



CZY TWOJA FIRMA POSIADA BEZPIECZNE IT?

AUTODIAGNOZA DLA MŚP

Odpowiedz na 12 krótkich pytań i sprawdź, czy Twoja firma jest przygotowana na awarię lub cyberatak.

→ Zsumuj punkty i sprawdź, jaki jest poziom Twoich zabezpieczeń.

→ Oceń, czy bezpłatna konsultacja IT może być dla Ciebie przydatnym rozwiązaniem.

1. Jak często spotykasz się z tym, że komputer lub program firmowy przestaje działać w niewłaściwym momencie?

- Nigdy (0 pkt)
- Przynajmniej 1 / rok (1 pkt)
- Przynajmniej 1 / miesiąc (2 pkt)
- Częściej niż 1 / miesiąc (3 pkt)

2. Co się dzieje w Twojej firmie, gdy padnie serwer?

- Mamy klaster / aplikacje z gwarancją wysokiej dostępności (0 pkt)
- Mamy urządzenie zapasowe, ale odtwarzanie wymaga czasu (1 pkt)
- Mamy kopie danych, ale potrzebujemy czasu na zakup urządzenia (2 pkt)
- Nie mamy kopii i zapasu – nigdy nic się poważnie nie zepsuło (3 pkt)

3. Czy wiesz, kiedy ostatnio była sprawdzana możliwość odtworzenia danych z kopii zapasowej?

- Robimy to regularnie (min. 1 / miesiąc) (0 pkt)
- W tym roku (1 pkt)
- Chyba w zeszłym roku (2 pkt)
- Nigdy tego nie sprawdzaliśmy (3 pkt)

4. Jak Twoi pracownicy logują się do systemów?

- Hasła są silne i dodatkowo potwierdzane (np. SMS, aplikacja) (0 pkt)
- Hasła są silne, ale bez dodatkowego potwierdzania (1 pkt)
- Każdy ma własne hasło – nie wiemy jak silne (2 pkt)
- Zdarzają się wspólne hasła, np. do programów lub WiFi (3 pkt)



5. Czy firma ma spisany plan działania na wypadek poważnej awarii IT lub cyberataku?

- Tak, dokument jest aktualny i walidowany cyklicznie (0 pkt)
- Jest plan – spisaliśmy go dawno temu (1 pkt)
- IT ma plan, ale chyba nie został spisany (2 pkt)
- Nie wiem, czy mamy konkretny plan działania (3 pkt)

6. Jak szybko możesz wznowić pracę po utracie głównego programu/serwera?

- Kilka minut/godzin (0 pkt)
- Jeden dzień (1 pkt)
- Kilka dni (2 pkt)
- Trudno powiedzieć (3 pkt)

7. Jak reagujecie na nietypowe zdarzenia w systemach (np. podejrzane logowanie)?

- Otrzymujemy powiadomienia i ktoś to sprawdza (0 pkt)
- Sprawdzamy okresowo logi, ręcznie (1 pkt)
- Reagujemy dopiero, gdy zauważymy coś nietypowego (2 pkt)
- W ogóle tego nie monitorujemy (3 pkt)

8. Kto odpowiada w firmie za IT?

- Dedykowany dział IT lub stała firma zewnętrzna (0 pkt)
- Mamy zewnętrzną pomoc - pomagają, gdy jest taka potrzeba (1 pkt)
- Jeden z nas zna się na komputerach (2 pkt)
- Nikt, szukamy wsparcia ad-hoc (3 pkt)

9. Czy wszyscy pracownicy wiedzą, jak rozpoznać podejrzany e-mail i co wtedy zrobić?

- Tak, szkolimy zespół regularnie (0 pkt)
- Tak, kiedyś mieliśmy wewnątrz szkolenie (1 pkt)
- Raczej tak, ale działają intuicyjnie (2 pkt)
- Nigdy nie rozmawialiśmy o tym w firmie (3 pkt)



10. W jakim stanie jest sprzęt IT w Twojej firmie?

- Metodycznie zarządzany i posiada wsparcie producenta (0 pkt)
- Kilkuletni, gwarancja się skończyła, ale daje radę (1 pkt)
- Przestarzały, są z nim problemy, ale nic poważnego (2 pkt)
- Bardzo stary, brak serwisu, była min. 1 poważna awaria (3 pkt)

11. Gdzie trzymacie najważniejsze dane firmowe?

- W zabezpieczonym systemie z kopią poza firmą (0 pkt)
- Na lokalnym serwerze/komputerze z backupem (1 pkt)
- Na pojedynczym komputerze lub dysku sieciowym - bez kopii (2 pkt)
- Rozproszone – na komputerach pracowników (3 pkt)

12. Jak oceniasz ogólnie przygotowanie firmy do poważniejszego incydentu IT?

- Jestem spokojny, mamy to pod kontrolą (0 pkt)
- Da się przeżyć, ale wiązałoby się to z dodatkowymi kosztami i stresem (1 pkt)
- Mogłoby być ciężko (2 pkt)
- Byłby to paraliż firmy na kilka dni (3 pkt)

SCORING

0–12 pkt – Zielony (niski poziom ryzyka)

Wygląda na to, że Twoja firma jest dobrze przygotowana. Warto jednak raz w roku zrobić przegląd i upewnić się, że wszystko działa.

13–24 pkt – Pomarańczowy (umiarkowane ryzyko)

Wyniki sugerują, że masz kilka słabszych punktów, które mogą przerodzić się w kosztowny problem. Warto je omówić podczas bezpłatnej konsultacji i wsparcia technicznego IT.

25–36 pkt – Czerwony (wysokie ryzyko)

Najwyraźniej Twoja firma może mieć poważny problem w przypadku awarii lub cyberzagrożenia. Warto podjąć działania i wdrożyć plan naprawczy – umów bezpłatną konsultację i wsparcie techniczne jak najszybciej.