

Cyberbezpieczeństwo i NIS2 · Moduł III: Incydenty, pracownicy i współczesne zagrożenia

Szkolenie otwarte · 18.09.2026 · Organizator: Platforma Wiedzy · Prowadzący: Paweł Maliszewski, Perfectinfo Sp. z o.o.

1 Nowoczesne zagrożenia i inżynieria społeczna	2 Środki techniczne i organizacyjne
3 CHECKLISTA PRACOWNIKA – bezpieczeństwo w codziennej pracy	4 STUDIUM PRZYPADKU – pierwsze 60 minut po wykryciu incydentu



Phishing, smishing i ataki ukierunkowane

☐ **Skala w Polsce (CERT Polska, 2025 r.):** 78 391 incydentów phishingu, w tym 28 462 pod szyldem OLX i 22 513 pod szyldem Allegro. Użytkownicy przekazali na numer 8080 295 169 podejrzanych SMS-ów. W UE phishing, w tym vishing (oszustwo głosowe), to ok. 60% wektorów wejścia w analizowanych incydentach (ENISA).

Rodzaj	Jak działa	Przykład z ostrzeżeń CERT Polska
Phishing	masowy e-mail podszyty pod instytucję lub firmę, link do fałszywej strony albo załącznik	„nieodebrana przesyłka urzędowa” z e-Doręczeń, która zostanie usunięta — strona wyłudza hasło do poczty
Smishing	SMS z linkiem	SMS podszyty pod InPost z prośbą o potwierdzenie danych przesyłki — strona wyłudza dane osobowe i dane kart (lipiec 2026 r.)
Ataki ukierunkowane (spear phishing)	wiadomość przygotowana pod konkretną organizację lub osobę	październik 2025 r.: e-maile do samorządów z domeny govministry[.]pl, podszyte pod wiceministra cyfryzacji — z plikiem XLSX z linkiem do złośliwego pliku wykonywalnego albo z prośbą o dane osób odpowiedzialnych za bezpieczeństwo IT

Wspólne mechanizmy według CERT Polska: podszywanie się pod zaufane instytucje, poczucie pilności i obietnica korzyści. Wiadomości bywają napisane poprawną polszczyzną — najważniejszą wskazówką pozostaje adres strony.

Zgłaszanie: podejrzany SMS — bezpłatnie na 8080; e-mail — cert@cert.pl albo formularz incydent.cert.pl.

Źródła: CERT Polska, Raport roczny 2025 (8.04.2026); ENISA Threat Landscape 2025 (1.10.2025); RMF FM za CERT Polska (7.07.2026); gov.pl, Baza wiedzy: zgłaszanie podejrzanych SMS-ów i e-maili do CERT Polska

Ćwiczenie 4: phishing czy nie?

Trzy wiadomości – przykład szkoleniowy, wzorowane na ostrzeżeniach CERT Polska. Prosimy wpisać na czacie trzy odpowiedzi, np. „1A 2B 3A”.

A = phishing		B = wiadomość prawdziwa	
1	2	3	
E-mail „e-Doręczenia” „Na skrzynce do doręczeń elektronicznych czeka nieodebrana przesyłka urzędowa. Brak odbioru w ciągu 24 godzin spowoduje jej usunięcie. Odbierz: e-doreczenia-odbior[.]com” – strona prosi o login i hasło do poczty.	E-mail od działu IT z firmowego adresu „W sobotę 9:00–13:00 system kadrowy będzie niedostępny z powodu aktualizacji. Nie trzeba nic robić. Pytania: helpdesk, tel. wew. 200.” – bez linku i załącznika, zgodnie z zapowiedzią w intranecie.	E-mail „wiceministra cyfryzacji” do urzędu „W związku z przygotowaniem do nowych obowiązków proszę do jutra przesłać imiona, nazwiska, telefony i adresy e-mail osób odpowiedzialnych za bezpieczeństwo teleinformatyczne.” – nadawca z domeny govministry[.]pl.	

Klucz odpowiedzi (po głosowaniu): 1 – A, 2 – B, 3 – A

1 A — phishing Sygnaly ostrzegawcze: presja czasu i groźba usunięcia, adres strony spoza gov.pl, prośba o hasło do poczty. Przesyłki z e-Doręczeń odbiera się po zalogowaniu na znanej stronie, a nie z linku w e-mailu.	2 B — prawdziwa Sygnalów ostrzegawczych brak: nadawca wewnętrzny, żadnej prośby o kliknięcie, logowanie ani dane, znany kanał kontaktu. W razie wątpliwości warto zadzwonić na znany numer helpdesku.	3 A — phishing Sygnaly ostrzegawcze: domena podszyta pod administrację (govministry zamiast gov.pl), nietypowa prośba o dane osób, presja terminu. To atak ukierunkowany: zebrane dane służą do kolejnych, bardziej precyzyjnych ataków.
---	--	---

Źródła: przykład szkoleniowy – wiadomości fikcyjne, wzorowane na opisach kampanii z Raportu rocznego CERT Polska 2025

Deepfake audio i wideo

Deepfake to sfałszowany przez AI obraz, nagranie wideo lub głos znanej osoby. ENISA: AI jest wykorzystywana zwłaszcza w vishingu i oszustwach z podszywaniem się pod inne osoby, z użyciem deepfake'ów.

W Polsce

NASK: od 1.01 do 1.07.2024 r. oszuści w reklamach podszywali się pod 121 znanych osób – najczęściej dziennikarzy (32%) i polityków (21%). Od czerwca 2024 r. do sierpnia 2025 r. NASK zidentyfikował ponad 13 tys. fałszywych reklam ze zmanipulowanymi materiałami audiowizualnymi.

UODO vs Meta: postanowieniem z 5.08.2024 r. Prezes UODO zakazał na 3 miesiące wyświetlania w Polsce na Facebooku i Instagramie fałszywych reklam z wizerunkiem Rafała Brzosi (art. 66 ust. 1 RODO – tryb pilny). Meta wycofała skargi do sądu, a postępowania umorzono (komunikat UODO z 24.03.2025).

W firmach

WPP, maj 2024 r.: przestępcy umówili spotkanie w Microsoft Teams z „prezesem” Markiem Readem, użyli klonu jego głosu i nagrań z YouTube. Chcieli wyłudzić pieniądze i dane osobowe od szefa jednej z agencji. WPP: incydentowi zapobiegła czujność pracowników.

Arup, styczeń 2024 r.: wideokonferencja z fałszywym dyrektorem finansowym – Historia na następnym slajdzie.

 **Jak się bronić:** oddzwonić na znany numer, zadać pytanie, na które odpowiedź zna tylko prawdziwa osoba, i nie wykonywać pilnych, poufnych poleceń finansowych bez drugiej osoby zatwierdzającej.

Źródła: ENISA Threat Landscape 2025 (1.10.2025); NASK (22.07.2024 i 29.10.2025); UODO, komunikaty z 9.08.2024 i 24.03.2025; Marketing-Interactive za The Guardian (20.05.2024)

Historia: Arup

Co się stało

W styczniu 2024 r. pracownik hongkońskiego biura Arup – globalnej firmy inżynieryjnej – wykonał 15 przelewów na 5 lokalnych kont bankowych, łącznie 200 mln HKD (ok. 25,6 mln USD). Zlecił je po wideokonferencji z dyrektorem finansowym i innymi osobami z firmy. Wszyscy uczestnicy poza nim byli podrobieni.

Jak do tego doszło

Najpierw przyszła wiadomość rzekomo od dyrektora finansowego z Wielkiej Brytanii o poufnej transakcji. Pracownik podejrzewał phishing. Wątpliwości rozwiąła wideokonferencja. Według policji w Hongkongu przestępcy przygotowali nagrania wcześniej, na podstawie publicznie dostępnych materiałów wideo i audio. Celem nie były systemy IT, tylko człowiek i proces zatwierdzania płatności.

Skutki

Oszustwo wyszło na jaw, gdy pracownik skontaktował się z centralą. Sprawę zgłoszono policji w Hongkongu 29.01.2024 r. Arup potwierdził w maju 2024 r. użycie fałszywych głosów i obrazów; według firmy jej stabilność finansowa i działalność nie zostały zagrożone, a żaden z wewnętrznych systemów nie został naruszony.

Lekcja dla Państwa

- Obraz i głos na wideokonferencji nie są dowodem tożsamości.
- Poufność i pośpiech przy przelewie to sygnał alarmowy, a nie powód, by pominąć procedurę.
- Duże przelewy: weryfikacja drugim kanałem na znany numer i druga osoba zatwierdzająca.

Źródła: Hong Kong Free Press za policję w Hongkongu (5.02.2024); South China Morning Post (17.05.2024); CNN (17.05.2024); Building: oświadczenie Arup (17.05.2024)

Anatomia ataku: deepfake na wideokonferencji

Wektor ataku

E-mail rzekomo od dyrektora finansowego z Wielkiej Brytanii o poufnej transakcji – pracownik „podejrzał phishing”. Wątpliwości rozwiązała wideokonferencja: głosy i twarze dyrektora finansowego i innych osób z firmy zbudowano z publicznie dostępnych nagrań – policja Hongkongu: „Scammers found publicly available video and audio of the impersonation targets via YouTube, then used deepfake technology to emulate their voices”. Nagrania przygotowano wcześniej i nie wchodziły w dialog z ofiarą; dalsze polecenia szły przez komunikatory i rozmowy jeden na jeden.

Dlaczego się udało

Technicznie: obraz i głos znanej osoby przestały być dowodem tożsamości – wystarczy kilka minut publicznych wystąpień; wideokonferencja nie weryfikuje, kto naprawdę siedzi po drugiej stronie.

Organizacyjnie: autoryzacja płatności opierała się na rozpoznaniu przełożonego i ustnym poleceniu; jeden pracownik wykonał 15 przelewów na 5 kont bez niezależnego potwierdzenia i bez drugiej osoby zatwierdzającej; „poufność” i pośpiech zadziałały nie jako sygnał ostrzegawczy, lecz jako argument, by pominąć procedurę. Oszustwo wyszło na jaw dopiero po kontakcie z centralą.

Jak temu zaradzić

Zabezpieczenia: próg kwotowy z podwójną autoryzacją w bankowości, konta i rachunki odbiorców zakładane osobno od zlecenia przelewów, MFA i limity dzienne, ostrzeżenie o rozmówcach spoza organizacji w wideokonferencjach.

Procedury (zalecenia policji Hongkongu): „ask questions during these meetings, ask the participants to move, and confirm requests made during those calls via alternative communication channels” – pytanie, na które odpowiedź zna tylko prawdziwa osoba (Ciekawostka 5), prośba o ruch głową, oddzwonienie na znany numer; zasada bez wyjątków „bo prosi zarząd”: żaden przelew na polecenie z wideo, telefonu lub komunikatora bez potwierdzenia drugim kanałem i drugiej osoby.

Źródła: Hong Kong Free Press za policję w Hongkongu (5.02.2024); Help Net Security za policję w Hongkongu (5.02.2024); South China Morning Post (17.05.2024)

AI w rękach przestępców

Narzędzia bez zabezpieczeń na sprzedaż (2023 r.)

WormGPT — reklamowany na forach przestępczych jako narzędzie do phishingu i ataków BEC, oparty na otwartym modelu językowym GPT-J.

FraudGPT — od lipca 2023 r. na kanałach Telegram, abonament od 200 USD miesięcznie do 1 700 USD rocznie; według sprzedawcy do pisania wiadomości spear phishingowych, tworzenia narzędzi do łamania zabezpieczeń i oszustw kartowych.

AI jako wykonawca ataku — raporty Anthropic

Sierpień 2025 r.: przestępca użył Claude Code do kradzieży danych i wymuszeń wobec co najmniej 17 organizacji — m.in. w ochronie zdrowia, służbach ratunkowych, administracji i instytucjach religijnych. AI decydowało, które dane wykraść, analizowało dane finansowe ofiar, żeby ustalić kwoty okupu, i przygotowywało noty z żądaniem od 75 do 500 tys. USD w bitcoinach. Anthropic zablokowało konta i przekazało wskaźniki ataku organom.

Listopad 2025 r.: grupa, którą Anthropic z wysoką pewnością wiąże z państwem chińskim, użyła Claude Code do prób włamań do ok. 30 organizacji — firm technologicznych, instytucji finansowych, producentów chemikaliów i agencji rządowych. AI wykonało 80–90% działań taktycznych, a kilka włamań się powiodło. AI często zawyżało też wyniki i czasem zmyślało dane.

❏ **FBI (IC3, 2025 r.):** ponad 22 tys. zgłoszeń oszustw z wykorzystaniem AI i ponad 893 mln USD strat.

Wniosek dla Państwa: AI obniża próg wejścia i przyspiesza ataki, ale nie zmienia skutecznej obrony: uwierzytelnianie odporne na phishing, weryfikacja poleceń drugim kanałem i monitorowanie nietypowej aktywności.

Źródła: The Hacker News za SlashNext (15.07.2023); Netenrich (25.07.2023); Anthropic: Threat Intelligence Report (27.08.2025); Anthropic: Disrupting the first reported AI-orchestrated cyber espionage campaign (13.11.2025); FBI IC3 Internet Crime Report 2025

Ransomware i wielopoziomowe wymuszenia

- ☐ **Szyfrowanie to tylko jeden z poziomów nacisku.** Verizon: ransomware w 48% naruszeń (rok wcześniej 44%). Mediana zapłaconego okupu spadła do 139 875 USD (ze 150 tys. USD), a 69% ofiar nie zapłaciło.

Poziom nacisku	Na czym polega
1. Szyfrowanie	organizacja traci dostęp do systemów i danych
2. Kradzież i groźba publikacji	„podwójne wymuszenie” (CISA) – kopie zapasowe nie pomogą, gdy dane są już u przestępców
3. Dodatkowy nacisk	nagłośnienie ataku, ataki DDoS, kontakt z klientami i partnerami ofiary (ENISA)
Wymuszenie bez szyfrowania	sama groźba publikacji wykradzionych danych (CISA) – tak działał przestępca z Claude Code opisany przez Anthropic

ALAB laboratoria (listopad 2023 r.)

Atak grupy RA World z żądaniem okupu. Spółka poinformowała, że nie negocjuje z cyberprzestępcami. Przestępcy opublikowali imiona, nazwiska, numery PESEL i wyniki ponad 50 tys. badań, a w grudniu kolejne dane, także pracowników i dostawców. CERT Polska i Centralny Ośrodek Informatyki dodały ok. 220 tys. numerów PESEL do serwisu bezpiecznedane.gov.pl, w którym można sprawdzić, czy dane wyciekły.

Wniosek dla Państwa: kopie zapasowe chronią przed szyfrowaniem, ale nie przed wyciekiem. Potrzebne są też szyfrowanie i segmentacja danych, monitorowanie nietypowego wysyłania danych na zewnątrz i gotowy plan zawiadomienia osób (art. 34 RODO).

Źródła: Verizon DBIR 2026 (19.05.2026); CISA #StopRansomware Guide; ENISA Threat Landscape for Ransomware Attacks (2022); Anthropic: Threat Intelligence Report (27.08.2025); ALAB, komunikat z 27.11.2023; Bankier.pl (21.12.2023); gov.pl, Baza wiedzy (22.12.2023); RODO (rozporządzenie 2016/679)

Historia: Gmina Janowo

Co się stało

28.07.2025 r. Gmina Janowo (powiat nidzicki, woj. warmińsko-mazurskie) przełała kilka milionów złotych należnych wykonawcy inwestycji z powiatu przasnyskiego – na rachunek przestępców.

Jak do tego doszło

Według Prokuratury Okręgowej w Olsztynie przestępcy przełamali zabezpieczenia poczty elektronicznej i przerobili fakturę VAT, wprowadzając gminę w błąd co do numeru rachunku odbiorcy. Nie podano, czyja skrzynka została przejęta.

Skutki

Odzyskano ponad 3 mln zł, ok. 1,5 mln zł nie odzyskano. Śledztwo w sprawie prania pieniędzy (art. 299 § 1 k.k.) zawieszono w oczekiwaniu na pomoc prawną ze Szwecji; nikt nie usłyszał zarzutów (stan z marca 2026 r.).

Lekcja dla Państwa

- Zmianę rachunku potwierdzamy telefonem pod numerem z umowy, a nie z e-maila z nową fakturą.
- Uwierzytelnianie wieloskładnikowe na poczcie utrudnia przejęcie skrzynki.
- Ten sam schemat kosztował Podlaski Zarząd Dróg Wojewódzkich ponad 3,7 mln zł w 2015 r.

BEC i CEO fraud: oszuści podszywają się pod kontrahenta, właściciela firmy albo członka zarządu i proszą o zmianę rachunku lub pilny przelew z pominięciem procedury (gov.pl, Europol). **Whaling** to atak wymierzony wprost w członków zarządu. **FBI, 2025 r.:** 24 768 zgłoszeń BEC i ok. 3,05 mld USD strat – druga kategoria po oszustwach inwestycyjnych.

Źródła: InfoPrasnysh za Prokuraturą Okręgową w Olsztynie (8.03.2026); Codziennik Mławski (2.09.2025); FBI IC3 Internet Crime Report 2025; gov.pl, Baza wiedzy: oszustwa typu BEC (20.12.2023); Europol: CEO/Business Email Compromise Fraud; TVN24 Białystok (7.10.2025)

Anatomia ataku: przejęta skrzynka i podmieniona faktura

Wektor ataku

Prokuratura: przelew wykonano „po uprzednim przełamaniu zabezpieczeń poczty elektronicznej” i „przerobieniu faktury VAT”, co wprowadziło gminę w błąd „co do rzeczywistego numeru rachunku bankowego odbiorcy”. Prawdziwa faktura, prawdziwy wykonawca, prawdziwa inwestycja – podmieniony był tylko numer rachunku. Nie ujawniono, czyja skrzynka została przejęta: gminy czy wykonawcy.

Dlaczego się udało

Technicznie: przejęta skrzynka pozwala czytać korespondencję i podstawić dokument w odpowiednim momencie – najczęściej przez hasło z wycieku lub phishing i brak MFA na poczcie; reguła przekierowania ukrywa odpowiedzi przed prawdziwym właścicielem konta.

Organizacyjnie: numer rachunku z faktury nie został porównany z umową ani z wykazem podatników VAT i nie potwierdzono go u wykonawcy pod numerem z umowy; kilkumilionowy przelew do wykonawcy przeszedł bez dodatkowej weryfikacji; ten sam schemat co w PZDW dziesięć lat wcześniej.

Jak temu zaradzić

Zabezpieczenia: MFA na każdej skrzynce, w tym urzędowej i kontrahentów; alert o nowych regułach przekierowania; SPF, DKIM i DMARC; sprawdzanie rachunku w wykazie podatników VAT wprost w systemie księgowym (API Ministerstwa Finansów); dwuosobowa autoryzacja przelewów powyżej progu w bankowości.

Procedury: zmiana rachunku tylko po oddzwonieniu na numer z umowy; rachunek na fakturze porównany z umową i wykazem przed każdym przelewem; „cztery oczy” dla przelewów na nowy rachunek; po pomyłce natychmiast bank i policja – czynności procesowe pozwoliły odzyskać ponad 3 mln zł, ok. 1,5 mln zł nie odzyskano; incydent w jednostce publicznej to także zgłoszenie do CSIRT i ocena, czy doszło do naruszenia danych.

Źródła: InfoPrzasnysz za Prokuraturą Okręgową w Olsztynie (8.03.2026); Codziennik Mławski (2.09.2025); KAS: Informacje o wykazie podatników VAT (gov.pl); CERT Polska, Raport roczny 2025 (8.04.2026)

Ciekawostka 5: Ferrari i pytanie o książkę

„Lipiec 2024 r.: menedżer Ferrari dostał na WhatsAppie wiadomości rzekomo od prezesa, Benedetta Vigny — z nieznanego numeru, ze zdjęciem profilowym Vigny na tle logo Ferrari. Chodziło o »duże przejęcie« i gotowość do podpisania umowy o poufności.”

Potem zadzwonił „prezes”. Głos wiernie naśladował jego akcent z południa Włoch. Rozmówca mówił o poufnej transakcji związanej z Chinami, wymagającej zabezpieczenia walutowego.

Menedżera coś zaniepokoiło. Zapytał o tytuł książki, którą Vigna polecił mu kilka dni wcześniej („*Decalogue of Complexity*” Alberta Felice De Toniego).

Rozmowa natychmiast się urwała. Ferrari wszczęło wewnętrzne dochodzenie.

- ❑ **Lekcja dla Państwa:** najprostsza obrona przed klonem głosu nie wymaga technologii — wystarczy pytanie, na które odpowiedź zna tylko prawdziwa osoba, albo oddzwonienie na znany numer. Warto uzgodnić to w zarządzie, zanim zadzwoni „prezes”.

Źródła: Fortune za Bloomberg (27.07.2024)

Uwierzytelnianie wieloskładnikowe (MFA)

Analogia: hasło to sam PIN. Uwierzytelnianie wieloskładnikowe (MFA) działa jak bankomat – potrzeba karty i PIN-u, więc samo podejrzenie PIN-u nie wystarczy złodziejowi.

❑ **Skuteczność:** MFA może zablokować ponad 99,9% ataków polegających na przejęciu konta (Microsoft, 2019).

Change Healthcare (USA, 2024 r.) — koszt braku MFA

12.02.2024 r. przestępcy zalogowali się skradzionymi danymi do portalu Citrix służącego do zdalnego dostępu. Portal nie miał MFA. Przemieszczali się po systemach i wykradali dane, a 21.02.2024 r. uruchomili ransomware (ALPHV/BlackCat). Prezes UnitedHealth w zeznaniu przed Kongresem: „decyzja o zapłacie okupu była moja”; kwotę 22 mln USD potwierdził ustnie podczas przesłuchania. Skutki: dane ok. 192,7 mln osób, a łączne skutki incydentu w 2024 r. to ok. 3,1 mld USD (koszty reakcji i utracone przychody).

MFA też można obejść

W 2022 r. napastnik z hasłem pracownika zewnętrznego Ubera – według Ubera prawdopodobnie kupionym w dark webie – logował się raz po raz, aż pracownik zatwierdził jedną z próśb o logowanie. CISA nazywa zasypywanie powiadomieniami „push bombing”.

❑ **Ustawa o KSC:** bezpieczne środki komunikacji elektronicznej uwzględniające uwierzytelnianie wieloskładnikowe „w stosownych przypadkach” to środek SZBI (art. 8 ust. 1 pkt 2 lit. I). **Najpierw:** poczta, dostęp zdalny, konta administratorów i systemy płatności.

Źródła: Microsoft Security Blog (20.08.2019); UnitedHealth Group: zeznanie A. Witty’ego przed Kongresem USA (1.05.2024); TechCrunch (1.05.2024); HIPAA Journal za HHS OCR (VIII 2025); UnitedHealth Group, formularz 8-K (16.01.2025); Uber, komunikat (19.09.2022); CISA: Implementing Phishing-Resistant MFA (2022); ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252)

Passkeys i FIDO2

CISA: każde MFA jest lepsze niż żadne, ale MFA odporne na phishing to „złoty standard”. Jedyne powszechnie dostępne uwierzytelnianie odporne na phishing to FIDO/WebAuthn.

Metoda (od najsilniejszej)	Ocena CISA
FIDO2/WebAuthn (passkeys, klucze sprzętowe), karty PKI	odporne na phishing
Kod z aplikacji lub tokena; powiadomienie z dopasowaniem numeru	podatne na phishing, odporne na „push bombing”
Powiadomienie „zatwierdź” bez dopasowania numeru	podatne na „push bombing” i pomyłki użytkownika
SMS i połączenie głosowe	podatne na phishing i przejęcie karty SIM — tylko w ostateczności

Passkeys (FIDO Alliance): poświadczenie oparte na standardach FIDO, przechowywane w telefonie, komputerze albo w kluczu sprzętowym. Logowanie wygląda jak odblokowanie urządzenia — odcisk palca, twarz, PIN. Poświadczenie jest przypisane do konta w konkretnej stronie lub aplikacji, więc nie ma hasła, które można wpisać na fałszywej stronie.

Microsoft (2025): MFA odporne na phishing zatrzymuje ponad 99% ataków na hasła, nawet gdy napastnik zna login i hasło.

 **Od czego zacząć:** administratorzy, zarząd, księgowość i dostęp zdalny; dla pozostałych — co najmniej aplikacja z dopasowaniem numeru zamiast SMS-ów.

Źródła: CISA: Implementing Phishing-Resistant MFA (2022); FIDO Alliance: Passkeys; Microsoft Digital Defense Report 2025 (16.10.2025)

Zero Trust



Zasada: żadnego domyślnego zaufania tylko dlatego, że użytkownik lub urządzenie są „w sieci firmowej” (NIST SP 800-207). Każdy dostęp jest sprawdzany: kto, z jakiego urządzenia, do czego i czy to typowe.

Analogia: biurowiec, w którym przepustkę sprawdza się przy każdych drzwiach, a nie tylko w recepcji – złodziej, który wszedł do holu, nie wejdzie do księgowości.

Pięć filarów modelu dojrzałości Zero Trust CISA (wersja 2.0, 2023 r.)

Filar	Przykład w praktyce
Tożsamość	MFA odporne na phishing, minimalne uprawnienia, szybkie odbieranie dostępów
Urządzenia	dostęp tylko z zarządzanych, aktualnych urządzeń
Sieci	segmentacja – np. oddzielenie sieci produkcyjnej od biurowej
Aplikacje i obciążenia	dostęp do konkretnej aplikacji zamiast do całej sieci przez VPN
Dane	klasyfikacja, szyfrowanie, kontrola wysyłania danych na zewnątrz

Przez wszystkie filary przechodzą trzy zdolności: widoczność i analityka, automatyzacja i orkestracja oraz zarządzanie. Organizacja przechodzi od etapu tradycyjnego przez początkowy i zaawansowany do optymalnego.

Po co: w Change Healthcare przestępcy po wejściu przez jeden portal swobodnie przemieszczali się po systemach. Zero Trust ogranicza taki ruch. To kierunek i program zmian, a nie jeden produkt do kupienia.

Źródła: NIST SP 800-207 (2020); CISA Zero Trust Maturity Model 2.0 (2023); UnitedHealth Group: zeznanie A. Witty'ego przed Kongresem USA (1.05.2024)

EDR i XDR

	Antywirus	EDR	XDR
Co widzi	pliki na komputerze	zachowanie stacji roboczych, telefonów i serwerów w czasie rzeczywistym	sygnały z punktów końcowych, sieci, chmury, poczty i tożsamości
Co robi	blokuje znane złośliwe pliki	wykrywa podejrzaną działalność i reaguje: izoluje komputer, zatrzymuje procesy, przenosi pliki do kwarantanny	łączy sygnały z wielu warstw w jeden incydent

EDR

Definicja z memorandum OMB M-22-01 dla administracji USA, 2021 r.: ciągłe monitorowanie i zbieranie danych z punktów końcowych połączone z automatyczną reakcją i analizą. Daje widoczność potrzebną wobec zaawansowanych zagrożeń, m.in. złośliwego oprogramowania zmieniającego postać i phishingu.

Reakcja: CISA wymienia typowe działania EDR — izolacja punktu końcowego, zatrzymanie procesów, kwarantanna plików.

XDR

Według opisu Microsoft: jedna platforma, która łączy sygnały z punktów końcowych, sieci, chmury, poczty, aplikacji SaaS i tożsamości.

- ❑ **Narzędzie to połowa sukcesu:** HSE Irlandia miało system, który wykrył narzędzia przestępców, ale działał tylko w trybie monitorowania (Moduł II). Alarm, którego nikt nie czyta, niczego nie zatrzyma. Potrzebny jest zespół, który obsługuje alerty także nocą i w weekend — własny albo dostawca usług zarządzanych w zakresie cyberbezpieczeństwa (art. 14 KSC). Monitorowanie w trybie ciągłym to środek SZBI (art. 8 ust. 1 pkt 2 lit. g KSC).

Źródła: OMB M-22-01 (8.10.2021); CISA CDM Technical Capabilities Vol. 2 (2023); Microsoft: What is XDR; PwC: Conti cyber attack on the HSE (3.12.2021); ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252)

Ryzyko → zabezpieczenie: mapa dla Państwa organizacji

Każde ryzyko ma dwa zabezpieczenia: techniczne i organizacyjne – jedno bez drugiego zawodzi. Tak rozumie to ustawa o KSC („środki techniczne i organizacyjne”, art. 8 ust. 1 pkt 2) i RODO (art. 32). Kolejne slajdy rozwijają każdy wiersz.

Ryzyko	Zabezpieczenia techniczne	Procedury	Przykład i slajd
phishing i socjotechnika	MFA odporne na phishing, filtr poczty, DMARC	weryfikacja drugim kanałem, zgłaszanie bez kary	Arup; Checklista pracownika
wykradzione hasła (infostealer)	menedżer haseł, MFA, zarządzane urządzenia	reset po wycieku, monitorowanie wycieków	Operation Endgame
przejęta skrzynka w chmurze	blokada starych protokołów, logi audytu	alert o regułach przekierowań	Storm-0558
podmieniona faktura (BEC)	wykaz podatników VAT w systemie, limity	telefon pod numer z umowy, „cztery oczy”	Janowo, PZDW
ransomware	EDR, kopie offline, segmentacja	plan reagowania, ćwiczenia	Moduł II
systemy bez wsparcia	inwentarz, automatyczne aktualizacje	plan wymiany, ryzyko zaakceptowane pisemnie	Windows 10
zgubiony laptop lub nośnik	szyfrowanie dysków, MDM	zgłoszenie w 72 h, zdalne czyszczenie	kary UODO
konta byłych pracowników	automatyczne wyłączanie kont, PAM	odejście z listą systemów, przeglądy dostępu	Tesla 2023
wyciek danych osobowych	pseudonimizacja, szyfrowanie, DLP	minimalizacja, retencja	ALAB, McDonald's
dane w narzędziach AI	firmowe konta AI, DLP	polityka AI, szkolenie	Samsung, IBM
DDoS	anty-DDoS, CDN, WAF	plan komunikacji, strona zapasowa	NoName057(16)
ryzyko resztkowe	dowody dla ubezpieczyciela	ubezpieczenie, umowa z zespołem reagowania	M&S i Co-op

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); RODO (rozporządzenie 2016/679); CIS Controls v8.1 (25.06.2024); ENISA: Technical Implementation Guidance on cybersecurity risk management measures (26.06.2025)

Ryzyko → zabezpieczenie: hasła w 2026 r.

- ❑ **Ryzyko:** hasła krótkie, powtarzane w wielu serwisach i układane ze wzorów z klawiatury łamie się słownikowo i wykorzystuje w atakach „credential stuffing”. Ponad 97% ataków na tożsamość to ataki na hasła (Microsoft). Wymuszona zmiana co 30 dni daje hasła „Wiosna2026!” i „Lato2026!”.

Zabezpieczenia techniczne — zgodne wytyczne NIST (2025) i CERT Polska

- długość zamiast złożoności: NIST — co najmniej 15 znaków, gdy hasło jest jedynym składnikiem, i co najmniej 8, gdy jest częścią MFA; CERT Polska — co najmniej 14 znaków; bez wymogu znaków specjalnych, cyfr i wielkich liter;
- bez okresowej zmiany haseł — zmiana tylko po wycieku lub podejrzeniu kompromitacji (NIST, CERT Polska);
- blokada haseł z list wycieków i haseł popularnych przy każdym ustawianiu hasła;
- menedżer haseł: firmowy, z współdzieleniem sejfów; system ma pozwalać na „wklej” w polu hasła;
- MFA na każdym koncie, które je obsługuje — najpierw poczta, dostęp zdalny, administratorzy.

Przykład: Snowflake (2024) — przestępcy logowali się hasłami z infostealerów do kont bez MFA; część haseł nie była zmieniana nawet 4 lata. Najpopularniejsze hasła w Polsce pokaże Ciekawostka 7.

Źródła: NIST SP 800-63B-4: Digital Identity Guidelines (VII 2025); CERT Polska: Kompleksowo o hasłach i Rekomendacje techniczne dla systemów uwierzytelniania (10.01.2022); Ministerstwo Cyfryzacji: bezpiecznedane.gov.pl, Bezpieczeństwo w sieci; Microsoft Digital Defense Report 2025 (16.10.2025); Mandiant: UNC5537 Targets Snowflake Customer Instances (10.06.2024)

Procedury

- aktualizacja polityki haseł do powyższych zasad (usunięcie wymogu zmiany co 30 lub 90 dni);
- jedno hasło = jedno konto (bezpiecznedane.gov.pl: „każde konto powinno mieć inne hasło”);
- reset hasła i drugiego składnika tylko po weryfikacji tożsamości pracownika przez dział IT;
- hasła do systemów współdzielone wyłącznie przez menedżer, nigdy w e-mailu ani na czacie.

Ryzyko → zabezpieczenie: wykradzione dane logowania i infostealery

- ❑ **Ryzyko:** infostealer — złośliwe oprogramowanie, które kopiuje hasła i ciasteczka sesji z przeglądarki i sprzedaje je hurtowo. Verizon (dane z 2024 r.): 30% zainfekowanych systemów to urządzenia z licencją firmową, a 46% systemów z firmowymi loginami to urządzenia niezarządzane, na których były też hasła prywatne. 54% ofiar ransomware z 2024 r. miało wcześniej domenę w wykradzionych danych logowania. Verizon (2026): wśród ofiar ransomware, u których wcześniej wykradzono dane logowania, połowa miała ten wyciek w ciągu 95 dni przed atakiem.

Zabezpieczenia techniczne

- MFA odporne na phishing (klucz sprzętowy, passkey) — skradzione hasło nie wystarcza;
- dostęp warunkowy: logowanie do systemów firmowych tylko z urządzeń zarządzanych (MDM, EDR, szyfrowanie);
- firmowy menedżer haseł zamiast zapisywania haseł w przeglądarce, zwłaszcza prywatnej;
- EDR na stacjach i krótki czas życia sesji, unieważnianie tokenów po wykryciu wycieku.

Procedury

- zakaz logowania do systemów firmowych z prywatnych komputerów bez MDM;
- monitorowanie wycieków domeny — bezpłatne powiadomienia moje.cert.pl o kontaktach z domeną organizacji w wyciekach, serwis bezpiecznedane.gov.pl, Have I Been Pwned;
- po wykryciu w wycieku — reset hasła, wylogowanie ze wszystkich sesji i sprawdzenie, skąd wyciekło.

Przykład — Operation Endgame (Europol, Eurojust)

Maj 2024 — ponad 100 serwerów wyłączonych, 4 zatrzymania; listopad 2025 — 1 025 serwerów, infostealer Rhadamanthys, VenomRAT i botnet Elysium; czerwiec 2026 — 326 serwerów, 142 domeny, 27 mln wykradzonych danych logowania odzyskanych, ponad 41 mln EUR kryptowalut zajętych. Odzyskane dane trafiają do Have I Been Pwned — warto sprawdzić domenę Państwa organizacji.

Źródła: Verizon DBIR 2025 (23.04.2025); Verizon DBIR 2026 (19.05.2026); Europol: Operation Endgame (30.05.2024, 13.11.2025, 24.06.2026); Eurojust (24.06.2026); operation-endgame.com (24.06.2026); CERT Polska: moje.cert.pl

Ciekawostka 6: klucze bezpieczeństwa w Google

„Nie mieliśmy żadnych zgłoszonych ani potwierdzonych przejęć kont od wdrożenia kluczy bezpieczeństwa.” — Google

Początek 2017 r.: Google wymagał od wszystkich ponad 85 tys. pracowników logowania fizycznymi kluczami bezpieczeństwa zamiast haseł i jednorazowych kodów.

KrebsOnSecurity (2018)

Od wdrożenia kluczy żaden pracownik Google nie padł ofiarą skutecznego phishingu na koncie służbowym.

Badanie Google (2019 r.)

Kod SMS zablokował 76% ataków ukierunkowanych, a powiadomienie na telefonie — 90%. Wśród użytkowników logujących się wyłącznie kluczami bezpieczeństwa nikt nie padł ofiarą ataku ukierunkowanego.

 **Lekcja dla Państwa:** klucze bezpieczeństwa i passkeys warto wdrażać najpierw u osób, które zatwierdzają przelewy, i u administratorów.

Źródła: KrebsOnSecurity (23.07.2018); Google Security Blog (17.05.2019)

Ryzyko → zabezpieczenie: poczta i konta w chmurze

- ❑ **Ryzyko:** przejęcie skrzynki lub całego konta w chmurze (Microsoft 365, Google Workspace): logowanie starym protokołem bez MFA, cicha reguła przekierowująca pocztę na zewnątrz, konto administratora bez ochrony – a potem podmieniona faktura (Historia Janowo) albo miesiące czytania korespondencji.

Zabezpieczenia techniczne — punkt odniesienia: bazowe konfiguracje CISA SCuBA dla Microsoft 365

- „Legacy authentication SHALL be blocked” — blokada starych protokołów (POP, IMAP, SMTP AUTH bez MFA);
- MFA odporne na phishing dla wszystkich użytkowników; blokada logowań i użytkowników wysokiego ryzyka;
- od 2 do 8 kont z rolą globalnego administratora, bez stałych przypisań najwyższych ról;
- automatyczne przekierowanie poczty do domen zewnętrznych wyłączone;
- SPF, DKIM i DMARC z polityką „p=reject” dla każdej domeny;
- audyt skrzynek włączony; logi Purview Audit (Standard) — od października 2023 r. bezpłatnie także dostęp do poczty, retencja 180 dni.

Procedury

- przegląd reguł skrzynek i przekierowań (alert przy nowej regule);
- przegląd administratorów co kwartał;
- eksport logów do własnego systemu;
- procedura „przejęta skrzynka”: wylogowanie sesji, zmiana hasła i drugiego składnika, sprawdzenie reguł i kontrahentów, którym wysłano „nowy rachunek”.

Przykład — Storm-0558 (2023)

Przestępcy fałszowali tokeny skradzionym kluczem podpisującym Microsoft i czytali skrzynki 22 organizacji oraz ponad 500 osób, m.in. Departamentu Stanu USA. Wykrył to SOC Departamentu Stanu dzięki logowi dostępu do poczty dostępnemu wówczas tylko w drogiej licencji. Rada CSRB: atak „preventable”, wynik „cascade of security failures”. Efekt: Microsoft udostępnił te logi wszystkim klientom bez dopłaty. Lekcja: logi w chmurze trzeba włączyć i czytać.

Źródła: CISA SCuBA: Microsoft 365 Secure Configuration Baselines (Entra ID, Exchange Online); CISA BOD 25-01 (17.12.2024); CSRB: Review of the Summer 2023 Microsoft Exchange Online Intrusion (2.04.2024); Microsoft Security Blog (19.07.2023 i 18.10.2023)

Ryzyko → zabezpieczenie: komunikatory i wideokonferencje

- ❑ **Ryzyko:** komunikatory i wideokonferencje to nowy kanał ataku: „IT help desk” pisze na Teams i prosi o zdalny dostęp, poufne decyzje zapadają w prywatnym komunikatorze, a obraz i głos rozmówcy można podrobić (Historia Arup).

Zabezpieczenia techniczne

- Teams i podobne: kontakt zewnętrzny tylko z zaufanych domen, ostrzeżenie „rozmówca spoza organizacji”, blokada czatów od nieznanych najemców;
- narzędzia zdalnego dostępu (Quick Assist, AnyDesk) dozwolone wyłącznie dla działu IT — reszta zablokowana polityką aplikacji;
- spotkania: poczekalnia, hasło, wyłączony anonimowy dostęp, imienne konta uczestników;
- firmowy komunikator z retencją i kopią zapasową dla spraw służbowych.

Procedury

- zasada „my dzwonimy do IT, nie IT do nas”: pracownik oddzwania na znany numer wewnętrzny, zanim udzieli zdalnego dostępu;
- sprawy poufne wyłącznie w kanałach firmowych — zakaz prywatnych komunikatorów w polityce i szkoleniu;
- przed omówieniem spraw poufnych — sprawdzenie listy uczestników i usunięcie nieznanych osób;
- pytanie kontrolne lub hasło dla nietypowych poleceń finansowych (Ciekawostka 5).

Przykłady

Storm-1811 / Black Basta (Microsoft, 15.05.2024): najpierw zalew skrzynki tysiącami newsletterów, potem połączenie w Teams od „pomocy technicznej”, prośba o Quick Assist i pełna kontrola nad komputerem — na końcu ransomware. ReliaQuest: napastnicy używali zewnętrznych najemców Microsoft 365 z nazwą „Help Desk”.

Signal, 24.03.2025: najwyżsi urzędnicy USA omawiali plany uderzeń w Jemenie w grupie na komunikatorze konsumenckim; do grupy przez pomyłkę dodano redaktora naczelnego „The Atlantic”, który dostał szczegóły ok. 2 godziny przed atakiem.

Źródła: Microsoft Threat Intelligence: Quick Assist w atakach socjotechnicznych (15.05.2024); ReliaQuest: Black Basta Social Engineering Technique — Microsoft Teams (25.10.2024); PBS NewsHour za AP (24.03.2025)

Ryzyko → zabezpieczenie: płatności i zmiana rachunku

- ❑ **Ryzyko:** oszustwo na fakturę i pilny przelew (BEC) omija każde zabezpieczenie techniczne, bo przelew wykonuje uprawniony pracownik. FBI (2025 r.): 24 768 zgłoszeń BEC i ok. 3,05 mld USD strat; oszustwa z użyciem AI – 22 364 zgłoszeń i ok. 893 mln USD. W Polsce: PZDW (2015) i Gmina Janowo (2025).

Zabezpieczenia techniczne

- sprawdzenie rachunku w Wykazie podatników VAT („biała lista”) przed każdym przelewem – automatycznie w systemie księgowym przez API Ministerstwa Finansów;
- dwuosobowa autoryzacja i limity kwotowe w bankowości elektronicznej; osobne uprawnienia do wprowadzania i zatwierdzania przelewów;
- MFA na poczcie i w systemie finansowo-księgowym; DMARC, żeby podszycie się pod Państwa domenę było trudniejsze;
- pole „rachunek kontrahenta” zmienia tylko wyznaczona osoba, z zapisem w historii zmian.

Procedury

- zmiana rachunku kontrahenta tylko po telefonie pod numer z umowy – nie z e-maila ani z nowej faktury;
- „cztery oczy” dla przelewów powyżej ustalonego progu i dla każdego przelewu na nowy rachunek;
- polecenie „pilne i poufne” od prezesa lub kontrahenta – zawsze weryfikacja drugim kanałem (Ferrari, Arup);
- prawo podatkowe pomaga: od 1.01.2020 przelew powyżej 15 000 zł na rachunek spoza wykazu oznacza brak kosztu podatkowego i solidarną odpowiedzialność za VAT sprzedawcy – chyba że w 7 dni złożą Państwo zawiadomienie ZAW-NR;
- po pomyłce: natychmiast bank (odwołanie przelewu) i policja – Gmina Janowo odzyskała ponad 3 mln zł.

Przykład: w Janowie i w PZDW zawiodła procedura, nie technologia: nikt nie zadzwonił pod numer z umowy.

Źródła: FBI IC3 Internet Crime Report 2025; KAS: Informacje o wykazie podatników VAT (gov.pl); podatki.gov.pl: zawiadomienie ZAW-NR; KAS: API Wykazu podatników VAT (wersja 1.6.0, 1.01.2025); InfoPrzasnysz za Prokuraturą Okręgową w Olsztynie (8.03.2026)

Ryzyko → zabezpieczenie: systemy bez wsparcia i aktualizacje stacji

- ❑ **Ryzyko:** system bez wsparcia nie dostaje poprawek bezpieczeństwa — każda nowa podatność zostaje otwarta na zawsze. Windows 10 stracił wsparcie 14.10.2025 r., a w sierpniu 2026 r. działał jeszcze na 24,9% komputerów w Polsce i 30,14% na świecie (StatCounter). Windows Server 2012 R2 — bez wsparcia od 10.10.2023 r. Wykorzystanie podatności to dziś najczęstszy wektor wejścia (Moduł II).

Zabezpieczenia techniczne

- inwentarz systemów i urządzeń z datą końca wsparcia (także drukarki, telefony VoIP, sterowniki, urządzenia brzegowe);
- automatyczne aktualizacje stacji, przeglądarek i aplikacji; łatki według ryzyka — najpierw systemy dostępne z internetu;
- Windows 10, jeśli musi zostać: program ESU — dla organizacji 61 USD za urządzenie w pierwszym roku, cena podwaja się co rok, maksymalnie 3 lata (wymaga wersji 22H2); dla urządzeń osobistych bezpłatnie z synchronizacją ustawień, za 1 000 punktów Rewards albo 30 USD — przedłużone do 12.10.2027 r.;
- system bez wsparcia, którego nie da się wymienić: odcięcie od internetu, osobny segment sieci, brak poczty i przeglądania.

Procedury

- plan wymiany z budżetem i terminami — środki finansowe na cyberbezpieczeństwo planuje kierownik (art. 8d pkt 2 KSC);
- zasada: system bez wsparcia = ryzyko zaakceptowane pisemnie przez kierownika, z datą wymiany;
- przegląd inwentarza co kwartał; koniec wsparcia jako zdarzenie w kalendarzu, nie niespodzianka;
- odbiór nowych urządzeń: aktualny firmware, zmienione hasła domyślne (Historia energetyki).

Przykład: Advanced (Wielka Brytania) — kara ICO 3 076 320 GBP m.in. za brak pełnego skanowania podatności i niewystarczające zarządzanie łatkami (Moduł I).

Źródła: Microsoft Learn: Windows 10 Extended Security Updates (17.11.2025); Microsoft: Windows 10 ESU dla urządzeń osobistych (stan 17.09.2026); Microsoft Learn: Windows Server 2012 R2 lifecycle; StatCounter: Windows version market share (VIII 2026); ICO, komunikat z 27.03.2025 (Advanced); ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252)

Ryzyko → zabezpieczenie: laptopy, telefony i praca zdalna

- ❑ **Ryzyko:** zgubiony pendrive lub skradziony laptop bez szyfrowania to naruszenie ochrony danych – i kara. Decyzje UODO: Res-Gastro (2024) – 238 345 zł za zgubiony niezaszyfrowany pendrive z danymi jednego pracownika; MOPS i MOSiR w Kutnie oraz firma wdrożeniowa (2024) – łącznie ok. 59 000 zł za pendrive z danymi ok. 1 500 osób, który otworzył znalazca; Wójt Gminy Dobrzyniewo Duże (2022) – 8 000 zł za kradzież laptopa zabezpieczonego tylko hasłem, choć procedura przewidywała szyfrowanie; Sąd Rejonowy w Zgierzu – 10 000 zł za pendrive kuratora z danymi 400 osób.

Zabezpieczenia techniczne

- pełne szyfrowanie dysków (BitLocker, FileVault) z kluczem odzyskiwania w Entra ID lub Active Directory; Windows 11 24H2 włącza szyfrowanie urządzenia automatycznie na większej liczbie komputerów – ale przy koncie lokalnym klucz pozostaje jawny i dane nie są chronione;
- zarządzanie urządzeniami mobilnymi (MDM): PIN, szyfrowanie, zdalne czyszczenie, oddzielenie danych firmowych;
- wyłącznie szyfrowane nośniki USB albo blokada portów; automatyczna blokada ekranu.

Przykład: Res-Gastro „informowała” o szyfrowaniu filmem instruktażowym, a analiza ryzyka nie przewidywała utraty nośnika – UODO uznał, że firma przerzuciła obowiązek na pracowników.

Źródła: UODO, komunikaty: 11.04.2022 (Zgierz), 16.11.2022 (Dobrzyniewo Duże), 17.05.2024 (Res-Gastro), 4.11.2024 (Kutno); Microsoft Learn: BitLocker overview (24.08.2026); RODO (rozporządzenie 2016/679)

Procedury

- szyfrowanie wdraża organizacja, nie pracownik – WSA za UODO: „pracownik nie może zastępować administratora w realizacji jego obowiązków”;
- rejestr urządzeń i nośników; zgłoszenie utraty natychmiast – od stwierdzenia naruszenia biegną 72 godziny na zgłoszenie do UODO (art. 33 RODO);
- praca zdalna: VPN lub dostęp warunkowy, brak drukowania danych poufnych w domu, czysty ekran w pociągu i kawiarni, zwrot sprzętu przy odejściu.

Ryzyko → zabezpieczenie: dostępy pracowników i odejścia z firmy

- ❑ **Ryzyko:** konta byłych pracowników i nadmiarowe uprawnienia. NIK w 2026 r. wskazała w urzędach nieodebrane uprawnienia byłych pracowników. Insider: w 2023 r. dwaj byli pracownicy Tesli przekazali niemieckiemu „Handelsblatt” dane 75 735 obecnych i byłych pracowników – imiona, adresy, numery ubezpieczenia społecznego, historię zatrudnienia; Tesla zgłosiła naruszenie prokuratorowi generalnemu stanu Maine 18.08.2023 r.

Zabezpieczenia techniczne

- centralna tożsamość (SSO) połączona z systemem kadrowym: koniec umowy = automatyczne wyłączenie wszystkich kont;
- PAM dla kont uprzywilejowanych – dostęp na czas zadania, zatwierdzany, z nagrywaniem sesji;
- uprawnienia według ról; alerty o masowym pobieraniu lub kopiowaniu danych (DLP);
- konta imienne dla pracowników dostawców, aktywne tylko w czasie prac, z MFA (Ćwiczenie 3).

Procedury

- proces „przyjęcie – zmiana – odejście” z listą systemów i właścicielem każdego dostępu;
- odebranie dostępu w dniu odejścia, także do chmury, VPN, kart i kluczy; przypomnienie o poufności na piśmie;
- przegląd uprawnień co kwartał przez właścicieli systemów (ISO/IEC 27001:2022, zał. A 5.18), ze szczególną uwagą na konta serwisowe i współdzielone;
- informacja z KRK przed dopuszczeniem do zadań z zakresu cyberbezpieczeństwa (art. 8f KSC).

Przykład: w Tesli dane wyniosły osoby, które miały do nich legalny dostęp – chroni przed tym nie hasło, lecz minimalne uprawnienia, monitorowanie eksportu i szybkie odbieranie dostępu.

Źródła: TechCrunch (21.08.2023); Fox Business (19.08.2023); NIK, komunikat z 21.07.2026: Cyberbezpieczny Samorząd; ISO/IEC 27001:2022; ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252)

Ryzyko → zabezpieczenie: dane osobowe — mniej znaczy bezpieczniej

- ❑ **Ryzyko:** im więcej danych i im dłużej je Państwo trzymają, tym większy wyciek i wyższa kara. ALAB (2023): przestępcy opublikowali wyniki ponad 50 tys. badań z numerami PESEL. McDonald's Polska (2025): numery PESEL i paszportów w grafikach pracy u agencji PR. UODO w planie kontroli na 2026 r.: monitoring wizyjny w podmiotach leczniczych (zwłaszcza dzieci), Biuletyny Informacji Publicznej, marketing, internetowe platformy dostaw, wielkoskalowe systemy UE.

Zabezpieczenia techniczne

- pseudonimizacja: identyfikatory zamiast danych osób, a klucz do ich odtworzenia poza systemem — EDPB: dane pseudonimizowane nadal są danymi osobowymi, ale ograniczają skutki nieuprawnionego dostępu;
- szyfrowanie baz danych i kopii zapasowych; maskowanie PESEL w widokach i raportach;
- DLP: kontrola eksportu i wysyłania danych na zewnątrz; automatyczne usuwanie po okresie retencji;
- osobne środowiska testowe bez danych produkcyjnych.

Przykład: gdyby grafiki pracy w McDonald's zawierały tylko imię i numer pracownika, wyciek nie objąłby numerów PESEL — minimalizacja działa, gdy zabezpieczenia zawiodą. EDPB: pseudonimizacja może też pozwolić oprzeć przetwarzanie na uzasadnionym interesie (art. 6 ust. 1 lit. f).

Źródła: RODO (rozporządzenie 2016/679); EDPB: Guidelines 01/2025 on pseudonymisation (wersja z 16.01.2025); UODO: Plan kontroli sektorowych na rok 2026 (8.01.2026); UODO, komunikat z 21.07.2025; ALAB, komunikat z 27.11.2023

Procedury

- minimalizacja (art. 5 ust. 1 lit. c RODO): nie zbierać PESEL, skanów dowodów ani danych o zdrowiu bez podstawy — test „po co nam to pole?”;
- retencja: dla każdej kategorii danych termin usunięcia i osoba odpowiedzialna;
- rejestr czynności (art. 30) i ocena skutków (art. 35) dla monitoringu, danych o zdrowiu i profilowania;
- klasyfikacja informacji i zasady pracy z dokumentami (Checklista pracownika).

Ryzyko → zabezpieczenie: sztuczna inteligencja w pracy

- ❑ **Ryzyko:** pracownicy wklejają do publicznych narzędzi AI kod, umowy, dane klientów i nagrania spotkań – „shadow AI”. IBM (2025): 13% organizacji zgłosiło naruszenia modeli lub aplikacji AI, z czego 97% nie miało kontroli dostępu do AI; co piąta organizacja miała naruszenie związane z shadow AI; organizacje z wysokim poziomem shadow AI ponosiły koszty naruszenia wyższe średnio o 670 tys. USD; 63% nie ma polityki zarządzania AI albo dopiero ją tworzy.

Zabezpieczenia techniczne

- firmowe konta w narzędziach AI: dane nie trenują modelu, umowa powierzenia, SSO i logowanie użycia;
- DLP w przeglądarce: blokada wklejania numerów PESEL, danych kart i dokumentów oznaczonych jako poufne;
- blokada niezatwierdzonych narzędzi AI na urządzeniach firmowych; kontrola dostępu do własnych modeli i agentów AI;
- rejestr narzędzi AI jako część rejestru aktywów i dostawców (Moduł II).

Procedury

- polityka użycia AI: zatwierdzone narzędzia, jakich danych nie wolno wprowadzać, obowiązek weryfikacji wyników – AI zawyża wyniki i zmyśla dane (raport Anthropic z listopada 2025 r.);
- szkolenie z kompetencji AI – obowiązek z art. 4 AI Act od 2.02.2025 r.; od 27.07.2026 r. w brzmieniu: podejmować środki wspierające rozwój kompetencji personelu (obowiązek działania, nie rezultatu); nadzór organów krajowych od 3.08.2026 r.;
- ocena dostawcy AI jak każdego dostawcy chmury: gdzie są dane, kto ma dostęp, jak usuwa.

Przykład – Samsung (wiosna 2023 r.): pracownicy wprowadzili do ChatGPT kod źródłowy i nagranie wewnętrznego spotkania, żeby dostać poprawki i protokół; od 1.05.2023 r. firma zakazała generatywnej AI na urządzeniach firmowych do czasu zbudowania bezpiecznego środowiska.

Źródła: IBM Cost of a Data Breach 2025 (30.07.2025); TechCrunch (2.05.2023); CIO Dive za The Economist Korea (7.04.2023); rozporządzenie (UE) 2024/1689 (AI Act), art. 4 i 113; rozporządzenie (UE) 2026/1744 (Dz.U. UE L z 24.07.2026); Komisja Europejska: AI literacy – Questions & Answers (stan 27.07.2026); Anthropic: Disrupting the first reported AI-orchestrated cyber espionage campaign (13.11.2025)

Ryzyko → zabezpieczenie: DDoS i dostępność usług

- ❑ **Ryzyko:** atak DDoS zalewa stronę lub e-usługę ruchem z tysięcy urządzeń – strona urzędu, e-rejestracja, sklep i logowanie klientów przestają działać, choć nikt się nie włamał. Sprawcami są często hakywiści: prorosyjska grupa NoName057(16) rekrutowała ok. 4 000 „ochotników”, którzy instalowali narzędzie DDoSia; w Niemczech przeprowadziła 14 fal ataków na ok. 230 organizacji, m.in. dostawców energii i urzędy (Eurojust). W polskim sektorze finansowym CSIRT KNF odnotował w 2025 r. 787 ataków DDoS.

Zabezpieczenia techniczne

- usługa anti-DDoS lub CDN przed serwerem – ruch filtrowany, zanim dotrze do Państwa łącza; WAF i limity liczby zapytań;
- rozdzielenie strony informacyjnej od systemów wewnętrznych; statyczna strona zapasowa u innego dostawcy;
- monitorowanie dostępności z zewnątrz i alarm, gdy strona nie odpowiada;
- własne usługi nie mogą wzmacniać cudzych ataków – CERT Polska ostrzega przed wystawionymi do internetu usługami NTP, SNMP, portmapper i SSDP.

Procedury

- umowa z dostawcą łącza i hostingu z zapisem o reakcji na DDoS i kontaktem całodobowym;
- plan komunikacji na czas niedostępności: strona zapasowa, media społecznościowe, infolinia, komunikat dla klientów;
- DDoS to incydent – ocena, czy poważny (art. 11 KSC), i zgłoszenie do CERT Polska (incydent.cert.pl);
- scenariusz „strona nie działa w dniu naboru albo rekrutacji” w ćwiczeniu sztabowym (Moduł II).

Przykład — Operation Eastwood (16.07.2025)

Europol i Eurojust z 12 państwami wyłączyły ponad 100 serwerów NoName057(16); 7 nakazów aresztowania (6 wobec osób przebywających w Rosji), 2 zatrzymania we Francji i Hiszpanii, przeszukania m.in. w Polsce; 1 100 uczestników i 17 administratorów otrzymało przez Telegram ostrzeżenie o odpowiedzialności karnej.

Źródła: Eurojust (16.07.2025); Europol (16.07.2025); KNF: podsumowanie działań CSIRT KNF za 2025 r.; CERT Polska, Raport roczny 2025 (8.04.2026); ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252)

Ryzyko → zabezpieczenie: ryzyko resztkowe — ubezpieczenie i zespół reagowania

- ❑ **Ryzyko:** nawet dobrze zabezpieczona organizacja może paść ofiarą. Zostaje ryzyko resztkowe: kto zapłaci za odbudowę, kto przyjedzie w nocy i kto zadzwoni do CSIRT. Marks & Spencer miało polisę: przy kosztach incydentu £101,6 mln wypłata z ubezpieczenia wyniosła £100 mln. Co-op nie miało ubezpieczenia od ryzyk cybernetycznych i wykazało £285 mln utraconej sprzedaży.

Zabezpieczenia techniczne

To one decydują o polisie: ubezpieczyciel w ankiecie pyta o MFA na dostępie zdalnym i poczcie, kopie zapasowe odseparowane od sieci, EDR, aktualizacje i plan reagowania. Braki podnoszą składkę albo zamykają drogę do polisy; sama ankieta to bezpłatny przegląd zabezpieczeń.

Procedury

- umowa z zespołem reagowania na incydynty (retainer) z gwarantowanym czasem reakcji albo dostawca usług zarządzanych w zakresie cyberbezpieczeństwa (art. 14 KSC) — Norsk Hydro odbudowywało systemy z zespołem Microsoft (Moduł II);
- ubezpieczenie cyber: zakres (koszty reakcji, odtworzenie, przerwa w działalności, odpowiedzialność wobec osób), wyłączenia i terminy zgłoszenia szkody — sprawdzone przed incydemem, nie po;
- lista kontaktów dostępna bez firmowych systemów: CSIRT (S46, incydent.cert.pl, cert@cert.pl), UODO, policja, ubezpieczyciel, kancelaria, zespół reagowania, rzecznik prasowy;
- decyzja o okupie podjęta zawczasu przez kierownictwo — Verizon: 69% ofiar nie zapłaciło; CISA odradza płacenie;
- coroczne ćwiczenie sztabowe z udziałem ubezpieczyciela lub zespołu reagowania.

Przykład: różnica między M&S i Co-op to nie tylko £100 mln wypłaty — to także gotowy zespół i procedury, które polisa wymusza jeszcze przed atakiem.

Źródła: M&S, wyniki półroczne (5.11.2025); Co-op, wyniki półroczne (25.09.2025); Talking Retail (26.03.2026); ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); Verizon DBIR 2026 (19.05.2026); CISA #StopRansomware Guide

Rola pracownika i need-to-know

Atak najczęściej nie zaczyna się od hakera przy serwerze, tylko od wiadomości do człowieka: phishing to 60% wektorów wejścia w incydentach analizowanych przez ENISA.

Rola pracownika w systemie bezpieczeństwa organizacji

- **Jestem częścią ochrony** — wiem, że atak często zaczyna się od zwykłego e-maila, SMS-a lub telefonu do pracownika, a nie od włamania do serwera.
- **Znam zasady w mojej organizacji** — wiem, gdzie są zasady bezpieczeństwa obowiązujące w mojej pracy i kogo pytać, gdy mam wątpliwości.

Zasada minimalnych uprawnień i need-to-know

- **Tylko potrzebne dostępy** — korzystam wyłącznie z dostępów potrzebnych do mojej pracy; zbędne, np. po zmianie stanowiska, zgłaszam do odebrania.
- **Nie pożyczam konta** — nie udostępniam nikomu loginu, hasła ani karty dostępu, także koledze „tylko na chwilę”.

□ **Analogia:** dostęp „need-to-know” działa jak karta hotelowa — otwiera Państwa pokój, a nie wszystkie drzwi w hotelu.

Źródła: ENISA Threat Landscape 2025 (1.10.2025); Checklista pracownika (PDF)

Czyste biurko, czysty ekran, dokumenty

Czyste biurko i czysty ekran

- ☐ Blokuję ekran
- ☐ Puste biurko po pracy
- ☐ Pilnuję, kto patrzy

Bezpieczna praca z informacją i dokumentami

- ☐ Sprawdzam adresata
- ☐ Dane firmy tylko w firmowych narzędziach
- ☐ Długie hasła i drugi składnik



☐ **Test na dziś:** czy po wyjściu z biura na biurku lub ekranie zostaje coś, czego nie powinien zobaczyć gość albo ekipa sprzątająca?

Źródła: Checklista pracownika (PDF)

Socjotechnika i weryfikacja poleceń

Rozpoznawanie prób wyłudzenia i socjotechniki

- ❑ Pośpiech to sygnał ostrzegawczy
- ❑ Sprawdzam nadawcę i link
- ❑ Nie podaję haseł ani kodów

Bezpieczna weryfikacja wiadomości, poleceń i tożsamości nadawcy

- ❑ Oddzwaniam na znany numer
- ❑ Zmiana numeru konta = sprawdzenie
- ❑ Polecenie od szefa też sprawdzam



❑ **Przykład z Polski:** SMS podszyty pod InPost z prośbą o „potwierdzenie danych przesyłki” i linkiem do fałszywej strony – ostrzeżenie CERT Polska z lipca 2026 r.

Źródła: CERT Polska, ostrzeżenie przed fałszywymi SMS-ami InPost (RMF FM, 7.07.2026); Checklista pracownika (PDF)

Kliknąłem, co teraz?

1 Zamknij stronę

Zamykam stronę i nie wpisuję już żadnych danych.

2 Odłącz od sieci

Odłączam urządzenie od sieci (kabel, Wi-Fi), ale go nie wyłączam.

3 Zadzwoń do IT

Od razu dzwonię pod numer z pola „Incident zgłaszam do”.

4 Zmień hasło

Z innego, bezpiecznego urządzenia zmieniam hasło, które mogło wyciec; przy danych karty dzwonię do banku.

5 Zapisz ślady

Zapisuję godzinę, adres strony i to, jakie dane zostały podane — i nie usuwam wiadomości.

Co zrobić po kliknięciu podejrzanego linku lub ujawnieniu danych

□ **Działam od razu** — po kliknięciu podejrzanego linku lub podaniu danych nie czekam, aż „samo przejdzie”, tylko wykonuję 5 kroków z ramki.

□ **Mówię wprost, co się stało** — przy zgłoszeniu podaję, jakie dane lub hasła zostały podane i kiedy; to nie jest powód do wstydu.

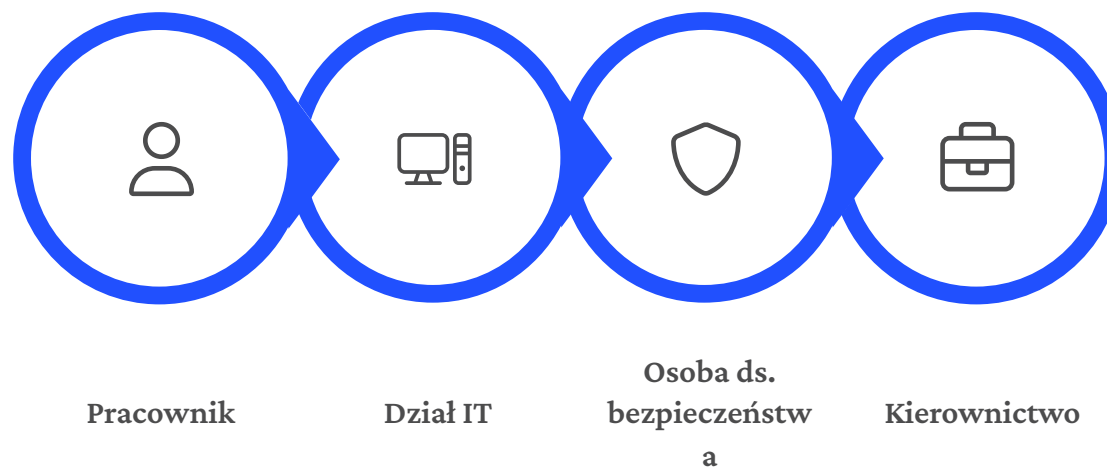
Źródła: Checklista pracownika (PDF)

Zgłaszanie i eskalacja

☐ Incyident zgłaszam do: ____ tel. ____

Szybkie zgłaszanie incydentów i wewnętrzna ścieżka eskalacji

- ☐ **Wiem, komu zgłaszam** – mam wpisany kontakt do zgłaszania incydentów, a gdy nikt nie odbiera, zgłaszam przełożonemu.
- ☐ **Zgłaszam też wątpliwości** – zgłaszam także to, czego nie jestem pewien lub pewna; lepsze zgłoszenie, które okaże się fałszywym alarmem, niż ukryty incydent.
- ☐ **Zachowuję ślady** – nie usuwam podejrzaney wiadomości i nie rozsyłam jej współpracownikom; postępuję z nią zgodnie ze wskazówkami działu IT.



24 h

Wczesne ostrzeżenie do CSIRT (KSC)

72 h

Zgłoszenie incydentu poważnego do CSIRT i naruszenia danych do UODO

8080

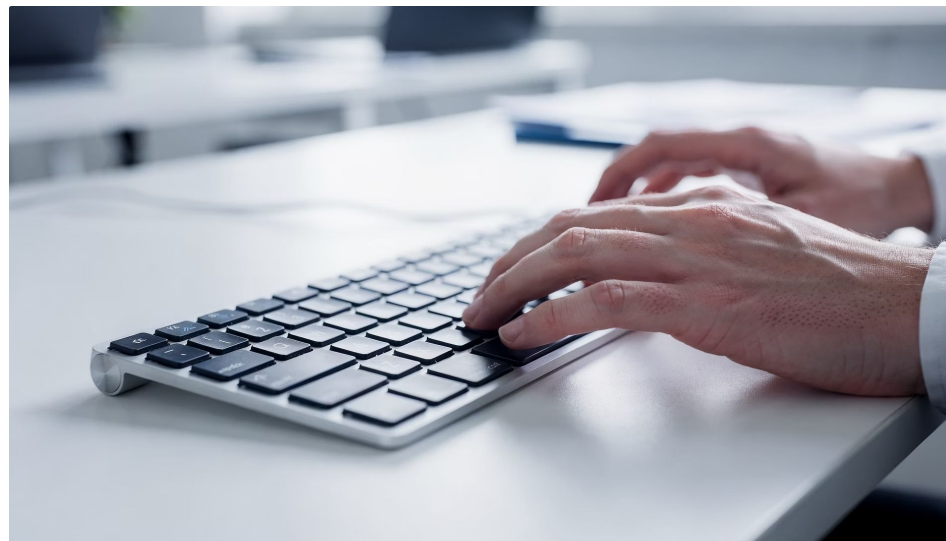
Podejrzany SMS na prywatnym telefonie – bezpłatnie do CERT Polska

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); RODO (rozporządzenie 2016/679); gov.pl, Baza wiedzy: zgłaszanie podejrzaných SMS-ów do CERT Polska (8080); Checklista pracownika (PDF)

Ciekawostka 7: najpopularniejsze hasła w Polsce 2025

Najpopularniejsze hasła w Polsce według NordPass (2025)

Dalej na liście są m.in. „password”, „Polska123” i „qwerty123”.



„zaq1@WSX” wygląda na mocne hasło: małe i wielkie litery, cyfra, znak specjalny. To jednak dwie sąsiednie kolumny klawiatury (z-a-q-1 w górę, 2-w-s-x w dół) – wzór, a nie przypadkowe znaki.

Zestawienie powstało z danych z wycieków i dark webu z okresu IX 2024 – IX 2025.

☐ **Lekcja dla Państwa:** długie hasło z menedżera haseł i drugi składnik logowania zamiast wzoru z klawiatury.

- 1 admin
- 2 123456
- 3 zaq1@WSX
- 4 12345678
- 5 zaq12wsx

Źródła: NordPass i NordStellar, Top 200 Most Common Passwords 2025; lista dla Polski: Spider's Web (XI 2025) i TELKO.in (20.11.2025)

Studium przypadku: scenariusz

- ❑ **Wisłomet sp. z o.o. — przykład szkoleniowy, spółka i zdarzenia fikcyjne.** Producent komponentów maszyn, 320 pracowników, dwie hale produkcyjne, podmiot ważny (zał. nr 2, „Produkcja”; art. 5 ust. 2 pkt 2 KSC). Przetwarza dane osobowe pracowników i klientów.

Piątek, 14:05

Księgowość zgłasza do działu IT, że pliki na dysku sieciowym mają dziwne rozszerzenia i nie da się ich otworzyć.

Na dwóch komputerach pojawia się plik z żądaniem okupu: „Dane firmy są skopiowane. Bez zapłaty okupu zostaną opublikowane”.

System ochrony stacji roboczych od godziny zgłasza alarmy z serwera plików. Nikt ich jeszcze nie przejrzał.

Dzień wcześniej pracownica księgowości otworzyła załącznik „faktura korygująca” z e-maila od znanego dostawcy.

Linie produkcyjne pracują. Za niecałe 3 godziny kończy się zmiana, a prezes jest w samolocie.

- ❑ **Pytanie na start:** kto w Państwa organizacji w piątek o 14:05 ma prawo zdecydować o odłączeniu systemów?

Elementy scenariusza pochodzą z prawdziwych Historii i przykładów: phishing z załącznikiem i nieobsłużone alarmy (HSE Irlandia), kradzież danych z groźbą publikacji (ALAB), odłączenie systemów i praca ręczna (Historia Norsk Hydro).

Źródła: przykład szkoleniowy — spółka i zdarzenia fikcyjne; ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252)

Minuty 0–15: wykrycie, zespół kryzysowy, izolacja

PRZYKŁAD SZKOLENIOWY · WISŁOMET SP. Z O.O.

14:05–14:10

Wykrycie: zgłoszenie z księgowości i alarmy z serwera plików to już podejrzenie incydentu. Zapisujemy godzinę wykrycia — od niej biegą terminy zgłoszeń z ustawy o KSC.

14:10

Zespół kryzysowy: osoba z uprawnieniem do decyzji w zastępstwie prezesa, IT i bezpieczeństwo, właściciel procesu produkcji, IOD i prawnik, osoba odpowiedzialna za komunikację; zewnętrzny zespół reagowania, jeśli jest umowa. Kanał zastępczy: telefony, nie firmowa poczta.

Ćwiczenie 5: co robi IT w pierwszych minutach? Prosimy wpisać na czacie literę.

A

Wyłącza zasilanie wszystkich komputerów i serwerów w firmie.

B ✓

Odłącza zainfekowane komputery i serwer plików od sieci, nie wyłączając ich, blokuje podejrzane konta i zabezpiecza ślady.

C

Od razu odtwarza serwer plików z kopii zapasowej, żeby księgowość mogła wrócić do pracy.

Klucz odpowiedzi (po głosowaniu): B

- **A** — wyłączenie wszystkiego zatrzymuje produkcję i kasuje ślady z pamięci ulotnej. CERT Polska i CISA: wyłączać tylko wtedy, gdy nie da się odłączyć urządzenia od sieci.
- **B** — izolacja zatrzymuje szyfrowanie i rozprzestrzenianie. CERT Polska: pamięć ulotna może zawierać informacje niezbędne do analizy incydentu i odzyskania zaszyfrowanych danych.
- **C** — przestępcy wciąż są w sieci: odtworzony serwer zostanie ponownie zaszyfrowany, a kopia może być już zainfekowana.

Źródła: przykład szkoleniowy — spółka i zdarzenia fikcyjne; CERT Polska: Poradnik ransomware (2021); CISA #StopRansomware Guide

Minuty 15–45: ocena skutków i zgłoszenia

PRZYKŁAD SZKOLENIOWY · WISŁOMET SP. Z O.O.

Ocena skutków (14:20–14:45): co stoi, czy skopiowano dane osobowe, czy przestępcy mają nadal dostęp i czy to incydent poważny (art. 11 ust. 1 pkt 3 KSC).

Obowiązek	Termin	Do kogo	Podstawa
Wczesne ostrzeżenie	24 h od wykrycia	CSIRT przez system S46	art. 11 ust. 1 pkt 4 KSC
Zgłoszenie incydentu poważnego	72 h od wykrycia	CSIRT przez system S46	art. 11 ust. 1 pkt 4a KSC
Sprawozdanie końcowe	miesiąc od zgłoszenia	CSIRT	art. 11 ust. 1 pkt 4c KSC
Zgłoszenie naruszenia danych osobowych, chyba że ryzyko dla osób jest mało prawdopodobne	bez zbędnej zwłoki, w miarę możliwości 72 h od stwierdzenia naruszenia	UODO	art. 33 RODO
Zawiadomienie osób	bez zbędnej zwłoki, przy wysokim ryzyku	pracownicy, klienci	art. 34 RODO

Do czasu uruchomienia CSIRT sektorowego zgłoszenia trafiają do CSIRT MON, CSIRT NASK albo CSIRT GOV (art. 44 nowelizacji). Obowiązki zgłoszeniowe z ustawy o KSC trzeba realizować najpóźniej od 3.04.2027 (art. 33 ust. 1 nowelizacji); RODO obowiązuje już dziś.

Jawność w pierwszych godzinach

Norsk Hydro

Wykrycie ataku tuż po północy 19.03.2019 r., komunikat jeszcze tego samego ranka, o 15:00 konferencja prasowa w Oslo.

Equifax

Wykrycie 29.07.2017 r., ujawnienie dopiero 7.09.2017 r., dane ok. 147 mln osób. Potem firmowy Twitter przez niemal 2 tygodnie odsyłał klientów na stronę phishingową (zamienione słowa w adresie).

PAP, 31.05.2024 r.

Fałszywą depeszę o częściowej mobilizacji, opublikowaną o 14:00 i 14:20 (według MSWiA prawdopodobnie rosyjski cyberatak), PAP za każdym razem natychmiast anulowała i zablokowała ścieżkę ataku.

Źródła: ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); ustawa z 23.01.2026 o zmianie ustawy o KSC (Dz.U. 2026 poz. 252); RODO (rozporządzenie 2016/679); Hydro: komunikat z 19.03.2019 (GlobeNewswire); Microsoft (16.12.2019); U.S. House Oversight Committee: The Equifax Data Breach (XII 2018); FTC (22.07.2019); RMF24 i Wirtualnemedi.pl (31.05–1.06.2024)

Minuty 45–60: komunikacja wewnętrzna i zewnętrzna

PRZYKŁAD SZKOLENIOWY · WISŁOMET SP. Z O.O.

Komunikacja wewnętrzna (14:50)

Krótką informacją dla pracowników kanałem zastępczym: co się stało, czego nie robić (nie włączać odłączonych komputerów, nie pisać o incydencie w mediach społecznościowych), komu zgłaszać podejrzone zdarzenia i kiedy będzie kolejna informacja.

Komunikacja zewnętrzna

Kluczowi klienci i dostawcy, ubezpieczyciel, policja; odbiorcy usług, jeśli incydent wpływa na świadczenie usługi (art. 11 ust. 2b KSC). Wyznaczeni rzecznicy i spójny przekaz we wszystkich kanałach (NCSC).

Ćwiczenie 6: 14:58 dzwoni dziennikarz lokalnego portalu: „Czy to prawda, że hakerzy ukradli dane pracowników?” Prosimy wpisać na czacie literę.

A

„Bez komentarza” — i koniec rozmowy.

B ✓

Wyznaczona osoba potwierdza incydent, mówi, że spółka działa z ekspertami i zawiadomiła właściwe instytucje, oraz podaje godzinę kolejnej informacji — bez spekulacji o sprawcy i zakresie.

C

Kierownik IT uspokaja: „Żadne dane nie wyciekły, wszystko jest pod kontrolą”.

Klucz odpowiedzi (po głosowaniu): B

- **A** — milczenie zostawia pole plotkom i przekazowi przestępców, którzy grożą publikacją danych.
- **B** — fakty, które spółka zna, i zapowiedź kolejnej informacji budują zaufanie bez ryzyka, że trzeba będzie coś odwoływać.
- **C** — po 50 minutach nikt nie wie, czy dane wyciekły, a nota okupowa mówi co innego. NCSC: unikać spekulacji i zapewnień o braku wpływu na dane osobowe, które trzeba będzie później odwołać.

Źródła: przykład szkoleniowy — spółka i zdarzenia fikcyjne; ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); NCSC: Guidance on effective communications in a cyber incident (2024)

5 rzeczy na poniedziałek

1 Status i termin

Sprawdzić, czy organizacja podlega ustawie o KSC i czy złożyła wniosek o wpis do wykazu – termin 3.10.2026 (Checklista zarządu).

2 Zespół kryzysowy

Wyznaczyć skład, zastępców z prawem decyzji i listę kontaktów dostępną bez firmowych systemów; opisać ścieżkę zgłoszeń 24 h / 72 h / miesiąc do CSIRT i 72 h do UODO.

3 Uwierzytelnianie wieloskładnikowe

Włączyć MFA, najlepiej odporne na phishing, na pocście, dostępie zdalnym i kontach administratorów.

4 Kopie zapasowe

Zlecić test odtworzenia jednego systemu krytycznego z kopii odseparowanej od sieci.

5 Ludzie

Przekazać pracownikom Checklistę pracownika i wprowadzić zasadę: każdą zmianę rachunku i każde pilne polecenie przelewu weryfikujemy drugim kanałem.

 **Dziękuję za wspólne 6 godzin.** Checklistę zarządu i Checklistę pracownika otrzymają Państwo od Organizatora.

Źródła: ustawa z 23.01.2026 o zmianie ustawy o KSC (Dz.U. 2026 poz. 252); komunikat MC z 8.04.2026 (Dz. Urz. Min. Cyfr. 2026 poz. 7); ustawa o KSC, tekst ujednolicony po nowelizacji (Dz.U. 2026 poz. 252); RODO (rozporządzenie 2016/679)

Zaufali nam



...oraz wiele, wiele innych firm.

Powyżej — wybrani z grona naszych Klientów.

POPULARNE Oto trzy scenariusze wojny z Rosją. Najgorszy oznacza katastrofę gospodarczą • Kryptoaktywa. Wyjaśniamy różnice między

BUSINESS INSIDER > BIZNES > 5 NAJLEPSZYCH FIRM WSPIERAJĄCYCH CYBERBEZPIECZEŃSTWO W BIZNESIE 2026 – WYBRALIŚMY NAJLEPSZYCH, KTÓRZY OCHRONIĄ TWÓJ BIZNES

5 najlepszych firm wspierających cyberbezpieczeństwo w biznesie 2026 – wybraliśmy najlepszych, którzy ochronią Twój biznes

Udostępnij artykuł

PerfectInfo



PerfectInfo – Najlepsza Firma Wspierająca Cyberbezpieczeństwo w Biznesie 2026

Bezpieczeństwo informacji, które nie blokuje biznesu

PerfectInfo to firma doradcza, która łączy dwa obszary: **cyberbezpieczeństwo oraz prawo**, a przy tym doskonale rozumie potrzeby biznesu. W jej podejściu bezpieczeństwo nie jest zbiorem dokumentów ani formalnością do odhaczania. lecz elementem wspierającym rozwój

TOP 5 firm cyberbezpieczeństwa w biznesie 2026 — Business Insider o nas

„Bezpieczeństwo informacji, które nie blokuje biznesu” — Business Insider Polska, 7 maja 2026 r.

Zapraszam do kontaktu

Dziękuję za udział. Zapraszam do pytań.

Paweł Maliszewski

Perfectinfo Sp. z o.o.

E-mail: pawel.maliszewski@perfectinfo.pl

Tel.: +48 606 19 19 15

WWW: www.perfectinfo.pl