KONINKRIJK BELGIË
Federale Overheidsdienst
Buitenlandse Zaken,
Buitenlandse Handel en
Ontwikkelingssamenwerking

You have been hacked : now what?

Anatomie van de hacking bij de FOD Buitenlandse Zaken

Jorg Leenaards
CISO

.be

FOD Buitenlandse Zaken

- Missie
  - Vertegenwoordigen (bilateraal – multilateraal)
  - Belgische belangen verdedigen & promoten
  - Consulaire diensten
  - Ontwikkelingssamenwerking

FOD Buitenlandse Zaken

- Organisatie
  - HQ Brussel
  - > 100 sites in buitenland (grootte van 2 tot >100)
  - > 3000 medewerkers (waarvan 2/3 in buitenland)

- ICT
  - Beheerd wide area netwerk
  - Gestandardiseerde IT architectuur in posten
  - 2 datacenters in Brussel
  - “follow the sun” support

FOD Buitenlandse Zaken

- Belang informatie & informatieveiligheid :
  - Confidentiality : geclassificeerde informatie (B, EU, NAVO), privacy-gevoelige informatie (biometrie)
  - Integrity : paspoorten, visa
  - Availability : crisissituaties, “daily bread and butter”

Historiek
fase 1 : ontdekking

- 28 april 2014 :
  vernemen via ADIV dat informatie van ons netwerk is gelekt
- 5 mei 2014 :
  infectie vastgesteld op 2 centrale servers – analyse ADIV : SNAKE
- 10 mei 2014 :
  incident lekt in de pers => beslissing om connectie naar internet af te sluiten
- 11 mei 2014 :
  oprichting Taskforce (ADIV, Cert.be, RCCU Brussel, VSSE, BUZA)

Historiek
fase 2 : analyse & damage control

- 12 mei tot 26 juni : Taskforce actief
- Uitdagingen TF :
  - Druk om kernprocessen (e-mail, visa, paspoorten,..) asap terug op te starten
  - Beperkte bandbreedte en bereikbaarheid diplomatieke posten
  - Scannen systemen
  - Loganalyse
  - Monitoring netwerkverkeer
  - Tegenpartij weet dat ze ontdekt is

.be

Historiek
fase 3 : maatregelen

- Korte termijn :
  - Clean install gecompromitteerde systemen (new golden image)
  - Reset paswoorden ☹
  - Whitelist internetsites ☹ ☹
  - Sneller patchen
  - Logging

.be

Historiek
fase 3 : maatregelen

- Middellange termijn :
  - Nieuwe DMZ (deels gemanaged) ☑
  - Nieuwe VPN-oplossing ☑
  - Beheer Admin accounts ☑
  - Secure by design ☑
  - Geclassificeerde informatie op afgezonderde systemen ☑
  - Data classification software ☑
  - Malware detonation software : ongoing
  - Awareness verhogen : ongoing

.be

Historiek
fase 3 : maatregelen

- Langere termijn:
  - CSOC (Cybersecurity Operations Center)
    - Experten recruteren (ongoing)
    - SIEM aankopen & configureren (ongoing)
  - Awareness (ongoing)

Lessons learned

- Voorbeeldige samenwerking tijdens crisis
- Communicatieplan, beslissingsstructuur
- Stretched out teams
- Paradigm shift : perimeter defensie ontoereikend – focus naar snel ontdekken van inbraken
- Human factor : awareness
- Cybersecurity = volgehouden (budgetaire) inspanning
- Cybersecurity : belangt de hele organisatie aan
- Federale structuur & expertise noodzakelijk (governance, CSOC)
- Publiek-private samenwerking

Dank U

jorg.leenaards@diplobel.fed.be

.be