telbit24

# Audyt i zabezpieczenie sieci

Raport przykładowy: wykonane prace i zalecenia

| | | | |
|---|---|---|---|
| **Dokument** | raport przykładowy, dane fikcyjne | **Router** | MikroTik RB4011iGS+, 192.168.50.1 |
| **Przygotował** | Telbit24 S.C., dział techniczny | **System** | RouterOS 7.24.6 |
| **Odbiorca** | Firma Przykładowa | **Sieć LAN** | 192.168.50.0/24 |

Audyt objął router brzegowy, widoczność sieci z Internetu, switch, sieć Wi-Fi, serwer i jego kopie zapasowe, rejestrator kamer oraz urządzenia w sieci wewnętrznej. Pozycje o priorytecie krytycznym i wysokim zostały wykonane: z Internetu odpowiada wyłącznie serwer VPN, chroniony certyfikatami, a urządzenia sieciowe mają aktualne oprogramowanie. Sekcja 2 zawiera zalecenia do zaplanowania.

## 1. Wykonane prace

| Priorytet | Zmiana | Efekt | Status |
|---|---|---|---|
| KRYTYCZNY | Aktualizacja systemu routera z wersji 7.15.3 do 7.24.6 wraz z oprogramowaniem układowym | Usunięte podatności ogłoszone przez producenta: usługa SSH (CVE-2026-67279 wykorzystywana w atakach, CVE-2026-86060, CVE-2026-67276), weryfikacja certyfikatów (CVE-2026-67278), jądro systemu (CVE-2026-98432). Nie stwierdzono oznak przejęcia routera wskazanych w ostrzeżeniu CERT Polska. Sieć i VPN pracują bez zmian. | ZROBIONE |
| KRYTYCZNY | Zamknięcie dostępu z Internetu do zarządzania routerem | Panel WWW, WinBox i SSH routera są dostępne wyłącznie przez VPN i z dwóch wskazanych komputerów. | ZROBIONE |
| KRYTYCZNY | Usunięcie przekierowania pulpitu zdalnego, port 3389, z Internetu do serwera | Serwer nie jest dostępny z Internetu. Praca zdalna na serwerze odbywa się po połączeniu z VPN. | ZROBIONE |
| KRYTYCZNY | Dysk sieciowy z kopiami: wyłączenie dostępu z Internetu do panelu, port 5001, i aktualizacja systemu DSM z wersji 7.2.1-69057-5 do 7.2.1-69057-6 | Usunięta podatność CVE-2024-10441, pozwalająca przejąć urządzenie bez logowania. Panel dysku sieciowego jest dostępny tylko z sieci wewnętrznej i z VPN. | ZROBIONE |
| WYSOKI | Aktualizacja oprogramowania punktów dostępowych Wi-Fi z wersji 7.00(ABTG.1) do 7.00(ABTG.2) | Usunięta podatność CVE-2024-7261, pozwalająca przejąć punkt dostępowy bez logowania. | ZROBIONE |
| WYSOKI | Aktualizacja oprogramowania switcha głównego z wersji V4.70(ABMH.7)C0 do V4.70(ABMH.8)C0 | Usunięta podatność CVE-2022-43393, pozwalająca zawiesić switch żądaniem wysłanym do panelu zarządzania. | ZROBIONE |
| WYSOKI | Sieć Wi-Fi: szyfrowanie WPA2 i WPA3 w miejsce WPA z TKIP, wyłączona funkcja WPS, nowe hasło | Sieć firmowa korzysta z aktualnych metod szyfrowania. Do sieci nie da się dołączyć kodem PIN z obudowy urządzenia. | ZROBIONE |
| WYSOKI | Osobna sieć Wi-Fi dla gości | Urządzenia gości mają dostęp tylko do Internetu, bez dostępu do serwera, komputerów i drukarek. | ZROBIONE |
| WYSOKI | Wyłączenie przekierowania portów 80 i 37777 z Internetu do rejestratora kamer; nowe hasło administratora w miejsce fabrycznego | Rejestrator nie jest dostępny z Internetu. Podgląd zdalny działa po połączeniu z VPN. | ZROBIONE |

| Priorytet | Zmiana | Efekt | Status |
|---|---|---|---|
| WYSOKI | VPN z certyfikatami i osobnymi kontami dla pięciu osób pracujących zdalnie | Każda osoba łączy się własnym kontem, które można wyłączyć bez wpływu na pozostałe. | ZROBIONE |
| WYSOKI | Wznowienie nocnej kopii serwera i ustawienie limitu przechowywanych wersji | Kopia serwera wykonuje się co noc. Dysk sieciowy przechowuje 30 wersji i ma wolne miejsce na kolejne. | ZROBIONE |
| ŚREDNI | Zmiana haseł fabrycznych w switchu, punktach dostępowych i urządzeniu wielofunkcyjnym | Panele zarządzania wymagają haseł przekazanych Klientowi. | ZROBIONE |
| ŚREDNI | Usunięcie kont byłych pracowników z VPN i z serwera | Dostęp do sieci i serwera mają wyłącznie osoby obecnie pracujące. | ZROBIONE |
| ŚREDNI | Stałe adresy dla serwera, dysku sieciowego, drukarek i rejestratora; synchronizacja czasu urządzeń | Urządzenia zachowują adresy po restarcie routera. Dzienniki i nagrania mają poprawny czas. | ZROBIONE |

## 2. Zalecenia

| # | Zalecenie | Stan obecny i zalecenie |
|---|---|---|
| **Kopie zapasowe** | | |
| Ocena: nocna kopia serwera wykonuje się poprawnie i obejmuje dane programów oraz pliki pracowników. Dysk sieciowy pracuje w układzie RAID 1, czyli każdy z dwóch dysków przechowuje te same dane. Stan dysków jest prawidłowy. Układ chroni dane przed awarią serwera i awarią jednego dysku. Poniższe zalecenia dotyczą zdarzeń obejmujących całą siedzibę i ochrony samych kopii. | | |
| 1 | **Kopia najważniejszych danych poza siedzibą** | Obecnie kopie serwera są przechowywane na dysku sieciowym, w tym samym pomieszczeniu co serwer. Zaleca się drugą kopię poza siedzibą: najważniejsze dane szyfrowane w firmie i wysyłane co noc do magazynu danych w Unii Europejskiej. Pożar, zalanie albo kradzież nie obejmują wtedy obu kopii. |
| 2 | **Ochrona kopii przed skasowaniem** | Obecnie folder kopii na dysku sieciowym jest dostępny do zapisu z komputerów pracowników. Zaleca się osobne konto używane wyłącznie do kopii oraz migawki na dysku sieciowym. Zaszyfrowanie plików na jednym komputerze nie obejmuje wtedy kopii. |
| 3 | **Powiadomienia o kopiach i próbne odtworzenie** | Obecnie wynik nocnej kopii jest zapisywany tylko na dysku sieciowym. Zaleca się powiadomienia e-mail o nieudanej kopii i o awarii dysku. Zaleca się też jednorazowe próbne odtworzenie serwera z kopii, poza godzinami pracy firmy. |
| **Serwer** | | |
| 4 | **System serwera** | Obecnie serwer pracuje w systemie Windows Server 2012 R2. Producent zakończył wydawanie poprawek bezpieczeństwa dla tej wersji w październiku 2023 r. Zaleca się przeniesienie programów i danych na aktualną wersję systemu. Do tego czasu serwer pozostaje niedostępny z Internetu. |
| 5 | **Zasilanie awaryjne** | Obecnie serwer i dysk sieciowy są zasilane bez zasilacza awaryjnego UPS. Zanik zasilania wyłącza je nagle, co grozi uszkodzeniem danych. Zaleca się UPS z nadzorem, który przy niskim stanie baterii zamyka systemy i wyłącza urządzenia. |
| 6 | **Zdalny dostęp serwisowy do serwera** | Obecnie do serwera można wejść zdalnie na dwa sposoby: przez VPN oraz przez program zdalnego pulpitu ze stałym hasłem. Zaleca się pozostawienie jednego sposobu: konta VPN przypisanego do osoby. Program zdalnego pulpitu zaleca się odinstalować albo uruchamiać tylko na czas sesji serwisowej. |

| # | Zalecenie | Stan obecny i zalecenie |
|---|---|---|
| **Łącze internetowe** | | |
| 7 | **Łącze zapasowe** | Obecnie firma pracuje na jednym łączu internetowym. Przerwa w łączu zatrzymuje pocztę, telefony i programy działające w chmurze. Zaleca się łącze zapasowe LTE z automatycznym przełączaniem na routerze. Router nie wymaga wymiany. |
| **Sieć i urządzenia** | | |
| 8 | **Podział sieci wewnętrznej** | Obecnie serwer, komputery, kamery i drukarki pracują w jednej sieci i mają do siebie bezpośredni dostęp. Zaleca się wydzielenie kamer i drukarek do osobnej sieci oraz ograniczenie dostępu do serwera do potrzebnych usług. Awaria albo infekcja jednego urządzenia nie obejmuje wtedy pozostałych. Router i switch pozwalają na taki podział bez wymiany sprzętu. |
| 9 | **Rejestrator kamer** | Obecnie rejestrator ma oprogramowanie z 2020 r., a jego panel działa bez szyfrowania. Zaleca się instalację bieżącej wersji od producenta i włączenie HTTPS. |
| 10 | **Urządzenie wielofunkcyjne** | Obecnie urządzenie zapisuje skany na serwerze starszym protokołem SMB 1. Zaleca się przełączenie skanowania na SMB 3 i wyłączenie SMB 1 na serwerze. |
| 11 | **Komputery pracowników** | Obecnie 3 z 12 komputerów pracują w systemie Windows 10. Producent zakończył wydawanie bezpłatnych poprawek dla tego systemu w październiku 2025 r. Zaleca się aktualizację do Windows 11 albo wymianę tych komputerów. |

Prace wykonuje Telbit24 zdalnie, w oknach uzgodnionych z Klientem; do rozpoczęcia potrzebne są decyzje i dostępy z załącznika B.

## 3. Inwentarz sieci

**Porty routera**

| Port | Rola | Co jest podłączone |
|---|---|---|
| ether1 | Internet | łącze główne, adres publiczny 203.0.113.10 |
| ether2 | sieć wewnętrzna | switch główny; sieć 192.168.50.0/24 |
| ether3 | sieć wewnętrzna | dysk sieciowy |
| ether4 do ether9 | sieć wewnętrzna | wolne |
| ether10 | Internet, łącze zapasowe | wolny; przewidziany na łącze zapasowe |

**Grupy urządzeń (producent i typ rozpoznane po adresie MAC, nazwie w DHCP i usługach; pełna lista w załączniku A)**

| Grupa | Adresy 192.168.50.x | Uwagi |
|---|---|---|
| Router | .1 | MikroTik RB4011iGS+, RouterOS 7.24.6 |
| Switch | .2 | Zyxel GS1920-24v2 |
| Punkty dostępowe Wi-Fi | .3, .4 | Zyxel NWA110AX; sieć firmowa i sieć dla gości |
| Serwer | .10 | Windows Server 2012 R2; program księgowy i pliki pracowników |
| Dysk sieciowy | .11 | Synology DS220+, dwa dyski w układzie RAID 1; nocne kopie serwera |
| Kamery | .20 do .26 | rejestrator Dahua i 6 kamer |
| Drukarki | .30, .31 | urządzenie wielofunkcyjne Kyocera; drukarka etykiet Zebra |
| Komputery | .100 do .111 | 12 komputerów; adresy z DHCP |
| Do identyfikacji | .50, .143 | domowy router Wi-Fi; urządzenie z modułem sieciowym Espressif |

## Załącznik A. Lista urządzeń

Wersja „brak” oznacza, że odczyt wymaga dostępu do urządzenia.

| Adres | MAC | Producent / model | Rola | Wersja |
|---|---|---|---|---|
| 192.168.50.1 | 48:a9:8a:3c:51:07 | MikroTik RB4011iGS+ | Router | RouterOS 7.24.6 |
| 192.168.50.2 | bc:cf:4f:19:a4:60 | Zyxel GS1920-24v2 | Switch główny | V4.70(ABMH.8)C0 |
| 192.168.50.3 | d4:1a:d1:72:0e:b1 | Zyxel NWA110AX | Punkt dostępowy Wi-Fi | 7.00(ABTG.2) |
| 192.168.50.4 | d4:1a:d1:72:0f:35 | Zyxel NWA110AX | Punkt dostępowy Wi-Fi | 7.00(ABTG.2) |
| 192.168.50.10 | 7c:d3:0a:5b:22:9e | Lenovo ThinkSystem ST50 | Serwer | Windows Server 2012 R2 |
| 192.168.50.11 | 00:11:32:c8:4d:12 | Synology DS220+ | Dysk sieciowy, kopie | DSM 7.2.1-69057-6 |
| 192.168.50.20 | 3c:ef:8c:a1:63:d0 | Dahua NVR4108HS | Rejestrator kamer | wersja z 2020 r. |
| 192.168.50.21 | 3c:ef:8c:a7:19:e2 | Dahua | Kamera | brak |
| 192.168.50.22 | 3c:ef:8c:a7:1b:06 | Dahua | Kamera | brak |
| 192.168.50.23 | 3c:ef:8c:a7:1b:5c | Dahua | Kamera | brak |
| 192.168.50.24 | 3c:ef:8c:a9:40:8d | Dahua | Kamera | brak |
| 192.168.50.25 | 3c:ef:8c:a9:42:f1 | Dahua | Kamera | brak |
| 192.168.50.26 | 3c:ef:8c:ac:05:73 | Dahua | Kamera | brak |
| 192.168.50.30 | 00:17:c8:6f:90:2a | Kyocera ECOSYS M2540dn | Urządzenie wielofunkcyjne | brak |
| 192.168.50.31 | 00:07:4d:8e:13:c4 | Zebra ZD421 | Drukarka etykiet | brak |
| 192.168.50.50 | c8:3a:35:4b:d6:10 | Tenda AC10 | Router Wi-Fi, do identyfikacji | brak |
| 192.168.50.100 | 54:bf:64:21:a0:3c | Dell OptiPlex | Komputer | Windows 11 |
| 192.168.50.101 | 54:bf:64:2e:a7:47 | Dell OptiPlex | Komputer | Windows 11 |
| 192.168.50.102 | 54:bf:64:3b:ae:52 | Dell OptiPlex | Komputer | Windows 11 |
| 192.168.50.103 | 54:bf:64:48:b5:5d | Dell OptiPlex | Komputer | Windows 11 |
| 192.168.50.104 | 54:bf:64:55:bc:68 | Dell OptiPlex | Komputer | Windows 11 |
| 192.168.50.105 | 3c:52:82:62:c3:73 | HP ProDesk | Komputer | Windows 11 |
| 192.168.50.106 | 3c:52:82:6f:ca:7e | HP ProDesk | Komputer | Windows 11 |
| 192.168.50.107 | 3c:52:82:7c:d1:89 | HP ProDesk | Komputer | Windows 11 |
| 192.168.50.108 | 3c:52:82:89:d8:94 | HP ProDesk | Komputer | Windows 11 |
| 192.168.50.109 | 8c:16:45:96:df:9f | Lenovo ThinkCentre | Komputer | Windows 10 |
| 192.168.50.110 | 8c:16:45:a3:e6:aa | Lenovo ThinkCentre | Komputer | Windows 10 |
| 192.168.50.111 | 8c:16:45:b0:ed:b5 | Lenovo ThinkCentre | Komputer | Windows 10 |
| 192.168.50.143 | a4:cf:12:5d:e7:08 | do identyfikacji | do identyfikacji | brak |

## Załącznik B. Decyzje i dostępy potrzebne do zaleceń

- Zalecenie 1: wybór magazynu danych i umowa powierzenia przetwarzania danych z jego dostawcą.
- Zalecenie 3: adres e-mail odbiorcy powiadomień; termin próbnego odtworzenia.
- Zalecenie 4: decyzja o zakupie licencji albo nowego serwera; potwierdzenie dostawcy programu księgowego.
- Zalecenie 5: zakup zasilacza UPS.
- Zalecenie 7: wybór operatora łącza zapasowego.
- Zalecenia 8 i 10: okno serwisowe z krótką przerwą w pracy sieci i drukarek.
- Zalecenie 9: okno serwisowe z krótką przerwą w nagrywaniu.
- Zalecenie 11: decyzja o aktualizacji albo wymianie trzech komputerów.

## Załącznik C. Pozycje do uzupełnienia

Do uzupełnienia po stronie Klienta.

| Pozycja | Opis |
|---|---|
| Urządzenie 192.168.50.143 | Urządzenie z modułem sieciowym Espressif, stosowanym w automatyce i urządzeniach domowych. Do uzupełnienia: co to za urządzenie. |
| Program zdalnego pulpitu | Do uzupełnienia: kto korzysta ze stałego dostępu do serwera przez program zdalnego pulpitu. |
| Domowy router Wi-Fi (192.168.50.50) | Urządzenie jest podłączone do switcha głównego i nadaje własną sieć bezprzewodową. Do uzupełnienia: kto z niego korzysta. Jeśli nie jest potrzebne, zaleca się jego odłączenie. |

Kontakt w sprawach technicznych: Telbit24, dział techniczny, tel. 14 658 40 40, biuro@telbit24.pl.