

Arkusz ćwiczeń

Analiza luk (Gap Analysis) · Rejestr ryzyk · Procedura reagowania na incydenty (IR)

Kontekst ćwiczeń — fikcyjna organizacja NordPak Logistyka

NordPak Logistyka Sp. z o.o. — fikcyjna firma logistyczno-spedycyjna, ok. 180 pracowników, siedziba w Łodzi, trzy magazyny regionalne. Infrastruktura IT: lokalny serwer plików i system ERP w siedzibie, poczta i dokumenty w chmurze Microsoft 365, zdalny dostęp VPN dla ok. 20-osobowego zespołu sprzedaży, integracje API z zewnętrznymi kurierami i sklepem internetowym klienta. Hasła do kont pracowniczych są ustalane indywidualnie i nie podlegają regularnej wymianie; uwierzytelnianie wieloskładnikowe (MFA) jest włączone wyłącznie dla 4 kont administratorów IT. Kopie zapasowe serwera plików wykonywane są raz w tygodniu na dysk sieciowy w tej samej serwerowni. Firma nie prowadziła dotąd cyklicznych szkoleń z bezpieczeństwa dla pracowników spoza działu IT. W nocy z 3 na 4 lutego 2026 r. doszło do ataku ransomware, opisanego szczegółowo w Ćwiczeniu 3.

Uwaga: Firma NordPak Logistyka oraz opisany incydent są fikcyjne i służą wyłącznie celom szkoleniowym. Wszelkie podobieństwo do rzeczywistych organizacji jest przypadkowe.

Ćwiczenie 1 — Analiza luk (Gap Analysis)

Ocena stanu zabezpieczeń NordPak wobec dobrych praktyk cyberbezpieczeństwa · Formularz do wypełnienia

Imię i nazwisko

Organizacja

Data szkolenia

Ćwiczenie nr

Cel ćwiczenia: Ocenic stan zabezpieczeń fikcyjnej firmy NordPak Logistyka wobec podstawowych dobrych praktyk cyberbezpieczeństwa zgodnych z zakresem CompTIA Security+, a następnie przećwiczyć tę samą metodykę na własnej organizacji.

Część A. Checklista dla NordPak — stan na 1.02.2026

Dla każdego wymagania wpisz status (spełnione / częściowo / niespełnione / nie dotyczy), dowód, którego zażądałby audytor, oraz priorytet zamknięcia luki (KRYTYCZNY / WYSOKI / ŚREDNI). Dwa pierwsze wiersze są wypełnione jako wzór — wynikają wprost z opisu w sekcji „Kontekst”.

ID	Wymaganie kontrolne	Status	Dowód, którego zażądałby audytor	Priorytet
A.1	Uwierzytelnianie wieloskładnikowe (MFA) obowiązuje na wszystkich kontach pracowniczych	częściowo	Konfiguracja Microsoft 365 — MFA aktywne tylko dla 4 kont administracyjnych IT	WYSOKI
A.2	Kopie zapasowe krytycznych danych przechowywane są w izolowanej lokalizacji (offline / offsite)	niespełnione	Harmonogram backupu — jedna kopia tygodniowa, w tej samej serwerowni	KRYTYCZNY
A.3	Polityka haseł wymusza minimalną długość, złożoność i regularną wymianę			
A.4	Na wszystkich stacjach roboczych wdrożono ochronę końcówek (EDR / antywirus nowej generacji)			
A.5	Ruch sieciowy między siecią biurową a systemami magazynowymi (WMS) jest segmentowany (VLAN / firewall)			
A.6	Pracownicy przechodzą cykliczne szkolenia z rozpoznawania phishingu i socjotechniki			
A.7	Istnieje udokumentowany i przynajmniej raz przetestowany plan reagowania na incydenty (IR)			
A.8	Dostęp uprzywilejowany (konta administracyjne) jest rozliczany i ograniczony zasadą najmniejszych uprawnień			
A.9	Krytyczne podatności (CVE) są łatanie zgodnie z ustalonym SLA priorytetyzacji (np. wg CVSS)			
A.10	Zdarzenia bezpieczeństwa z kluczowych systemów są centralnie logowane i monitorowane			
A.11	Dane wrażliwe są szyfrowane w spoczynku i w transporcie			
A.12	Dostawcy zewnętrzni (np. integracje kurierskie) podlegają ocenie bezpieczeństwa przed podłączeniem do systemów			

Część B. Pięć luk do zamknięcia w pierwszej kolejności

Wybierz pięć pozycji z Części A. Uzasadnienie ma odnosić się do skutku pozostawienia luki, nie do łatwości jej usunięcia. Oszacuj orientacyjny nakład w roboczościach oraz to, czy zamknięcie luki wymaga zewnętrznego wsparcia (koszt zewn.).

Lp.	ID i nazwa luki	Dlaczego właśnie ta — skutek pozostawienia	Nakład (rd)	Koszt zewn.
1				
2				
3				
4				
5				

Pytanie kontrolne: Która z luk, gdyby została zamknięta przed 3 lutego 2026 r., z największym prawdopodobieństwem zatrzymałaby atak opisany w Ćwiczeniu 3? Odpowiedz i uzasadnij, odwołując się do osi czasu z Części A Ćwiczenia 3.

Część C. Twoja organizacja

Powtórz ocenę dla własnej organizacji. Wypełniaj tylko te wiersze, przy których masz wiedzę — pozostałe oznacz jako „do ustalenia” i wpisz, kogo musisz o to zapytać.

ID	Wymaganie kontrolne	Status	Dowód / gdzie leży	Kto to wie
B.1	A.1 MFA na wszystkich kontach			
B.2	A.2 kopie zapasowe offline / 3-2-1			
B.3	A.6 szkolenia z phishingu			
B.4	A.7 plan IR			
B.5	A.10 centralne logowanie i monitoring			

Do wykonania po szkoleniu: Uzupełnij kolumnę „Kto to wie” i umów rozmowę z tą osobą w ciągu dwóch tygodni od szkolenia.

Ćwiczenie 2 — Rejestr ryzyk

Analiza ryzyka dla wybranych aktywów NordPak metodą $P \times S$ · Formularz do wypełnienia

Imię i nazwisko

Organizacja

Data szkolenia

Ćwiczenie nr

Cel ćwiczenia: Zbudować rejestr ryzyk dla wybranych aktywów NordPak Logistyka, stosując klasyczną metodę oceny ryzyka prawdopodobieństwo $\times$ skutek ($P \times S$), a następnie przećwiczyć tę samą metodykę na własnej organizacji.

Krok 1. Kryteria akceptacji ryzyka

Zanim ocenisz ryzyka, ustal progi kwalifikacji. W realnym procesie zatwierdza je zarząd — tu przyjmij poniższą propozycję. Skala: P (prawdopodobieństwo) 1–5, S (skutek) 1–5, $R = P \times S$.

Poziom $R = P \times S$	Kwalifikacja	Wymagane działanie
1 – 6	Niskie	Akceptować i monitorować przy okazji przeglądów okresowych
8 – 12	Średnie	Zaplanować działanie ograniczające w ciągu najbliższego kwartału
15 – 25	Wysokie	Działanie natychmiastowe — zgłoszenie do kierownictwa, plan naprawczy w ciągu 30 dni

Krok 2. Rejestr ryzyk NordPak

Dwa pierwsze wiersze są wypełnione jako wzór, na podstawie opisu w sekcji „Kontekst” i incydentu z Ćwiczenia 3. Uzupełnij pozostałe — dla minimum trzech kolejnych aktywów wskaż zagrożenie, podatność i pełną ocenę.

Aktywo	Zagrożenie	Podatność	P	S	R	Postępowanie	Właściciel
Serwer plików działu księgowości i kadr	Infekcja ransomware przez załącznik phishingowy	Brak MFA na kontach e-mail; jedna kopia zapasowa w tej samej sieci; brak segmentacji	4	5	20	Modyfikacja: MFA na wszystkich kontach, kopia offline wg zasady 3-2-1, segmentacja sieci	Kier. IT
Konta e-mail pracowników (Microsoft 365)	Przejęcie konta przez phishing / wyłudzenie hasła	MFA tylko dla adminów; brak blokady makr z Internetu; słabe filtrowanie załączników	4	4	16	Modyfikacja: MFA dla wszystkich, blokada makr, filtr antyphishingowy	Kier. IT
Kontrolery i terminale WMS w magazynie							
Portal / API integracji z kurierami zewnętrznymi							
Zdalny dostęp VPN zespołu sprzedaży							
Kopie zapasowe (backup)							

Krok 3. Pytania kontrolne

a) Które z zapisanych ryzyk nie jest ryzykiem czysto technicznym? Wskaż je i uzasadnij.

b) Które ryzyka wymagają decyzji zarządu, a które może zamknąć samodzielnie zespół IT?

c) Które ryzyko zmaterializowało się jako pierwsze w osi czasu z Części A Ćwiczenia 3?

Krok 4. Twoja organizacja

Wybierz jeden proces krytyczny dla Twojej organizacji i wskaż pięć aktywów, które go wspierają.

Proces krytyczny:

Aktywo	Zagrożenie	Podatność	P	S	R	Postępowanie	Właściciel

Zasada: Zaczynij od opisu, nie od liczby. Liczby P i S mają sens tylko wtedy, gdy wynikają z konkretnego, opisanego zagrożenia i podatności — nie odwrotnie.

Ćwiczenie 3 — Procedura IR — pierwsze godziny

Symulacja reagowania na incydent ransomware w NordPak · Formularz do wypełnienia

Imię i nazwisko

Organizacja

Data szkolenia

Ćwiczenie nr

Cel ćwiczenia: Odtworzyć chronologię pierwszych godzin incyduentu ransomware oraz zaprojektować właściwą kolejność działań, zgodną z cyklem reagowania na incydenty NIST SP 800-61 (przygotowanie → detekcja i analiza → powstrzymanie, eliminacja, odtworzenie → wnioski).

Jak było naprawdę: 3.02.2026, 14:20 — pracownik księgowości otwiera załącznik „Faktura_0221.pdf” z makrem, w mailu podszywającym się pod stałego dostawcę. 14:22 — makro pobiera i uruchamia złośliwy ładunek w tle, bez widocznych objawów. 22:40 — ransomware rozpoczyna szyfrowanie udostępnionego dysku sieciowego księgowości i kadr. 4.02.2026, 07:15 — pierwszy pracownik zgłasza do IT brak dostępu do plików na dysku wspólnym. 07:50 — IT potwierdza obecność plików z rozszerzeniem „.locked” oraz notatki z żądaniem okupu. 08:10 — IT odcina zainfekowany serwer od sieci.

Część A. Moment startu zegara

W wielu procedurach IR liczy się czas od uzyskania wiedzy o incydencie, nie od jego faktycznego początku. Wskaż moment z osi czasu, od którego Twoim zdaniem powinien zacząć się liczyć czas reakcji zespołu IR, i uzasadnij wybór — to jest najtrudniejsza decyzja w całym ćwiczeniu.

Kandydat na moment startu	Data i godzina	Za czym przemawia / co przeczy
Otwarcie złośliwego załącznika przez pracownika	3.02, 14:20	
Uruchomienie ładunku w tle	3.02, 14:22	
Rozpoczęcie szyfrowania dysku sieciowego	3.02, 22:40	
Zgłoszenie problemu przez pracownika do IT	4.02, 07:15	
Potwierdzenie przez IT charakteru zdarzenia (ransomware)	4.02, 07:50	

Wybrany moment startu zegara i uzasadnienie:

Część B. Klasyfikacja — jak poważny jest to incydent

Oceń incydent według trzech ogólnych kryteriów istotności stosowanych w praktyce IR. Dla każdego wskaż, czy jest spełnione, i podaj fakt ze scenariusza, który to potwierdza.

Kryterium	Spełnione?	Fakt ze scenariusza, który to potwierdza
Zakłócenie działania krytycznego procesu biznesowego (tu: obsługa księgowa i kadrowa)		
Ryzyko utraty lub ujawnienia danych osobowych pracowników / kontrahentów		
Skala zdarzenia wykracza poza pojedynczą stację roboczą		

Rozstrzygnięcie — wpisz jedno zdanie: „Ten incydent jest incydem [niskiego / średniego / wysokiego] priorytetu, ponieważ...”.

Część C. Harmonogram pierwszych godzin — jak powinno być

Dla każdej fazy cyklu NIST SP 800-61 rozpisz konkretne działanie, osobę odpowiedzialną oraz produkt, który po tym działaniu zostaje udokumentowany (w systemie lub na papierze). Kolejność faz ma znaczenie — nie zmieniaj jej.

Faza (NIST SP 800-61)	Działanie	Kto odpowiada	Produkt / dowód
Detekcja i analiza			
Powstrzymanie (containment)			
Zbieranie dowodów			
Eliminacja			
Odtworzenie			
Wnioski (lessons learned)			

Uwaga: Zbieranie dowodów z pamięci (RAM) musi nastąpić PRZED odłączeniem zasilania i PRZED pełną eliminacją malware — inaczej dowody ulotne znikają bezpowrotnie.

Część D. Wewnętrzny formularz zgłoszenia incydentu

Wypełnij na podstawie danych ze scenariusza i własnych ustaleń z Części C.

Pole formularza	Treść
Data i godzina wykrycia	
Osoba zgłaszająca (imię, nazwisko, dział)	
Systemy / dane, których dotyczy incydent	
Wstępna klasyfikacja (niski / średni / wysoki / krytyczny)	
Działania podjęte do tej pory	
Osoba odpowiedzialna za koordynację reakcji	
Status (otwarty / w trakcie / zamknięty)	

Część E. Pytanie kontrolne

Które z działań w Części C powinno nastąpić PRZED zebraniem dowodów z pamięci, a które PO? Uzasadnij, odwołując się do zasady „order of volatility” omówionej na szkoleniu (Dzień 2, Blok 10).

Część F. Twoja organizacja

Odpowiedz na trzy pytania o własnej organizacji. Jeżeli nie znasz odpowiedzi — to również jest wynik tego ćwiczenia.

1. Kto u Was podejmuje decyzję o eskalacji poważnego incydentu poza godzinami pracy (np. w nocy, w weekend), i jak się z tą osobą skontaktować?

2. Gdzie leży (fizycznie lub cyfrowo) wypełniony wcześniej formularz z danymi stałymi potrzebnymi przy zgłoszeniu incydentu, żeby nie zbierać ich pod presją czasu?

3. Ile czasu zajęłoby Wam dziś zabezpieczenie logów z kluczowych systemów i kto ma do nich dostęp?
