Cyberbezpieczenstwo firmy od podstaw: przewodnik dla menedzerow

Od polityki hasel i MFA po Zero Trust i SIEM - co wdrozyc najpierw i jak ustalic priorytety w 2026 roku

Marek Sobieralski · 08.09.2026

W marcu 2025 roku jeden z moich klientow - firma logistyczna z Poznania, 180 pracownikow - stracil dostep do calej infrastruktury na 11 dni. Ransomware dostal sie przez konto serwisowe z haslem Admin2019, ktore nikt nie zmienil od czterech lat. Okup: 280 000 euro. Zaplacili. Odtworzenie srodowiska zajelo kolejny tydzien. Laczne straty? Ponad 1,2 miliona zlotych. A caly ten scenariusz mozna bylo zablokowac za kilkaset zlotych miesiecznie - MFA i porzadna polityka hasel. Tyle.

Ten artykul jest dla menedzerow, ktorzy wiedza, ze cyberbezpieczenstwo liczy sie, ale nie maja pojecia, gdzie zaczac. Nie bedzie tu akademickiego zargonu - za to konkretna kolejnosc dzialan, liczby i realne priorytety na 2026 rok.

1. Zacznij od audytu: nie mozesz chronic tego, czego nie widzisz

Pierwszy krok to nie zakup oprogramowania. To inwentaryzacja - brzmi nudnie, ale bez niej kazde kolejne dzialanie to strzal w ciemno. Musisz wiedziec, co masz: ile urzadzen, jakie systemy operacyjne, ktore aplikacje maja dostep do Internetu, gdzie siedzi Twoja najcenniejsza data.

Audyt techniczny obejmuje trzy warstwy:

- Warstwa sieciowa - mapa topologii, otwarte porty, urzadzenia IoT podlaczone do sieci (drukarki, kamery, termostaty)
- Warstwa aplikacyjna - lista oprogramowania, wersje, daty aktualizacji, konta z dostepem administratora
- Warstwa danych - gdzie sa dane osobowe, gdzie finansowe, kto tam ma dostep i czy to ma sens

Narzedzia takie jak Nmap czy darmowa wersja Nessus moga w kilka godzin wygenerowac raport o otwartych portach i podatnosciach. Dla firm powyzej 50 pracownikow warto zlecic zewnetrzny test penetracyjny - koszt to zwykle 8 000 do 25 000 zl w zaleznosci od zakresu.

2. Polityka hasel i MFA - fundament, ktory wiekszosc firm wciaz ignoruje

W 2026 roku firmowe hasla bez wieloskladnikowego uwierzytelniania to jak jazda bez pasow. Raport Verizon z 2025 roku mowi jasno: 74% naruszen danych wiaze sie z przejetymi lub slabymi haslami. Ta liczba nie spada od lat, bo firmy nie wdrazaja podstaw.

Minimalne standardy na 2026:

MFA musi byc obowiazkowe dla kazdego, kto ma dostep do systemow produkcyjnych, poczty firmowej lub VPN. Najlepsze opcje to aplikacje TOTP (Microsoft Authenticator, Google

Authenticator) lub klucze sprzetowe FIDO2 (YubiKey 5 to okolo 350 zl). SMS-owe kody to cos, ale podatne na SIM swapping - nie polecam jako jedyna metoda dla finansow czy opieki zdrowotnej.

Menedzer hasel dla calej organizacji (1Password Teams, Bitwarden for Business) kosztuje 15-25 zl na uzytkownika miesiecznie i eliminuje problem powtarzajacych sie hasel. To jeden z najlepszych stosunkow ceny do bezpieczenstwa w calym spektrum cyberochrony.

3. Zarzadzanie dostepem i zasada minimalnych uprawnien

To konto serwisowe z haslem Admin2019 - wlasnie takie zniszczylo poznanska firme. Problem nie byl techniczny, byl organizacyjny: nikt nie wiedzial, ze konto w ogole istnieje, bo zalozyl je podwykonawca trzy lata temu i nigdy go nie usunal.

Zasada minimalnych uprawnien to cos, co brzmi nudnie, ale dziala. Kazdy uzytkownik i kazda aplikacja powinni miec dostep wylacznie do tego, co faktycznie potrzebuja. Nic wiecej.

W praktyce:

- Regularne przeglady uprawnien - co kwartal sprawdzisz, kto ma dostep do czego. Ludzie zmienia role, odejda z firmy, a ich konta zostaja aktywne.
- Separacja kont administratorskich - administrator powinien miec dwa konta: jedno do normalnej pracy (bez uprawnien), drugie wylacznie do zadan admin.
- Zarzadzanie dostepem uprzywilejowanym (PAM) - CyberArk, BeyondTrust czy Delinea automatycznie rotuja hasla serwisowe i nagrywaja kazda sesje admin.

Dla firm do 100 osob wystarczy Azure Active Directory (Microsoft Entra ID) z odpowiednimi grupami bezpieczenstwa. To czesc licencji Microsoft 365 Business Premium - okolo 95 zl na uzytkownika miesiecznie.

4. Ochrona punktow koncowych - EDR zamiast starego antywirusa

Tradycyjny antywirus szuka znanych sygnatur - rozpoznaje zagrozenia, ktore juz widzial. Problem: atakujacy od lat uzywaja bezplikowych technik, ktore nie pozostawiaja pliku na dysku. Zaden tradycyjny antywirus ich nie zlapie.

EDR (Endpoint Detection and Response) to zupelnie inna gra. Zamiast szukac sygnatur, monitoruje zachowanie procesow w czasie rzeczywistym. Kiedy proces nagle szyfruje tysiace plikow na sekunde - EDR to widzi i moze automatycznie odizolowac urzadzenie zanim cokolwiek wiecej sie szyfruje.

Liderzy rynku to CrowdStrike Falcon (od ok. 200 zl rocznie na endpoint), Microsoft Defender for Endpoint (wbudowany w Microsoft 365 E3/E5) oraz SentinelOne. Dla mniejszych firm SentinelOne, Malwarebytes for Teams lub Bitdefender GravityZone - tansze, ale znacznie lepsze niz tradycyjny antywirus.

EDR bez odpowiedniej konfiguracji to jak kamera bez nagrywania. Sama instalacja to za malo - ktos musi reagowac na alerty. Jesli nie masz wewnetrznego SOC, wez MDR (Managed Detection and Response), gdzie dostawca monitoruje za ciebie.

5. Zero Trust - architektura dla swiata bez granic sieci