GMINA DAMNICA

SZKOLENIE

W RAMACH AKADEMII OCHRONY LUDNOŚCI I OBRONY CYWILNEJ W 2026 ROKU

„BEZPIECZEŃSTWO INFORMACYJNE I CYFROWE - SPRAWDZANIE ŹRÓDEŁ INFORMACJI, OGRANICZANIE ROZPOWSZECHNIANIA TREŚCI NIEZIDENTYFIKOWANYCH, OCHRONA URZĄDZEŃ, HASEŁ I DANYCH, REAGOWANIE NA PODEJRZANE WIADOMOŚCI, LINKI I ZAŁĄCZNIKI ORAZ STOSOWANIE UWIERZYTELNIANIA DWUSKŁADNIKOWEGO I KOPII ZAPASOWYCH”

BEZPIECZEŃSTWO INFORMACYJNE I CYFROWE - SPRAWDZANIE ŹRÓDEŁ INFORMACJI, OGRANICZANIE ROZPOWSZECHNIANIA TREŚCI NIEZIDENTYFIKOWANYCH, OCHRONA URZĄDZEŃ, HASEŁ I DANYCH, REAGOWANIE NA PODEJRZANE WIADOMOŚCI, LINKI I ZAŁĄCZNIKI ORAZ STOSOWANIE UWIERZYTELNIANIA DWUSKŁADNIKOWEGO I KOPII ZAPASOWYCH

I. SPRAWDZANIE ŹRÓDEŁ INFORMACJI I OGRANICZANIE DEZINFORMACJI

1. Weryfikacja wiarygodność informacji (OSINT w praktyce).

1) Weryfikacja wiarygodności informacji w OSINT opiera się na przejściu od surowych danych (OSINF) do sprawdzonej wiedzy wywiadowczej (OSINT) poprzez systemowe odrzucanie fałszu i manipulacji. Kluczem praktycznego białego wywiadu jest zasada: nigdy nie ufaj pojedynczemu źródłu oraz stosowanie tzw. Kodu Admiralskiego (macierzy oceny wiarygodności źródła i pewności samej informacji).

2) Podział metod weryfikacji w zależności od rodzaju analizowanych danych:
   a. Weryfikacja tekstu i informacji (fakty)
      - Krzyżowe sprawdzanie danych: porównywanie informacji w niezależnych od siebie źródłach (np. rejestry państwowe vs. media społecznościowe vs. prasa).
      - Google Dorks: zaawansowane operatory wyszukiwania pozwalające dotrzeć do pierwotnych plików źródłowych (np. filetype:pdf "ściśle jawne") lub wykluczyć szum informacyjny.
      - Analiza metaprogramów i języka: badanie botów i farm trolli poprzez analizę powtarzalności fraz, składni oraz czasu publikacji postów.
   b. Weryfikacja zdjęć i wideo (obraz)
      - Geolokalizacja: ustalanie dokładnego miejsca wykonania materiału. Wykorzystuje się do tego detale architektoniczne, ukształtowanie terenu, znaki drogowe oraz narzędzia mapowe (np. Google Maps, Google Earth Pro, SunCalc do analizy cieni i pory dnia).
      - Chronolokalizacja: określanie czasu zdarzenia na podstawie warunków pogodowych (historyczne dane meteo), układu cieni (kąt padania słońca) oraz detali (np. faza przebudowy drogi).

- Wsteczne wyszukiwanie obrazem: narzędzia takie jak Google Lens, Yandex Images czy TinEye pozwalają znaleźć pierwsze publiczne użycie zdjęcia i wykryć, czy nie zostało ono zmanipulowane lub wycięte z innego kontekstu.
- Analiza metadanych (EXIF): narzędzia typu JPEGsnoop lub exiftool wyciągają ukryte informacje o aparacie, dacie wykonania i współrzędnych GPS (o ile nie zostały wyczyszczone przez platformy społecznościowe).

c. Weryfikacja infrastruktury i podmiotów (cyber/biznes)

Obszar weryfikacji	Metoda/Narzędzie OSINT	Cel
Strony WWW i domeny	• Rekordy WHOIS • DNSDumpster • Historia DNS	Kto jest prawdziwym właścicielem, jaka jest historia domeny i powiązane subdomeny.
Wiarygodność firm	• Krajowy Rejestr Sądowy (KRS) • CEIDG • Rejestr REGON	Sprawdzenie powiązań kapitałowych, historii finansowej i legalności biznesu.
Infrastruktura sieciowa	• Shodan • Censys	Analiza otwartych portów i urządzeń podpiętych do sieci w celu wykrycia fałszywych serwerów.

3) Złote zasady OPSEC podczas weryfikacji

Podczas prowadzenia OSINT-u należy bezwzględnie dbać o własne bezpieczeństwo operacyjne (OPSEC):

a. Nie dotykaj celu bezpośrednio: odwiedzenie profilu podejrzanej osoby na LinkedIn ze swojego prywatnego konta natychmiast zdradzi Twoją tożsamość. Korzystaj z kont typu sock puppet (fałszywych profili dedykowanych do śledztw).

b. Izoluj środowisko: używaj dedykowanych maszyn wirtualnych (np. systemów Linux takich jak Tsurugi Linux lub Kali Linux) oraz zaufanych połączeń VPN, aby nie zdradzić swojego adresu IP badanej infrastrukturze.



Fot. Melissa Anderson, VP Marketing/ Źródło: https://www.ivix.ai

2. Zagrożenie dezinformacją i fake newsy w pracy samorządu.

1) Dezinformacja i fake newsy stanowią jedno z kluczowych zagrożeń dla stabilności i zaufania społecznego na poziomie lokalnym, bezpośrednio uderzając w strukturę samorządową. Zjawisko to przestało być jedynie problemem wizerunkowym, stając się narzędziem destabilizacji politycznej, a nawet elementem wojny hybrydowej prowadzonej przez obce państwa.

2) Główne zagrożenia dla samorządu

- Paraliż pracy urzędów i hejt: fałszywe informacje napędzają hejt internetowy i agresję wymierzoną w urzędników oraz radnych. Dochodzi do nękania pracowników, zakłócania porządku publicznego w urzędach czy manipulowania nagraniami z obsługi interesantów. Skutkuje to kryzysem kadrowym i brakiem chętnych do startu w wyborach samorządowych.
- Podważanie zaufania do instytucji: przemyślana dezinformacja (będąca celowym sabotażem) systematycznie niszczy zaufanie mieszkańców do decyzji wójtów, burmistrzów i radnych.
- Wywoływanie paniki i niepokojów: fake newsy mogą sztucznie generować kryzysy – od rzekomych skandali korupcyjnych, przez fałszywe alarmy dotyczące bezpieczeństwa (np. zanieczyszczenia wody, zagrożenia awariami), aż po konflikty społeczne i zamieszki.

3) Obrona samorządów przed zagrożeniami

Przeciwdziałanie dezinformacji stało się jednym z obowiązków nowoczesnej administracji publicznej. Zgodnie z rekomendacjami ekspertów i instytucji takich jak NASK, kluczowe działania obejmują:

Obszar działania	Konkretne narzędzia i rozwiązania
Szybkie reagowanie	Wykorzystywanie własnych, sprawdzonych kanałów (oficjalne strony WWW, zweryfikowane profile w mediach społecznościowych) do natychmiastowego prostowania kłamstw.
Zgłaszanie incydentów	Przekazywanie podejrzanych treści do analityków NASK poprzez dedykowane formularze oraz zachęcanie mieszkańców do samodzielnego raportowania.
Edukacja lokalna	Budowanie odporności informacyjnej poprzez szkolenia dla urzędników oraz kampanie edukacyjne dla społeczności lokalnej.
Transparentność	Prowadzenie jasnej, zrozumiałej i wyprzedzającej komunikacji, która nie pozostawia przestrzeni na domysły i plotki.

Wsparcie na poziomie krajowym zapewnia m.in. powołane przez rząd Centrum Walki z Dezinformacją (CWD), które koordynuje wymianę informacji o incydentach w przestrzeni publicznej.

Jednocześnie środowiska samorządowe coraz głośniej apelują o zmiany w prawie, które pozwoliłyby skuteczniej chronić pracowników przed agresją i manipulacją w sieci.



Fot. Autor nieznany/ Źródło: https://opolska.policja.gov.pl/op/kwp-opole

3. Ograniczanie rozpowszechniania treści niezidentyfikowanych.

1) Ograniczanie rozpowszechniania treści niezidentyfikowanych (często utożsamianych z dezinformacją, fake newsami lub treściami o niezweryfikowanym pochodzeniu) opiera się na wieloaspektowych działaniach technologicznych, prawnych i edukacyjnych.
2) Zestawienie kluczowych strategii stosowanych przez platformy internetowe, rządy oraz organizacje pozarządowe:
   a. Rozwiązania technologiczne i algorytmiczne
      - Depriorytetyzacja (shadowbanning/demotion): algorytmy platform społecznościowych obniżają zasięgi postów, które zostały oznaczone jako potencjalnie szkodliwe lub niezweryfikowane, przez co nie pojawiają się one w sekcjach „Proponowane" czy „Trendy".
      - Systemy automatycznej detekcji: wykorzystanie sztucznej inteligencji (AI) do wykrywania botów, farm trolli oraz nietypowych, gwałtownych skoków popularności danych fraz (co może świadczyć o zorganizowanej kampanii manipulacyjnej).

- Etykietowanie i ostrzeżenia: dodawanie widocznych komunikatów pod postami (np. „Treść niezweryfikowana" lub „Te informacje są kwestionowane przez niezależnych weryfikatorów").

b. Współpraca z Fact-Checkingiem
   - Niezależni weryfikatorzy (fact-checkers): platformy (takie jak Meta czy Google) współpracują z certyfikowanymi organizacjami (np. AFP, Demagog), które sprawdzają zgłaszane treści.
   - Społecznościowa weryfikacja: narzędzia typu Community Notes (np. na platformie X), gdzie zaangażowana społeczność wspólnie tworzy kontekst i prostuje nieprawdziwe informacje na podstawie wiarygodnych źródeł.

c. Regulacje prawne i standardy (np. w UE)
   - Akt o usługach cyfrowych (DSA): unijne prawo nakłada na bardzo duże platformy internetowe (VLOPs) obowiązek szybkiego reagowania na nielegalne treści oraz audytowania systemów rekomendacji pod kątem ryzyka rozprzestrzeniania dezinformacji.
   - Kodeks postępowania w zakresie dezinformacji: dobrowolne (ale rygorystycznie monitorowane) zobowiązanie sygnatariuszy branży technologicznej do walki z manipulacją, m.in. poprzez odcinanie witryn szerzących dezinformację od zysków z reklam (demonetyzacja).

d. Edukacja i odporność społeczna
   - Prebunking (inokulacja psychologiczna): edukowanie użytkowników o technikach manipulacji zanim zetkną się z fałszywą informacją (np. poprzez krótkie gry, quizy czy kampanie wideo wyjaśniające, jak działają mechanizmy clickbaitu).
   - Edukacja medialna (media literacy): promowanie krytycznego myślenia, weryfikacji źródeł (sprawdzanie autora, daty publikacji, innych źródeł) oraz higieny cyfrowej w szkołach i kampaniach społecznych.



Fot. © Arloo (Fotolia)/ Źródło: https://warsawinstitute.org/pl

4. Zasada ograniczonego zaufania do informacji zewnętrznych.

1) Zasada ograniczonego zaufania do informacji zewnętrznych to fundamentalna reguła bezpieczeństwa, zgodnie z którą każda informacja pochodząca z zewnętrznego źródła powinna być traktowana jako potencjalnie niewiarygodna, niekompletna lub zmanipulowana, dopóki nie zostanie odpowiednio zweryfikowana. Choć historycznie termin ten wywodzi się z prawa o ruchu drogowym, współcześnie odgrywa kluczową rolę w cyberbezpieczeństwie, analizie informacji oraz zarządzaniu danymi w organizacjach. W erze cyfrowej zasada ta stanowi podstawę ochrony przed manipulacją, wyłudzeniami (np. phishing) oraz incydentami naruszenia danych.
2) Key Areas of Application (kluczowe obszary zastosowania)
   a. Cyberbezpieczeństwo i architektura Zero Trust: nowoczesne systemy IT rezygnują z tradycyjnego podejścia opartego na zaufaniu do sieci wewnętrznej. Zgodnie z koncepcją Zero Trust („nigdy nie ufaj, zawsze weryfikuj"), każdy użytkownik, urządzenie i pakiet danych próbujący uzyskać dostęp do zasobów – nawet wewnątrz organizacji – jest traktowany jako zewnętrzne i potencjalnie niebezpieczne źródło.
   b. Obrona przed socjotechniką: przestępcy internetowi często podszywają się pod zaufane instytucje (banki, urzędy, kurierów). Stosowanie zasady ograniczonego zaufania oznacza np. nieklikanie w linki w wiadomościach e-mail i niesprawdzone załączniki, lecz samodzielne weryfikowanie tożsamości nadawcy alternatywnym kanałem komunikacji.
   c. Higiena informacyjna (przeciwdziałanie fake news): w kontekście konsumpcji mediów zasada ta wymaga krytycznego podejścia do sensacyjnych wiadomości, postów w mediach społecznościowych czy opinii. Każda informacja zewnętrzna powinna być weryfikowana w kilku niezależnych i rzetelnych źródłach przed wyciągnięciem wniosków lub podaniem jej dalej.
   d. Weryfikacja danych w biznesie i programowaniu: podczas tworzenia oprogramowania programiści stosują zasadę weryfikacji danych wejściowych (input validation). System nie może ufać, że dane wprowadzone przez użytkownika lub zewnętrzny interfejs API są poprawne i bezpieczne, ponieważ mogą one zawierać złośliwy kod (np. próby ataków typu SQL Injection).

e. How to Apply This Principle in Practice? (Jak stosować tę zasadę w praktyce?)

Działanie	Opis
Weryfikacja tożsamości źródła	Zawsze sprawdzaj dokładny adres e-mail nadawcy, certyfikat SSL strony internetowej lub autentyczność profilu w mediach społecznościowych.
Zasada drugiego kanału	Jeśli otrzymasz pilną prośbę o przelew lub podanie danych od rzekomego kontrahenta, banku lub znajomego, skontaktuj się z nim telefonicznie, korzystając z oficjalnego, znanego Ci wcześniej numeru.
Krytyczna ocena intencji	Zastanów się, czy zewnętrzny komunikat nie próbuje wywrzeć na Tobie presji czasu, strachu lub obietnicy szybkiego zysku (typowe techniki manipulacji manipulacji psychologicznej).
Rozdzielanie uprawnień	Ograniczaj dostęp zewnętrznych systemów i aplikacji do swoich prywatnych danych lub sieci firmowej do absolutnego, niezbędnego minimum.

Stosowanie zasady ograniczonego zaufania do informacji zewnętrznych nie oznacza popadania w paranoję, lecz rozwinięcie nawyku zdrowego sceptycyzmu, który w świecie zdominowanym przez zaawansowane techniki manipulacji i cyberataki stanowi najlepszą linię obrony.



Fot. Alina Kowalska/ Źródło: https://horyzonty.info

II. OCHRONA URZĄDZEŃ, HASEŁ I DANYCH OSOBOWYCH

1. Zasady tworzenia silnych, unikalnych haseł (metoda zdań/fraz).

Metoda zdań (fraz hasłowych) to jeden z najskuteczniejszych sposobów tworzenia haseł, które są niezwykle trudne do złamania dla komputerów, a jednocześnie łatwe do zapamiętania dla człowieka. Polega ona na rezygnacji z pojedynczych, skomplikowanych słów na rzecz całych wyrażeń.

1) Zasady i główne sposoby wykorzystania metody:
   a. Sposób 1
      - pełna fraza hasłowa (Passphrase) zamiast jednego słowa, Twoim hasłem staje się całe, logiczne (lub abstrakcyjne) zdanie.
      - zasada: łączysz kilka słów, dodając wielkie litery, cyfry i znaki specjalne.

- przykład: zamiast słabego Piesek123 tworzysz bezpieczną frazę: Mój! Czarny#Pies$Biega27Szybko.

b. Sposób 2

- metoda pierwszych liter zdania - wymyślasz zdanie, które łatwo zapamiętasz, a jako hasło zapisujesz wyłącznie pierwsze litery każdego ze słów, wplatając w nie znaki i cyfry.
- zdanie-baza: „w każdy poniedziałek piję gorącą kawę z 2 łyżeczkami cukru**!**"
- gotowe hasło: Wkppgkz2łc!

2) Główne zasady tworzenia silnych haseł tą metodą

Cecha hasła	Opis i dobre praktyki
Odpowiednia długość	Absolutne minimum to 12–14 znaków. Metoda zdań pozwala bez problemu osiągnąć tę długość.
Unikalność	Jedno konto = jedno hasło. Nigdy nie używaj tej samej frazy w kilku miejscach.
Miks znaków	Mieszaj WIELKIE i małe litery, cyfry oraz znaki specjalne (np. !, @, #, $) jako separatory słów.
Brak danych osobistych	Zdanie nie może zawierać Twojego imienia, nazwiska, daty urodzenia ani imion członków rodziny czy zwierząt.
Zero oczywistych wzorców	Unikaj popularnych przysłów, cytatów z filmów jeden do jednego oraz ciągów typu 123456 czy qwerty.

3) Dodatkowa ochrona kont

Nawet najsilniejsze hasło może paść ofiarą wycieku z bazy danych danego serwisu. Aby w pełni zabezpieczyć swoje dane:

- Włącz uwierzytelnianie dwuskładnikowe (2FA/MFA): wymóg potwierdzenia logowania np. kodem z SMS lub aplikacji (jak Google Authenticator) drastycznie utrudnia włamanie.
- Używaj menedżera haseł: narzędzia takie jak Bitwarden czy 1Password zapamiętają wszystkie skomplikowane frazy za Ciebie.



Fot. Autor nieznany/ Źródło: https://bezpiecznymiesiac.pl

2. Bezpieczne przechowywanie haseł (menedżery haseł).

1) Menedżer haseł to najbezpieczniejsze narzędzie do przechowywania cyfrowych danych logowania, które eliminuje konieczność zapamiętywania dziesiątek unikalnych haseł. Działa jak zaszyfrowany cyfrowy sejf, do którego dostęp uzyskujesz za pomocą jednego, bardzo silnego hasła głównego.

2) Pozytywy korzystania z menedżera haseł:
   - Generowanie silnych haseł: narzędzie automatycznie tworzy długie, losowe i skomplikowane ciągi znaków (np. p$9!mK2@zL99), które są niemożliwe do złamania metodą prób i błędów.
   - Zasada „Zero-Knowledge": najlepsze programy szyfrują Twoje dane lokalnie na urządzeniu, zanim trafią one do chmury. Dostawca usługi nie zna Twojego hasła głównego i nie ma technicznej możliwości podejrzenia Twoich danych.
   - Wygoda i automatyzacja: aplikacje same uzupełniają formularze logowania na stronach internetowych i w aplikacjach mobilnych.
   - Wsparcie dla Passkeys: nowoczesne menedżery pozwalają na logowanie biometryczne (odciskiem palca lub skanem twarzy) zamiast tradycyjnych haseł.

3) Porównanie popularnych menedżerów haseł (stan na 2026 rok)

Menedżer haseł	Typ przechowywania	Model biznesowy	Główne zalety
Bitwarden	Chmura lub serwer własny	Darmowy (świetny plan bez limitu haseł/urządzeń)	Kod otwartoźródłowy (open source), wysokie bezpieczeństwo, pełna synchronizacja za darmo.
1Password	Chmura	Płatny (brak wersji darmowej)	Wyjątkowo dopracowany interfejs, funkcja Secret Key (dodatkowy klucz ochrony konta).
Proton Pass	Chmura (Szwajcaria)	Freemium (darmowy z ograniczeniami)	Silna ochrona prywatności, wbudowany generator aliasów e-mail chroniący przed spamem.
KeePass / KeePassXC	Lokalnie (plik na dysku)	Całkowicie darmowy	Pełna kontrola nad danymi, brak serwerów chmurowych, dla zaawansowanych użytkowników.

4) Bezpieczne wdrażanie menedżera haseł
   a. Stwórz pancerne hasło główne: to najważniejszy krok. Hasło główne powinno składać się z minimum 14–16 znaków. Najlepiej użyć metody frazy pasażowej – połącz 4–5 losowych, niezwiązanych ze sobą słów (np. KawaKrzesloBalonJezioro!).

b. Włącz uwierzytelnianie dwuskładnikowe (2FA): zabezpiecz dostęp do samego menedżera za pomocą aplikacji uwierzytelniającej (np. Google Authenticator) lub klucza sprzętowego (np. YubiKey).

c. Zrób kopię zapasową klucza awaryjnego: podczas rejestracji otrzymasz klucz odzyskiwania konta. Wydrukuj go lub zapisz offline – jeśli zapomnisz hasła głównego, nikt (nawet pomoc techniczna) nie odzyska Twoich danych.



Fot. Aneta Tomczyk/ Źródło: https://nano.komputronik.pl

3. Ochrona fizyczna urządzeń (zasada czystego biurka/ekranu, blokowanie stacji roboczej).

Ochrona fizyczna urządzeń to jeden z filarów bezpieczeństwa informacji. Zapobiega nieautoryzowanemu dostępowi osób trzecich do danych widocznych na ekranie lub pozostawionych na biurku.

1) Najważniejsze zasady i dobre praktyki podzielone na kluczowe obszary:

a. Zasada czystego biurka (Clean Desk Policy)

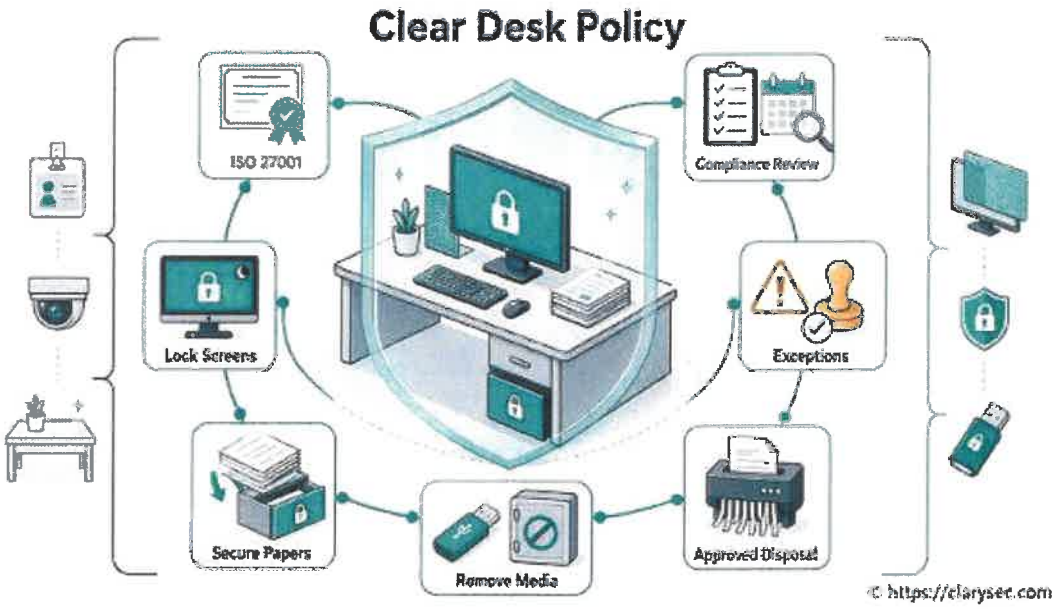
- Chowanie dokumentów: wszystkie dokumenty papierowe, nośniki danych (pendrive'y, dyski zewnętrzne) oraz notatki (np. żółte karteczki) zawierające informacje poufne muszą być schowane do zamykanych szuflad lub szaf, gdy nie są używane.
- Niszczenie danych: dokumenty przeznaczone do wyrzucenia należy niezwłocznie zniszczyć w niszczarce (o odpowiedniej klasie tajności), zamiast wrzucać je do zwykłego kosza.
- Czystość po pracy: po zakończeniu dnia pracy na biurku nie powinny pozostawać żadne materiały operacyjne ani nośniki informacji.

b. Zasada czystego ekranu i blokowanie stacji roboczej

- Blokowanie ekranu: Każde oddalenie się od stanowiska pracy – nawet na kilka sekund (np. wyjście po kawę czy do toalety) – wymaga zablokowania komputera.
- Skrót klawiszowy: Windows + L (Windows) lub Ctrl + Cmd + Q (macOS).
- Automatyczna blokada: konfiguracja systemu do automatycznego wygaszania i blokowania ekranu po krótkim czasie bezczynności (np. maksymalnie 2–5 minut).
- Filtry prywatyzujące: stosowanie specjalnych nakładek na monitor (filtrów polaryzacyjnych), które uniemożliwiają odczytanie zawartości ekranu osobom patrzącym z boku.
- Pozycjonowanie monitora: ustawienie ekranu w taki sposób, aby nie był widoczny dla osób postronnych (np. przechodzących korytarzem lub stojących w oknie).

c. Ogólna ochrona fizyczna sprzętu

- Zabezpieczenia mechaniczne: stosowanie linek blokujących (np. typu Kensington Lock) do przypięcia laptopa do biurka w miejscach publicznych lub otwartych przestrzeniach biurowych (open space).
- Nadzór nad sprzętem: zakaz pozostawiania urządzeń służbowych bez opieki w miejscach publicznych (np. w kawiarniach, pociągach czy na lotniskach) oraz w widocznych miejscach w samochodzie.



Fot. Autor nieznany/Źródło: https://clarysec.com/products/pl

4. Bezpieczna praca zdalna i mobilna.

Bezpieczna praca zdalna i mobilna wymaga połączenia odpowiednich nawyków, zabezpieczeń technicznych oraz dbałości o zdrowie fizyczne i psychiczne. Pracując poza biurem, jesteś narażony zarówno na cyberzagrożenia, jak i na problemy wynikające z nieergonomicznego stanowiska pracy.

1) Kluczowe zasady podzielone na trzy najważniejsze obszary:
   a. Bezpieczeństwo cyfrowe (Cybersecurity)
      - Zabezpiecz sieć: nigdy nie łącz się z bankiem ani zasobami firmowymi przez otwarte, publiczne sieci Wi-Fi. Korzystaj z szyfrowanego połączenia VPN oraz domowego Wi-Fi zabezpieczonego silnym hasłem i protokołem WPA3.
      - Silne uwierzytelnianie: włącz weryfikację dwuetapową (2FA/MFA) na wszystkich kontach. Do zarządzania unikalnymi hasłami używaj menedżera haseł.
      - Ochrona sprzętu: blokuj ekran komputera za każdym razem, gdy od niego odchodzisz (skrót Win + L lub Cmd + Ctrl + Q). W miejscach publicznych używaj filtra prywatyzującego na ekran.
      - Aktualizacje i oprogramowanie: regularnie aktualizuj system operacyjny, antywirusa i przeglądarkę. Nie instaluj prywatnego oprogramowania na sprzęcie służbowym.
   b. Ergonomia i zdrowie fizyczne
      - Prawidłowa postawa: ustaw monitor tak, aby jego górna krawędź znajdowała się na linii Twoich oczu w odległości około 50–70 cm. Podeprzyj odcinek lędźwiowy kręgosłupa.
      - Zasada 20-20-20: aby chronić wzrok, co 20 minut spójrz na obiekt oddalony o 20 stóp (ok. 6 metrów) przez co najmniej 20 sekund.
      - Ruch: rób krótkie, kilkuminutowe przerwy co godzinę na rozciąganie lub krótki spacer po pokoju.
   c. Higiena pracy i zdrowie psychiczne
      - Rozgraniczenie czasu: ustal sztywne godziny rozpoczęcia i zakończenia pracy, aby uniknąć zatarcia granicy między życiem prywatnym a zawodowym (tzw. blurring).
      - Rytuał „powrotu do domu": po zakończeniu pracy zamknij laptopa i schowaj go z widoku, co da Twojemu mózgowi jasny sygnał do odpoczynku.



Fot. Autor nieznany/Źródło: https://rcponline.pl/blog

III. REAGOWANIE NA PODEJRZANE WIADOMOŚCI, LINKI I ZAŁĄCZNIKI

1. Socjotechnika w administracji: Phishing, Spear phishing, Smishing, Vishing.

Socjotechnika w administracji publicznej opiera się na manipulacji psychologicznej urzędników w celu wyłudzenia danych, haseł lub dostępu do systemów państwowych. Zamiast łamać zabezpieczenia technologiczne, przestępcy wykorzystują autorytet instytucji, pośpiech oraz rutynę pracowników.

1) Tabela charakterystyki kluczowych zagrożeń:

Metoda ataku	Kanał (Medium)	Mechanizm działania w urzędzie	Cel ataku
Phishing	E-mail	Masowe, fałszywe wiadomości (np. udające Ministerstwo Finansów lub dostawcę energii) z linkiem do pobrania dokumentu lub logowania.	• Przejęcie konta e-mail urzędnika • Infekcja stacji roboczej.
Spear phishing	E-mail	Ukierunkowany, spersonalizowany atak na konkretnego urzędnika (np. kadrową, księgową) przy użyciu zebranych wcześniej informacji o urzędzie.	• Kradzież danych wrażliwych obywateli • Autoryzacja fałszywych faktur (ataki BEC).
Smishing	SMS	Wiadomości tekstowe na telefony służbowe, np. o rzekomej blokadzie profilu zaufanego, ePUAP lub niedopłacie za przesyłkę.	Wyłudzenie danych logowania do systemów państwowych.
Vishing	Telefon	Rozmowa głosowa, w której napastnik podszywa się pod audytora, policjanta (pretexting) lub pracownika wsparcia IT.	• Zresetowanie hasła przez telefon • Przekazanie poufnych procedur wewnętrznych.

2) Kluczowe zasady obrony w administracji

a. Zasada ograniczonego zaufania: zawsze weryfikuj tożsamość rozmówcy lub nadawcy wiadomości alternatywnym kanałem komunikacji (np. dzwoniąc na oficjalny numer instytucji).

b. Weryfikacja URL: przed zalogowaniem się do systemów takich jak EZD, ePUAP, eDoręczenia czy poczta służbowa, dokładnie sprawdź adres strony w przeglądarce.

c. Higiena haseł: wdrażanie nieuwierzytelniających się metod wieloskładnikowych (MFA) zabezpiecza konto, nawet gdy urzędnik ujawni hasło.



Fot. Igor/Źródło: https://dataone.pl

2. Jak rozpoznać fałszywe wiadomości e-mail/SMS (analiza nagłówków, linków).

Fałszywe wiadomości e-mail oraz SMS (phishing) najskuteczniej rozpoznasz poprzez szczegółową analizę adresu nadawcy, ukrytych odnośników (linków) oraz nagłówków technicznych. Współczesne ataki są bardzo dopracowane wizualnie, dlatego poniższa instrukcja krok po kroku wyjaśnia, jak wykryć manipulację.

1) Analiza adresu e-mail i nadawcy (pole "Od:"). Oszuści często zmieniają nazwę wyświetlaną (np. na "Twój Bank"), jednak pełny adres e-mail zdradza ich intencje:
   - Sprawdź domenę po znaku @: jeśli wiadomość od banku lub firmy kurierskiej kończy się na darmowej skrzynce (np. @gmail.com, @wp.pl) albo zawiera podejrzany ciąg znaków (np. kontakt@dhl-weryfikacja24.com), jest to oszustwo.
   - Szukaj literówek (typosquatting): przestępcy tworzą domeny łudząco podobne do oryginałów, np. @al1orbank.pl zamiast @aliorbank.pl.
   - Uwaga na homoglify: znaki z innych alfabetów (np. cyrylicy) mogą wyglądać identycznie jak litery łacińskie. Zamiast "o" oszust może użyć znaku, który w przeglądarce otworzy zupełnie inną witrynę.
2) Zaawansowana analiza nagłówków e-mail (weryfikacja SPF, DKIM, DMARC).
   Aby mieć 100% pewności, należy wyświetlić tzw. nagłówek wiadomości (w gmailu: Więcej - > Pokaż oryginał; w Outlooku: Plik - > Właściwości - > nagłówki internetowe). Szukaj w nim trzech kluczowych zabezpieczeń:

Protokół	Co sprawdza?	Wynik prawidłowy	Wynik podejrzany
SPF (Sender Policy Framework)	Czy serwer wysyłający maila ma uprawnienia do używania tej domeny.	SPF: PASS	SPF: FAIL lub SOFTFAIL
DKIM (DomainKeys Identified Mail)	Czy wiadomość posiada cyfrowy podpis potwierdzający, że nie została zmieniona w locie.	DKIM: PASS	DKIM: FAIL
DMARC	Określa politykę postępowania, jeśli SPF lub DKIM zawiodą.	DMARC: PASS	DMARC: FAIL

3) Analiza linków (URL) w wiadomościach e-mail i SMS

Nigdy nie klikaj bezrefleksyjnie w hiperłącza. Zamiast tego przeprowadź ich weryfikację:

- W e-mailu (najedź kursorem): umieść kursor myszy nad linkiem bez klikania. W lewym dolnym rogu ekranu wyświetli się rzeczywisty adres URL. Tekst linku w mailu może brzmieć www.mojbank.pl, podczas gdy pod spodem kryje się złośliwa domena.
- W wiadomości SMS: skracacze linków: uUważaj na adresy typu bit.ly, tinyurl.com, t.co. Prawdziwe instytucje rzadko korzystają ze skracaczy w oficjalnych komunikatach alarmowych.
- Wyizoluj domenę główną: przeanalizuj adres od prawej strony do lewej. Domena główna znajduje się bezpośrednio przed pierwszym pojedynczym znakiem /. Przykładowo: w adresie://bank.com domeną główną jest bank.com, ale w ://zlosliwa-strona.com domeną jest zlosliwa-strona.com.

4) Psychologiczne sygnały ostrzegawcze

Techniczna doskonałość wiadomości może uśpić czujność, dlatego zawsze zwracaj uwagę na treść:

- Presja czasu i strach: komunikaty typu „Twoje konto zostanie zablokowane w ciągu 2 godzin" lub „Dopłać 1,50 zł do paczki, inaczej zostanie zwrócona" to klasyczne techniki manipulacji.
- Błędy i nienaturalny język: choć oszuści coraz częściej używają zaawansowanego AI do tłumaczeń, wciąż zdarzają się dziwne sformułowania, brak polskich znaków lub ogólnikowe zwroty typu „Drogi Kliencie" zamiast Twojego imienia.

5) Sposoby gdy wiadomość budzi wątpliwości

- Stosuj zasadę ograniczonego zaufania: nie korzystaj z linków w wiadomości. Jeśli chcesz sprawdzić status sprawy, wejdź na oficjalną stronę instytucji, wpisując adres ręcznie w przeglądarce.

- Zgłoś incydent: podejrzane wiadomości SMS oraz e-mail możesz przesłać do ekspertów z państwowego instytutu badawczego CERT Polska.
- SMS: przekaż całą treść wiadomości na darmowy numer 799 448 084.
- E-mail: Wyślij jako załącznik na adres incydent@cert.pl.



Fot. Mateusz Nowak/Źródło: https://android.com.pl

3. Procedura zgłaszania incydentów do administratora IT/IOD/CERT.

Procedura zgłaszania incydentów określa ścieżkę postępowania w przypadku wykrycia problemów technicznych, naruszenia ochrony danych osobowych (RODO) lub zagrożeń cyberbezpieczeństwa. Efektywne zgłoszenie wymaga skierowania sprawy do odpowiedniej roli: Administratora IT (problemy techniczne i bezpieczeństwo lokalne), Inspektora Ochrony Danych/IOD (wyciek danych osobowych) lub zespołu CERT/CSIRT (poważne cyberataki i incydenty krajowe).

1) Tabela podziału odpowiedzialności, kanały zgłoszeniowe oraz wymagany czas reakcji dla poszczególnych podmiotów:

Odbiorca zgłoszenia	Typ zgłaszanego incydentu	Kanał zgłoszenia	Czas na zgłoszenie
Administrator IT	• Awarie sprzętu • Złośliwe oprogramowanie • Podejrzane e-maile (Phishing) • Blokada konta	• Wewnętrzny system Helpdesk • E-mail IT • Telefon alarmowy	Natychmiast po wykryciu incydentu
Inspektor Ochrony Danych (IOD)	• Wyciek danych osobowych • Zagubienie pendrive'a/laptopa z danymi • Błędna wysyłka maila do wielu osób	• Dedykowany e-mail (np. iod@firma.pl) • Formularz wewnętrzny RODO	Niezwłocznie (Administrator danych ma max 72h na zgłoszenie do PUODO)
CERT/CSIRT	• Ataki DDoS • Krytyczne podatności • Poważne incydenty sieciowe • Incydenty krajowe	Formularz [CERT Polska] (cert.pl „Zgłoś incydent"	CERT.PL") E-mail: cert@cert.pl



Fot. Autor nieznany/Źródło: https://ratels.pl/blog

4. Zgłoszenie incydentu - krok po kroku

1) Identyfikacja i zabezpieczenie: zauważenie anomalii (np. zaszyfrowane pliki, podejrzana wiadomość). W przypadku infekcji odłącz komputer od sieci Wi-Fi/Ethernet, ale nie wyłączaj go (aby zachować zawartość pamięci RAM dla celów dowodowych).
2) Kwalifikacja incydentu: ustala się, czy incydent dotyczy infrastruktury (IT), danych osobowych (IOD) czy bezpieczeństwa zewnętrznego (CERT). Jeśli incydent łączy te obszary, zgłoszenie należy wysłać równolegle.
3) Przygotowanie informacji: zgłoszenie powinno zawierać:
   - Datę i godzinę wykrycia.
   - Opis sytuacji (co się stało, jakie systemy/pliki zostały dotknięte).
   - Zrzuty ekranu, komunikaty o błędach lub nagłówki podejrzanych wiadomości e-mail.
   - Informację o skali (np. ile osób straciło dostęp, czy wyciekły dane klientów).
   - Współpraca i analiza: pozostawanie w kontakcie z zespołem technicznym lub IOD, wdrożenie działań naprawczych i wyciągnięcie wniosków w celu uniknięcia podobnych zdarzeń w przyszłości.

IV. UWIERZYTELNIANIE DWUSKŁADNIKOWE (2FA) I KOPIE ZAPASOWE

1. Rola i rodzaje 2FA (SMS, aplikacje, klucze sprzętowe).

Rola 2FA (dwuskładnikowego uwierzytelniania) polega na stworzeniu dodatkowej warstwy obrony, która zapobiega nieautoryzowanemu dostępowi do konta, nawet jeśli cyberprzestępca poznał tradycyjne hasło.

Wymaga ona przedstawienia dwóch niezależnych dowodów tożsamości z różnych kategorii: tego, co wiesz (hasło) oraz tego, co posiadasz (np. telefon lub klucz).

Porównanie rodzajów 2FA

Rodzaj 2FA	Jak działa	Poziom bezpieczeństwa	Główne zalety	Główne wady / Zagrożenia
Kody SMS	Serwis wysyła jednorazowy kod numeryczny na numer telefonu użytkownika.	Niski	• Nie wymaga instalacji aplikacji • Działa na każdym telefonie	• Podatność na SIM-swapping (wyrobienie duplikatu karty SIM) • Ryzyko przejęcia kodu przez złośliwe oprogramowanie
Aplikacje uwierzytelniające	Generują lokalnie kody TOTP (zmienne co 30-60 sekund) bez użycia sieci (np. Google Authenticator, [Microsoft Authenticator](https://www.microsoft.com/pl-pl/security/business/security-101/what-is-two-factor-authentication-2fa "Co to jest uwierzytelnianie dwuskładnikowe (2FA)?	Rozwiązania zabezpieczające firmy Microsoft	Średni / Wysoki	• Działają w trybie offline • Kod nie krąży w sieci komórkowej
Klucze sprzętowe (U2F/FIDO2)	Fizyczne urządzenia (np. YubiKey) wpinane do portu USB lub łączące się przez NFC.	Najwyższy	• Odporne na phishing (działają tylko na prawdziwej domenie) • Szybkie logowanie jednym kliknięciem	• Koszt zakupu urządzenia • Ryzyko fizycznego zgubienia klucza



Fot. Kamil Woźniak/Źródło: https://prosteit.pl

2. Zasady tworzenia i testowania kopii zapasowych (zasada 3-2-1).

Zasada 3-2-1 to sprawdzona i powszechnie rekomendowana strategia ochrony danych, która wymaga posiadania 3 kopii danych na 2 różnych nośnikach, z czego 1 kopia musi znajdować się w innej lokalizacji. Strategia ta minimalizuje ryzyko trwałej utraty danych w wyniku awarii sprzętu, ataków ransomware, błędów ludzkich czy katastrof naturalnych. Poniżej znajduje się szczegółowy podział zasad tworzenia oraz testowania kopii zapasowych w oparciu o ten model.

1) Składniki zasady 3-2-1:
   - 3 kopie danych: oprócz oryginalnych danych, na których pracujesz na co dzień, musisz posiadać dwie niezależne kopie zapasowe. Oryginał nie jest backupem.
   - 2 różne nośniki: kopie powinny być zapisane na co najmniej dwóch różnych typach urządzeń lub technologii (np. dysk wewnętrzny komputera, zewnętrzny dysk USB, pamięć flash, serwer sieciowy NAS lub chmura obliczeniowa). Chroni to przed sytuacją, w której jedna wada fabryczna lub usterka niszczy wszystkie nośniki.
   - 1 lokalizacja zewnętrzna (offsite): przynajmniej jedna kopia zapasowa musi znajdować się w zupełnie innym miejscu fizycznym niż dane główne – na przykład w innej siedzibie firmy, u zaufanej rodziny lub w bezpiecznej chmurze internetowej od dostawców takich jak Dropbox. Zabezpiecza to przed pożarem, zalaniem lub kradzieżą w miejscu, gdzie znajduje się główny sprzęt.

2) Zasady tworzenia kopii zapasowych w praktyce:
   - Automatyzacja procesów: ustaw regularne, automatyczne tworzenie kopii (np. codzienne przyrostowe, cotygodniowe pełne), aby nie polegać na pamięci i dyscyplinie ludzkiej.
   - Niezmienność (immutability): warto rozbudować klasyczną zasadę o nowoczesne standardy (np. model 3-2-1-1-0), dbając o to, aby przynajmniej jedna kopia była niemodyfikowalna i odporna na usunięcie przez złośliwe oprogramowanie szyfrujące pliki.
   - Wersjonowanie plików: przechowuj wiele wersji historycznych tego samego pliku, co pozwala przywrócić stan sprzed infekcji wirusem lub przypadkowego nadpisania danych.

3) Zasady testowania kopii zapasowych:

Posiadanie backupu nie oznacza, że dane da się odzyskać. Testowanie to kluczowy element strategii, o którym często się zapomina.

- Regularny harmonogram testów: przeprowadzaj próbne odtwarzanie danych przynajmniej raz na kwartał lub po każdej większej zmianie w systemie IT.
- Testowe przywracanie plików: skopiuj wybrane losowo archiwa z backupu na czyste środowisko, aby sprawdzić, czy proces odzyskiwania przebiega poprawnie i czy pliki nie są uszkodzone.
- Weryfikacja integralności: używaj narzędzi oferujących automatyczne sumy kontrolne (checksums), które potwierdzają, że zapisane dane są spójne i gotowe do odczytu.
- Dokumentacja procedur: Spisz jasny plan odzyskiwania po awarii (ang. Disaster Recovery Plan), aby w sytuacji kryzysowej każdy krok był zrozumiały i szybki do wykonania.



Fot. Autor nieznany/Źródło: https://penta.com.pl

3. Odpowiedzialność pracownika za ciągłość działania jednostki.

Pracownik nie ponosi bezpośredniej odpowiedzialności prawnej za ogólną ciągłość działania jednostki, ponieważ ryzyko prowadzenia działalności w pełni obciąża pracodawcę. Odpowiedzialność za zapewnienie ciągłości funkcjonowania (zarówno w sensie organizacyjnym, jak i finansowym) spoczywa na kierowniku jednostki (np. dyrektorze, zarządzie JST). Pracownik może jednak ponieść indywidualną odpowiedzialność (dyscyplinarną, porządkową lub materialną), jeśli jego konkretne zaniedbanie lub celowe działanie doprowadzi do przerwania tej ciągłości albo wyrządzi szkodę.

Podział odpowiedzialności w jednostce

Kto odpowiada	Zakres odpowiedzialności za ciągłość działania
Kierownik jednostki	Pełna i osobista. Odpowiada za kontrolę zarządczą, finanse, procedury oraz zawieranie umów niezbędnych do ciągłości działania jednostki.
Pracownik	Służbowa i rzetelnościowa. Odpowiada wyłącznie za sumienne wykonywanie powierzonych mu obowiązków w wyznaczonym obszarze.

Pracownik może odpowiedzieć za zakłócenie ciągłości działania jeśli przez zaniechanie lub błąd pracownika dojdzie do awarii, przestoju lub straty, pracodawca może wyciągnąć konsekwencje na podstawie Kodeksu pracy:

1) Odpowiedzialność porządkowa i dyscyplinarna:
   - Za rażące naruszenie obowiązków (np. niepojawienie się kluczowego pracownika w pracy, ignorowanie procedur bezpieczeństwa) grozi upomnienie, nagana, kara pieniężna, a w skrajnych przypadkach zwolnienie dyscyplinarne (art. 52 k.p.).
2) Odpowiedzialność materialna (finansowa):
   - Wina nieumyślna (niedbalstwo, błąd): jeśli pracownik doprowadził do przestoju niechcący, jego odpowiedzialność odszkodowawcza jest ograniczona do kwoty 3-miesięcznego wynagrodzenia.
   - Wina umyślna: jeśli pracownik celowo sabotował działanie firmy lub doprowadził do szkody, odpowiada za nią w pełnej wysokości.
3) Granice odpowiedzialności – Zasada ryzyka pracodawcy:
   Pracownik nie odpowiada za przerwy w działaniu jednostki, jeśli wynikają one z ryzyka prowadzonej działalności:
   - Brak procedur: Jeśli pracodawca nie wdrożył planów awaryjnych (np. wg normy ISO 22301) lub zastępstw.
   - Brak narzędzi lub szkoleń: pracownik nie odpowiada za skutki awarii sprzętu, którego nie potrafił obsłużyć z winy pracodawcy (brak szkoleń).
   - Przyczynienie się pracodawcy: odpowiedzialność pracownika jest wykluczona lub zmniejszona w stopniu, w jakim to pracodawca przyczynił się do problemu.