
Computer- en
Netwerkbeveiliging
24 November 2025 door HaarmanB ICT

Oops, mijn ‘vlieg’-PC doet het niet

- hoe lang kun je zonder?
- hoeveel tijd tot weer ‘vliegklaar’?
- gebruik alleen voor Flight Sim?
- stand-alone of Internettoegang nodig?
  - !! maatregelen alsof het een ‘normale’ PC is !!


Bedreigingsvectoren: een top 10
1. Session Stealing
2. Zero-Day Attack
3. Malware/Trojan Horse/Ransomware/PUPs
4. Impersination
5. Phishing
6. Distributed Denial of Service
7. Injection Attack
8. Man-in-the-Middle Attack
9. Spoofing
10. Brute Force Attack
WGFS Lamama 24 nov 2025 | @ HaarmanB ICT

Brute Force Attack

Wat is het?

- heel snel heel veel wachtwoordcombinaties proberen

Tegenmaatregelen:

- inlogscherm: lengte van wachtwoord NIET weergeven
- beperk aantal aanmeldpogingen
- Multi-Factor Authenticatie
- Password Manager icm Password Policy
- black listing


Spoofing
Wat is het?
• jezelf voordoen als iemand/iets anders:
• IP/DNS spoofing (omleiding naar gekloonde website)
• http spoofing
• email spoofing
• buiten deze context: telefoonspoofing
Tegenmaatregelen
• Security Awareness Training (mn. URL-links)
• email anti-spoofing
• black listing
WGFS Lamama 24 nov 2025 | @ HaarmanB ICT

Man-in-the-Middle Attack

Wat is het?

- cybercrimineel maakt ongemerkt deel uit van de verbinding tussen computer en website
  - gebruiker denkt een rechtstreeks verbinding te hebben
  - cybercrimineel kan datastroom zien en manipuleren
- komt met name voor bij publieke WiFi (!)

Tegenmaatregelen

- Security Awareness (gebruik GEEN publieke WiFi)
- HTTPS ipv HTTP tijdens het browsen
- Multi-Factor Authenticatie
- Zero Trust (ringfencing)


Injection Attack
Wat is het?
• misbruik van kwetsbaarheden in OS / programma's
• injecteren van gemanipuleerde data wat feitelijk kwaadaardige code is
• oneigenlijke toegang tot data
• 'voor de gek houden'
Tegenmaatregelen
• Endpoint Detection & Response
• AI gebaseerd
• rollback functionaliteit
• invoervalidatie
• uitgaan van 'Least Privilege'
WGFS Lamama 24 nov 2025 | @ HaarmanB ICT

Distributed Denial of Service (DDOS)

Wat is het?

- overspoelen van website / apparatuur met foutieve verbindingsaanvragen
  - website / apparaat onbereikbaar

Tegenmaatregelen

- modem/router/switches met DDOS detectie & beveiliging
- Firewall & DNS instellingen
- Patch Management (firmware)

Phishing

Wat is het?

- gebruiker verleiden om gevoelige informatie te geven
  - aanmeldgegevens
  - creditkaart
  - persoonlijke gegevens

Tegenmaatregelen

- Security Awareness Training (mn. URL-links: direct naar website ipv links)
- spamfilter
- email anti-spoofing

Impersination

Wat is het?

- cybercrimineel doet zich voor als vertrouwd persoon teneinde de gebruiker aan te zetten tot schadelijke acties of afgeven van informatie
  - financieel
  - aanmeldgegevens

Tegenmaatregelen

- Security Awareness Training (mn. tijdsdruk/onverwacht → verificatie)
- Multi-Factor Authenticatie
- email anti-spoofing
- eerst ‘even rustig ademhalen’, dan pas handelen


Malware/Trojan Horse/Ransomware/PUPs
Wat is het?
• computervirus
Tegenmaatregelen
• Endpoint Detection & Response
• backup (! off-site !!)
WGFS Lamama 24 nov 2025 | @ HaarmanB ICT


Zero-Day Attack
Wat is het?
• misbruik maken van een nog niet ontdekt/opgelost beveiligingslek
• OS / programma's
• firmware
Tegenmaatregelen
• Patch Management (OS, 3e partij programma's, firmware)
• Vulnerability Scan
• PenTesting
• Zero Trust (USB block)
WGFS Lamama 24 nov 2025 | @ HaarmanB ICT

Session Stealing

Wat is het?

- het ongemerkt overnemen van session tokens
  - !! MFA omzeilen (authenticatie heeft al plaatsgevonden)

Tegenmaatregelen

- monitoren ongebruikelijk netwerkactiviteit
- Zero Trust (monitoren aanmeldlocaties/tijdstippen)
- isoleren van netwerk
- SysMon (Windows Logboeken)


Beveiligingsmaatregelen: een top 10
1. Patch Management
2. Vulnerability Scan / PenTesting
3. Endpoint Detection & Response
4. Zero Trust / Ringfencing / USB Block
5. Network Monitoring / SysMon
6. Backup
7. Password Manager / Password Policy / MFA
8. Multi-Factor Authenticatie
9. Firewall & DNS (modem/router)
10. Black Listing / Security Awareness Training
WGFS Lamama 24 nov 2025 | @ HaarmanB ICT


Samenvatting
• indien computer verbonden met Internet
• beveiligingsmaatregelen
• er zijn veel bedreigingsvectoren
• er zijn gelukkig ook veel beveiligingsmaatregelen


HaarmanB ICT
HaarmanB ICT
0592 580170
www.haarmanb-ict.nl
support@haarmanb-ict.nl