Top 8 praktische beveiligingsmaatregelen ten aanzien van computer- en netwerk-beveiliging

Kader: de FlightSim Computer

Geen exact uitgewerkt stappenplan, want dat gaat in de praktijk niet werken.
Wél een korte omschrijving en reden van het waaróm van de maatregel.

OPMERKING
Indien geen tijd en/of geen zin en/of geen kennis van zaken ➔ uitbesteden 😊
Alle onderstaande maatregelen kunnen door HaarmanB ICT ingevuld worden.
Nadere informatie en/of implementatie via:

- reseller@haarmanb-ict.nl
- +31 (0) 592 580170

Onderstaande heeft als kader computers met als besturingssysteem Windows.
Alle genoemde maatregelen gelden echter ook voor macOS en Linux.
Vrijwel alle genoemde maatregelen zijn ook beschikbaar voor deze besturingssystemen.

Overzicht van aanbevolen beveiligingsmaatregelen

1. Update Beheer (Patch Management)

Wat:
Minstens 1x per week voor zowel het besturingssysteem als voor ***alle*** geïnstalleerde programma's controleren op beschikbare updates en deze laten doorvoeren. Denk aan het eventueel noodzakelijk herstarten van de computer (!).

Waarom:
Updates zijn er om ontdekte kwetsbaarheden (achterdeurtjes, buffer overflow, fouten, stabiliteit, etc.) te herstellen en op te lossen.

Hoe:
Windows: via Instellingen | Windows Updates
Los programma: meestal bij het starten ervan, anders vrijwel altijd via Menu | Help of 'Controleren op updates'.

2. Scannen op kwetsbaarheden (Vulnerability Scan)

Wat:
Minstens 1x per week opsporen van kwetsbaarheden in computers, geïnstalleerde programma's en netwerken (netwerkapparatuur), incl. fouten in configuratie-instellingen.

Waarom:
Het alleen uitvoeren van Update Beheer is (niet altijd) voldoende. Bijvoorbeeld het verkeerd instellen van open poorten op het modem/router kan onbedoelde cyber-aanvallen veroorzaken

Hoe:
Eigenlijk alleen met daarvoor bedoelde tools, maar je kunt in elk geval controleren op open poorten via www.grc.com | Services ➔ ShieldsUp

3. Vervang je bestaande handtekening gebaseerde antivirus door Endpoint-Detection-and-Response (kortweg: EDR)

Wat:
Een EDR is volledig gebaseerd op Kunstmatige Intelligentie en biedt bijna Real-Time beveiliging tegen elk soort malware.
Een van de betere EDR-engines is SentinelOne. Zoek maar eens op het Internet met zoeksleutel "review endpoint detection and response engines" en bekijk de review van Gartner.

Waarom:
Elk op een database met inmiddels bekend malware gebaseerde antivirusprogramma staat per definitie op achterstand met malwarebouwers.
Immers: een door cybercriminelen ontdekte techniek moet eerst ontdekt en vervolgens 'gepatched' worden.
Zelfs als deze antivirusprogramma's uitgerust zijn met technieken als 'heuristisch' scannen en technieken om zichzelf veranderende malware (polymorfe malware) zijn deze niet meer bestand tegen de huidig gebruikte door cybercriminelen gebruikte technieken.

Hoe:
Een EDR is een betaalde dienst. Er zijn natuurlijk meerdere aanbieders, zo ook HaarmanB ICT.

4. Hanteren van een Zero Trust beleid

Wat:
Zero Trust is een concept gebaseerd op één regel: alles waar niets voor geregeld is wordt geblokkeerd.
Implementatie gebeurt dus niet 'zomaar', er dient eerst sprake te zijn van een zgn. inleerperiode tijdens waarvan beoordeeld wordt wat er geblokkeerd *zou* worden.
Op basis van al bekende situaties of handmatige beoordeling worden vervolgens beleids-regels gecreëerd (met name 'toestaan').
Hierdoor zal het aantal toekomstige blokkeringen minimaal zijn en zelfs dan kan de gebruiker interactief vragen om toestemming/aanpassing.

Waarom:
Cybercriminelen maken steeds meer gebruik van legitiem aanwezige en gebruikte programma's (Windows onderdelen zoals Kladblok) of 'gefröbelde' bestanden (bv. PDF)

om gebruikers ongemerkt scripts of andere code te laten uitvoeren. Deze code kan allerlei redenen hebben, zoals data-extractie of installeren van Ransomware.

Hoe:
Eigenlijk alleen met speciaal daarvoor ontwikkelde tools.
Beoordeling van resultaten vergt uitgebreide ICT-ervaring.

5. Maak regelmatig backups (off-site)

Wat:
Het regelmatig in de cloud opslaan van belangrijke databestanden (gebruikersfolders, configuratiebestanden, logboeken, etc.)

Waarom:
Het regelmatig maken van backups van bestanden die je beslist niet wil kwijtraken is natuurlijk een logische stap.
Maar wordt toch heel vaak nagelaten.
Of vergeten.
Of de backup wordt gemaakt op een lokaal aanwezig opslagmedium (externe schijf) die vervolgens gewoon bij de computer aanwezig blijft.
Zelfs een backup naar een lokale NAS brengt NIET de gewenste zekerheid dat in geval van een incident data kan worden teruggezet (bijv. brand…)

Hoe:
Eén van de wereldwijd meest betrouwbare aanbieders van Cloud Backup is Cove Backup (het voormalige IASO uit Emmeloord).
De hier gebruikte backuptechniek is zo efficiënt dat een backupsessie minstens 5x zo snel is ten opzichte van het aloude grootvader-vader-zoon principe (lees: backup op basis van blokken in plaats van gehele bestanden).
Gecombineerd met military-grade versleuteling zowel tijdens backup/restore als in de opslag is deze vorm van backup al jaren in gebruik bij HaarmanB ICT.

6. Implementeren van SysMon

Wat:
SysMon is een superklein programma waarmee Windows Logboeken aangevuld worden met zinvolle informatie in het kader van forensisch onderzoek naar aanleiding van een crash, ransomware aanval, etc.

Waarom:
De standaardinstellingen met betrekking tot wát in de Windows logboeken wordt vast-gelegd zijn beslist onvoldoende om in relevante gevallen informatie te vergaren wat er aan de hand is geweest.

Hoe:
Implementeren van SysMon service in combinatie met een aangepast configuratie-bestand (zowel inclusies als exclusies). Het is dan tevens nodig om in het Windows Logboek programma een zgn. Custom View te definiëren voor snelle toegang.

En denk er ook aan om het betreffende logboekbestand mee te nemen in de backupselectie…

7. Gebruik een Wachtwoord Beheerder (Password Manager)

Wat:

Een versleutelde database met daarin opgeslagen aanmeldgegevens en andere gevoelige informatie. Toegang tot de database door middel van een (heel) sterk en uniek wachtwoord.
Vrijwel alle Password Managers bieden tevens een wachtwoordgenerator waarmee je sterke en unieke wachtwoorden kunt creëren zonder ze te hoeven onthouden (je slaat ze immers op in de database nietwaar?).

Waarom:

Slechts één (heel sterk) wachtwoord te onthouden om alle in de database opgeslagen aanmeldgegevens en andere gevoelige informatie te kunnen gebruiken.

Hoe:

Er zijn in de basis twee soorten Password Managers:

a. Offline
   Voordeel:
   Database staat lokaal op het apparaat, dus geen Internetverbinding nodig
   Nadeel:
   Indien synchronisatie gewenst is op meerdere apparaten risico van conflicten (synchronisatie op bestandsniveau)
b. Online
   Voordeel:
   Synchronisatie vindt plaats op recordniveau, kans op conflicten heel klein
   Nadeel:
   Internettoegang noodzakelijk

Een voorbeeld van een offline Password Manager is KeePass
Voorbeelden van een online PassWord Manager zijn BitWarden en LastPass

Tegenwoordig is er ook een hybride vorm van Password Manager met de voordelen van beide varianten zonder de nadelen: JumpCloud Password Manager (in gebruik bij HaarmanB ICT).
Hiermee is het mogelijk om op meerdere apparaten gevoelige informatie te zien, bewerken. Desnoods op dat moment zonder Internetverbinding, synchronisatie vindt plaats op recordniveau als er Internetverbinding is.

8. Pas de DNS-instellingen aan in je modem/router/laptop

Wat:

Om het mogelijk te maken dat je computer het Internet kan benaderen wordt gebruik gemaakt van zogeheten DNS-instellingen. DNS staat voor Dynamic Name Service.

Bij vrijwel elke computer is dat out-of-the-box automatisch ingesteld doordat alle netwerkadapters (bekabeld of draadloos) staan ingesteld op DHCP (Dynamic Host

Control Protocol), waardoor bij het koppelen aan het netwerk automatisch de noodzakelijke DNS-instellingen worden opgevraagd en ingesteld.

Waarom:
In vrijwel alle netwerken (met name in Nederland) is het standaard dat gebruik wordt gemaakt van de DNS servers van Google of CloudFare. Op zich heel betrouwbaar en stabiel, maar wel Amerikaans.
Er is een Zwitserse (Quad9, quad9.net) organisatie die niet alleen DNS aanbiedt, maar daarmee tevens een verhoogde beveiliging en privacy.

Hoe:
Modem/Router
De exacte instructies zijn uiteraard afhankelijk van het merk en type van je modem/router, maar in algemene zin:

a. log in op de webinterface van je modem/router
b. zoek in het menu naar het gedeelte waar je de IP-adressen van de primaire en secundaire DNS server kunt aanpassen
c. gebruik als primaire DNS IP adres: 9.9.9.9
d. gebruik als secundaire DNS IP adres: 149.112.112.112

N.B.: gebruik vooralsnog géén versleuteling aangezien Windows daar niet stabiel mee omgaat

Laptop (Windows):

a. klik met de rechtermuisknop op het icoon op de Taakbalk dat aangeeft dat er sprake is van een Internetverbinding
b. klik op 'Netwerk en Internet Instellingen'
c. klik op Ethernet (o.a. IP en DNS instellingen)
d. klik naast het gedeelte DNS server toewijzing op Aanpassen
e. stel de DNS in op Handmatig
f. gebruik als primaire DNS IP adres: 9.9.9.9
g. gebruik als secundaire DNS IP adres: 149.112.112.112

Advies: schakel IPv6 uit

Waarom geen vergelijkbare instructies voor een desktop?
Simpel: een desktop zal gekoppeld zijn aan je eigen netwerk en dus de DNS-instellingen van je modem/router krijgen.