PODRĘCZNIK

CYBERBEZPIECZEŃSTWA I ODPORNOŚCI

BW advisory

#CyberMadeInPoland

akademia // ITGRC

SPIS TREŚCI

1. WPROWADZENIE

1.1. Cel i zakres podręcznika

Celem niniejszego podręcznika jest dostarczenie przedsiębiorcom – zarówno małym i średnim firmom (MŚP), jak i większym organizacjom – praktycznego zestawu dobrych praktyk w zakresie cyberbezpieczeństwa, ochrony informacji i budowania odporności operacyjnej. Dokument ten nie jest zbiorem sztywnych wymagań, ale przewodnikiem, który pokazuje, jak krok po kroku rozwijać zdolności organizacji, od podstawowej higieny cyberbezpieczeństwa po zaawansowane procesy zarządzania ryzykiem i zarządzaniem zgodnością z wymaganiami prawnymi i klientów.

Podręcznik uwzględnia specyfikę polskiego i europejskiego otoczenia regulacyjnego, a także globalne standardy. Adresowany jest do osób odpowiedzialnych za zarządzanie IT, bezpieczeństwo informacji, compliance i ciągłość działania, jak również do właścicieli firm, zarządów i kadry menedżerskiej.

1.2. Jak korzystać z podręcznika

Podręcznik został opracowany w sposób modułowy. Poszczególne rozdziały można czytać niezależnie, ale pełne wykorzystanie następuje przy przejściu przez cały cykl: od analizy zagrożeń, przez wdrożenie dobrych praktyk, aż po planowanie odporności i reagowanie na incydenty. Dzięki temu każda organizacja może dostosować zakres wdrożeń do własnych potrzeb, branży i zasobów.

1.3. Kontekst Polski i Unii Europejskiej

Polska w ostatnich latach, na bazie regulacji UE, wdrożyła szereg regulacji i praktyk, które bezpośrednio wpływają na sposób, w jaki przedsiębiorcy powinni podchodzić do bezpieczeństwa informacji:

- **Krajowy System Cyberbezpieczeństwa (KSC)** – wprowadzający obowiązki zgłaszania incydentów i budowania odporności dla podmiotów kluczowych i operatorów usług kluczowych.
- **RODO** – wymagający zapewnienia poufności, integralności i dostępności danych osobowych oraz raportowania naruszeń w ciągu 72 godzin.

- **DORA (Digital Operational Resilience Act)** – obowiązujący w całej UE, szczególnie w sektorze finansowym, nakładający wymogi testowania odporności cyfrowej, zarządzania ryzykiem dostawców ICT i raportowania incydentów do regulatorów. DORA poprzez wymagania zarządzania ryzykiem dostawców nakłada na podmioty świadczące usługi ICT dla sektora finansowego dodatkowe wymagania bezpieczeństwa.

- **Wytyczne KNF** – w szczególności dotyczące outsourcingu usług ICT, chmury obliczeniowej oraz zarządzania ryzykiem.

- **NIS2** – to dyrektywa Unii Europejskiej, której celem jest podniesienie poziomu cyberbezpieczeństwa w całej wspólnocie. Obejmuje szerszy zakres podmiotów niż wcześniejsza NIS, w tym kluczowe sektory gospodarki oraz dostawców usług cyfrowych, energetycznych, zdrowotnych czy transportowych. Nakłada obowiązki w zakresie zarządzania ryzykiem, raportowania incydentów i wdrażania środków ochronnych, aby zwiększyć odporność organizacji na cyberzagrożenia.

- **Wytyczne ENISA (European Union Agency for Cybersecurity)** – – ENISA to agencja unijna publikująca przewodniki i raporty wspierające państwa członkowskie i organizacje europejskie w budowaniu cyberodporności.

Te ramy prawne, zasady, wytyczne i dobre praktyki stanowią fundament, który każdy przedsiębiorca działający w Polsce i UE musi uwzględniać w swojej strategii cyberbezpieczeństwa oraz w zapewnieniu zgodności z prawem.

1.4. Międzynarodowe standardy i wymagania klientów

Obok regulacji krajowych i unijnych, przedsiębiorcy powinni czerpać z globalnych standardów, które stanowią punkt odniesienia w obszarze bezpieczeństwa informacji oraz bardzo często są wymagane przez klientów:

⇒ **ISO/IEC 27001** – międzynarodowy standard dot. systemu zarządzania bezpieczeństwem informacji (ISMS), certyfikowalny i powszechnie wymagany w relacjach biznesowych, zwłaszcza w Euroazji.

⇒ **ISO 22301** – standard zarządzania ciągłością działania, integrujący cyberbezpieczeństwo z planowaniem odporności biznesowej. Podobnie jak ISO 27001, jest to standard certyfikowalny i powszechnie wymagany w relacjach biznesowych.

⇒ **TSC (Trust Services Criteria)** – kryteria opracowane przez AICPA, będące podstawą raportów SOC 1, SOC2, SOC2+, SOC3 oraz pozostałych raportów SOC (System and Organizational Controls); obejmują pięć zasad: bezpieczeństwo, dostępność, integralność przetwarzania, poufność i prywatność. Jest to wymóg w relacjach biznesowych z organizacjami z Ameryki Północnej, Wielkiej Brytanii, Australii i Nowej Zelandii (rzadziej w UE). Coraz częściej wymagane w relacjach biznesowych na całym świecie jako tzw: „złoty standard zapewnienia". Powszechnie ceniony i uznawany jako wystarczający dla zapewnienia klientów o wysokim poziomie bezpieczeństwa konkretnych usług.

⇒ **Raport SOC 1** – dotyczy kontroli mających wpływ na sprawozdawczość finansową użytkownika usług. SOC 1 jest dedykowany firmom, które świadczą usługi mające wpływ na dane finansowe swoich klientów – – m.in. dostawcom usług przetwarzania roszczeń ubezpieczeniowych, powiernikom aktywów inwestycyjnych, dostawcom oprogramowania i środowisk technologicznych, operatorom chmury oraz centrom danych. Jeżeli przetwarzane dane wpływają na szeroko pojmowaną sprawozdawczość finansową Klienta, zazwyczaj żąda on okazania atestowanego raportu SOC 1.

⇒ **Raport SOC 2** – skupia się na kontrolach związanych z bezpieczeństwem, dostępnością, integralnością przetwarzania, poufnością i prywatnością. Raport przeznaczony jest dla zarządów organizacji usługowych, klientów, partnerów biznesowych i audytorów technicznych. SOC 2 jest szczególnie istotny dla dostawców usług IT, chmurowych i outsourcingowych, ponieważ potwierdza ich zaangażowanie w ochronę danych i ciągłość działania. Jest standardem dużo bardziej rygorystycznym niż ISO27001, ale przez to bardziej cenionym przez Klientów o szczególnych wymaganiach.

2. AKTUALNY STAN ZAGROŻEŃ

2.1. Dynamika cyberzagrożeń w Polsce i UE

W ostatnich latach Polska i Unia Europejska znalazły się w centrum eskalującej fali cyberataków. Według raportów głównymi kategoriami ataków pozostają: ransomware, phishing, ataki na łańcuch dostaw oraz zagrożenia związane ze sztuczną inteligencją. Sa one stałym elementem trwającej wojny hybrydowej.

W Polsce, zgodnie z raportami CSIRT NASK i CERT Polska, rośnie liczba incydentów związanych z phishingiem i oszustwami finansowymi – w ostatnim roku odnotowano kilkadziesiąt tysięcy przypadków kampanii podszywających się pod banki, platformy kurierskie i operatorów telekomunikacyjnych. Trend ten wzmocniła rosnąca skala wykorzystania deepfake'ów głosowych i wideo w atakach socjotechnicznych.

Jednocześnie rośnie presja regulacyjna – od 2025 r. obowiązuje DORA (Digital Operational Resilience Act) oraz NIS2 (Dyrektywa UE 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej). UODO od wielu lat nakłada znaczące kary, które stanowią dotkliwy wymiar finansowy, jak i wpływają na reputację administratorów lub procesorów danych osobowych.

2.2. Geopolityka i wojna hybrydowa

Rosyjska agresja na Ukrainę pokazała, że cyberprzestrzeń jest jednym z kluczowych pól walki hybrydowej. Polska, jako kraj wspierający Ukrainę i strategiczny hub NATO, stała się celem kampanii dezinformacyjnych i prób ataków na infrastrukturę krytyczną.

Ataki te obejmują m.in.:

- próby włamań do systemów finansowych, energetycznych, transportowych, ochrony zdrowia i produkcj,
- kampanie phishingowe,
- kampanie dezinformacyjne prowadzone w mediach społecznościowych.

Według raportów cyberbezpieczeństwa, Polska jest najczęściej atakowanym krajem w Unii Europejskiej, a rosyjskie grupy APT (Advanced Persistent Threats) aktywnie testują zabezpieczenia systemów w Polsce i regionie, łącząc cyberataki z operacjami dezinformacyjnymi lub propagandowymi.

2.3. Najważniejsze zagrożenia

Największe firmy cyberbezpieczeństwa potwierdzają, że zagrożenia ewoluują szybciej niż obrona. Poniżej przedstawiono najpoważniejsze z nich.

- **Ransomware** – cyberprzestępcy przejmują kontrolę nad systemami i szyfrują dane ofiary, żądając okupu w kryptowalucie za przywrócenie dostępu. Coraz częściej stosowane są tzw. podwójne lub potrójne wymuszenia: oprócz szyfrowania danych grożą ich publikacją w sieci, a także atakami DDoS na infrastrukturę ofiary. Ransomware atakuje nie tylko firmy prywatne, ale również instytucje publiczne i szpitale, co powoduje paraliż usług krytycznych. Często zapłacony okup usypia czujność ofiary i jest ona atakowana kilka razy, tę samą metodą, przy czym cena okupu może rosnąć.

- **Łańcuch dostaw** – atakujący wykorzystują zaufanie, jakim obdarza się dostawców oprogramowania, usług chmurowych lub sprzętu. Włamanie do jednego dostawcy pozwala rozprzestrzenić złośliwy kod do tysięcy klientów w tym samym czasie. Tego typu ataki są wyjątkowo trudne do wykrycia, bo złośliwe komponenty trafiają do organizacji jako „legalne" aktualizacje czy integracje.

- **Phishing i BEC (Business Email Compromise)** – celem jest wyłudzenie poufnych danych lub pieniędzy za pomocą sfałszowanych wiadomości e-mail. W phishingu użytkownik klika w link prowadzący do fałszywej strony logowania, albo otwiera zainfekowany załącznik. W BEC oszuści podszywają się pod dyrektora lub kontrahenta i nakłaniają pracowników księgowości do wykonania przelewu na konto przestępców. Ataki są coraz bardziej spersonalizowane i trudne do rozpoznania.

- **Ataki oparte na sztucznej inteligencji** – przestępcy wykorzystują AI do automatycznego generowania wiadomości phishingowych, testowania haseł, a nawet do omijania systemów wykrywania intruzów. AI umożliwia też tworzenie bardziej realistycznych fałszywych profili w mediach społecznościowych i symulowanie zachowania użytkowników, co zwiększa skuteczność ataków socjotechnicznych.

- **Deepfake i manipulacja informacją** – zaawansowane narzędzia do tworzenia obrazu i dźwięku pozwalają na generowanie fałszywych nagrań osób publicznych czy menedżerów firm. Oszust może np. zadzwonić do pracownika, używając syntetycznego głosu przełożonego, i wydać polecenie przelewu. W szerszej skali deepfake'i wykorzystywane są do manipulowania opinią publiczną i prowadzenia kampanii dezinformacyjnych.

- **Ataki na infrastrukturę krytyczną i systemy OT** – systemy odpowiedzialne za sterowanie procesami przemysłowymi (energia, transport, produkcja, wodociągi, szpitale) coraz częściej podłączane są do sieci IT. Brak odpowiednich zabezpieczeń powoduje, że ataki mogą zatrzymać produkcję, zakłócić dostawy energii czy sparaliżować komunikację, a nawet zagrozić bezpośrednio zdrowiu lub życiu ludzkiemu. Takie incydenty mają wymiar nie tylko finansowy, ale i bezpieczeństwa publicznego.

- **Exploity zero-day i usługi „as-a-service"** – luki zero-day to nieznane jeszcze błędy w oprogramowaniu, które pozwalają atakującym przejąć kontrolę nad systemami, zanim pojawi się poprawka. Coraz częściej sprzedawane są one w formie usług – np. Malware-as-a-Service, tzn.każdy może wynająć gotową infrastrukturę do przeprowadzania ataków. Obniża to tzw. finansowy próg wejścia do cyberprzestępczości i zwiększa liczbę ataków i ich ofiar.

- **IoT i urządzenia medyczne** – urządzenia inteligentnego domu, sensory przemysłowe czy sprzęt medyczny, są często podłączone do internetu, ale rzadko aktualizowane. Atakujący mogą przejąć nad nimi kontrolę i wykorzystać jako element botnetu (np. w atakach DDoS), a w przypadku urządzeń medycznych – zagrozić zdrowiu i życiu pacjentów (np. powodując zdarzenia niepożądane lub prowokując błędy medyczne).

- **Shadow AI** – pracownicy, chcąc usprawnić swoją pracę, korzystają z nieautoryzowanych narzędzi AI, do których wprowadzają poufne dane. Może to prowadzić do niekontrolowanych wycieków, ponieważ dane są przechowywane i przetwarzane poza kontrolą organizacji.

- **Vishing (voice phishing)** – oszustwo telefoniczne, w którym przestępcy podszywają się pod pracowników banku, firm kurierskich, a nawet przełożonych w organizacji. Celem jest nakłonienie ofiary do podania danych dostępowych, zainstalowania złośliwego oprogramowania na komputerze lub telefonu, albo wykonania przelewu. Coraz częściej stosowane są technologie zmiany głosu i automatyzacja rozmów.

- **Scam inwestycyjny i finansowy** – ofiary otrzymują propozycje szybkiego zysku w „pewnych" inwestycjach w aktywa (np. kryptowaluty, akcje, metale szlachetne). Atakujący przygotowują fałszywe strony internetowe, aplikacje lub platformy inwestycyjne, za pomocą których ofiara wpłaca środki, które natychmiast są kradzione. Takie oszustwa są trudne do wykrycia, bo często wyglądają bardzo profesjonalnie.

- **Wyłudzenia z firm (fraudy korporacyjne)** – cyberprzestępcy podszywają się pod kontrahentów lub członków zarządu. Najczęstszy scenariusz to wysyłanie sfałszowanych faktur z nowym numerem konta

bankowego lub kontakt telefoniczny od „dyrektora" z poleceniem pilnej zapłaty. Ataki tego typu wykorzystują presję czasu i zaufanie w relacjach biznesowych.

Należy zauważyć, że powyżej wymienione zagrożenia często występują grupami lub są powiązane wzajemnie w łańcuchy przyczynowo-skutkowe. Oznacza to, że jedno zagrożenie może stanowić preludium do innego lub kliku łącznie.

2.4. Luka dojrzałości bezpieczeństwa

Badania pokazują, że istnieje poważna luka pomiędzy świadomością zagrożeń a realnymi zdolnościami obronnymi firm:

- **Brak strategii** – wiele przedsiębiorstw, szczególnie w sektorze MŚP, nie posiada formalnej strategii bezpieczeństwa i jej dokumentów wykonawczych (polityka cyberbezpieczeństwa, procedury reagowania na incydenty, plany ciągłości działania). W przypadku poważnego ataku organizacje często improwizują, co zwiększa skalę strat i wydłuża czas przywracania działania systemów. Zwiększa też zagrożenia o te najbardziej dotkliwe (życie i zdrowie ludzkie).

- **Ograniczone zasoby** – niedobór specjalistów IT i bezpieczeństwa powoduje, że firmy stosują rozwiązania reaktywne (gaszenie pożarów) zamiast proaktywnych (zapobieganie incydentom). Brak kompetencji wewnętrznych sprawia, że wiele organizacji nie potrafi prawidłowo ocenić ryzyka, ani wdrożyć odpowiednich zabezpieczeń. Outsourcing w tym zakresie jest nadal postrzegany jako niepotrzebne lub pozastandardowe usługi o dużych kosztach.

- **Niewystarczająca integracja z zarządzaniem ryzykiem** – cyberzagrożenia wciąż postrzegane są jako domena działu IT, zamiast być elementem zarządzania strategicznego. To prowadzi do sytuacji, w której zarząd nie bierze pod uwagę konsekwencji cyberataków w szerszym kontekście biznesowym, np. zastojów operacyjnych, utraty reputacji, zaufania klientów czy kar regulacyjnych.

- **Brak dopasowanego systemu zarządzania bezpieczeństwem** – organizacje często nie wdrażają całościowych systemów zarządzania bezpieczeństwem informacji. Brakuje procesów ciągłego monitorowania, reagowania i doskonalenia.

- **Brak proaktywnego wykrywania podatności i strategii ich łatania** – firmy rzadko prowadzą regularne skany podatności, testy penetracyjne czy ćwiczenia typu „red team". To powoduje, że krytyczne luki pozostają niewykryte, aż do momentu, gdy zostaną wykorzystane przez atakujących.

- **Brak identyfikacji aktywów IT** – wiele przedsiębiorstw nie ma aktualnej ewidencji swoich zasobów informatycznych, takich jak serwery, urządzenia sieciowe, oprogramowanie i jego wersje. Utrudnia to zarządzanie aktualizacjami, łatkami bezpieczeństwa i kontrolę nad infrastrukturą.

2.5. Wnioski dla przedsiębiorców

- **Skala zagrożeń rośnie** – przedsiębiorcy w Polsce muszą liczyć się z tym, że cyberataki są kwestią „kiedy", a nie „czy".

- **Regulacje wymuszają działania** – NIS2 (KSC), RODO i DORA powodują, że ignorowanie kwestii cyberbezpieczeństwa staje się niemożliwe prawnie i biznesowo. Należy zauważyć, iż wysokość, dotkliwość i częstotliwość nakładanych kar systematycznie rośnie.

- **AI zmienia zasady gry** – nowe ataki (deepfake, AI worms, automatyczne phishingi) wymagają inwestycji w nowoczesne narzędzia detekcji i budowania odporności. Koszty rosną – i przewidywalnie bedą rosły.

- **Odporność = przewaga konkurencyjna** – firmy, które wdrażają normy (ISO 27001, ISO 22301, SOC 1, SOC 2), zwiększają nie tylko swoje bezpieczeństwo, ale także atrakcyjność dla klientów i partnerów.

2.6. Kontekst regulacyjny: NIS2 w Polsce i UE

Dyrektywa NIS2 (Network and Information Security 2) weszła w życie w styczniu 2023 r. i zastępuje wcześniejszą dyrektywę NIS z 2016 r. Jej głównym celem jest podniesienie wspólnego poziomu cyberbezpieczeństwa w UE.

Kluczowe elementy NIS2:

- **Rozszerzony zakres** – obejmuje nie tylko operatorów usług kluczowych, ale także szeroką grupę „podmiotów istotnych" (np. dostawcy usług cyfrowych, infrastruktury IT, firmy z sektorów transportu, energii, zdrowia, gospodarki odpadami czy dostawcy usług pocztowych).

- **Obowiązki w zakresie zarządzania ryzykiem** – organizacje muszą wdrożyć środki techniczne i organizacyjne proporcjonalne do ryzyka, m.in.: polityki bezpieczeństwa, kontrolę dostępu, zarządzanie podatnościami, plany ciągłości działania i odzyskiwania.
- **Raportowanie incydentów** – obowiązek zgłoszenia poważnych incydentów w ciągu 24 godzin do właściwego CSIRT, a raport końcowy w ciągu miesiąca.
- **Odpowiedzialność zarządu** – kierownictwo ponosi osobistą odpowiedzialność za wdrożenie i nadzorowanie polityk bezpieczeństwa.
- **Sankcje** – w przypadku naruszeń możliwe są dotkliwe kary finansowe (analogicznie do RODO).

NIS2 musi zostać implementowana w krajowym prawie. W Polsce odbędzie się to poprzez nowelizację ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC). Oznacza to, że tysiące przedsiębiorców zostanie objętych obowiązkami raportowania i stosowania polityk bezpieczeństwa.

Powiązania z innymi regulacjami:

- **DORA** – w sektorze finansowym DORA uzupełnia NIS2, wprowadzając bardziej szczegółowe wymogi testowania odporności i kontroli dostawców ICT.
- **RODO** – oba akty nakładają obowiązki w obszarze ochrony danych osobowych, co w praktyce oznacza konieczność integrowania działań zapewnienia zgodności (compliance).

2.7. Podsumowanie

Na polskich przedsiębiorców oddziałuje jednocześnie kilka sił: rosnąca liczba cyberataków, napięta sytuacja geopolityczna, szybka ewolucja zagrożeń opartych na AI oraz coraz bardziej wymagające przepisy. W efekcie cyberbezpieczeństwo staje się nie tylko kwestią techniczną, lecz strategiczną – wymaganą przez prawo i oczekiwaną przez klientów oraz partnerów biznesowych.

3. NAJPOWAŻNIEJSZE I NAJPOPULARNIEJSZE ATAKI

3.1. Ransomware – największe zagrożenie dla biznesu

Ransomware od kilku lat pozostaje najgroźniejszym i najkosztowniejszym typem ataku. Polega na zaszyfrowaniu danych ofiary i żądaniu okupu za ich odblokowanie. Obecnie dominują tzw. model „double extortion" – czyli równoczesne szyfrowanie danych i ich kradzież w celu dodatkowego szantażu. Coraz częściej pojawia się też „triple extortion", gdzie napastnicy grożą ujawnieniem danych klientom lub partnerom biznesowym, aby wywrzeć maksymalną presję.

W Polsce atakami ransomware dotknięto m.in. szpitale i instytucje publiczne, a w UE ofiarą padły duże sieci logistyczne i przedsiębiorstwa przemysłowe. Średni czas potrzebny cyberprzestępcom na rozprzestrzenienie się w sieci ofiary („breakout time") skrócił się do kilkunastu minut, co radykalnie ogranicza czas reakcji zespołów IT.

3.2. Ataki na łańcuch dostaw

Ataki na dostawców oprogramowania i usług stają się coraz bardziej powszechne. Najbardziej znane przykłady globalne to incydent SolarWinds czy zainfekowane aktualizacje w Kaseya. W Europie głośnym przypadkiem był atak na VoIP provider 3CX, którego skutkiem było naruszenie bezpieczeństwa u tysięcy klientów.

Dla polskich przedsiębiorców szczególnie istotne są:

- zależność od dostawców chmurowych (AWS, Microsoft, Google) – – błędna konfiguracja może oznaczać wyciek danych,
- integracje B2B i outsourcing usług IT – brak kontroli nad podwykonawcami często oznacza „otwartą furtkę" do systemów.

Dyrektywy NIS2 i DORA nakładają obowiązek kontroli ryzyka w łańcuchu dostaw oraz wprowadzania wymagań bezpieczeństwa do umów z dostawcami.

3.3. Phishing, BEC i socjotechnika

Phishing pozostaje najpopularniejszym wektorem ataku. W Polsce dominują fałszywe wiadomości SMS i e-maile podszywające się pod banki, firmy kurierskie i urzędy.

Coraz bardziej niebezpieczne staje się BEC (Business Email Compromise) – – przejęcie lub podszycie się pod konto poczty firmowej w celu wyłudzenia środków. Straty globalne liczone są w miliardach dolarów.

Nowym trendem jest wykorzystanie deepfake voice i video. W 2023 r. w Europie odnotowano przypadki, gdy przestępcy podszywali się pod dyrektorów finansowych, nakazując pracownikom przelewy w oparciu o zmanipulowany głos i obraz. W Polsce CERT ostrzegał już przed próbami fraudów telefonicznych z wykorzystaniem syntetycznych głosów.

3.4. Nadużycia tożsamości i dostępu

Coraz więcej ataków koncentruje się na kradzieży sesji i tokenów (np. cookies, refresh tokens), które pozwalają ominąć mechanizmy MFA. Popularne są także ataki na systemy VPN i RDP, szczególnie w małych i średnich firmach, gdzie brakuje segmentacji sieci i zaawansowanych mechanizmów wykrywania.

Napastnicy stosują techniki:

- **MFA fatigue** – wysyłanie setek powiadomień push, aż użytkownik zaakceptuje dostęp,
- **SIM swapping** – przejęcie numeru telefonu ofiary w celu obejścia SMS-owego MFA,
- **Pass-the-cookie i Pass-the-hash** – przejęcie aktywnych sesji.

3.5. Ataki na dane i usługi w chmurze

Rosnąca popularność chmury oznacza także wzrost ataków na usługi SaaS, PaaS i IaaS. Najczęstsze błędy:

- brak szyfrowania danych w spoczynku,
- błędna konfiguracja uprawnień (np. „publiczny bucket S3"),
- brak monitorowania dostępu administracyjnego.

Ataki te są szczególnie groźne, bo mogą prowadzić do kradzieży ogromnych zbiorów danych w krótkim czasie.

3.6. Ataki na OT/IoT

Systemy Operational Technology (OT) i urządzenia IoT są coraz częściej celem cyberataków, co ma krytyczne znaczenie dla przemysłu, energetyki i transportu.

- W Europie głośne były ataki na systemy wodociągowe i energetyczne,
- W Polsce CERT NASK raportował próby skanowania i ataków na niezabezpieczone sterowniki PLC.

IoT to także codzienne urządzenia biurowe: drukarki, kamery, routery – często niedostatecznie aktualizowane i stanowiące słaby punkt w infrastrukturze.

3.7. Wnioski

- Ransomware i phishing pozostają dominującymi zagrożeniami dla przedsiębiorców każdej wielkości.
- Łańcuch dostaw i chmura stają się głównymi wektorami ataku, wymagającymi nowego podejścia do zarządzania ryzykiem.
- Socjotechnika wspierana AI (deepfake, generatywny phishing) to nowe wyzwanie, szczególnie dla MŚP.
- Tożsamość cyfrowa (IAM, MFA, PAM) jest dziś kluczowym elementem obrony, a jej kompromitacja – jednym z głównych celów przestępców.

4. ZAGROŻENIA ZWIĄZANE Z WYKORZYSTANIEM AI

4.1. Nowe klasy ataków opartych na AI

Sztuczna inteligencja wprowadziła rewolucję w cyberbezpieczeństwie – zarówno po stronie obrony, jak i ataku. Z punktu widzenia przedsiębiorców szczególnie groźne są:

- **Prompt injection** – manipulowanie modelami AI poprzez wprowadzanie ukrytych instrukcji, które nakazują systemowi wykonywanie działań niepożądanych (np. ujawnienie poufnych danych).
- **Data/model poisoning** – wprowadzanie do danych treningowych szkodliwych elementów, które obniżają skuteczność modeli lub powodują ich nieprzewidywalne zachowania.
- **Adversarial examples** – subtelne zmiany w danych wejściowych (np. obrazy, dźwięk), które wprowadzają model w błąd i mogą prowadzić do błędnych decyzji biznesowych czy bezpieczeństwa.

4.2. Szkodliwe oprogramowanie AI

Nowa kategoria zagrożeń związana jest z wykorzystaniem sztucznej inteligencji do tworzenia złośliwego oprogramowania zdolnego do samodzielnego rozprzestrzeniania się. Tego rodzaju ataki mogą w przyszłości:

- automatycznie przenosić się pomiędzy różnymi aplikacjami i środowiskami chmurowymi,eskalować dostęp do danych i systemów bez bezpośredniej interwencji człowieka, pozostawać niewidoczne dla tradycyjnych mechanizmów wykrywania zagrożeń.

Dla organizacji oznacza to konieczność wprowadzania dodatkowych mechanizmów monitorowania środowisk oraz regularnego testowania ich bezpieczeństwa przed wdrożeniem do użytku produkcyjnego.

4.3. Deepfake i wyłudzenia finansowe

Deepfake – czyli fałszywe, syntetyczne nagrania audio i wideo – stały się jednym z najbardziej niebezpiecznych narzędzi w cyberprzestępczości:

- **w Europie** odnotowano przypadki podszywania się pod ministrów i prezesów firm w celu wyłudzenia milionowych przelewów,
- **w Polsce** CERT ostrzegał przed próbami wyłudzeń z wykorzystaniem głosu generowanego sztucznie, podszywającego się pod osoby zaufania publicznego.

Zagrożenie to szczególnie dotyka:

- **bankowości i finansów** – wyłudzenia przelewów,
- **firm produkcyjnych i logistycznych** – fałszywe zlecenia,
- **administracji i polityki** – manipulacja informacyjna.

4.4. Ryzyka dużych modeli językowych (LLM)

Coraz więcej firm korzysta z usług typu ChatGPT, Gemini czy Copilot. Jednak bez odpowiednich zabezpieczeń LLM mogą stać się źródłem poważnych incydentów:

- **wycieki danych** – przypadkowe przekazywanie poufnych informacji do modelu (tzw. shadow-AI w pracy zespołów),
- **manipulacja danymi treningowymi** – atakujący mogą zatruwać modele poprzez dane dostępne publicznie,
- **brak kontroli nad dostawcami** – zgodnie z DORA i NIS2 firmy muszą rozliczać dostawców ICT (w tym AI) z bezpieczeństwa i odporności usług.

4.5. Bezpieczeństwo AI w fazie projektowania

Aby ograniczyć ryzyko, przedsiębiorcy powinni wdrożyć zasady bezpieczeństwa AI w fazie projektowania. Obejmują one:

- **Ład i odpowiedzialność** – wprowadzenie polityki korzystania z AI (np. kto może korzystać z LLM, w jakich celach i przy jakiej ochronie danych).
- **Red teaming modeli** – testowanie AI pod kątem prompt injection, manipulacjii nadużyć.
- **Monitoring** – bieżące wykrywanie anomalii w pracy modelu, np. nienaturalne odpowiedzi czy nietypowe żądania.
- **Audyt dostawców** – weryfikacja, czy dostawca usługi AI spełnia wymogi bezpieczeństwa (ISO 27001, ISO 42001, SOC 2 lub SOC2 + regulacje i wymagania AI).

4.6. Wnioski

- AI przyspiesza ewolucję cyberataków – tradycyjne narzędzia ochrony nie są wystarczające wobec nowych zagrożeń.
- Deepfake i fraudy głosowe/wideo to realne zagrożenia w Polsce, mogą uderzać w przedsiębiorców każdej wielkości.
- LLM bez nadzoru stanowią ryzyko wycieku danych i naruszenia wymogów prawnych.
- Bezpieczeństwo AI w fazie projektowania musi stać się elementem strategii cyber w firmach – podobnie, jak wcześniej MFA czy backup.

5. DOBRE PRAKTYKI DLA PRZEDSIĘBIORCÓW

5.1. Obrona wielowarstwowa i obrona w głąb w cyberbezpieczeństwie

Obrona wielowarstwowa to podstawowy fundament w ochronie firm przed cyberzagrożeniami. Polega na tym, aby nie opierać się tylko na jednym czy dwóch zabezpieczeniach, bo w dzisiejszych realiach to zdecydowanie za mało. Jeśli atakujący przełamie jedną barierę, kolejne warstwy ochrony mogą go zatrzymać i uchronić przedsiębiorstwo przed stratami. Dzięki temu nawet udany atak nie musi oznaczać katastrofy – ryzyko poważnych konsekwencji zostaje ograniczone.

W praktyce oznacza to wprowadzenie zabezpieczeń na wielu poziomach: od ochrony sieci i urządzeń, przez kontrolę dostępu do danych i aplikacji, aż po monitoring nietypowych działań. Ważną częścią jest również praca z ludźmi – szkolenia, budowanie świadomości zagrożeń oraz opracowane procedury na wypadek incydentu. To właśnie połączenie technologii, ludzi i procesów daje najskuteczniejszą ochronę.

Z obroną wielowarstwową ściśle wiąże się obrona w głąb. To podejście zakłada, że każda warstwa bezpieczeństwa jest kolejną linią oporu, która spowalnia lub zatrzymuje atakującego. Nawet jeśli cyberprzestępca przełamie pierwsze zabezpieczenie, kolejne bariery – takie jak dodatkowe hasła, segmentacja sieci czy systemy wykrywania anomalii – znacząco utrudnią mu osiągnięcie celu. Dzięki temu firma zyskuje czas, aby wykryć incydent i odpowiednio zareagować.

Obie koncepcje dobrze wpisują się w tzw. cyber kill chain, czyli model opisujący etapy ataku: od przygotowań przestępców, przez włamanie, aż po kradzież danych. Wdrożenie wielu warstw i głębokich linii obrony zwiększa szansę, że atak zostanie zatrzymany na wczesnym etapie albo że jego skutki będą ograniczone.

Dla przedsiębiorców oznacza to, że inwestowanie w różnorodne mechanizmy ochrony oraz w ludzi i procedury nie jest już opcją, ale koniecznością. Obrona wielowarstwowa i obrona w głąb to fundament skutecznej strategii cyberbezpieczeństwa, który daje firmie odporność, elastyczność i większą kontrolę nad ryzykiem.

5.2. Inwentaryzacja aktywów i danych

Pierwszym krokiem w budowaniu cyberodporności jest wiedza o tym, co firma posiada i co musi chronić.

- Sporządź spis aktywów IT/OT/IoT (najlepiej w specjalnych aplikacjach do zarządzania): komputery, serwery, urządzenia mobilne, drukarki, systemy przemysłowe, wykorzystywane oprogramowanie oraz ich wersje.
- Utwórz rejestr danych – jakie informacje są krytyczne (np. dane klientów, dane finansowe, know-how), gdzie są przechowywane i kto ma do nich dostęp.
- Ustal priorytety – które zasoby są najbardziej krytyczne dla funkcjonowania firmy (np. system księgowy, system produkcji).
- Określ właścicielstwo – wskaż, kto w organizacji odpowiada za daną klasę aktywa lub aktywo.

5.3. Zarządzanie ryzykiem i rejestr ryzyka

Zarządzanie cyberbezpieczeństwem musi być elementem szerszego systemu zarządzania ryzykiem.

- **Zidentyfikuj zagrożenia i zabezpieczenia** – dokonaj identyfikacji, co może Ci zagrażać i jakie masz środki, aby temu zapobiec.
- **Prowadź rejestr ryzyka** – spis zagrożeń, ich prawdopodobieństwa i potencjalnych skutków.
- **Regularnie aktualizuj rejestr** – np. raz na kwartał, uwzględniając zmiany technologii i środowiska biznesowego. Zarządzanie ryzykiem to nie rejestr ryzyka, ale codzienne podejmowanie decyzji zarządczych, więc nie traktuj tego, jako wymogu biurokratycznego, ale narzędzie ułatwiające codzienne i świadome podejmowanie decyzji.
- **Łącz zarządzanie ryzykiem IT z biznesowym** – cyberatak to nie tylko problem IT, ale głównie ryzyko biznesowe.

5.4. Ład i polityki

Silne cyberbezpieczeństwo wymaga jasno zdefiniowanych zasad i ról.

- Ustal polityki bezpieczeństwa – obejmujące dostęp do systemów, zarządzanie hasłami, korzystanie z poczty i internetu, ochronę danych osobowych.
- Określ role i odpowiedzialności – kto odpowiada za IT, kto za zgłaszanie incydentów, kto za decyzje biznesowe w kryzysie.
- Zarząd powinien zatwierdzać i cyklicznie przeglądać polityki, aby mieć kontrolę nad poziomem bezpieczeństwa (w rzeczywistości w zależności od wielkości organizacji dokumentacja bezpieczeństwa powinna mieć swoich właścicieli, którzy odpowiadają za aktualność dokumentacji oraz ich stosowanie).

5.5. Zarządzanie dostawcami i łańcuchem dostaw

Ataki na łańcuch dostaw są jednym z najszybciej rosnących zagrożeń.

- Wymagaj od dostawców zgodności ze standardami (ISO 27001, SOC 2).
- Dodaj do umów klauzule bezpieczeństwa (np. obowiązek zgłaszania incydentów, audyty bezpieczeństwa).
- Prowadź oceny ryzyka dostawców – szczególnie tych, którzy: mają dostęp do danych klientów, danych osobowych lub systemów krytycznych, przetwarzają wrażliwe dane firmy lub dane osobowe lub dostarczone produkty lub usługi mogą wpływać na ciągłość działania organizacji.

5.6. Edukacja i świadomość pracowników

Ludzie to często bardzo zawodne ogniwo cyberbezpieczeństwa – ale dobrze wyedukowani mogą ograniczyć to ryzyko. Jednakże żadne, nawet najlepsze szkolenie i edukacja, nie ograniczą ryzyka opartego na czynniku ludzkim i niezbędne są inne – najczęściej techniczne – zabezpieczenia.

- Prowadź regularne szkolenia – co najmniej raz w roku dla wszystkich pracowników, częściej dla działów krytycznych (np. finanse).
- Dostosowuj zakres szkoleń do odpowiedzialności pracy poszczególnych działów.
- Nie stosuj szkoleń tylko po to, aby spełnić wymóg prawny, ale aby w ciekawy sposób pokazać, że cyberzagrożenia są realne i mogą wpływać nie tylko na bezpieczeństwo firmy, ale również na pracownika, jego dane, finanse lub prywatność.
- Ucz pracowników rozpoznawania phishingu i deepfake'ów.
- Działy finansowe i zarządu powinny być szkolone, w jaki sposób wprowadzić i testować procedury ograniczające ryzyka wyłudzeń.
- Wprowadź symulowane kampanie phishingowe – aby testować czujność w praktyce.
- Promuj kulturę bezpieczeństwa – pracownicy powinni czuć się odpowiedzialni za ochronę informacji, a nie obawiać się zgłaszania incydentów.

5.7. Wnioski

1. Inwentaryzacja i klasyfikacja danych to fundament – bez tego firma nie wie, co chroni.
2. Rejestr ryzyka i ład przenosi cyberbezpieczeństwo z działu IT na poziom zarządu.
3. Dostawcy i łańcuch dostaw muszą być weryfikowani – atak na partnera może być atakiem na nas.
4. Edukacja i świadomość są tak samo ważne, jak technologie – dobrze poinformowany pracownik może zatrzymać atak, zanim wyrządzi szkody.

6. OCHRONA

6.1. Tożsamość i dostęp

Kontrola dostępu do systemów i danych jest kluczowa.

MFA (uwierzytelnienie wieloskładnikowe) – wprowadź MFA jako domyślny standard dla wszystkich kont. Tam, gdzie to możliwe, stosuj aplikacje lub klucze sprzętowe (obowiązkowe dla pracowników działów IT, managerów i stanowisku o dostępie do kluczowych systemów).

Zasada najmniejszych uprawnień – każdy pracownik ma dostęp tylko do tego, co niezbędne. Zbyt wysokie uprawnienia do ryzyko dla firmy. Regularnie przeglądaj i usuwaj zbędne uprawnienia.

Privileged Access Management (PAM, zarządzanie kontami uprzywilejowanymi) – dla administratorów i systemów krytycznych stosuj dodatkowe mechanizmy (sesje monitorowane, ograniczone okna czasowe).

Monitorowanie logowań – wdrażaj systemy alarmujące o nietypowych próbach logowania, w tym z nowych lokalizacji, urządzeń, nietypowych godzin, czy wielokrotnych prób logowania.

6.2. Bezpieczeństwo danych

Dane to kluczowy zasób firmy – ich ochrona musi obejmować cały cykl życia.

Szyfrowanie – stosuj szyfrowanie danych w spoczynku i ruchu. Szyfrowanie to nie tylko podstawowe zabezpieczenie, to wymóg prawa – RODO. Główna zasada – o ile to możliwe, szyfruj zawsze i wszystko.

DLP (Data Loss Prevention) – to narzędzia, które pozwalają monitorować przepływ danych w firmie i blokować próby ich nieautoryzowanego wyniesienia. Dzięki nim można np. wychwycić sytuację, w której pracownik próbuje przesłać poufne pliki mailem poza organizację, skopiować je na prywatny pendrive czy umieścić w nieautoryzowanej chmurze.

Anonimizacja i pseudonimizacja – to techniki, które pomagają chronić dane osobowe zgodnie z wymogami RODO. Anonimizacja polega na trwałym usunięciu elementów umożliwiających identyfikację osoby, tak aby dane nie mogły być już powiązane z konkretną osobą. Pseudonimizacja natomiast zastępuje dane identyfikacyjne innymi oznaczeniami (np. numerem ID), co pozwala dalej przetwarzać dane, ale bez bezpośredniego ujawniania tożsamości.

Bezpieczne niszczenie danych – każdy nośnik informacji, zarówno fizyczny (np. dyski twarde, pamięci USB, dokumenty papierowe), jak i wirtualny (np. zasoby przechowywane w chmurze), powinien być usuwany w kontrolowany sposób. W praktyce oznacza to stosowanie procedur, takich jak nadpisywanie danych, czy fizyczne niszczenie nośników. Ważne jest także przestrzeganie polityki retencji danych – – czyli określenia, jak długo firma przechowuje konkretne dane i kiedy powinny zostać usunięte.

6.3. Platformy i konfiguracje

Wiele incydentów wynika z błędnej konfiguracji systemów.

Hardening systemów – oznacza „utwardzanie" systemów poprzez wyłączanie wszystkich zbędnych usług i portów oraz stosowanie bezpiecznych ustawień zgodnych z rekomendacjami (np. benchmarki CIS czy NIST). Dzięki temu zmniejsza się powierzchnia ataku, czyli liczba potencjalnych punktów, przez które przestępca może dostać się do systemu.

Patch management – regularne i możliwie zautomatyzowane aktualizowanie systemów operacyjnych, aplikacji oraz urządzeń sieciowych. Badania pokazują, że ogromna część udanych ataków opiera się na lukach, dla których łatki były dostępne od wielu miesięcy.

Bezpieczna konfiguracja chmury – usługi chmurowe często domyślnie oferują ustawienia, które mogą być wygodne, ale niekoniecznie bezpieczne (np. publiczny dostęp do danych czy nadmiarowe uprawnienia dla użytkowników). Do zarządzania tym ryzykiem warto stosować narzędzia CSPM (Cloud Security Posture Management), które automatycznie monitorują środowisko chmurowe i wykrywają nieprawidłowe konfiguracje.

6.4. Odporność sieci i segmentacja

Sieci firmowe są często pierwszym celem ataków, ponieważ stanowią bramę do wszystkich systemów i danych organizacji. Dlatego ich odpowiednie zaprojektowanie, segmentacja i monitoring to kluczowe elementy ochrony.

- **Segmentacja sieci** – polega na podzieleniu infrastruktury na odrębne strefy, tak aby np. systemy krytyczne, biurowe czy urządzenia IoT były od siebie oddzielone. Dzięki temu nawet jeśli atakujący lub szkodliwy kod dostanie się do jednej części sieci, nie ma swobodnego dostępu do wszystkiego. To znacząco ogranicza skutki ataku i utrudnia przemieszczanie się intruza po środowisku IT.

- **Zero Trust** – to podejście, w którym firma nie ufa automatycznie żadnemu urządzeniu, użytkownikowi czy aplikacji. Każde żądanie dostępu jest weryfikowane, niezależnie od tego, czy pochodzi z sieci wewnętrznej czy z zewnątrz. W praktyce oznacza to częste sprawdzanie tożsamości, uprawnień i kontekstu działania użytkowników w specjalnych dedykowanych rozwiązaniach IT.

- **Bezpieczne VPN i ZTNA (Zero Trust Network Access)** – tradycyjne VPN często dają zbyt szeroki dostęp do zasobów firmy i w przypadku przejęcia konta stanowią poważne zagrożenie. Nowoczesne rozwiązania ZTNA pozwalają przyznać użytkownikowi dostęp tylko do wybranych aplikacji i systemów, których rzeczywiście potrzebuje.

- **IDS/IPS i firewall nowej generacji** – systemy IDS (Intrusion Detection System) i IPS (Intrusion Prevention System) służą do wykrywania i blokowania podejrzanych działań w sieci. W połączeniu z nowoczesnymi firewallami (które powinny być prawidłowo skonfigurowane) mogą one analizować ruch w czasie rzeczywistym, wykrywać anomalie i zatrzymywać próby włamań.

6.5. Kopie zapasowe, odzyskiwanie danych i odporność infrastruktury

W świecie rosnących zagrożeń cyfrowych kopie zapasowe i dobrze zaplanowane procesy odzyskiwania danych to fundament bezpieczeństwa każdej firmy. Same backupy nie wystarczą, jeśli nie towarzyszy im plan działania, który pozwoli szybko przywrócić kluczowe systemy i ograniczyć straty biznesowe. Kluczowe jest więc myślenie o odporności całej infrastruktury – od danych, przez aplikacje, aż po zasoby sieciowe. Poniżej przedstawiono najważniejsze praktyki, które każda organizacja powinna wdrożyć:

- **Zasada 3-2-1-1** – trzy kopie danych, na dwóch różnych nośnikach, jedna poza siedzibą firmy i jedna offline/immutable, odporna na modyfikacje. Takie podejście zwiększa szanse, że firma zachowa dostęp do danych nawet w przypadku ataku ransomware czy awarii fizycznej infrastruktury.

- **Regularne testy odtwarzania** – planowe próby przywracania danych w kontrolowanych warunkach; tylko sprawdzony backup daje pewność bezpieczeństwa. Testy pozwalają sprawdzić, czy kopie są kompletne i czy czas ich odtwarzania odpowiada potrzebom biznesu.

- **Szyfrowanie kopii zapasowych** – ochrona przed wykorzystaniem danych w przypadku ich kradzieży lub nieuprawnionego dostępu. Dzięki temu nawet w razie utraty nośnika poufne informacje pozostają bezużyteczne dla atakującego.

- **Segmentacja backupów** – przechowywanie kopii krytycznych danych w odrębnej strefie sieciowej, aby ograniczyć skutki potencjalnego ataku na systemy produkcyjne.

- **Integracja z planem DRP (Disaster Recovery Plan, Plan Odtworzenia Awaryjnego)** – jasne określenie priorytetów odtwarzania systemów, dopuszczalnego czasu niedostępności (RTO) i maksymalnej utraty danych (RPO).

- **Redundancja i wysoka dostępność** – stosowanie zapasowych centrów danych (lub stref w środowisku chmurowym), nadmiarowych łączy i mechanizmów wysokiej dostępności, aby minimalizować przestoje.

- **Monitorowanie środowiska backupowego** – bieżąca kontrola poprawności wykonywania kopii i raportowanie niepowodzeń w procesach backupowych.

6.6. Wnioski

- Tożsamość i dostęp są dziś najważniejszą warstwą obrony – kompromitacja konta często otwiera drogę do całej infrastruktury.

- Szyfrowanie i DLP chronią dane nawet wtedy, gdy dojdzie do incydentu.

- Hardening i patching eliminują najczęstsze luki wykorzystywane przez przestępców.

- Segmentacja i Zero Trust ograniczają skutki potencjalnego włamania.

- Backup i testy odtwarzania to podstawa odporności – bez nich każda firma jest zakładnikiem ransomware.

7. WYKRYWANIE

7.1. Rola wykrywania w odporności cyber

Nawet najlepsze zabezpieczenia techniczne nie dają 100% ochrony. Współczesne zagrożenia – od ransomware, szkodliwego oprogramowania, przez phishing, po ataki z użyciem AI – wymagają stałego monitorowania i detekcji. Kluczowe pytanie brzmi: „Jak szybko wykrywamy, że coś jest nie tak?".

Według globalnych raportów średni czas potrzebny cyberprzestępcy do przejęcia kontroli nad siecią to kilkanaście minut. Tymczasem w wielu firmach w Polsce wykrycie incydentu zajmuje dni lub tygodnie. To pokazuje, że budowa skutecznych zdolności detekcji jest niezbędna.

7.2. Monitorowanie i telemetria

- **Logowanie i centralizacja zdarzeń** – wszystkie systemy (serwery, stacje robocze, sieć, aplikacje chmurowe) powinny wysyłać logi do centralnego repozytorium.
- **SIEM (Security Information and Event Management)** – narzędzia, które korelują logi z wielu źródeł i wykrywają podejrzane wzorce.
- **Antywirus/EDR/XDR** – rozwiązania na stacjach roboczych i serwerach, którerejestrują aktywność i automatycznie wykrywają anomalie (np. nietypowe procesy, ruch sieciowy).
- **Monitoring chmury (CSPM, CWPP)** – kontrola konfiguracji i wykrywanie anomalii w środowiskach AWS, Azure, Google Cloud.
- **Alertowanie** – system musi informować odpowiednie osoby w czasie rzeczywistym.

7.3. Analityka i detekcja anomalii

- **AI w detekcji** – nowoczesne rozwiązania wykorzystują sztuczną inteligencję do rozpoznawania nietypowych zachowań użytkowników.

Korelacja zdarzeń – powiązanie informacji z wielu źródeł, np. próba logowania z nietypowej lokalizacji połączona z nietypowym ruchem w sieci może wskazywać na włamanie.

7.4. Informacja o zagrożeniach

Źródła zagrożeń – subskrybuj informacje o aktualnych kampaniach, podatnościach i atakach.

CERT Polska / CSIRT NASK – w Polsce to kluczowe instytucje udostępniające raporty i ostrzeżenia o bieżących zagrożeniach.

Współpraca branżowa – poszczególne bardziej rozwinięte sektory gospodarki korzystają np. z ISAC (Information Sharing and Analysis Centers), które pozwalają wymieniać się informacjami o incydentach.

7.5. Centrum monitorowania bezpieczeństwa (Security Operations Center (SOC))

Duże organizacje tworzą własne SOC, czyli centra monitorowania bezpieczeństwa. Mniejsze firmy mogą korzystać z usług dostawców takich usług i w zależności od potrzeb wspierać różne linie SOC.

Dla MŚP outsourcing SOC to często jedyne efektywne rozwiązanie – koszty budowy własnego zespołu są bardzo wysokie.

7.6. Wnioski

1. Czas wykrycia incydentu jest kluczowy – im szybciej, tym mniejsze straty.
2. Centralizacja logów i SIEM/EDR to fundament – nawet dla małych firm.
3. Bieżące monitorowanie zagrożeń dzięki podejściu proaktywnej obrony zwiększają szanse na wykrycie i zapobieganiu ataków.
4. SOC (wewnętrzny lub zewnętrzny) powinien być elementem wartym rozważenia – to inwestycja w odporność firmy.

8. REAGOWANIE I ODZYSKIWANIE

8.1. Rola planów reagowania i odzyskiwania

Nawet najlepsze zabezpieczenia i monitorowanie nie zapobiegną wszystkim incydentom. Dlatego kluczowe jest posiadanie planów reagowania na incydenty i planów odtworzenia awaryjnego i ciągłości działania (DRP/BCP).

reagowanie – szybkie i skoordynowane działania mające na celu ograniczenie skutków ataku.

odtworzenie – przywrócenie normalnego funkcjonowania firmy, usług i procesów krytycznych.

Nie chodzi o to, aby mieć plany w szufladzie lub szafie, ale regularnie je testować i weryfikować, czy są adekwatne i na ich podstawie w sytuacji kryzysu będziemy w stanie odtworzyć środowisko IT, przywrócić dane oraz kluczowe procesy operacyjne.

8.2. Plan reagowania na incydenty

Każda firma powinna posiadać dokument opisujący kroki działania w przypadku cyberincydentu. Typowa struktura obejmuje:

Identyfikację i zgłoszenie – kto i jak zgłasza incydent (np. phishing, ransomware, wyciek danych).

Ocena i klasyfikacja – ocena powagi zdarzenia (niski, średni, krytyczny).

Zespół zarządzania incydentem – osoby odpowiedzialne: bezpieczeństwo, ochrona danych, IT, prawnik, PR, zarząd.

Ograniczenie – jak ograniczyć rozprzestrzenianie się ataku (odłączenie systemów, blokada kont).

Komunikacja – procedury kontaktu z pracownikami, klientami, regulatorami.

Raportowanie – NIS2 wymaga zgłoszenia incydentu w ciągu 24 godzin, RODO – w ciągu 72 godzin, a klienci zgodnie z zapisami umownymi.

Analiza po incydencie – dokumentowanie, wnioski, usprawnienie procesów.

8.3. Analiza powłamaniowa i współpraca zewnętrzna

- Analiza powłamaniowa – przygotowanie systemów do zabezpieczenia dowodów cyfrowych (logi, kopie pamięci, obrazy dysków).
- Współpraca z CERT Polska, CSIRT NASK lub innym wskazanym CSIRTem – zgłaszanie incydentów i korzystanie ze wsparcia ekspertów.
- Ubezpieczenie cyber – coraz częściej element zarządzania ryzykiem, zapewniający środki na odzyskanie działalności i pokrycie kosztów prawnych.

8.4. Komunikacja kryzysowa

Cyberatak to nie tylko problem techniczny, ale również kryzys reputacyjny.

- **Przygotuj scenariusze komunikacyjne** – dla pracowników, klientów, partnerów i mediów.
- **Zadbaj o transparentność** – ukrywanie incydentów pogarsza zaufanie klientów i może narazić firmę na większe kary.
- **Włącz w plan dział PR i prawny** – reakcja powinna być spójna i zgodna z wymaganiami prawnymi.

8.5. Plany odzyskiwania i ciągłości działania (DRP/BCP)

Odporność firmy zależy od zdolności szybkiego przywrócenia działalności. Najlepsze praktyki wskazują, że każdy plan DRP/BCP powinien obejmować:

- **Identyfikację procesów krytycznych** – które usługi muszą działać w pierwszej kolejności.
- **Cele RTO/RPO** – w jakim czasie należy przywrócić systemy (Recovery Time Objective) i ile danych można maksymalnie utracić (Recovery Point Objective).

- **Plany alternatywne** – np. praca zdalna, systemy zapasowe, lokalizacje zastępcze.
- **Testy i ćwiczenia** – regularna weryfikacja i testowanie, czy procedury działają w praktyce.

8.6. Wnioski

1. Planowanie reakcji i odzyskiwania to obowiązek prawny (NIS2, DORA, RODO) i wymóg biznesowy.
2. Szybkość i koordynacja są kluczowe – chaos w reakcji zwiększa szkody.
3. Analiza powłamaniowa i komunikacja budują zaufanie klientów i ułatwiają współpracę z regulatorami.
4. Regularne testy planów DRP/BCP decydują o realnej odporności – dokument niećwiczony w praktyce jest martwy.

9. PROGRAM DLA MŚP: PODSTAWOWY POZIOM OCHRONY (PPO)

9.1. Dlaczego PPO jest konieczny

Większość małych i średnich firm w Polsce nie ma własnych działów bezpieczeństwa IT. Często korzystają z outsourcingu lub jednego administratora IT. Dlatego potrzebny jest zestaw prostych, tanich i skutecznych działań, które tworzą podstawowy poziom ochrony (PPO).

9.2. Lista 20 działań podstawowych

Tożsamość i dostęp

- Włącz MFA na wszystkich kontach (e-mail, bankowość, SaaS).
- Używaj menedżera haseł.
- Regularnie usuwaj nieaktywne konta i sprawdzaj listę uprawnień.
- Stosuj zasadę najmniejszych uprawnień – każdy pracownik ma dostęp tylko do tego, co konieczne.

Urządzenia i systemy

- Aktualizuj systemy i aplikacje automatycznie (Windows Update, aktualizacje macOS/Linux, aktualizacje telefonów).
- Stosuj oprogramowanie antywirusowe/EDR – nawet podstawowe rozwiązania blokują większość zagrożeń.
- Szyfruj dyski komputerów i urządzeń mobilnych (BitLocker, FileVault).
- Zabezpiecz urządzenia mobilne (PIN, biometria, możliwość zdalnego wyczyszczenia).

Dane i kopie zapasowe

- Wykonuj regularne kopie zapasowe danych krytycznych (dokumenty, e-maile, baza klientów, krytyczne dane firmowe).
- Testuj odtwarzanie backupów – sprawdzaj co najmniej raz w roku, czy kopie da się przywrócić.
- Przechowuj jedną kopię offline lub w chmurze (zasada 3-2-1).

Sieć i infrastruktura

- Zmień domyślne hasła na routerach, urządzeniach sieciowych, kamerach i urządzeniach IoT.
- Segmentuj sieć – zbuduj kilka segmentów sieci oraz oddziel urządzenia IoT od komputerów biurowych.
- Korzystaj z VPN dla pracy zdalnej.
- Zablokuj nieużywane porty i usługi w urządzeniach sieciowych.

Świadomość i procedury

- Edukuj pracowników z rozpoznawania różnych ataków dotyczących ich pracy, w tym phishingu i bezpiecznego korzystania z poczty.
- Prowadź testy phishingowe – np. wysyłaj kontrolne fałszywe e-maile, aby sprawdzić czujność zespołu.
- Wyznacz osobę ds. bezpieczeństwa (nawet jeśli to dodatkowa rola) – ktoś musi odpowiadać za koordynację działań.
- Ustal prostą procedurę zgłaszania incydentów – np. dedykowany adres e-mail oraz numer telefonu.
- Przygotuj plan awaryjny – kto odpowiada, jeśli firma padnie ofiarą ataku (IT, prawnicy, ubezpieczenie, komunikacja z klientami). Rozważ polisę od cyberzagrożeń.

10. PODSUMOWANIE

10.1. Kluczowe wnioski z podręcznika

1. **Cyberzagrożenia są realne i rosnące** – ransomware, ataki na łańcuch dostaw, phishing i deepfake są w Polsce codziennością. AI przyspiesza ewolucję ataków, staje po jasnej, jak i po ciemnej stronie mocy.
2. **Regulacje wymuszają działania** – przedsiębiorcy w Polsce muszą uwzględniać KSC, NIS2, RODO, a sektor finansowy także DORA. Brak wdrożenia grozi karami lub w skrajnej sytuacji upadkiem przedsiębiorstwa.
3. **Odporność to przewaga konkurencyjna** – firmy, które inwestują w bezpieczeństwo i zgodność z normami (ISO 27001, ISO 22301, SOC 2), budują zaufanie klientów i partnerów oraz otwierają drogę po nowe kontrakty. Sprawdzenie klienta w łańcuchu dostaw jest wymogiem prawnym.
4. **Ludzie są równie ważni jak technologia** – szkolenia, świadomość i kultura bezpieczeństwa są kluczowe dla skutecznej obrony. Szkolenia dla kadry zarządczej są obecnie wymogiem prawnym.
5. **Podstawowe praktyki chronią przed większością popularnych ataków** – MFA, backup, aktualizacje i segmentacja sieci mogą uratować firmę przed poważnym kryzysem.

10.2. Rekomendacje dla polskich przedsiębiorców

⇒ **Zacznij od podstaw** – wdrożenie PPO to szybka i tania poprawa bezpieczeństwa: 20 działań podstawowych opisanych w **Rozdziale 9**. Ignorowanie zagadnień bezpieczeństwa to prosta droga do katastrofy.

⇒ **Uwzględnij regulacje** – przygotuj się na NIS2 i DORA, bo ich wymagania będą egzekwowane, a naruszenia poważnie sankcjonowane.

⇒ **Planuj certyfikację** – ISO 27001 i 22301 to inwestycja w zaufanie klientów i partnerów.

⇒ **Myśl globalnie** – SOC1 lub SOC2 to przepustka do współpracy międzynarodowej lub do dużych klientów.

⇒ **Włącz zarząd i pracowników** – cyberbezpieczeństwo to odpowiedzialność całej organizacji, a nie tylko działu IT.

⇒ **Cyberbezpieczeństwo nie jest już opcją** – to warunek przetrwania i rozwoju w cyfrowym świecie. Polska, jako część Unii Europejskiej i aktywny uczestnik globalnej gospodarki, musi sprostać wyzwaniom rosnącej liczby cyberataków, wymagań regulacyjnych i postępu technologicznego.

11. SŁOWNIK POJĘĆ I SKRÓTÓW

APT (Advanced Persistent Threat)
Zaawansowane, długotrwałe ataki prowadzone przez dobrze zorganizowane grupy, często sponsorowane przez państwa.

AI (Artificial Intelligence) / SI (Sztuczna Inteligencja)
Zestaw technik umożliwiających maszynom wykonywanie zadań wymagających „inteligencji" – np. rozpoznawania wzorców, generowania treści czy podejmowania decyzji.

BCP (Business Continuity Plan)
Plan ciągłości działania – dokument określający, jak organizacja utrzyma kluczowe procesy w przypadku kryzysu.

BEC (Business Email Compromise)
Atak polegający na przejęciu lub podszyciu się pod konta e-mailowe w celu wyłudzenia środków finansowych lub poufnych danych.

CERT / CSIRT
Zespół reagowania na incydenty komputerowe. W Polsce działa CERT Polska i CSIRT NASK.

CIS Benchmark
Zestaw dobrych praktyk i wytycznych konfiguracji systemów i aplikacji opracowany przez Center for Internet Security.

DLP (Data Loss Prevention)
Narzędzia i procesy służące do zapobiegania nieautoryzowanemu wyciekom danych.

DORA (Digital Operational Resilience Act)
Rozporządzenie UE obowiązujące od 2025 r., nakładające wymogi odporności cyfrowej na instytucje finansowe i ich dostawców ICT.

DRP (Disaster Recovery Plan)
Plan odtwarzania systemów i danych po poważnym incydencie lub awarii.

EDR (Endpoint Detection and Response)
System monitorowania i reagowania na zagrożenia na stacjach roboczych i serwerach.

ENISA (European Union Agency for Cybersecurity)
Agencja UE ds. cyberbezpieczeństwa, przygotowująca analizy, wytyczne i raporty dla państw członkowskich.

GDPR / RODO (General Data Protection Regulation)
Rozporządzenie o ochronie danych osobowych obowiązujące w całej UE.

IAM (Identity and Access Management)
Systemy i procesy zarządzania tożsamością i dostępem użytkowników do systemów i aplikacji.

IoC (Indicator of Compromise)
Ślad techniczny wskazujący na to, że system mógł zostać naruszony (np. podejrzany adres IP, plik, hash).

IoT (Internet of Things)
Urządzenia podłączone do sieci – np. kamery, czujniki, routery, systemy przemysłowe.

ISO/IEC 27001
Międzynarodowy standard systemu zarządzania bezpieczeństwem informacji (ISMS).

ISO/IEC 27005
Standard ISO określający metody zarządzania ryzykiem w obszarze bezpieczeństwa informacji.

ISO 22301
Międzynarodowy standard systemu zarządzania ciągłością działania (BCMS).

KSC (Krajowy System Cyberbezpieczeństwa)
Ustawa regulująca cyberbezpieczeństwo w Polsce, obejmująca m.in. operatorów usług kluczowych i dostawców usług cyfrowych.

MFA (Multi-Factor Authentication)
Wieloskładnikowe uwierzytelnianie – łączenie hasła z dodatkowym czynnikiem, np. SMS, aplikacja mobilna, klucz sprzętowy.

MITRE ATT&CK
Baza wiedzy opisująca taktyki, techniki i procedury (TTPs) używane przez cyberprzestępców.

MSSP (Managed Security Service Provider)
Firma zewnętrzna świadcząca usługi monitorowania i ochrony cybernetycznej.

NIS2 (Network and Information Security Directive 2)
Dyrektywa UE z 2023 r. rozszerzająca wymagania cyberbezpieczeństwa na szerszą grupę firm i sektorów.

NIST (National Institute of Standards and Technology)
Amerykański instytut opracowujący standardy, m.in. Cybersecurity Framework (CSF).

PAM (Privileged Access Management)
Narzędzia i procesy do kontroli dostępu użytkowników z uprawnieniami administracyjnymi.

Phishing
Atak polegający na podszywaniu się pod zaufane instytucje lub osoby w celu wyłudzenia danych.

RPO (Recovery Point Objective)
Określenie, ile danych maksymalnie można utracić (np. ostatnie 4 godziny transakcji).

RTO (Recovery Time Objective)
Określenie, w jakim czasie trzeba przywrócić systemy po awarii/incydencie.

SIEM (Security Information and Event Management)
System do zbierania i korelowania logów z wielu źródeł w celu wykrywania zagrożeń.

SOC (Security Operations Center)
Centrum monitorowania bezpieczeństwa – wewnętrzne lub zewnętrzne (outsourcing MSSP).

SOC 1 / SOC 2
Raporty atestacyjne zgodne z amerykańskimi standardami:

- SOC 1 – kontrole wpływające na sprawozdawczość finansową.
- SOC 2 – kontrole dotyczące bezpieczeństwa i ochrony danych (oparte na TSC).

SOAR (Security Orchestration, Automation and Response)
Rozwiązania do automatyzacji reakcji na incydenty bezpieczeństwa.

SCRM (Supply Chain Risk Management)
Zarządzanie ryzykiem w łańcuchu dostaw, w tym bezpieczeństwem dostawców IT i oprogramowania.

TSC (Trust Services Criteria)
Kryteria opracowane przez AICPA, obejmujące pięć zasad: bezpieczeństwo, dostępność, integralność przetwarzania, poufność i prywatność.

UEBA (User and Entity Behavior Analytics)
Analiza zachowań użytkowników i urządzeń w celu wykrycia anomalii wskazujących na włamania.

Zero Trust
Model bezpieczeństwa zakładający, że żaden użytkownik ani urządzenie nie powinno być domyślnie zaufane – każdy dostęp musi być zweryfikowany.

12. O BW ADVISORY

BW Advisory sp. z o.o., z siedzibą w Polsce i oddziałami w Wielkiej Brytanii oraz Zjednoczonych Emiratach Arabskich, jest wiodącym dostawcą usług w zakresie technologii, bezpieczeństwa informacji oraz zarządzania ryzykiem zgodności i audytu (GRC&Audit). Nasz wykwalifikowany zespół ekspertów przeprowadza kompleksowe audyty i zarządza ryzykiem reputacyjnym, szczególnie na rynkach regulowanych.

Oferujemy szeroki zakres usług audytorskich, w tym audyty SOC 1, SOC 2, SOC 3 oraz inne specjalistyczne audyty SOC, skupiając się na sektorach finansowym, energetycznym i ICT. Nasze usługi obejmują audyty IT i bezpieczeństwa, integrację systemów GRC, analizę ryzyka oraz ocenę zgodności z międzynarodowymi standardami cyberbezpieczeństwa.

Dzięki udokumentowanemu doświadczeniu w realizacji złożonych projektów dla sektora prywatnego i publicznego, w tym dla renomowanych instytucji i krytycznie ważnych infrastruktur, BW Advisory sp. z o.o. dąży do zapewnienia klientom sukcesu poprzez wykorzystanie najwyższej klasy wiedzy specjalistycznej w obszarach technologii, bezpieczeństwa i zgodności z przepisami.

Nasze usługi są zaprojektowane tak, aby wspierać organizacje w zarządzaniu złożonymi wyzwaniami związanymi z cyfryzacją, cyberbezpieczeństwem oraz zgodnością z regulacjami, przyczyniając się do budowania odpornych i konkurencyjnych przedsiębiorstw w dynamicznie zmieniającym się środowisku biznesowym.

Dane kontaktowe:
BW Advisory sp. z o.o.
ul. Boczańska 25
03-156 Warszawa
NIP: 5252818352

e-mail: kontakt@itgrc.pl
www: https://www.itgrc.pl

13. O KLASTRZE CYBER MADE IN POLAND

CyberMadeInPoland to klaster zrzeszający polskie firmy i instytucje z sektora cyberbezpieczeństwa. Jego celem jest rozwój krajowych kompetencji, promocja polskich technologii na rynkach międzynarodowych oraz wspieranie współpracy między biznesem, nauką i administracją. Klaster działa na rzecz budowy silnego ekosystemu cyberbezpieczeństwa w Polsce i zwiększania konkurencyjności polskich podmiotów w Europie i na świecie.

Dane kontaktowe:
Polski Klaster Cyberbezpieczeństwa
CyberMadeInPoland Sp. z o.o.
ul. Ogrodowa 1/6, 31-155 Kraków
KRS: 0000854192
NIP: 6762583919
REGON: 386754317

Telefon: +48 669 614 854
email: office@cybermadeinpoland.pl
www: https://cybermadeinpoland.pl