Sprawdź poziom cyberbezpieczeństwa fabryki w 15 minut

20 pytań, które ujawniają luki w bezpieczeństwie dla małych i średnich firm produkcyjnych.



Ten dokument jest dla Ciebie, jeśli:

- Prowadzisz firmę produkcyjną zatrudniającą od 20 do 500 osób.
- Twój dział IT to jedna lub kilka osób, które robią wszystko.
- Nie masz pewności, czy Twoja sieć jest monitorowana 24/7.
- Słyszałeś o NIS 2, ale nie wiesz, czy Cię dotyczy.

Przygotowane przez ekspertów ADQ: centrum operacji bezpieczeństwa (SOC) specjalizujące się w ochronie firm produkcyjnych, logistycznych i farmaceutycznych w Polsce.

Co znajdziesz w tym dokumencie

Dlaczego hakerzy celują właśnie w produkcję? 03

Jak korzystać z dokumentu. Autorzy. 04

Checklista bezpieczeństwa dla firm produkcyjnych. 05

Szybkie zwycięstwo: jedna rzecz, którą niskim nakładem możesz zrobić już dziś. 08

Bezpłatny audyt cyberbezpieczeństwa. 09



Dlaczego hakerzy celują właśnie w produkcję?

Sektor produkcyjny jest od 2022 roku najczęściej atakowaną branżą na świecie, wyprzedza nawet finanse i ochronę zdrowia (IBM X-Force Threat Intelligence Index 2024).

49%

polskich firm produkcyjnych doświadczyło incydentu cyberbezpieczeństwa

1 mln

średni koszt incydentu dla MŚP w PLN

11 dni

średni czas przestoju linii produkcyjnej po ataku

Najważniejsze zagrożenia dla firmy produkcyjnej:

Zatrzymanie linii produkcyjnej

Ransomware szyfruje systemy sterowania (SCADA/PLC). Maszyny się zatrzymują. Każda godzina postoju to tysiące złotych straty. **Średni czas przestoju wynosi 11 dni.**

Kradzież know-how bez Twojej wiedzy

To często bagatelizowany scenariusz, dopóki receptury nie pojawią się u konkurencji, a lista kontrahentów nie trafi do spółki, która kilka miesięcy wcześniej była podwykonawcą. Szpiegostwo przemysłowe przez cyberatak jest ciche, cierpliwe i statystycznie trwa **niemal 6 miesięcy** (181 dni według raportu IBM z 2025 roku), zanim zostanie wykryte.

Odpowiedzialność prawna i kary

Unijna dyrektywa NIS2 nakłada obowiązek zgłaszania incydentów w ciągu 24 godzin i stosowania aktywnego monitoringu. Kary sięgają **10 mln EUR lub 2% globalnego obrotu.** Nieświadomość przepisów nie jest okolicznością łagodzącą.

Jak korzystać z tego dokumentu?

Raport zaprojektowaliśmy tak, aby można go było przeczytać w 15 minut. Nie musisz znać się na IT. Każdy punkt wyjaśniamy językiem biznesowym: czas, pieniądze, ryzyko, konsekwencje.

Kluczowym elementem jest checklista bezpieczeństwa. Odpowiedz na każde pytanie szczerze, żeby dokładnie ocenić stan obecny. Taki sposób użycia checklisty zapewni Ci największą wartość. Jeśli przy więcej niż trzech zaznaczysz „NIE" lub „NIE WIEM", skontaktuj się z nami. Przeprowadzimy bezpłatny audyt Twojej firmy.

O ADQ Technologies

ADQ Technologies to polskie centrum operacji bezpieczeństwa (SOC) świadczące usługi monitoringu 24/7/365 dla małych i średnich firm. Specjalizujemy się w ochronie infrastruktury OT/IT w sektorach: produkcji, logistyki, farmacji, e-commerce i administracji.



Checklista cyberbezpieczeństwa dla firm produkcyjnych

Odpowiedz na każde pytanie szczerze, żeby dokładnie ocenić obecny stan cyberbezpieczeństwa. Taki sposób użycia checklisty zapewni Ci największą wartość.

1. Dostępy, hasła i konta

1.1 Wszyscy pracownicy używają unikalnych haseł do systemów firmowych (nie występuje współdzielenie kont)

☐ TAK ☐ NIE ☐ NIE WIEM

1.2 Konta administracyjne (z dostępem do serwerów, systemów ERP) mają włączone uwierzytelnianie dwuskładnikowe (2FA/MFA).

☐ TAK ☐ NIE ☐ NIE WIEM

1.3 Po odejściu pracownika jego konto jest dezaktywowane w ciągu 24 godzin.

☐ TAK ☐ NIE ☐ NIE WIEM

1.4 Dostęp do danych produkcyjnych i dokumentacji technicznej jest ograniczony; mają go tylko osoby, które faktycznie potrzebują.

☐ TAK ☐ NIE ☐ NIE WIEM

2. Sieć, urządzenia, OT i IT

2.1 Sieć biurowa jest odseparowana od sieci maszyn i sterowania (OT/SCADA). Maszyny nie komunikują się bezpośrednio z Internetem.

☐ TAK ☐ NIE ☐ NIE WIEM

2.2 Znasz listę wszystkich urządzeń podłączonych do sieci, w tym starych maszyn, drukarek, kamer i czujników

☐ TAK ☐ NIE ☐ NIE WIEM

2.3 Firewall i router są regularnie aktualizowane (co najmniej raz na kwartał).

☐ TAK ☐ NIE ☐ NIE WIEM

2.4 Sieć Wi-Fi dla gości i podwykonawców jest całkowicie oddzielona od sieci produkcyjnej.

☐ TAK ☐ NIE ☐ NIE WIEM

2.5 Ruch sieciowy jest monitorowany pod kątem anomalii, co oznacza, że masz narzędzia lub usługę, które to robią 24/7, przez 365 dni w roku.

☐ TAK ☐ NIE ☐ NIE WIEM

3. Pracownicy i świadomość zagrożeń

3.1 Pracownicy przeszli szkolenie z cyberbezpieczeństwa w ciągu ostatnich 12 miesięcy.

☐ TAK ☐ NIE ☐ NIE WIEM

3.2 Firma przeprowadziła test phishingowy (fałszywy e-mail) i zna jego wyniki.

☐ TAK ☐ NIE ☐ NIE WIEM

3.3 Istnieje jasna procedura: co pracownik ma zrobić, gdy podejrzewa atak lub kliknął podejrzany link.

☐ TAK ☐ NIE ☐ NIE WIEM

4. Kopie zapasowe i ciągłość działania

4.1 Kopie zapasowe danych produkcyjnych i dokumentacji są wykonywane automatycznie co najmniej raz dziennie.

☐ TAK ☐ NIE ☐ NIE WIEM

4.2 Kopie zapasowe są przechowywane w oddzielnej lokalizacji (nie tylko na tym samym serwerze lub w tej samej sieci).

☐ TAK ☐ NIE ☐ NIE WIEM

4.3 Ostatnie przywrócenie danych z kopii zostało przetestowane w ciągu ostatnich 6 miesięcy. Wiesz, że działa.

☐ TAK ☐ NIE ☐ NIE WIEM

5. Procedury reagowania na incydenty

5.1 Firma posiada udokumentowany plan reagowania na cyberatak (choćby podstawowy: kto dzwoni, co odłącza, kogo informuje).

☐ TAK ☐ NIE ☐ NIE WIEM

5.2 Posiadasz umowę z dostawcą usług bezpieczeństwa (SOC/CERT) lub wiesz, do kogo zadzwonić w przypadku ataku o 3:00 w nocy.

☐ TAK ☐ NIE ☐ NIE WIEM

5.3 Logi z urządzeń sieciowych i serwerów są przechowywane przez co najmniej 12 miesięcy (wymóg NIS 2 i ubezpieczycieli).

☐ TAK ☐ NIE ☐ NIE WIEM

6. Zgodność i ubezpieczenie

6.1 Wiesz, czy Twoja firma podlega dyrektywie NIS 2 i jakie ma obowiązki.

☐ TAK ☐ NIE ☐ NIE WIEM

6.2 Polisa cyberubezpieczenia firmy jest aktualna, a ubezpieczyciel zaakceptował stan zabezpieczeń.

☐ TAK ☐ NIE ☐ NIE WIEM

6.3 Podwykonawcy i dostawcy mający dostęp do Twojej sieci są objęci wymogami bezpieczeństwa (umowa, audyt).

☐ TAK ☐ NIE ☐ NIE WIEM

Jeśli przy więcej niż 3 punktach zaznaczyłeś odpowiedzi „NIE" lub „NIE WIEM", skontaktuj się z nami.
Przeprowadzimy bezpłatny audyt cyberbezpieczeństwa Twojej firmy. Bez zobowiązań. Z konkretnymi wynikami i rekomendacjami.

Jedna rzecz, którą możesz wprowadzić niskim nakładem, żeby zrobić znaczący krok w stronę cyberbezpieczeństwa

Jako bonus dla Ciebie dołączamy opis szybkiego zwycięstwa, które możesz wdrożyć od razu: jedna rzecz, która mało kosztuje, da się szybko wdrożyć i znacząco podnosi poziom cyberbezpieczeństwa w firmie.

Wdrożenie segmentacji sieci i oddzielenie OT od IT

Co to znaczy i dlaczego to takie istotne?

Większość firm produkcyjnych ma jedną wspólną sieć, w której wszystkie urządzenia (komputery biurowe, maszyny CNC, drukarki, kamery i serwer ERP) są wpięte do tego samego routera. W efekcie gdy haker wejdzie przez jedno urządzenie, w kilka minut może być przy sterownikach maszyn.

Jak to wdrożyć?

Krok 1: Inwentaryzacja (2–4 godziny)
Spisz wszystkie urządzenia podłączone do sieci. Wydrukuj listę urządzeń z panelu routera lub przełącznika (każdy router to potrafi). Zdziwisz się, ile rzeczy jest podłączonych.

Krok 2: Dwie sieci zamiast jednej (1 dzień roboczy)
Poproś swój dział IT lub zewnętrznego specjalistę o skonfigurowanie VLAN-ów (wirtualnych sieci lokalnych): jednej dla biura i pracowników, drugiej wyłącznie dla maszyn i sterowników. Ruch między nimi powinien przechodzić przez zaporę (firewall).

Krok 3: Osobna sieć Wi-Fi dla gości i podwykonawców
Jeśli masz Wi-Fi, stwórz osobną sieć gości (funkcja dostępna bezpłatnie w każdym nowoczesnym routerze). Żaden zewnętrzny serwisant nie powinien mieć dostępu do tej samej sieci co Twoje maszyny.

Dlaczego to działa?

Segmentacja sieci to zasada minimalnych uprawnień w praktyce: nawet jeśli haker włamie się do komputera biurowego, nie dotrze do maszyn produkcyjnych, bo sieć go zablokuje. Eliminuje też ryzyko tzw. lateral movement, czyli przemieszczania się atakującego przez całą infrastrukturę po jednym przełamaniu.

Ważna uwaga: Segmentacja sieci to punkt wyjścia, a nie całościowe rozwiązanie. Nie zastąpi aktywnego monitoringu. Haker może próbować obejść segmentację i wtedy potrzebujesz kogoś, kto to zauważy o 2:00 w nocy, zanim dojdzie do incydentu.

Wypełniłeś checklistę. Czas na konkrety.

Jeśli przy kilku punktach wybrałeś odpowiedź „nie" albo „nie wiem", nie jesteś wyjątkiem. Większość firm produkcyjnych, które do nas trafiają, ma dokładnie te same luki.

Główny problem zazwyczaj leży w braku czasu i braku wiedzy o tym, co dzieje się w sieci.

Dlatego zamiast kolejnej listy rzeczy do zrobienia, proponujemy jedno konkretne działanie:

Bezpłatny audyt cyberbezpieczeństwa

Przyjeżdżamy do Twojej firmy. Sprawdzamy stan faktyczny infrastruktury sieciowej, urządzeń i procedur. Po audycie otrzymujesz pisemny raport w trzech obszarach:

Co jest krytyczne

Lista luk, które wymagają natychmiastowej reakcji.

Co możesz zrobić szybko, sam

Szybkie zwycięstwa bez dużych nakładów.

Co warto zlecić

Z szacunkowym kosztem i priorytetem.

Audyt trwa zwykle 2–4 godziny. Nie wymaga od Ciebie przygotowań technicznych. Nie jest wstępem do nachalnej sprzedaży. Jeśli nie będziemy właściwym partnerem dla Twojej firmy, powiemy Ci o tym wprost.

+48 786 088 383

info@adq.com.pl

adqtechnologies.pl