Jakub Gorący
Audyt bezpieczeństwa IT

RAPORT Z AUDYTU BEZPIECZEŃSTWA

PRZYKŁAD – Biuro Rachunkowe Demo sp. z o.o.

ul. Przykładowa 1, 00-000 Miasto (dane fikcyjne)

Numer raportu	AUD/2026/001
Data audytu	20.11.2026, 9:00–15:00
Lokalizacja	siedziba klienta + kontrole zdalne
Osoba kontaktowa	Anna Przykładowa, prezes zarządu
Audytor	Jakub Gorący

DOKUMENT POUFNY – przeznaczony wyłącznie dla zleceniodawcy. Zawiera informacje o słabościach infrastruktury; nie przesyłać dalej bez potrzeby.

1. Podsumowanie dla zarządu



OCENA: SŁABA

2 krytyczne	**2** wysokie
4 średnie	**1** niskie

Firma ma dobre podstawy (aktualne systemy na większości komputerów, włączony antywirus, porządek w kontach), ale dwie słabości wymagają natychmiastowej reakcji: panel NAS z dokumentami klientów jest dostępny z internetu, a jedyna kopia zapasowa stoi w tym samym pomieszczeniu i jest dostępna z każdego komputera – atak ransomware zaszyfrowałby i dane, i kopię. Po usunięciu tych dwóch problemów ocena wzrosłaby do poziomu „do poprawy", a po wdrożeniu pełnego planu – do „dobrej".

Najważniejsze ryzyka

- KRYTYCZNE **Panel administracyjny NAS dostępny z internetu** – Każdy w internecie może próbować logowania do serwera z dokumentami klientów; panele NAS są masowo atakowane (zgadywanie haseł, znane podatności, ransomware).
- KRYTYCZNE **Jedyna kopia zapasowa podatna na ransomware** – Ransomware z dowolnego komputera zaszyfruje jednocześnie dane i kopię. Pożar, zalanie lub kradzież zniszczy wszystko naraz. Firma może utracić dokumentację klientów (obowiązki z RODO i ordynacji podatkowej).
- WYSOKIE **Brak MFA na skrzynkach pocztowych Microsoft 365** – Przejęcie hasła (phishing, wyciek) daje pełny dostęp do korespondencji z klientami i możliwość podszycia się pod biuro, np. w sprawie przelewów.
- WYSOKIE **Rejestrator kamer w sieci biurowej z domyślnym hasłem** – Przejęte urządzenie IoT w sieci biurowej to wygodny punkt startowy ataku na komputery i NAS; dodatkowo podgląd kamer biura.

Co działa dobrze

- Microsoft Defender włączony i aktualny na wszystkich zbadanych komputerach
- Konta byłych pracowników zablokowane (lista sprawdzona z kadrami)
- Sieć gości odizolowana od sieci biurowej (test z sieci gości – brak dostępu)
- Certyfikat strony WWW ważny, TLS 1.2/1.3

2. Zakres i metodyka

Zakres audytu

- Sieć biurowa 192.168.1.0/24 oraz sieć gości (Wi-Fi "Demo-Goscie")
- Router/firewall, 2 punkty dostępowe Wi-Fi, NAS, 8 stacji roboczych, drukarka, rejestrator kamer
- Adres publiczny 203.0.113.10 (skan z zewnątrz)
- Domena demo-biuro.pl: poczta (SPF, DKIM, DMARC), certyfikat strony WWW
- Kopie zapasowe, konta i uprawnienia, procedury

Poza zakresem

- Testy socjotechniczne (phishing) pracowników
- Infrastruktura dostawców (hosting strony, operator internetu, Microsoft 365 po stronie Microsoft)
- Audyt kodu aplikacji i programu księgowego

Metodyka

- Wywiad z osobą odpowiedzialną za IT i ankieta wstępna
- Inwentaryzacja urządzeń (ARP, DHCP, skan sieci)
- Skanowanie portów i usług oraz skan podatności sieci wewnętrznej z ręczną weryfikacją wyników
- Przegląd konfiguracji routera, Wi-Fi i NAS za udostępnionym dostępem administratora
- Skan zewnętrzny adresu publicznego i kontrola rekordów DNS domeny
- Lista kontrolna 12 obszarów (wersja 1.0), każde ustalenie poparte dowodem

Skala ryzyka

Poziom	Znaczenie
KRYTYCZNE	Łatwe do wykorzystania z internetu lub daje pełną kontrolę nad danymi. Naprawić natychmiast.
WYSOKIE	Realna droga do wycieku lub utraty danych. Naprawić w ciągu 30 dni.
ŚREDNIE	Osłabia ochronę, groźne w połączeniu z innymi słabościami.
NISKIE	Dobra praktyka do wdrożenia przy okazji.

Audyt trwał jeden dzień roboczy. Trzy stacje robocze były wyłączone w trakcie skanu – zbadano je tylko na podstawie ankiety. Raport opisuje stan z dnia audytu.

3. Wyniki w obszarach

Kod	Obszar	Najwyższe ryzyko	Ustaleń
BRZ	Brzeg sieci – router i firewall	bez zastrzeżeń	–
WIF	Sieć bezprzewodowa (Wi-Fi)	bez zastrzeżeń	–
SEG	Segmentacja i urządzenia IoT	WYSOKIE	1
INW	Inwentaryzacja i stacje robocze	ŚREDNIE	1
SRV	Serwery, NAS i udostępnienia	ŚREDNIE	1
KON	Konta, hasła i MFA	WYSOKIE	1
DOM	Poczta i domena	ŚREDNIE	1
WEB	Aplikacja webowa i formularze	ŚREDNIE	1
EKS	Ekspozycja w internecie	KRYTYCZNE	1
KOP	Kopie zapasowe	KRYTYCZNE	1
AKT	Aktualizacje i podatności	bez zastrzeżeń	–
OCH	Ochrona stacji roboczych	bez zastrzeżeń	–
FIZ	Bezpieczeństwo fizyczne i procedury	NISKIE	1

4. Ustalenia szczegółowe

U–01 KRYTYCZNE Ekspozycja w internecie • kontrola EKS-03

Panel administracyjny NAS dostępny z internetu

Co stwierdzono: Router przekierowuje porty 5000 i 5001 z internetu na NAS. Panel logowania DSM jest widoczny dla każdego, a w wyszukiwarce Shodan adres firmy jest oznaczony jako Synology.

Dlaczego to ważne: Każdy w internecie może próbować logowania do serwera z dokumentami klientów; panele NAS są masowo atakowane (zgadywanie haseł, znane podatności, ransomware).

Dowód

```
$ nmap -Pn -sV -p 5000,5001 203.0.113.10
PORT     STATE SERVICE  VERSION
5000/tcp open  http     Synology DSM
5001/tcp open  ssl/http Synology DSM

Router → Przekierowania portów: 5000→192.168.1.20:5000, 5001→192.168.1.20:5001
```

Rekomendacja: Usunąć oba przekierowania portów. Dostęp zdalny wyłącznie przez VPN z MFA (np. WireGuard na routerze lub Tailscale). Do czasu zmiany: włączyć 2FA i autoblokadę w DSM.

Pracochłonność: mały (ok. 1 h) • Zalecany termin: natychmiast

U–02 KRYTYCZNE Kopie zapasowe • kontrola KOP-03

Jedyna kopia zapasowa podatna na ransomware

Co stwierdzono: Kopia dokumentów jest wykonywana co noc na dysk USB podłączony na stałe do NAS w tym samym pomieszczeniu. Folder kopii jest udostępniony w sieci z prawem zapisu dla wszystkich użytkowników. Brak kopii poza biurem i brak wersjonowania.

Dlaczego to ważne: Ransomware z dowolnego komputera zaszyfruje jednocześnie dane i kopię. Pożar, zalanie lub kradzież zniszczy wszystko naraz. Firma może utracić dokumentację klientów (obowiązki z RODO i ordynacji podatkowej).

Dowód

```
Hyper Backup: zadanie "Dokumenty" → USB1, codziennie 23:00, wersjonowanie: wyłączone
Udostępnienie \\NAS\kopia — grupa "users": odczyt/zapis
Ostatni test odtworzenia: brak (wg wywiadu)
```

Rekomendacja: Wdrożyć zasadę 3-2-1: włączyć wersjonowanie i niezmienne snapshoty na NAS, zabrać prawo zapisu do folderu kopii, dodać szyfrowaną kopię poza biurem (chmura lub drugi NAS u właściciela). Raz na kwartał test odtworzenia.

Pracochłonność: średni (1 dzień + koszt chmury) • Zalecany termin: natychmiast

U–03 WYSOKIE Konta, hasła i MFA • kontrola KON-01

Brak MFA na skrzynkach pocztowych Microsoft 365

Co stwierdzono: Na 9 kontach M365 tylko 1 ma włączone uwierzytelnianie dwuskładnikowe. Konto biuro@ jest współdzielone przez 4 osoby jednym hasłem.

Dlaczego to ważne: Przejęcie hasła (phishing, wyciek) daje pełny dostęp do korespondencji z klientami i możliwość podszycia się pod biuro, np. w sprawie przelewów.

Dowód

```
Centrum administracyjne M365 → Użytkownicy aktywni → Stan MFA: 1/9 włączone
biuro@demo-biuro.pl — logowania z 4 komputerów (zamaskowano adresy)
```

Rekomendacja: Włączyć Security Defaults lub zasady MFA dla wszystkich kont; biuro@ zamienić na skrzynkę współdzieloną (bez własnego hasła) z dostępem dla wybranych osób.

Pracochłonność: mały (2–3 h) • Zalecany termin: 30 dni

U–04 WYSOKIE Segmentacja i urządzenia IoT • kontrola SEG-02

Rejestrator kamer w sieci biurowej z domyślnym hasłem

Co stwierdzono: Rejestrator NVR jest w tej samej sieci co komputery księgowe. Panel WWW przyjmuje domyślne hasło producenta (sprawdzone za zgodą zleceniodawcy). Firmware z 2021 r.

Dlaczego to ważne: Przejęte urządzenie IoT w sieci biurowej to wygodny punkt startowy ataku na komputery i NAS; dodatkowo podgląd kamer biura.

Dowód

```
$ nmap -sV -p80,554,8000 192.168.1.64
80/tcp   open http  Hikvision-Webs
554/tcp  open rtsp
8000/tcp open http-alt
Logowanie hasłem domyślnym producenta: UDANE (hasło zamaskowane)
```

Rekomendacja: Zmienić hasło, zaktualizować firmware, przenieść kamery i NVR do osobnej sieci/VLAN bez dostępu do komputerów.

Pracochłonność: średni (pół dnia) • Zalecany termin: 30 dni

U–05 ŚREDNIE Serwery, NAS i udostępnienia • kontrola SRV-03

NAS dopuszcza przestarzały protokół SMB1

Co stwierdzono: Minimalna wersja protokołu udostępniania plików na NAS to SMB1.

Dlaczego to ważne: SMB1 ma znane, poważne podatności wykorzystywane przez robaki ransomware (np. WannaCry).

Dowód

```
$ nmap -p445 --script smb-protocols 192.168.1.20
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.0.2  2.1  3.0  3.0.2  3.1.1
```

Rekomendacja: W DSM: Panel sterowania → Usługi plików → SMB → minimalna wersja SMB2 (lepiej SMB3). Sprawdzić skaner w drukarce, jeśli zapisuje skany na NAS.

Pracochłonność: mały (15 min) • Zalecany termin: 90 dni

U–06 ŚREDNIE Poczta i domena • kontrola DOM-03

Brak rekordu DMARC dla domeny

Co stwierdzono: Domena ma poprawny SPF, DKIM jest włączony w M365, ale brak polityki DMARC.

Dlaczego to ważne: Oszuści mogą łatwiej wysyłać wiadomości „od biura” do klientów (np. z fałszywym numerem konta).

Dowód

```
$ dig +short TXT _dmarc.demo-biuro.pl
(brak odpowiedzi)
$ dig +short TXT demo-biuro.pl
"v=spf1 include:spf.protection.outlook.com -all"
```

Rekomendacja: Dodać rekord _dmarc z p=none i raportami, po 2–4 tygodniach obserwacji zmienić na p=quarantine, docelowo p=reject.

Pracochłonność: mały (30 min + obserwacja) • Zalecany termin: 90 dni

U–10 ŚREDNIE Aplikacja webowa i formularze • kontrola WEB-06

Strona WWW na WordPressie z nieaktualną wtyczką

Co stwierdzono: Strona firmowa działa na WordPressie. Jedna z wtyczek formularza kontaktowego jest w wersji z publicznie znaną podatnością; panel logowania dostępny pod standardowym adresem /wp-admin bez ograniczeń i bez logowania dwuetapowego. Nie testowano wstrzyknięć na środowisku produkcyjnym (brak zgody na testy aktywne).

Dlaczego to ważne: Przestarzała wtyczka to jedna z najczęstszych dróg przejęcia strony (zmiana treści, podrzucenie złośliwego kodu, phishing na klientach firmy).

Dowód

```
Generator: <meta name="generator" content="WordPress 6.4">
Wtyczka: contact-form-xx 4.1 (aktualna 4.7; CVE opublikowane)
/wp-admin → formularz logowania, brak limitu prób, brak 2FA
```

Rekomendacja: Zaktualizować WordPressa i wszystkie wtyczki, włączyć automatyczne aktualizacje bezpieczeństwa, ograniczyć dostęp do /wp-admin (hasło, 2FA, ewentualnie ograniczenie po IP). Rozważyć osobny audyt aplikacji webowej z testami na kopii testowej.

Pracochłonność: mały (1–2 h) • Zalecany termin: 90 dni

U–07 ŚREDNIE Inwentaryzacja i stacje robocze • kontrola INW-02

Komputer z Windows 10 bez aktualizacji bezpieczeństwa

Co stwierdzono: Stanowisko w recepcji pracuje na Windows 10 22H2 bez programu ESU – od 14.10.2025 nie dostaje poprawek bezpieczeństwa.

Dlaczego to ważne: Nowe podatności systemu nie będą łatane; komputer ma dostęp do NAS i poczty.

Dowód

```
winver: Windows 10 Pro 22H2 (19045.6456)
Windows Update: "Ta wersja systemu Windows osiągnęła koniec wsparcia"
```

Rekomendacja: Aktualizacja do Windows 11 (sprzęt to obsługuje) albo wykupienie ESU na rok przejściowy.

Pracochłonność: średni (2–3 h) • Zalecany termin: 90 dni

U–08 NISKIE Bezpieczeństwo fizyczne i procedury • kontrola FIZ-02

Brak UPS dla routera i NAS

Co stwierdzono: Router i NAS są zasilane bezpośrednio z listwy; zanik prądu oznacza twarde wyłączenie NAS.

Dlaczego to ważne: Ryzyko uszkodzenia systemu plików NAS i przerwy w pracy.

```
Dowód
Zdjęcie szafki — plik FIZ-02_szafka.jpg
```

Rekomendacja: UPS ok. 600–800 VA z podłączeniem USB do NAS (bezpieczne zamknięcie).

Pracochłonność: mały (zakup ok. 400–600 zł) • Zalecany termin: 90 dni

U–09 INFO Sieć bezprzewodowa (Wi-Fi) • kontrola WIF-04

Sieć gości poprawnie odizolowana

Co stwierdzono: Z sieci gości nie ma dostępu do urządzeń w sieci biurowej.

Dlaczego to ważne: Brak – obserwacja pozytywna.

```
Dowód
$ nmap -sn 192.168.1.0/24   (z sieci gości)
Nmap done: 256 IP addresses (0 hosts up)
```

Rekomendacja: Utrzymać. Zmieniać hasło sieci gości co kwartał.

Pracochłonność: – • Zalecany termin: –

5. Plan naprawczy

Kolejność według ryzyka. Kolumnę „Odpowiedzialny / data” warto uzupełnić na spotkaniu podsumowującym.

Natychmiast (do 7 dni)

	ID	Zadanie	Pracochłonność	Odpowiedzialny / data
☐	U–01	Panel administracyjny NAS dostępny z internetu	mały (ok. 1 h)	
☐	U–02	Jedyna kopia zapasowa podatna na ransomware	średni (1 dzień + koszt chmury)	

W ciągu 30 dni

	ID	Zadanie	Pracochłonność	Odpowiedzialny / data
☐	U–03	Brak MFA na skrzynkach pocztowych Microsoft 365	mały (2–3 h)	
☐	U–04	Rejestrator kamer w sieci biurowej z domyślnym hasłem	średni (pół dnia)	

W ciągu 90 dni

	ID	Zadanie	Pracochłonność	Odpowiedzialny / data
☐	U–05	NAS dopuszcza przestarzały protokół SMB1	mały (15 min)	
☐	U–06	Brak rekordu DMARC dla domeny	mały (30 min + obserwacja)	
☐	U–10	Strona WWW na WordPressie z nieaktualną wtyczką	mały (1–2 h)	
☐	U–07	Komputer z Windows 10 bez aktualizacji bezpieczeństwa	średni (2–3 h)	
☐	U–08	Brak UPS dla routera i NAS	mały (zakup ok. 400–600 zł)	

Po wdrożeniu poprawek zalecany jest audyt powtórny (weryfikacja), najlepiej w ciągu 3–6 miesięcy.

6. Inwentaryzacja urządzeń

Adres IP	Nazwa	Typ	System / firmware	Uwagi
192.168.1.1	router	router/firewall	RouterOS 7.16	U-01
192.168.1.2–3	AP-biuro, AP-sala	punkty dostępowe Wi-Fi	firmware 5.1 (aktualny)	
192.168.1.20	NAS	Synology DS220+	DSM 7.2.2	U-01, U-02, U-05
192.168.1.31–38	PC-01…PC-08	stacje robocze	Windows 11 (7), Windows 10 (1)	U-07 (PC-08)
192.168.1.50	drukarka	urządzenie wielofunkcyjne	firmware 2024	
192.168.1.64	NVR	rejestrator kamer	firmware 2021	U-04

Oświadczenie i ograniczenia

Audyt przeprowadzono w zakresie i w terminie określonym w upoważnieniu zleceniodawcy. Raport odzwierciedla stan infrastruktury w dniu badania i nie gwarantuje braku innych podatności. Raport ma charakter techniczny i nie stanowi porady prawnej. Dane osobowe i hasła w dowodach zostały zamaskowane.

.....

Jakub Gorący