CHECKLIST DIGITÁLNÍ BEZPEČNOSTI

Počet síťových zařízení se neustále zvyšuje. Proto bude pro kybernetické útočníky stále snazší identifikovat a zneužít slabé postupy ZABEZPEČENÍ sítě k zajištění přístupu ke kritickým datům. Zkontrolujte svou síť pomocí tohoto kontrolního seznamu. Na první pohled uvidíte, co již máte dobře chráněno a kde je ještě co zlepšovat.

Projděte si postupně všechny důležité body zabezpečení. Každé zaškrtnuté políčko odpovídá jednomu bodu. Čím více bodů máte, tím lépe jsou vaše data a zařízení chráněna. Celkem můžete dosáhnout 43 bodů.

Ochrana počítače a mobilních zařízení

Body /4

- ☐ Aktualizujte svůj operační systém
- ☐ Nainstalujte si spolehlivý antivirový software a pravidelně provádějte úplné skenování
- ☐ Protokol RDP (Remote Desktop Protocol) povolte pouze v případě, že je vzdálený přístup nezbytně nutný, abyste se chránili před útoky
- ☐ Při používání veřejné Wi-Fi vždy šifrujte připojení pomocí připojení VPN

Ochrana zařízení IoT

Body /3

- ☐ Zablokujte přístup zařízení (např. IP kamer, tiskáren, telefonů atd.) k internetu, pokud zařízení ke své funkci nevyžaduje komunikaci s internetovým serverem
- ☐ Připojte zařízení IoT k síti pro hosty a odpojte je od zařízení vlastněných uživatelem, jako jsou počítače, chytré telefony a NAS, abyste zabránili únosu zařízení IoT a napadení dalších zařízení ve stejné síti
- ☐ Pokud zařízení vykazuje známky podezřelé aktivity, okamžitě jej zablokujte. Prošetřete incidenty a v případě potřeby obnovte zařízení/nově nainstalujte.

Ochrana pro síťové úložiště NAS

Body /12

- ☐ Použijte vlastní účet správce a zakažte výchozí účty správce a hosta
- ☐ Aktivujte dvoufázové ověřování
- ☐ Použijte silná pravidla pro sílu hesla pro všechny uživatele
- ☐ Omezte uživatelům přístupová práva ke sdíleným složkám a službám, které nepotřebují
- ☐ Změňte výchozí porty systému, např. Port 5000/5001 pro rozhraní správy operačního systému NAS (DiskStation Manager, zkráceně DSM), na nové vlastní porty ve vyšším pětimístném rozsahu
- ☐ Pokud je pro váš NAS povoleno přesměrování portů, použijte vlastní porty namísto dobře známých portů (např. 5000/5001) veřejných portů na směrovači
- ☐ Aktivujte automatické blokování IP proti útokům hrubou silou
- ☐ Povolte protokol HTTPS pro služby spuštěné v systému DSM s platným certifikátem SSL
- ☐ Povolte e-mailová, SMS nebo push oznámení, abyste měli aktuální informace o kritických událostech
- ☐ Povolte automatickou aktualizaci pro DSM
- ☐ Pravidelně spouštějte nástroj Security Advisor, abyste odhalili zranitelnosti systému a identifikovali malware
- ☐ Nainstalujte si antivirový balíček do svého NAS zařízení a pravidelně provádějte úplné skenování

Ochrana perimetru směrovačů

Body /14

Zabezpečení systému

- ☐ Použijte svůj vlastní účet správce a zakažte výchozí účty správce a hosta
- ☐ Aktivujte dvoufázové ověřování
- ☐ Změňte výchozí porty systému, např. port 8000/8001 rozhraní pro správu, na nové vlastní porty, pokud používáte Synology Router Manager (SRM)
- ☐ Zapněte automatické blokování IP proti útokům hrubou silou
- ☐ Povolte HTTPS pro služby spuštěné v SRM s platným certifikátem SSL
- ☐ Povolte e-mailová, SMS nebo push oznámení, abyste měli aktuální informace o kritických událostech
- ☐ Povolte automatickou aktualizaci firmwaru směrovače a všech integrovaných bezpečnostních databází

Zabezpečení sítě

- ☐ Přistupujte k zařízením v kanceláři nebo doma prostřednictvím sítě VPN
- ☐ Povolte funkci Synology Safe Access, která blokuje škodlivé domény a IP adresy
- ☐ Povolte možnost Threat Prevention a hloubkovou kontrolu paketů
- ☐ Povolte šifrování DNS přes HTTPS, abyste zabránili únosu DNS
- ☐ Povolte pravidla brány firewall GeoIP
- ☐ Povolte filtrování Mac adres a vytváření bílých seznamů známých zařízení pro používání WiFi
- ☐ Povolte pravidelné hlášení o provozu, abyste mohli sledovat využití sítě

Ochrana dat pomocí zálohování

Body /10

Zálohování počítače

- ☐ Povolte službě Synology Drive zálohovat důležité soubory a složky
- ☐ Povolte službu Active Backup for Business pro zálohování celého systému

Zálohování NAS

- ☐ Povolte funkci Hyper Backup pro zálohování sdílených složek, jednotek LUN a konfigurací systému/balíčků
- ☐ V nástroji Hyper Backup nakonfigurujte práh varování pro změny souborů mezi dvěma verzemi záloh tak, abyste byli automaticky upozorněni na abnormální chování a mohli tak zabránit případné ztrátě dat
- ☐ Povolte replikaci snímků a vytvářejte snímky důležitých sdílených složek
- ☐ Zapnutím funkce Object Storage můžete průběžně přenášet soubory a složky do zabezpečeného veřejného cloudového úložiště, jako je Synology C2

Zálohování externích zařízení (např. pevných disků USB)

- ☐ Pomocí funkce USB Copy můžete centrálně zálohovat všechna externí zařízení na NAS

Další důležitá nastavení zálohování

- ☐ Uchovávejte alespoň jednu kopii mimo pracoviště pro obnovu po havárii
- ☐ Naplánujte automatické spouštění všech úloh zálohování
- ☐ Po prvním zálohování vyzkoušejte, zda lze data ze záložní kopie obnovit. Poté tento postup pravidelně opakujte, abyste měli jistotu, že v případě selhání, můžete vždy provést úplnou obnovu