LISTA KONTROLNA BEZPIECZEŃSTWA CYFROWEGO

Liczba urządzeń podłączonych do sieci stale rośnie. Tak więc dla cyberprzestępców zawsze będzie łatwiej zidentyfikować i wykorzystać słabe zabezpieczenia sieci by zapewnić sobie dostęp do krytycznych danych. Sprawdź swoją sieć za pomocą tej listy kontrolnej. Już na pierwszy rzut oka widać, co już dobrze chronisz, a gdzie jeszcze jest miejsce na ulepszenia.

Przejdź krok po kroku przez wszystkie ważne punkty bezpieczeństwa. Każde zaznaczone pole wyboru odpowiada punktowi. Im więcej masz punktów, tym lepiej.

Ochrona danych i urządzeń. W sumie można zdobyć 44 punkty.

Ochrona komputera i urządzeń mobilnych

Punkty /4

- ☐ Aktualizuj swój system operacyjny
- ☐ Zainstaluj niezawodne oprogramowanie antywirusowe i regularnie przeprowadzaj pełne skanowanie
- ☐ Włącz Remote Desktop Protocol (RDP) tylko wtedy, gdy dostęp zdalny jest absolutnie konieczny, aby chronić się przed atakami wykorzystującymi luki w bezpieczeństwie
- ☐ Podczas korzystania z publicznej sieci Wi-Fi zawsze szyfruj połączenie za pomocą połączenia VPN

Ochrona urządzeń IoT

Punkty /4

- ☐ Użyj silnego hasła
- ☐ Zablokuj dostęp do Internetu urządzeniom (np. kamerom IP, drukarkom, telefonom itp.), chyba że urządzenie tego wymaga.
- ☐ Podłącz urządzenia IoT do sieci gościnnej i odłącz je od urządzeń należących do użytkowników, takich jak komputery, smartfony i NAS, aby zapobiec przejęciu urządzenia IoT i atakowaniu innych urządzeń w tej samej sieci
- ☐ Natychmiast zablokuj urządzenie, jeśli wykazuje ono oznaki podejrzanej aktywności. Zbadaj incydenty i zresetuj urządzenie, jeżeli to konieczne odinstaluj/zainstaluj ponownie urządzenie.

Ochrona NAS

Punkty /12

- ☐ Użyj niestandardowego konta administratora i wyłącz domyślne konta administratora i użytkownika
- ☐ Włącz uwierzytelnianie dwuetapowe
- ☐ Zastosuj silne reguły mocy hasła do wszystkich użytkowników
- ☐ Ogranicz prawa dostępu użytkowników do folderów współdzielonych i usług, których nie potrzebują
- ☐ Zmień domyślne porty systemowe, np. B. Port 5000/5001 dla interfejsu zarządzania systemem operacyjnym NAS (DiskStation Manager, w skrócie DSM) do nowych niestandardowych portów w wyższym zakresie 5-cyfrowym
- ☐ Jeśli w serwerze NAS jest włączone przekierowanie portów, użyj niestandardowych portów publicznych na routerze, zamiast dobrze znanych (np. 5000/5001).
  porty publiczne na routerze
- ☐ Włącz automatyczne blokowanie adresów IP przed silnymi atakami
- ☐ Włącz HTTPS dla usług działających w systemie DSM z ważnym certyfikatem SSL
- ☐ Włącz powiadomienia e-mail, SMS lub push, aby być na bieżąco z krytycznymi zdarzeniami
- ☐ Włącz automatyczną aktualizację DSM (jeśli jest taka potrzeba, możesz wybrać tylko poprawki związane z bezpieczeństwem)
- ☐ Regularnie uruchamiaj Security Advisor, aby wykrywać luki w zabezpieczeniach systemu i identyfikować złośliwe oprogramowanie
- ☐ Zainstaluj pakiet antywirusowy na serwerze NAS i regularnie przeprowadzaj pełne skanowanie

Ochrona obwodowa dla routerów

Punkty /14

Zabezpieczenia systemu

- ☐ Użyj niestandardowego konta administratora i wyłącz domyślne konta administratora i użytkownika
- ☐ Aktywuj uwierzytelnianie dwuetapowe
- ☐ Zmień domyślne porty systemowe, np. port 8000/8001 interfejsu zarządzania na nowe niestandardowe porty, jeśli używasz Synology Router Manager (SRM)
- ☐ Włącz automatyczne blokowanie adresów IP przed silnymi atakami
- ☐ Włącz HTTPS dla usług działających na SRM z ważnym certyfikatem SSL
- ☐ Włącz powiadomienia e-mail, SMS lub push, aby być na bieżąco z krytycznymi zdarzeniami
- ☐ Włącz automatyczną aktualizację oprogramowania sprzętowego routera i wszystkich wbudowanych baz danych zabezpieczeń

Bezpieczeństwo sieci

- ☐ Korzystaj z dostępu do urządzeń w biurze lub w domu przez VPN
- ☐ Włącz Synology Safe Access, aby blokować złośliwe domeny i adresy IP
- ☐ Włącz zapobieganie zagrożeniom i głęboką kontrolę pakietów (Threat Prevention)
- ☐ Włącz szyfrowanie DNS przez HTTPS, aby zapobiec przejęciu DNS
- ☐ Włącz reguły zapory GeoIP
- ☐ Włącz filtrowanie komputerów Mac i umieszczanie na białej liście znanych urządzeń do korzystania z Wi-Fi
- ☐ Włącz regularnie zaplanowane raporty o ruchu, aby monitorować wykorzystanie sieci

Ochrona danych z kopią zapasową

Punkty /10

Kopia zapasowa komputera

- ☐ Włącz Synology Drive, aby tworzyć kopie zapasowe ważnych plików i folderów
- ☐ Włącz usługę Active Backup for Business, aby utworzyć kopię zapasową całego systemu, jeśli ten pakiet jest dostępny na Twój serwer.

Kopia zapasowa NASa

- ☐ Włącz Hyper Backup, aby tworzyć kopie zapasowe folderów współdzielonych, jednostek LUN i konfiguracji systemu/pakietu
- ☐ W Hyper Backup skonfiguruj próg ostrzegawczy dla zmian plików między dwiema wersjami kopii zapasowych, abyś mógł być automatycznie powiadamiany o nietypowym zachowaniu, a tym samym mieć możliwość zapobiec możliwej utracie danych.
- ☐ Włącz replikację migawek, aby tworzyć migawki ważnych folderów współdzielonych
- ☐ Włącz Cloud Sync, aby stale przesyłać pliki i foldery do bezpiecznego dostawcy chmury publicznej, takiego jak bezpieczna pamięć masowa Synology C2

Kopia zapasowa urządzeń zewnętrznych (np. dysków twardych USB)

- ☐ Użyj funkcji USB Copy, aby centralnie tworzyć kopie zapasowe wszystkich urządzeń zewnętrznych na serwerze NAS

Inne ważne ustawienia kopii zapasowej

- ☐ Zachowaj co najmniej jedną kopię poza siedzibą firmy na wypadek awarii
- ☐ Zaplanuj automatyczne uruchamianie wszystkich zadań tworzenia kopii zapasowych
- ☐ Po utworzeniu pierwszej kopii zapasowej sprawdź, czy możesz przywrócić dane z kopii zapasowej. Następnie powtarzaj tę czynność okresowo, aby mieć pewność, że zawsze możesz przeprowadzić pełne odzyskiwanie w przypadku awarii