BEZPIECZNE DANE SP. Z O. O.
ochrona prywatności

PORADNIK UCZESTNIKA · BEZPŁATNY FRAGMENT

Cyberbezpieczeństwo w praktyce

Kurs dla pracowników jednostek samorządu terytorialnego

Fragment: rozdział 1 z 12

Pełny poradnik: 43 strony, procedury postępowania, słowniczek

Podstawa: § 19 rozporządzenia KRI (Dz.U. 2024 poz. 773), RODO



> **To jest bezpłatny fragment poradnika.** Pełny poradnik w formacie PDF jest dołączany bezpłatnie do każdego kursu i udostępniany do pobrania po wykupieniu dostępu.

Kurs: K02 · **Wersja poradnika:** 1.0 · **Liczba lekcji:** 12 · **Czas materiału wideo:** ok. 2 h 10 min

Dla kogo. Poradnik jest przeznaczony dla wszystkich pracowników jednostek publicznych — urzędów gmin i miast, ośrodków pomocy społecznej, szkół i przedszkoli, bibliotek, domów kultury i jednostek podległych. Nie wymaga wiedzy technicznej — każde pojęcie fachowe jest wyjaśnione przy pierwszym użyciu.

Czego dotyczy. Kurs nie uczy technologii — uczy rozpoznawania ataku wymierzonego w człowieka. Dwanaście lekcji prowadzi od skali zjawiska, przez pocztę, załączniki, hasła, przeglądarkę, telefon i nośniki wymienne, aż po reakcję na zdarzenie, które już się wydarzyło.

Podstawa obowiązku szkoleniowego. Szkolenie z zakresu cyberhigieny realizuje obowiązek zapewnienia pracownikom szkolenia w zakresie bezpieczeństwa informacji, wynikający z § 19 ust. 2 pkt 6 rozporządzenia Rady Ministrów z 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (Dz.U. 2024 poz. 773), oraz obowiązek wdrożenia odpowiednich środków ochrony danych osobowych z art. 32 RODO.

Czas pracy z poradnikiem. Około 2 godzin; same listy kontrolne — około 30 minut.

Jak korzystać z tego poradnika

Poradnik nie jest transkrypcją nagrań ani ich streszczeniem. Zawiera to, czego z filmu nie da się przepisać: progi liczbowe, gotowe procedury i listy kontrolne. Najlepiej mieć go otwartego obok odtwarzacza: sekcja „Konkrety do zapamiętania” pozwala nie notować w pośpiechu, a „Lista kontrolna” zamienia lekcję w zestaw czynności na najbliższe dni. Każdy rozdział jest samodzielny: można go przeczytać bez pozostałych i bez znajomości poprzednich lekcji. Pytania w sekcji „Sprawdź się” nie mają jednej poprawnej odpowiedzi — służą do odniesienia treści lekcji do własnego stanowiska pracy. Poradnik pokazuje też kontrolerowi zakres szkolenia bez odtwarzania nagrań.

Rozdział 1. Czy Państwa jednostka jest celem ataku?

> **Lekcja w kursie:** Czy Państwa jednostka jest celem ataku? · **Czas nagrania:** 10 min

W SKRÓCIE

Zdanie „u nas nie ma czego kraść” opiera się na błędnym założeniu, że przestępca wybiera ofiarę tak, jak włamywacz wybiera dom. Zdecydowana większość dzisiejszych ataków to masowa wysyłka setek tysięcy wiadomości i czekanie, aż ktokolwiek odpowie. Liczby z raportów krajowych i unijnych pokazują, że administracja publiczna jest sektorem atakowanym najczęściej, a napastnicy wchodzą do środka przez czyjeś konto, a nie przez lukę w serwerze.

CO TRZEBA WIEDZIEĆ

Skala zjawiska

Zespół CERT Polska, działający w Naukowej i Akademickiej Sieci Komputerowej, publikuje coroczny raport o incydentach w polskiej sieci. W raporcie za 2025 r. odnotowano 260 783 unikalne incydenty — o 152% więcej niż rok wcześniej. Aż 97% z nich to oszustwa komputerowe, czyli sytuacje, w których ktoś kogoś przekonał, żeby kliknął, zalogował się albo zapłacił. Osobno odnotowano 179 ataków polegających na zaszyfrowaniu danych i zażądaniu okupu.

Kto obrywa najczęściej i którędy

Sektorem numer jeden pod względem liczby incydentów w Unii Europejskiej jest administracja publiczna — około 38% przypadków. W jednostkach szczebla lokalnego około 58% zdarzeń to włamania, a dopiero za nimi plasują się ataki polegające na zablokowaniu strony zalewem sztucznego ruchu. Proporcja jest wymowna: zablokowanie strony to atak na sprzęt i łącze, a włamanie to wejście do środka — do systemu, do skrzynki pocztowej, do bazy danych. Około 60% początkowych dróg wejścia do zaatakowanych organizacji to fałszywa wiadomość podszywająca się pod znaną instytucję (phishing, od angielskiego słowa oznaczającego łowienie ryb). Kolejne urządzenie zabezpieczające kupione do serwerowni tej drogi nie zamyka — zamyka ją uważność osoby czytającej wiadomość.

Dlaczego akurat Państwa jednostka

Miejsce pracy	Co przechodzi przez biurko
Oświata	numery ewidencyjne dzieci, adresy, dane rodziców, orzeczenia poradni
Pomoc społeczna	sytuacja majątkowa rodzin, stan zdrowia, niepełnosprawność
Urząd gminy	ewidencja ludności, podatki, nieruchomości, wnioski mieszkańców
Biblioteka, dom kultury	bazy czytelników i uczestników zajęć, w tym dzieci

Numer ewidencyjny dziecka jest dla przestępcy szczególnie cenny, bo przez kilkanaście lat nikt nie sprawdzi, czy ktoś nie zaciągnął na nie zobowiązania. Informacja o kłopotach zdrowotnych albo finansowych to materiał do szantażu, a komplet danych o mieszkańcach — gotowa lista do kolejnego oszustwa, w którym dzwoniący zna imię, adres i numer sprawy.

Skutek i rozpoznanie celu

Atak nie jest awarią komputera, tylko przerwaniem usługi publicznej: nie uruchamia się dziennik elektroniczny, nie da się przygotować list wypłat świadczeń, mieszkaniec nie dostanie dziś zaświadczenia potrzebnego mu w banku. Napastnik nie liczy na to, że jednostka ma dużo pieniędzy — liczy na to, że nie może sobie pozwolić na przestój. Wie też, do kogo napisać, bo jednostka publiczna z mocy prawa ujawnia strukturę organizacyjną, nazwiska osób na stanowiskach kierowniczych i dane kontaktowe. Tak powstaje wiadomość bez literówek, podpisana właściwym nazwiskiem, dotycząca sprawy, która naprawdę się toczy. Im wiadomość jest bardziej dopasowana, tym mniej wygląda na atak. Dopasowanie nie jest dowodem prawdziwości — jest dowodem przygotowania.

KONKRETY DO ZAPAMIĘTANIA

Rzecz	Wartość
Incydenty odnotowane przez CERT Polska w 2025 r.	260 783 unikalne incydenty, wzrost o 152% rok do roku
Udział oszustw komputerowych	97% wszystkich odnotowanych incydentów
Ataki szyfrujące dane dla okupu w 2025 r.	179
Administracja publiczna w Unii Europejskiej	sektor nr 1, ok. 38% incydentów
Jednostki szczebla lokalnego	ok. 58% zdarzeń to włamania, nie ataki na łącze

LISTA KONTROLNA — DO ZASTOSOWANIA OD JUTRA

- [ ] Wypisać, jakie kategorie danych osobowych przechodzą przez moje stanowisko w ciągu zwykłego tygodnia.
- [ ] Sprawdzić, co o mnie i o mojej komórce organizacyjnej widnieje w Biuletynie Informacji Publicznej i na stronie jednostki.

- [ ] Ustalić, komu w mojej jednostce zgłasza się podejrzaną wiadomość, telefon albo prośbę o dane, i zapisać ten kontakt przy stanowisku.
- [ ] Przy najbliższej pilnej wiadomości zatrzymać się na kilka sekund i spojrzeć na adres nadawcy przed otwarciem załącznika.
- [ ] Sprawdzić, czy w moim prywatnym profilu w mediach społecznościowych widać moje miejsce pracy i terminy nieobecności.

NAJCZĘSTSZY BŁĄD

Najczęstsze błędne przekonanie brzmi: „jesteśmy zbyt mali i zbyt nieciekawi, żeby ktoś się nami zainteresował". W rzeczywistości większość ataków nie wybiera ofiary — to masowa wysyłka, w której adres jednostki znalazł się dlatego, że jest jawny. Drugie oblicze tego błędu to przekonanie, że w małej jednostce „nie ma czego kraść" — tymczasem dane uczniów, podopiecznych i mieszkańców mają wartość rynkową niezależnie od wielkości urzędu. Wielkość jednostki nie jest tarczą. Tarczą jest kilka sekund zatrzymania się przed kliknięciem.

SPRAWDŹ SIĘ

1. Które kategorie danych przetwarzanych na Państwa stanowisku miałyby dla przestępcy największą wartość i dlaczego?
2. Co konkretnie przestałoby działać w Państwa jednostce, gdyby przez trzy dni nie było dostępu do systemów — i kto by to odczuł jako pierwszy?
3. Jakie informacje o Państwa jednostce można zebrać w kwadrans, korzystając wyłącznie ze źródeł jawnych?

Dalsza część poradnika

To jest bezpłatny fragment. Pełny poradnik obejmuje jeszcze:

- Rozdział 2. Socjotechnika, czyli jak oszuści oszukują ludzki mózg
- Rozdział 3. Anatomia fałszywej wiadomości
- Rozdział 4. Załączniki: koń trojański w fakturze
- Rozdział 5. Ransomware: cyfrowy porywacz danych
- Rozdział 6. Hasła: pierwsza linia obrony
- Rozdział 7. Bezpieczne korzystanie z przeglądarki internetowej
- Rozdział 8. Urządzenia mobilne: smartfon to też komputer
- Rozdział 9. Nośniki wymienne: pendrive'y pułapki
- Rozdział 10. Media społecznościowe: prywatność pracownika a bezpieczeństwo jednostki
- Rozdział 11. Dezinformacja i fałszywe informacje
- Rozdział 12. Reakcja na atak: pierwsze minuty
- Słowniczek
- Podstawy prawne przywołane w kursie
- Notatki własne

Pełną wersję — wraz z listami kontrolnymi, słowniczkiem i wykazem podstaw prawnych — otrzymują Państwo bezpłatnie po wykupieniu dostępu do kursu.