Wij werden gehackt! Wat deden we toen?

Dilbeek

- De situatie vooraf
- De feiten
- De weg naar herstel
- Impact
- Lessons learned

De situatie vooraf

Het serverpark bestaat uit:

- Windows server 2008,2012,2016, 2019
- Linux

- 2008 servers: historische toepassingen
- De rest: productieservers

De feiten

Woensdag 18 november

- een traagheid in servers en toepassingen
- meerdere gebruikers meldden dit eveneens
- bij verder nazicht: het groot aantal servers op 100% processorcapaciteit

De feiten

- 1 server met virusscanmelding: wormvirus in quarantaine.
- Na overleg beslist het volledige serverpark groep Dilbeek stil te leggen.
- ICT team zelf op zoek gegaan
- Na een tweetal uren: Real Dolmen gecontacteerd.

De feiten

Zelfde symptomen als bij andere case van Real Dolmen
- Servers en enkele pc’s die PowerShell scripts trachtten te downloaden en te laten uitvoeren

Zoektocht gaat verder

Firewalls worden volledig dichtgeschroefd

Alle administratorwachtwoorden worden gewijzigd

DE BOOSDOENER

Wannamine virus

- Wormvirus
- Gebruikt servercapaciteit om coins te generen
- Maakt gebruik van SMBv1 protocol voor de verspreiding
- Kan in slapende toestand al langer aanwezig zijn

Eerste stappen naar herstel

Donderdagochtend

- Aankoop van bijkomende antivirussoftware ter vervanging van MS Defender
- Alle draagbare toestellen worden teruggeroepen naar IT
- Verplichte wachtwoordwijziging wordt ingesteld

Beheersmaatregelen om te dichten

- Server per server: script meerdere malen laten lopen
  - Servers die worden vrijgegeven → opnieuw opstarten
  - SMBv1 protocol wordt uitgeschakeld
  - Nieuwe AV geïnstalleerd
  - Windows 2008 servers: niet meer opnieuw opgestart
- Bestelling nieuwe Veeam BU server
  - Risico van aanwezige vuile bestanden te groot
- Instellingen firewall: ”dicht wat gevaarlijk is” → “Open wat veilig is”

Beheersmaatregelen om te dichten

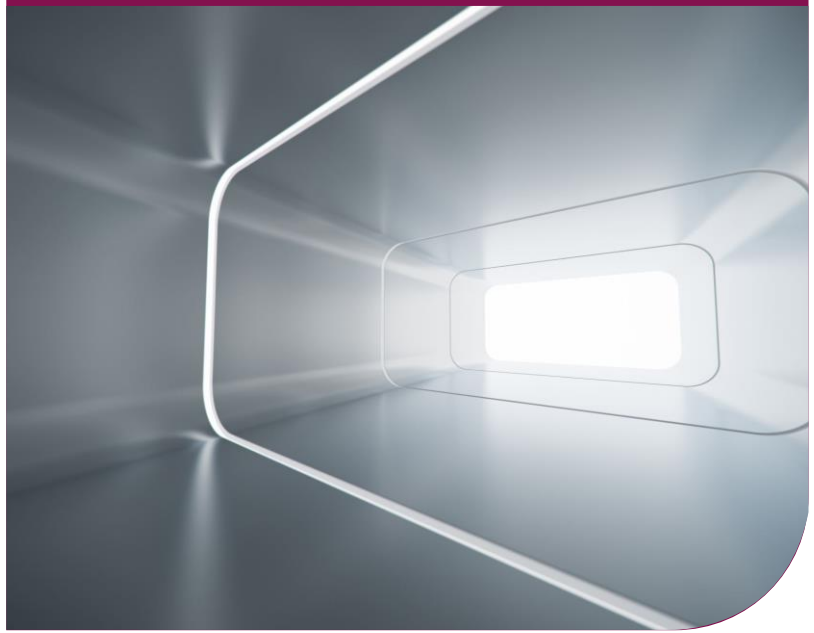
Vrijdag

- Aanpassingen aan binnengebrachte laptops en pc’s (op locatie)
- Met hulp van andere teams

Maandag

- Ophalen van draagbare toestellen
  - Check op wachtwoordwijziging
- Laatste servers worden in werking gesteld

We zijn er bijna



Dinsdag

- Teams testen de werking

Woensdag

- Diensten voor de bevolking: Up and running
  - Kleine problemen met printers

Impact

- Back up server wordt niet opnieuw opgestart
- Servers met historische data (oud loonpakket, oude postregistratie, oude Sharepointservers) worden niet opnieuw opgestart
- Hierdoor verlies data, maar gelukkig zijn er geen datalekken gevonden.
- Herinstallatie van Domain Controllers wat toch wel wat werk met zich meebrengt.

Impact

- 4,5 dagen volledig gesloten voor burgers
- Herstart met mondjesmaat
- Financiële gevolgen
  - Nieuwe Veeam
  - Externe hulp tijdens aanval: 9 mandagen
  - Externe hulp na aanval: 20 mandagen
  - Personeelskost

Lessons learned

- Serverpark best recente serverversies
- Netwerktoestellen
  - steeds laatste patches
  - Beter iets te veel dichtgeschroefd
- Monitoring nooit onderschatten
  - Antivirus
  - Firewalls
  - …
- Pc’s steeds de laatste updates
  - Mogelijkheid tot weigeren updates vermijden
- 2FA is geen overbodige luxe
  - Overtuigingskracht nodig, zelfs na ons debacle
- We hebben een chronisch tekort aan mensen op IT
  - Steeds mogelijkheid tot hulp op afroep voorzien

DILBEEK.BE