DIGITAL SECURITY ASSESSMENT CHECKLIST

Hoe gebruik je deze checklist?

- Elk aangevinkt hokje is gelijk aan een punt.
- Vink de items aan die je hebt geïmplementeerd en bereken je score voor elk onderdeel.
- Verzeker je van optimale beveiliging door alle items op de checklist af te vinken!
- Totaalscore lager dan 35 punten? Werk aan de winkel, neem contact met ons op!

1 Netwerk/systeem beveiliging / Router

SCORE / 14

Systeem beveiliging

- ☐ 01. Gebruik een aangepast beheerdersaccount en schakel de standaard accounts “admin” en “guest” uit.
- ☐ 02. Schakel 2-staps verificatie in
- ☐ 03. Wijzig de “systeem default ports” naar het “management interface”, als u Synology Router Manager (SRM) gebruikt, in nieuwe aangepaste poorten
- ☐ 04. Schakel IP Auto Block in om brute-force aanvallen te voorkomen
- ☐ 05. HTTPS inschakelen voor services die op SRM draaien met een geldig SSL-certificaat
- ☐ 06. E-mail-, sms- of pushmeldingen inschakelen om op de hoogte te blijven van kritieke gebeurtenissen
- ☐ 07. Automatische update inschakelen voor de firmware van de router en alle ingebouwde beveiligingsdatabases

Netwerk beveiliging

- ☐ 08. Log bij apparaten op kantoor of thuis altijd in via een VPN
- ☐ 09. Synology Safe Access inschakelen om schadelijke domeinen en IP adressente blokkeren
- ☐ 10. Bedreigingspreventie en Deep Packet Inspection inschakelen
- ☐ 11. DNS over HTTPs-encryptie inschakelen om DNS-kaping te voorkomen
- ☐ 12. GeoIP firewallregels inschakelen
- ☐ 13. Mac-filtering inschakelen en bekende apparaten whitelisten voor Wi-Fi-gebruik
- ☐ 14. Regelmatig geplande “traffic reports” uit laten voeren om het netwerkgebruik te controleren

2 Eindpuntbeveiliging / NAS

SCORE / 12

- ☐ 01. Gebruik een aangepast beheerdersaccount en schakel de standaard accounts “admin” en “guest” uit.
- ☐ 02. Schakel 2-staps verificatie in
- ☐ 03. Pas regels voor wachtwoordsterkte toe op alle gebruikers
- ☐ 04. Beperk de toegangsrechten van gebruikers tot alleen de gedeelde mappen en services die ze nodig hebben
- ☐ 05. Wijzig de standaard systeempoorten, bijvoorbeeld poort 5000/5001 naar de DSM management interface naar de nieuwe aangepaste poorten
- ☐ 06. Als poort doorsturen is ingeschakeld voor uw NAS, gebruik dan aangepaste openbare poorten op de router in plaats van bekende poorten (bijv. 5000/5001)
- ☐ 07. IP automatisch blokkeren inschakelen tegen brute-force aanvallen
- ☐ 08. HTTPS inschakelen voor services die op DSM draaien met een geldig SSL-certificaat
- ☐ 09. E-mail-, sms- of pushmeldingen inschakelen om op de hoogte te blijven van kritieke gebeurtenissen
- ☐ 10. Automatische update inschakelen voor DSM Voer regelmatig Security
- ☐ 11. Advisor uit om kwetsbaarheden in het systeem te ontdekken en malware te identificeren
- ☐ 12. Installeer een antiviruspakket en voer regelmatig volledige scans uit

3 Eindpuntbeveiliging / Computers & mobile apparaten

SCORE / 4

- ☐ 01. Houd je besturingssysteem up-to-date
- ☐ 02. Gebruik betrouwbare antivirussoftware en voer regelmatig volledige scans uit
- ☐ 03. Schakel het Remote Desktop Protocol (RDP) alleen in als toegang op afstand absoluut noodzakelijk is, zodat je beschermd bent tegen aanvallen die misbruik maken van dit protocol.
- ☐ 04. Als je openbare Wi-Fi gebruikt, versleutel de verbinding dan altijd door een VPN te gebruiken.

4 Eindpuntbeveiliging / IoT apparaten

SCORE / 4

- ☐ 01. Gebruik een sterk wachtwoord
- ☐ 02. Blokkeer apparaten (zoals IP-camera’s, printers, telefoons, enz.) voor toegang tot het internet, tenzij het apparaat communicatie met de server nodig heeft om te kunnen functioneren.
- ☐ 03. Sluit IoT-apparaten aan op het gastnetwerk en scheid ze van apparaten die eigendom zijn van de gebruiker, zoals computers, smartphones en NAS, om te voorkomen dat een IoT-apparaat wordt gehackt en andere apparaten in hetzelfde netwerk aanvalt.
- ☐ 04. Blokkeer een apparaat onmiddellijk als het tekenen van verdachte activiteiten vertoont, onderzoek de incidenten en reset/herinstalleer het apparaat indien nodig

5 Data backup

SCORE / 10

Computers

- ☐ 01. Synology Drive inschakelen om een back-up te maken van belangrijke bestanden en mappen
- ☐ 02. Active Backup for Business inschakelen om een back-up te maken van het hele systeem

NAS backup

- ☐ 03. Hyper Backup inschakelen om een back-up te maken van gedeelde mappen, LUN’s en systeem-/pakketconfiguraties
- ☐ 04. Een waarschuwingsdrempel configureren in Hyper Backup voor bestandswijzigingen tussen twee back-upversies, zodat u automatisch op de hoogte wordt gebracht van abnormaal gedrag en wordt voorkomen dat alle intacte versies stilzwijgend worden overschreven.
- ☐ 05. Snapshotreplicatie inschakelen om snapshots te maken van belangrijke gedeelde mappen
- ☐ 06. Cloud Sync inschakelen om continu een back-up te maken van bestanden en mappen naar een veilige publieke cloudprovider zoals Synology C2 Backup

Externe apparaten (bijv. USB-sticks)

- ☐ 07. Gebruik USB Copy om een back-up te maken van alle externe apparaten naar uw NAS en beheer de bestanden vanaf één plek.

Backup uitvoering

- ☐ 08. Bewaar minstens één offsite kopie voor noodherstel
- ☐ 09. Plan al je back-up taken automatisch
- ☐ 10. Test na het instellen van een back-up taak onmiddellijk of je gegevens kunt herstellen vanaf de back-up kopie.
  gegevens kunt herstellen vanaf de reservekopie, en herhaal dit daarna regelmatig om ervoor te zorgen dat je altijd op tijd een volledig herstel kunt uitvoeren als er een ongeluk gebeurt