Cyber Security Pentest

Poradnik cyberbezpieczeństwo dla małych firm

W dzisiejszych czasach zrozumienie podstaw cyberbezpieczeństwa jest niezbędne dla każdej firmy – niezależnie od jej wielkości. Małe firmy, które często nie posiadają dedykowanego działu IT, są szczególnie narażone na cyberzagrożenia. Poniższy poradnik zawiera praktyczne wskazówki, które pomogą skutecznie chronić Twoją firmę przed cyberatakami.

---

1. Szkolenie pracowników

Najczęstszą przyczyną skutecznych ataków cybernetycznych jest brak świadomości pracowników.

Zalecenia:

- Organizuj regularne szkolenia z zakresu cyberbezpieczeństwa.
- Ucz, jak rozpoznawać podejrzane e-maile, linki i załączniki, jak należy zabezpieczać urządzenia i na co należy uważać.
- Opracuj jasne procedury postępowania w przypadku podejrzenia naruszenia bezpieczeństwa (np. nieznane e-maile, podejrzane telefony, podłączone urządzenia USB, próby wyłudzenia informacji, danych itp.).

---

2. Zabezpieczenie urządzeń firmowych

Każde urządzenie w firmie (routery, komputery, smartfony, drukarki, dyski zewnętrzne) może stać się celem ataku, stanowić potencjalne wejście cyberprzestępców do Twojej sieci do Twoich danych.

Zalecenia:

- **Aktualizuj oprogramowanie** – systemy operacyjne, aplikacje i urządzenia sieciowe, wiele ataków wykorzystuje luki tzw. podatności, które są łatwe do naprawienia przez aktualizację.
- **Stosuj oprogramowanie zabezpieczające** – płatne dobre programy antywirusy z funkcją VPN.

- **Szyfruj dane** – szczególnie na urządzeniach przenośnych. Dane przechowywane na laptopie lub smartfonie mogą zostać łatwo wykorzystane po kradzieży.

---

3. Silne hasła i uwierzytelnianie wieloskładnikowe (MFA)

Słabe hasła to jedna z głównych dróg dostępu dla cyberprzestępców.

Zalecenia:

- Stosuj unikalne, trudne do odgadnięcia hasła (minimum 14 znaków, złożone z dużych i małych liter, cyfr i symboli).
- Stosuj tylko jedno hasło do jednego „miejsca" logowania, unikaj stosowania tych samych haseł w różnych miejscach.
- Wprowadź MFA (np. aplikacje typu Google Authenticator, SMS, biometryka).
- Korzystaj z menedżerów haseł, np. **KeePass** – zabezpieczony silnym hasłem (min. 24 znaki), lokalnie przechowywany.

---

4. Zabezpieczenie sieci firmowej

Nieprawidłowo skonfigurowana sieć to otwarte drzwi dla atakujących.

Zalecenia:

- Zmień domyślne ustawienia routera (nazwa sieci, silne, długie nieprzewidywalne hasło).
- Włącz szyfrowanie WPA3 lub WPA2 i stosuj silne hasło Wi-Fi (min. 24 znaki).
- Skonfiguruj **firewall** – zarówno programowy, jak i na poziomie routera.
- Wdróż **VPN** dla wszystkich pracowników zdalnych oraz urządzeń łączących się przez Wi-Fi.
- Podziel sieć na segmenty (osobne sieci dla gości, urządzeń biurowych, krytycznych systemów).
- Monitoruj urządzenia podłączone do sieci, prowadź inwentaryzację i analizuj logi routera.
- Zabezpiecz się na wypadek awarii – miej zapasowy router i alternatywne łącze internetowe.

---

5. Ochrona danych

Dane to najcenniejszy zasób firmy – ich utrata lub wyciek może mieć poważne konsekwencje.

Zalecenia:

- Regularnie twórz kopie zapasowe (lokalne i w chmurze), zaszyfrowane np. przy użyciu BitLockera.
- Przechowuj wyłącznie dane niezbędne do działania firmy.
- Wdróż politykę ograniczonego dostępu – pracownicy powinni mieć dostęp tylko do danych potrzebnych im w pracy.

---

6. Zarządzanie dostępem

Ograniczenie uprawnień jest kluczowe dla ograniczenia ryzyka.

Zalecenia:

- Ustal role i przypisz odpowiednie uprawnienia – unikaj udzielania praw administratora.
- Regularnie przeglądaj konta użytkowników – usuwaj nieaktywne i aktualizuj dostępy po zmianie stanowiska.
- Zabezpieczaj konta mailowe byłych pracowników (zmiana hasła, przekierowania).
- Monitoruj aktywność użytkowników – możesz wykorzystać systemy takie jak:
    - Proxmox (serwer wirtualizacji),
    - pfSense, Pi-hole (zapora i filtr DNS),
    - Wazuh (system SIEM - monitorowanie bezpieczeństwa komputerów).
- Opracuj i kontroluj listę dozwolonego oprogramowania, zapewnij pracownikom dostęp do sprawdzonych instalatorów.
- Zdefiniuj którzy pracownicy, lub komputery musza mieć dostęp do Internetu, na co pozwala ten dostęp.

---

7. Zarządzanie incydentami

Atak może się zdarzyć nawet przy najlepszych zabezpieczeniach.

Zalecenia:

- Opracuj plan reagowania na incydenty (zgłaszanie, ocena, reakcja).

- Wyznacz osoby odpowiedzialne za reagowanie na incydenty i przeprowadź ich szkolenie.
- Przygotuj komunikację z klientami w przypadku wycieku danych.
- Stwórz plan **Disaster Recovery (DRP)** – scenariusze awaryjne, np. szybkie przywrócenie działania po ataku ransomware.

---

8. Zabezpieczenie aplikacji i oprogramowania

Aplikacje biznesowe (CRM, ERP, księgowość online) muszą być odpowiednio chronione.

Zalecenia:

- Dbaj o aktualizacje systemów, aplikacji i wtyczek.
- Od dostawców oprogramowania wymagaj raportów z testów bezpieczeństwa, skanów podatności, aktualizacji i wdrażania poprawek po pentestach.
- Jeśli tworzysz własne aplikacje – stosuj dobre praktyki programistyczne, testy bezpieczeństwa i kontrolę podatności.

---

9. Polityki bezpieczeństwa

Formalne zasady pomagają w utrzymaniu porządku i odpowiedzialności.

Zalecenia:

- Ustal politykę tworzenia i zmiany haseł.
- Opracuj politykę używania prywatnych urządzeń – czy można podłączać je do sieci lub systemów firmowych?
- Zdefiniuj politykę dostępu do danych – dostęp tylko dla osób, którym jest to niezbędne do pracy.

---

10. Współpraca z profesjonalistami

Nie musisz wszystkiego robić samodzielnie – warto korzystać z pomocy ekspertów.

Zalecenia:

- Skorzystaj z usług konsultantów ds. bezpieczeństwa IT.
- Rozważ outsourcing IT – firmy zewnętrzne mogą zarządzać Twoją infrastrukturą i przeprowadzać:

- audyty,
- testy penetracyjne,
- skanowanie podatności,
- konfigurację zabezpieczeń (hardening urządzeń i systemów np. według CIS CONTROLS),
- szkolenia pracowników.

Podsumowanie

Cyberbezpieczeństwo to inwestycja, nie koszt. Nawet proste środki, jak regularne aktualizacje, szkolenia czy silne hasła, mogą znacząco zwiększyć poziom ochrony firmy. Dla małych i średnich firm kluczowe jest podejście oparte na świadomości, planowaniu i wdrażaniu sprawdzonych praktyk – wszystko to można osiągnąć przy stosunkowo niewielkich nakładach finansowych.

Zespół CyberSecurityPentest