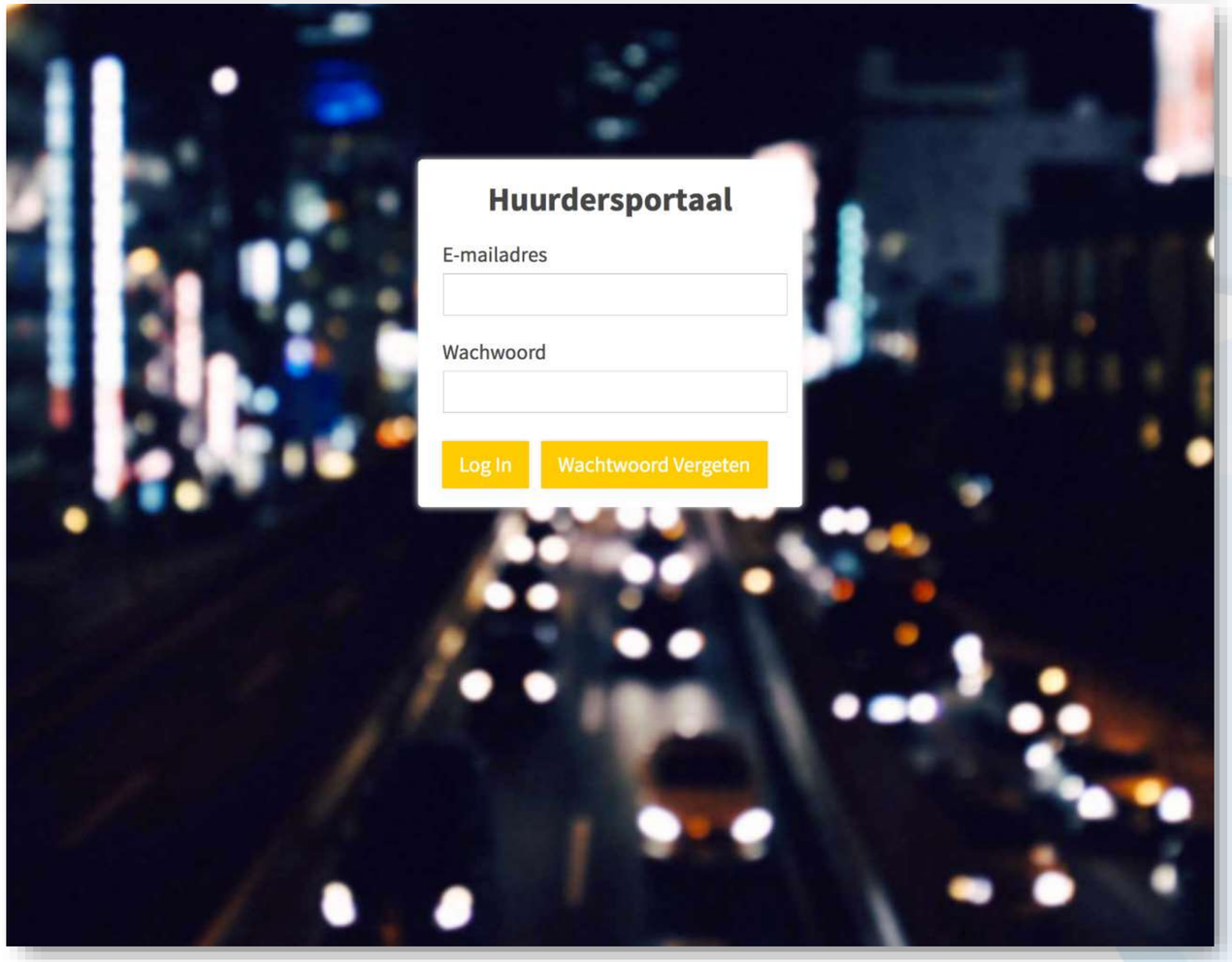
- *Preventie*
- *Detectie*
- *Response*
- *Recovery*

Preventie

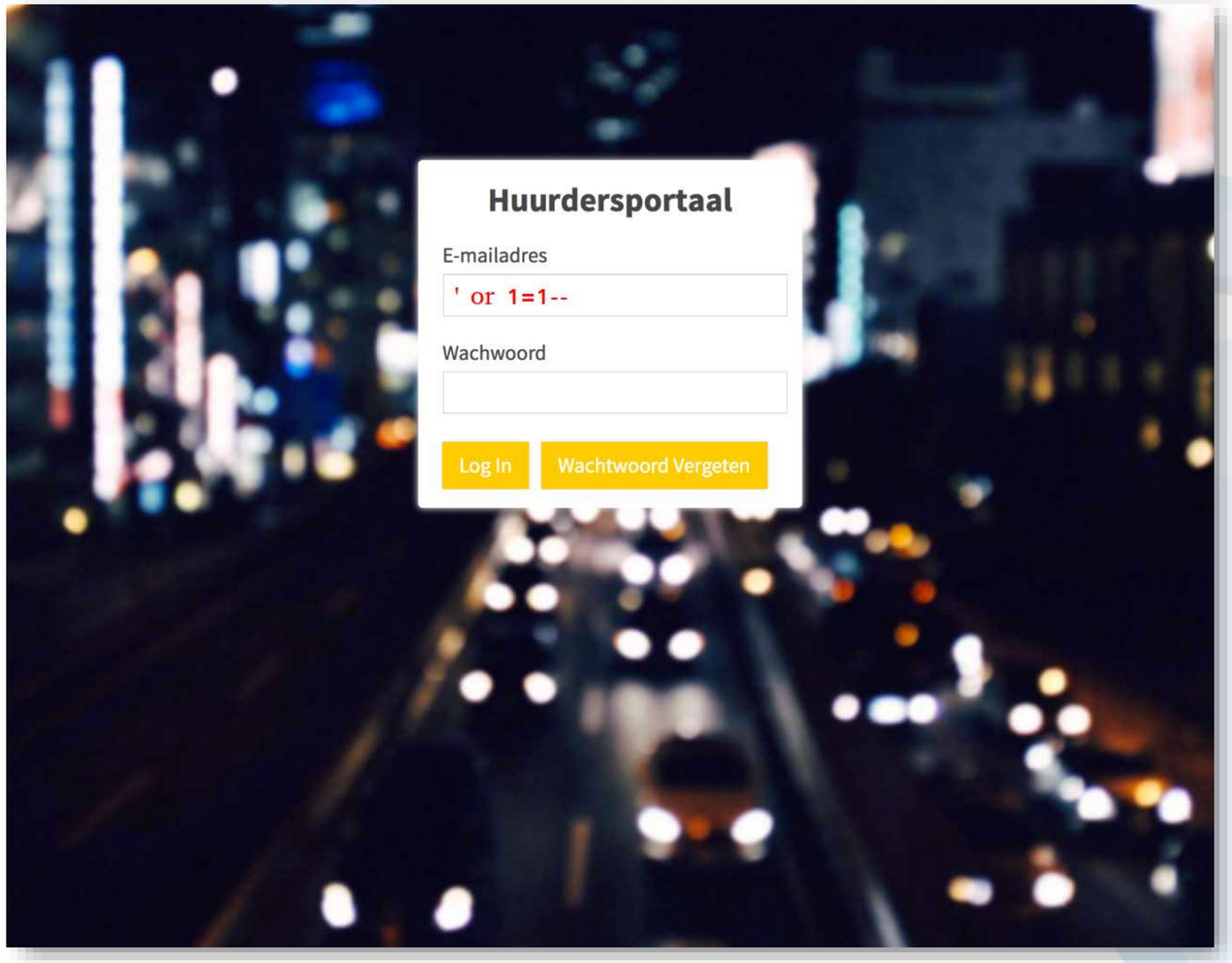
- Wat zijn de oorzaken van digitale inbraken?
  - Fouten in software
  - Misplaatst vertrouwen
  - Fouten in IT-infrastructuur
  - Fouten in technisch beheer
  - Fouten in functioneel beheer

- Niet: BLUNDERS!!!!1!

Ingang 1: uw software aan het internet



Ingang 1: uw software aan het internet



Is het echt zo eenvoudig?

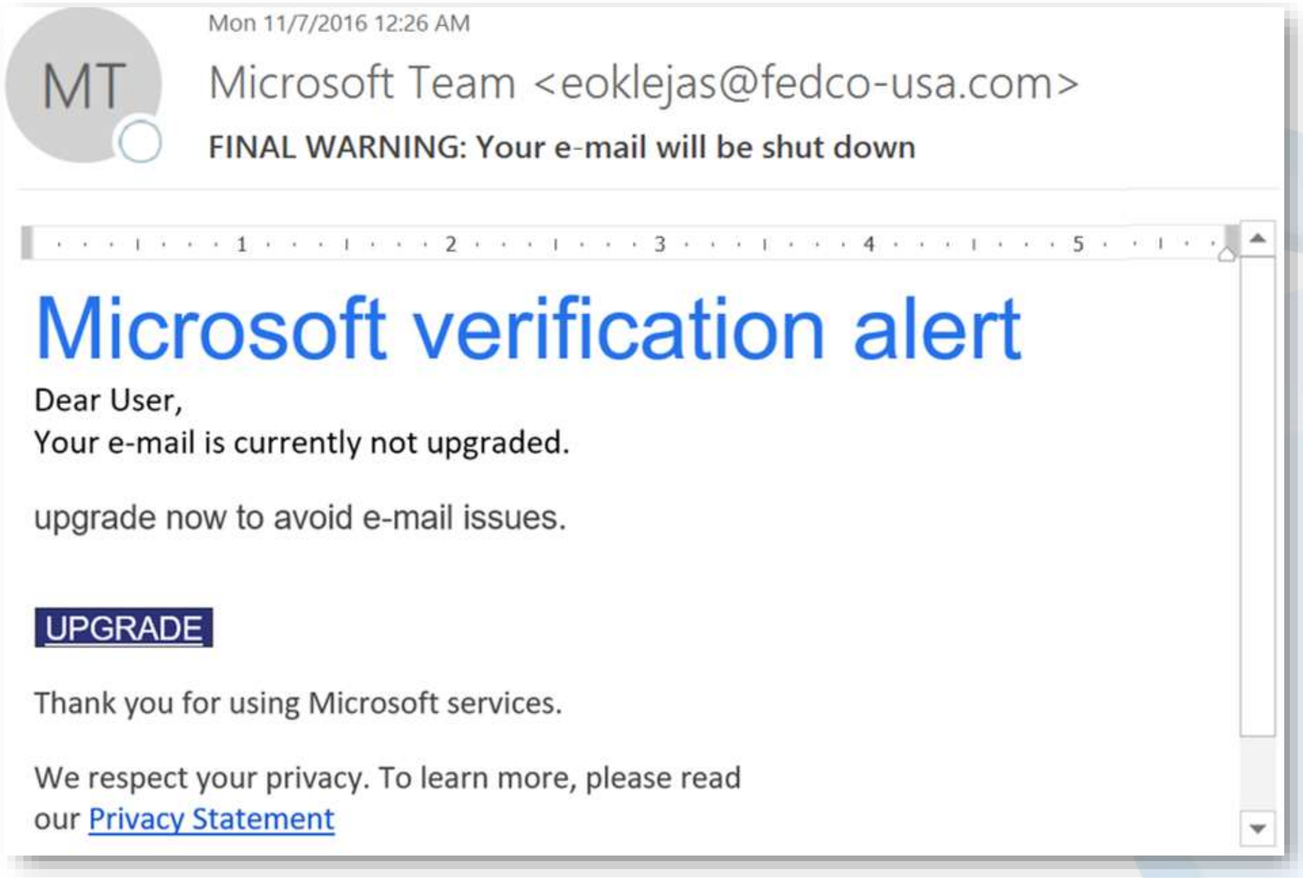
- Vaak wel…
- Kwaliteit van software is evenredig aan
  - Financiën
  - Tijdsdruk
  - Specificaties
- Opdrachtgeverschap!
  - Software wordt geleverd zoals gevraagd
  - Vaak worden alleen functionele eisen gesteld
  - Of onmeetbaar: “*de software moet veilig zijn*”

Meer software security war stories

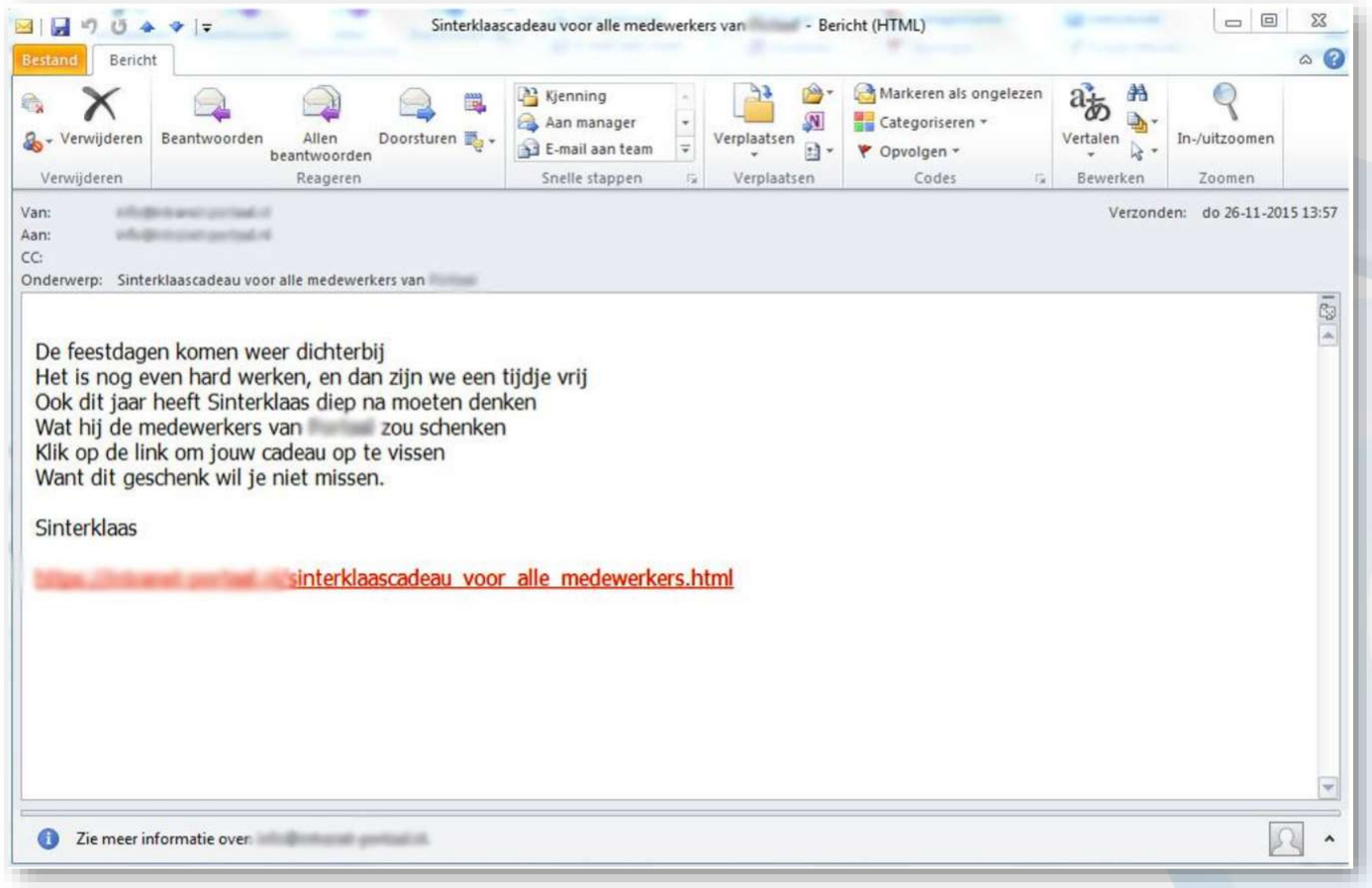
- €-100.00
- Android-app die medische gegevens op SD-kaart schrijft
- Subtiel

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

Ingang 2: Misplaatst vertrouwen



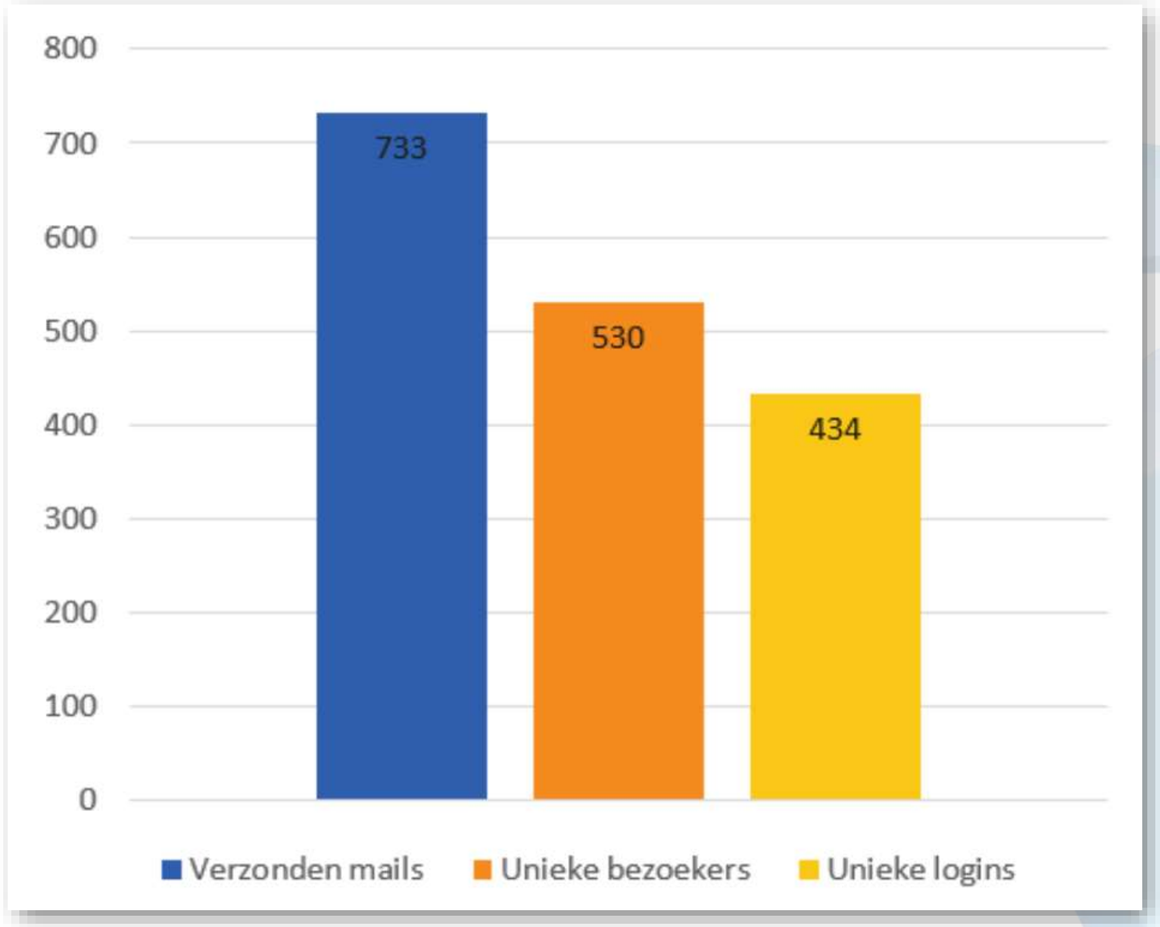
Ingang 2: Misplaatst vertrouwen



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

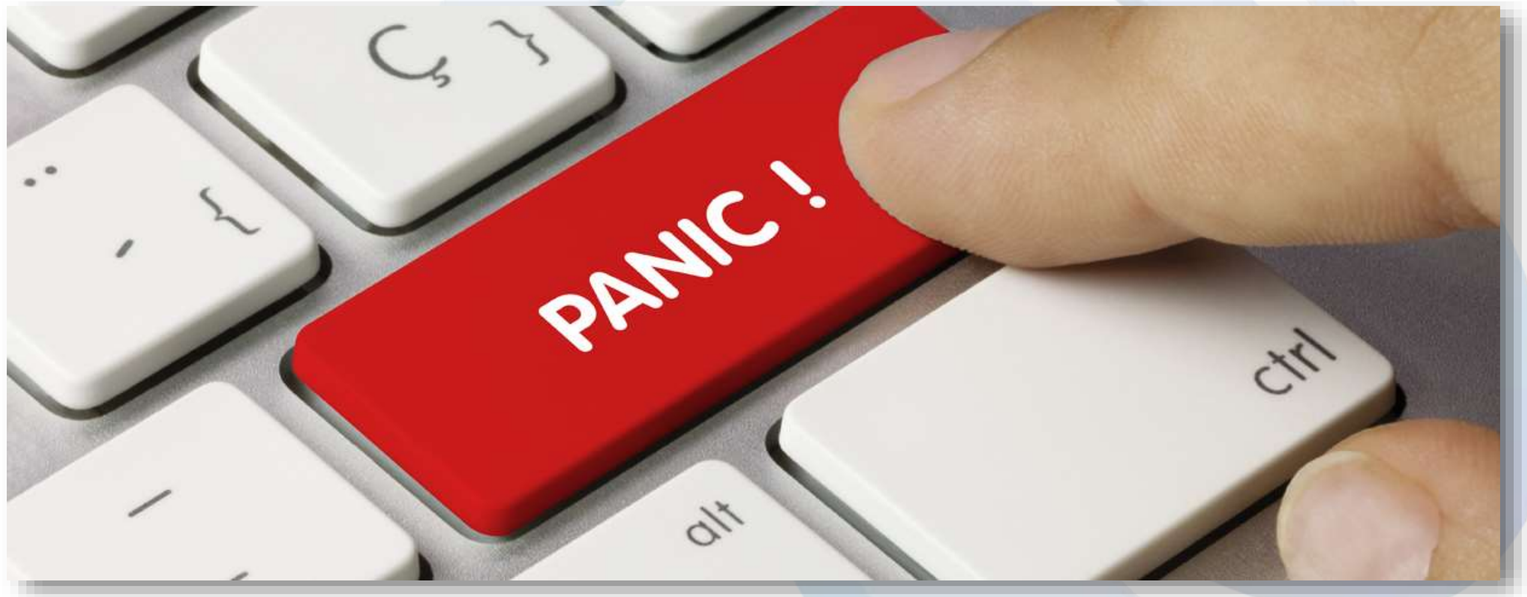
- Klassieker: niet patchen, of 2x per jaar
- Autorisatiebeheer
- Rechten voor iedereen

Detectie


zeker weten met wie u via internet afspraken maakt
www.diginotar.nl
DigiNotar
Internet Trust Services
Uw elektronische handtekening

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

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