MESH PC

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

RAPORT Z AUDYTU IT

Kancelaria Przykładowa (raport demonstracyjny)

Data audytu: 25 listopada 2026 · kancelaria-demo.example · Audytor: Sebastiano Blanco, MeshPC · 3 komputerów

OCENA OGÓLNA

Wymaga pilnych działań

Są zagrożenia, które mogą zatrzymać firmę lub doprowadzić do wycieku danych.

Wynik w obszarach

Domena i poczta e-mail	Microsoft 365	Konta, hasła i MFA	Komputery
Do poprawy sprawdzono 10 z 10	Nie sprawdzono	Do poprawy sprawdzono 1 z 1	Pilne sprawdzono 12 z 12

Kopie zapasowe	Sieć i Wi-Fi	Gotowość na NIS2
Nie sprawdzono	Pilne sprawdzono 6 z 6	Nie sprawdzono

Dobrze · Do poprawy · Pilne · Nie sprawdzono

Obszary oznaczone jako „Nie sprawdzono" nie były objęte tym raportem. Pełny audyt sprawdza wszystkie 8 obszarów i trwa 60–90 minut.

Najważniejsze do naprawy

1. **System operacyjny ze wsparciem producenta**
   System bez wsparcia nie dostaje poprawek bezpieczeństwa – znane luki zostają otwarte na zawsze.
   Co znaleźliśmy: 3 z 3: RECEPCJA-PC – Windows 10 Pro 22H2 – wsparcie zakończone 14.10.2025; LAPTOP-SZEF – Windows ...
   Zalecenie: Aktualizacja do wersji objętej wsparciem (Windows 11 25H2; macOS 15, 26 lub 27); sprzęt niespełniający wymagań – wymiana lub przejściowo Windows 10 ESU.

2. **Instalowanie aktualizacji**
   Brak aktualizacji to najczęstsza droga ataku ransomware na małe firmy.
   Co znaleźliśmy: 2 z 3: RECEPCJA-PC – ostatnia aktualizacja 2026-08-02 (115 dni temu); MacBook-Kasia – ostatnia ...
   Zalecenie: Automatyczna instalacja aktualizacji systemu i aplikacji z wymuszonym restartem w ciągu kilku dni (np. Windows Update for Business / Intune) oraz okresowa kontrola zgodności.

3. **Antywirus / EDR aktywny i aktualny**
   Bez aktywnej ochrony złośliwe oprogramowanie działa niezauważone.
   Co znaleźliśmy: 3 z 3: RECEPCJA-PC – kilka aktywnych antywirusów naraz: Windows Defender, Avast Free Antivirus ...
   Zalecenie: Jeden aktywny program ochronny na komputer; rozwiązanie klasy EDR (np. Microsoft Defender for Business) z ochroną przed manipulacją i centralnym podglądem alertów.

PRZYKŁAD

MESH PC

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

Plan działań

Priorytet wynika z wagi zagrożenia: punkty, które mogą zatrzymać pracę firmy lub doprowadzić do wycieku danych, są oznaczone jako pilne.

PILNE – DO 7 DNI

D1 **System operacyjny ze wsparciem producenta** — Pilne

Co znaleźliśmy: 3 z 3: RECEPCJA-PC – Windows 10 Pro 22H2 – wsparcie zakończone 14.10.2025; LAPTOP-SZEF – Windows 11 Pro 24H2 – wsparcie zakończone 2026-10-13; MacBook-Kasia – macOS 14.7 – bez poprawek bezpieczeństwa

Zalecenie: Aktualizacja do wersji objętej wsparciem (Windows 11 25H2; macOS 15, 26 lub 27); sprzęt niespełniający wymagań – wymiana lub przejściowo Windows 10 ESU.

D2 **Instalowanie aktualizacji** — Pilne

Co znaleźliśmy: 2 z 3: RECEPCJA-PC – ostatnia aktualizacja 2026-08-02 (115 dni temu); MacBook-Kasia – ostatnia aktualizacja 2026-10-20 (36 dni temu)

Zalecenie: Automatyczna instalacja aktualizacji systemu i aplikacji z wymuszonym restartem w ciągu kilku dni (np. Windows Update for Business / Intune) oraz okresowa kontrola zgodności.

D3 **Antywirus / EDR aktywny i aktualny** — Pilne

Co znaleźliśmy: 3 z 3: RECEPCJA-PC – kilka aktywnych antywirusów naraz: Windows Defender, Avast Free Antivirus; LAPTOP-SZEF – Windows Defender (bez EDR); MacBook-Kasia – tylko wbudowany XProtect

Zalecenie: Jeden aktywny program ochronny na komputer; rozwiązanie klasy EDR (np. Microsoft Defender for Business) z ochroną przed manipulacją i centralnym podglądem alertów.

D4 **Szyfrowanie dysku (BitLocker / FileVault)** — Pilne

Co znaleźliśmy: 3 z 3: RECEPCJA-PC – dysk niezaszyfrowany; LAPTOP-SZEF – BitLocker włączony, brak potwierdzenia kopii klucza; MacBook-Kasia – FileVault wyłączony (laptop)

Zalecenie: BitLocker z TPM (Windows) lub FileVault (macOS) na wszystkich komputerach, w pierwszej kolejności na laptopach; klucze odzyskiwania przechowywane w Entra ID lub MDM.

G1 **Usługi biura widoczne z internetu** — Pilne

Co znaleźliśmy: adres biura 203.0.113.25: otwarte porty 443, 3389

Zalecenie: Usunąć na routerze przekierowania portów usług administracyjnych (RDP, SMB, panel NAS, SSH); dostęp zdalny wyłącznie przez VPN z MFA.

WYSOKI – DO 30 DNI

A9 **Domeny łudząco podobne do Państwa domeny** — Pilne

Co znaleźliśmy: Podobne domeny z działającą pocztą: kancelaria-dem0.example; zarejestrowane: kancelaria-demo.example.com, kancelariademo.example

Zalecenie: Sprawdzić właścicieli domen (WHOIS/RDAP), nadużycia zgłosić rejestratorowi, rozważyć rejestrację kluczowych wariantów i uprzedzić pracowników oraz księgowość.

PRZYKŁAD

MESH PC

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

D7 **Programy do zdalnego dostępu** Pilne

Co znaleźliśmy: 2 z 3: RECEPCJA-PC – AnyDesk, TeamViewer; MacBook-Kasia – AnyDesk (niezarządzany)

Zalecenie: Jedno narzędzie zdalnego wsparcia z kontem firmowym, MFA i rejestrem sesji; pozostałe odinstalować i zablokować ich instalację.

D8 **Przestarzałe lub podatne oprogramowanie** Pilne

Co znaleźliśmy: 2 z 3: RECEPCJA-PC – WinRAR 6.11.0 (CVE-2025-8088), Microsoft Office Professional Plus 2016 – bez wsparcia, Java 8 Update 251; LAPTOP-SZEF – 7-Zip 23.01

Zalecenie: Odinstalować oprogramowanie bez wsparcia producenta, zaktualizować pozostałe do bieżących wersji i objąć je automatycznymi aktualizacjami.

F5 **Ryzykowne usługi w sieci (SMBv1, Telnet, RDP)** Pilne

Co znaleźliśmy: 192.168.1.1 Telnet; 192.168.1.10 nas.local SMBv1

Zalecenie: Wyłączyć SMBv1 i Telnet na wszystkich urządzeniach (w razie potrzeby aktualizacja firmware NAS i drukarek), ograniczyć RDP do wybranych adresów lub do połączeń przez VPN.

F6 **Filtrowanie DNS (blokada złośliwych stron)** Pilne

Co znaleźliśmy: 3 z 3 bez filtrowania (DNS: 192.168.1.1)

Zalecenie: Filtrowanie DNS blokujące domeny złośliwe i phishingowe (np. Quad9, Cloudflare Gateway, DNSFilter), ustawione na routerze oraz na laptopach używanych poza biurem.

A7 **Aktualność oprogramowania strony www** Pilne

Co znaleźliśmy: Strona działa na PHP 8.1 bez wsparcia bezpieczeństwa.

Zalecenie: Aktualizacja CMS, wtyczek i PHP do wersji objętych wsparciem bezpieczeństwa; ukrycie nagłówków Server/X-Powered-By i znacznika generator.

D6 **Automatyczna blokada ekranu** Pilne

Co znaleźliśmy: 3 z 3: RECEPCJA-PC – brak automatycznej blokady; LAPTOP-SZEF – blokada po 15 min; MacBook-Kasia – blokada po 15 min

Zalecenie: Blokada ekranu po maks. 10 minutach bezczynności, wymuszona zasadą (GPO, Intune lub profil MDM) i wymagająca hasła lub PIN-u.

D10 **Wiek sprzętu** Pilne

Co znaleźliśmy: 2 z 3: RECEPCJA-PC – OptiPlex 3050, BIOS z 2017; MacBook-Kasia – MacBook Air M1 (~2020)

Zalecenie: Plan wymiany komputerów starszych niż 6 lat, w pierwszej kolejności tych, które nie spełniają wymagań Windows 11.

D12 **Kontrola pamięci USB** Pilne

Co znaleźliśmy: 3 z 3: RECEPCJA-PC – pamięci USB bez ograniczeń; LAPTOP-SZEF – pamięci USB bez ograniczeń; MacBook-Kasia – pamięci USB bez ograniczeń

Zalecenie: Zasada blokująca lub rejestrująca użycie nośników USB (GPO lub Intune Device Control), z wyjątkami dla zatwierdzonych, szyfrowanych urządzeń.

PRZYKŁAD

MESH PC

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

PLANOWY – DO 90 DNI

A6 **Certyfikat SSL i HTTPS strony www** — Do poprawy

Co znaleźliśmy: kancelaria-demo.example: brak nagłówka HSTS; www.kancelaria-demo.example: brak nagłówka HSTS

Zalecenie: Certyfikat odnawiany automatycznie, przekierowanie 301 z http na https dla domeny i www, nagłówek Strict-Transport-Security z max-age co najmniej 6 miesięcy (RFC 6797).

A10 **Firmowe adresy e-mail w znanych wyciekach danych** — Do poprawy

Co znaleźliśmy: Adresy firmowe wyłącznie w starszych wyciekach.

Zalecenie: Zmienić hasła kont występujących w wyciekach, wymusić MFA i sprawdzić, czy te same hasła nie są używane w innych usługach.

C6 **Uprawnienia administratora na komputerach** — Do poprawy

Co znaleźliśmy: 2 z 3: RECEPCJA-PC – użytkownik anna jest administratorem; MacBook-Kasia – użytkownik kasia jest administratorem

Zalecenie: Codzienna praca na koncie standardowym; instalacje przez osobne konto administracyjne zarządzane np. przez Windows LAPS lub Intune Endpoint Privilege Management.

D5 **Zapora sieciowa (firewall) komputera** — Do poprawy

Co znaleźliśmy: 2 z 3: RECEPCJA-PC – zapora wyłączona: Private; MacBook-Kasia – zapora macOS wyłączona

Zalecenie: Zapora włączona dla profili domena, prywatny i publiczny, zarządzana centralnie; reguły przychodzące tylko dla wymaganych usług.

D9 **Stan i wolne miejsce dysku** — Do poprawy

Co znaleźliśmy: 2 z 3: RECEPCJA-PC – wolne 9% (21 GB); MacBook-Kasia – wolne 12% (30 GB)

Zalecenie: Kopia danych i wymiana dysku z ostrzeżeniami SMART; zwolnienie miejsca do co najmniej 20% wolnej przestrzeni na dysku systemowym.

D11 **Centralne zarządzanie komputerami (Intune / RMM)** — Do poprawy

Co znaleźliśmy: 2 z 3: RECEPCJA-PC – niezarządzany; MacBook-Kasia – niezarządzany

Zalecenie: Rejestracja komputerów w Microsoft Intune (lub innym MDM/RMM), aby egzekwować zasady bezpieczeństwa, aktualizacje i inwentaryzację.

G2 **Znane podatności na publicznym adresie IP** — Do poprawy

Co znaleźliśmy: 203.0.113.25: potencjalne podatności do weryfikacji (2): CVE-2023-44487, CVE-2024-3400

Zalecenie: Zweryfikować wskazane CVE na urządzeniu brzegowym (router, firewall, NAS) i zainstalować aktualizacje firmware lub wyłączyć narażoną usługę.

A4 **Dostawca poczty (rekordy MX)** — Do poprawy

Co znaleźliśmy: Poczta na serwerze hostingowym: mx.hosting-provider.example

Zalecenie: Rozważyć pocztę z ochroną antyspamową i antyphishingową klasy biznesowej (np. Exchange Online z Defender for Office 365); do tego czasu włączyć dostępne filtrowanie u obecnego dostawcy.

PRZYKŁAD

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

A5 **Szyfrowanie poczty między serwerami (TLS, MTA-STS)** — Do poprawy

Co znaleźliśmy: Nie udało się sprawdzić STARTTLS (port 25 zablokowany po drodze); brak MTA-STS.

Zalecenie: Wymagać TLS dla połączeń SMTP, opublikować politykę MTA-STS w trybie enforce (RFC 8461) oraz raporty TLS-RPT (RFC 8460).

A8 **Ochrona domeny (DNSSEC, blokada transferu)** — Do poprawy

Co znaleźliśmy: DNSSEC: nie, blokada transferu: tak; domena opłacona do 2027-10-01

Zalecenie: Włączyć DNSSEC u operatora DNS i opublikować rekord DS u rejestratora (RFC 4033); utrzymać blokadę transferu i automatyczne odnawianie domeny.

F4 **Urządzenia w sieci biura** — Do poprawy

Co znaleźliśmy: urządzenia w sieci 192.168.1.25/24: 3 – lista w załączniku do potwierdzenia z klientem; bez nazwy, z otwartymi portami administracyjnymi: 192.168.1.1 (80,443,23)

Zalecenie: Inwentaryzacja urządzeń sieciowych z przypisanym właścicielem, zmiana haseł domyślnych i odłączenie urządzeń nieznanych.

Następny krok
Chętnie omówimy wyniki, odpowiemy na pytania dotyczące poszczególnych punktów i pomożemy ustalić kolejność działań. Kontakt: +48 789 599 983, info@meshpc.pl.

PRZYKŁAD

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

Załącznik: wszystkie sprawdzone punkty

NR	PUNKT KONTROLI	STATUS	CO ZNALEŹLIŚMY
A. Domena i poczta e-mail			
A1	Rekord SPF (kto może wysyłać pocztę z domeny)	Dobrze	`v=spf1 a mx include:_spf.hosting-provider.example ~all (zapytania DNS: 4)`
A2	Podpis DKIM wysyłanych wiadomości	Dobrze	`DKIM: x (2048-bit+)`
A3	Polityka DMARC (ochrona przed podszywaniem się)	Dobrze	`v=DMARC1; p=quarantine; sp=quarantine; adkim=r; aspf=r; fo=1; rua=mailto:dmarc@kancelaria-demo.example`
A4	Dostawca poczty (rekordy MX)	Do poprawy	`Poczta na serwerze hostingowym: mx.hosting-provider.example`
A5	Szyfrowanie poczty między serwerami (TLS, MTA-STS)	Do poprawy	`Nie udało się sprawdzić STARTTLS (port 25 zablokowany po drodze); brak MTA-STS.`
A6	Certyfikat SSL i HTTPS strony www	Do poprawy	`kancelaria-demo.example: brak nagłówka HSTS; www.kancelaria-demo.example: brak nagłówka HSTS`
A7	Aktualność oprogramowania strony www	Pilne	`Strona działa na PHP 8.1 bez wsparcia bezpieczeństwa.`
A8	Ochrona domeny (DNSSEC, blokada transferu)	Do poprawy	`DNSSEC: nie, blokada transferu: tak; domena opłacona do 2027-10-01`
A9	Domeny łudząco podobne do Państwa domeny	Pilne	`Podobne domeny z działającą pocztą: kancelaria-dem0.example; zarejestrowane: kancelaria-demo.example.com, kancelariademo.example`
A10	Firmowe adresy e-mail w znanych wyciekach danych	Do poprawy	`Adresy firmowe wyłącznie w starszych wyciekach.`
C. Konta, hasła i MFA			
C6	Uprawnienia administratora na komputerach	Do poprawy	`2 z 3: RECEPCJA-PC – użytkownik anna jest administratorem; MacBook-Kasia – użytkownik kasia jest administratorem`
D. Komputery			
D1	System operacyjny ze wsparciem producenta	Pilne	`3 z 3: RECEPCJA-PC – Windows 10 Pro 22H2 – wsparcie zakończone 14.10.2025; LAPTOP-SZEF – Windows 11 Pro 24H2 – wsparcie zakończone 2026-10-13; MacBook-Kasia – macOS 14.7 – bez poprawek bezpieczeństwa`

PRZYKŁAD

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

NR	PUNKT KONTROLI	STATUS	CO ZNALEŹLIŚMY
D2	Instalowanie aktualizacji	Pilne	2 z 3: RECEPCJA-PC – ostatnia aktualizacja 2026-08-02 (115 dni temu); MacBook-Kasia – ostatnia aktualizacja 2026-10-20 (36 dni temu)
D3	Antywirus / EDR aktywny i aktualny	Pilne	3 z 3: RECEPCJA-PC – kilka aktywnych antywirusów naraz: Windows Defender, Avast Free Antivirus; LAPTOP-SZEF – Windows Defender (bez EDR); MacBook-Kasia – tylko wbudowany XProtect
D4	Szyfrowanie dysku (BitLocker / FileVault)	Pilne	3 z 3: RECEPCJA-PC – dysk niezaszyfrowany; LAPTOP-SZEF – BitLocker włączony, brak potwierdzenia kopii klucza; MacBook-Kasia – FileVault wyłączony (laptop)
D5	Zapora sieciowa (firewall) komputera	Do poprawy	2 z 3: RECEPCJA-PC – zapora wyłączona: Private; MacBook-Kasia – zapora macOS wyłączona
D6	Automatyczna blokada ekranu	Pilne	3 z 3: RECEPCJA-PC – brak automatycznej blokady; LAPTOP-SZEF – blokada po 15 min; MacBook-Kasia – blokada po 15 min
D7	Programy do zdalnego dostępu	Pilne	2 z 3: RECEPCJA-PC – AnyDesk, TeamViewer; MacBook-Kasia – AnyDesk (niezarządzany)
D8	Przestarzałe lub podatne oprogramowanie	Pilne	2 z 3: RECEPCJA-PC – WinRAR 6.11.0 (CVE-2025-8088), Microsoft Office Professional Plus 2016 – bez wsparcia, Java 8 Update 251; LAPTOP-SZEF – 7-Zip 23.01
D9	Stan i wolne miejsce dysku	Do poprawy	2 z 3: RECEPCJA-PC – wolne 9% (21 GB); MacBook-Kasia – wolne 12% (30 GB)
D10	Wiek sprzętu	Pilne	2 z 3: RECEPCJA-PC – OptiPlex 3050, BIOS z 2017; MacBook-Kasia – MacBook Air M1 (~2020)
D11	Centralne zarządzanie komputerami (Intune / RMM)	Do poprawy	2 z 3: RECEPCJA-PC – niezarządzany; MacBook-Kasia – niezarządzany
D12	Kontrola pamięci USB	Pilne	3 z 3: RECEPCJA-PC – pamięci USB bez ograniczeń; LAPTOP-SZEF – pamięci USB bez ograniczeń; MacBook-Kasia – pamięci USB bez ograniczeń
F. Sieć i Wi-Fi			
F2	Zabezpieczenie sieci Wi-Fi	Dobrze	Firma: WPA2-Personal CCMP (siłę hasła sprawdzamy z klientem)
F4	Urządzenia w sieci biura	Do poprawy	urządzenia w sieci 192.168.1.25/24: 3 – lista w załączniku do potwierdzenia z klientem; bez nazwy, z otwartymi portami administracyjnymi: 192.168.1.1 (80,443,23)
F5	Ryzykowne usługi w sieci (SMBv1, Telnet, RDP)	Pilne	192.168.1.1 Telnet; 192.168.1.10 nas.local SMBv1

PRZYKŁAD

+48 789 599 983
info@meshpc.pl
www.meshpc.pl

NR	PUNKT KONTROLI	STATUS	CO ZNALEŹLIŚMY
F6	Filtrowanie DNS (blokada złośliwych stron)	Pilne	`3 z 3 bez filtrowania (DNS: 192.168.1.1)`
G. Serwery i dostęp z internetu			
G1	Usługi biura widoczne z internetu	Pilne	`adres biura 203.0.113.25: otwarte porty 443, 3389`
G2	Znane podatności na publicznym adresie IP	Do poprawy	`203.0.113.25: potencjalne podatności do weryfikacji (2): CVE-2023-44487, CVE-2024-3400`

Komputery objęte audytem

KOMPUTER	SYSTEM	MODEL	UŻYTKOWNIK	OSTATNIA AKTUALIZACJA
RECEPCJA-PC	Windows 10 Pro 22H2	Dell Inc. OptiPlex 3050	anna	2026-08-02
LAPTOP-SZEF	Windows 11 Pro 24H2	Lenovo ThinkPad T14 Gen 4 (laptop)	jan	2026-11-12
MacBook-Kasia	macOS 14.7	Apple MacBook Air (laptop)	kasia	2026-10-20

Urządzenia znalezione w sieci biura

ADRES IP	NAZWA	MAC	OTWARTE PORTY
192.168.1.1	– (router)	`AA-BB`	`80, 443, 23`
192.168.1.10	nas.local	`CC`	`445, 5000 SMBv1`
192.168.1.25	RECEPCJA-PC (RECEPCJA-PC)		`445`
192.168.1.40	–		`9100, 80`

Audyt był wyłącznie do odczytu – niczego nie zmieniliśmy w Państwa systemach. Dane z audytu przechowujemy zgodnie z umową o zachowaniu poufności i usuwamy po 90 dniach.

PRZYKŁAD