Imię i nazwisko: _____ **Data:** _____ **Wynik:** _____

Ataki ransomware i biznes Odzyskiwanie

Wykonanie ładunku, kryptograficzne szyfrowanie plików, kopie zapasowe offline, procedury powstrzymania zagrożenia i odtwarzanie po awarii.

PRZEGLĄD NAUKI O ATAKACH RANSOMWARE

CHRONIONY
SZYFROWANIE DANYCH
Standard AES 256-bitowy

ZGODNY
STANDARDY GLOBALNE
Ramy prawne RODO (GDPR) i CCPA

ZERO TRUST
POLITYKA DOSTĘPU
Uwierzytelnianie wieloskładnikowe

Witaj! Ten pakiet ćwiczeń przeprowadzi cię przez ataki ransomware i odtwarzanie działalności firmy. Poznasz wykonywanie ładunku, szyfrowanie plików, kopie zapasowe offline, powstrzymywanie zagrożeń, płatności w kryptowalutach i plany odtwarzania po awarii.

PUNKTY KONTROLNE KARTY PRACY

- [ ] **Część 1–4: Opanuj cyberbezpieczeństwo i zapobieganie zagrożeniom.**
- [ ] **Część 5–7: Rozwiąż krzyżówkę i wykreślankę.**
- [ ] **Część 8–9: Rozwiąż studia przypadków i wyzwanie z szyfrem.**
- [ ] **Część 10: Przejrzyj strony z podstawowymi i zaawansowanymi najczęściej zadawanymi pytaniami.**
- [ ] **Część 11: Poznaj 10 ciekawych faktów z praktyki.**
- [ ] **Bonus: wyzwanie Myśl szybko.**

Otwórz przewodnik VPN.com po cyberbezpieczeństwie

URL: https://www.vpn.com/pl/cyberbezpieczenstwo/atak-ransomware/

Twoja ścieżka nauki: odzyskiwanie po ataku ransomware

- Rozróżnij ładunki trojanów, ransomware i spyware.
- Przeanalizuj złośliwe pliki w bezpiecznych środowiskach sandbox.
- Opracuj procedury szybkiej izolacji sieci i powstrzymywania incydentu.

INSTRUKCJE PRZEWODNIKA O ATAKACH RANSOMWARE

Odpowiedz na pytania testu wielokrotnego wyboru oraz pytania prawda/fałsz, uzupełnij zdania z lukami za pomocą banku wyrazów, dopasuj definicje i rozwiąż krzyżówkę oraz wykreślankę. Zastosuj swoją wiedzę z zakresu odzyskiwania danych po ataku ransomware. Zakończ zadaniem dodatkowym Myśl szybko.

ATAKI RANSOMWARE I ODTWARZANIE PO AWARII (WPROWADZENIE)

Ładunki ransomware kryptograficznie blokują nośniki systemowe, żądając zapłaty w kryptowalucie za klucze deszyfrujące. Ograniczanie tego zagrożenia obejmuje reguły izolacji sieci, analizę złośliwego oprogramowania w piaskownicy oraz solidne, odizolowane od sieci (air-gapped) zimne kopie zapasowe.

PRZECZYTAJ UWAŻNIE KAŻDY PUNKT KONTROLNY I WYBIERZ LUB NAPISZ POPRAWNĄ ODPOWIEDŹ.

Punkt kontrolny 1: Wyzwanie – test wielokrotnego wyboru

1. Jaki jest główny mechanizm ataku ransomware?

- A. Kryptograficzne szyfrowanie plików użytkownika w celu odmowy dostępu do systemu
- B. Wstrzykiwanie złośliwych poleceń SQL do pól formularzy
- C. Podsłuchiwanie pakietów sieciowych w publicznej sieci Wi-Fi
- D. Fałszowanie nagłówków e-mail w celu ominięcia walidacji SPF

2. Czym jest kopia zapasowa offline (zimna)?

- A. Kopia danych odłączona od sieci, aby chronić ją przed rozprzestrzenianiem się złośliwego oprogramowania
- B. Kopia zapasowa przechowywana na dysku twardym głównego serwera WWW
- C. Tymczasowa pamięć podręczna dzienników rejestru systemowego
- D. Narzędzie administracyjne do resetowania haseł użytkowników

3. W jaki sposób zespoły bezpieczeństwa powinny izolować zainfekowane systemy podczas ataku ransomware?

- A. Natychmiast odłącz kable sieciowe i wyłącz interfejsy bezprzewodowe
- B. Aktualizacja bazy sygnatur antywirusowych
- C. Wyłącz główny serwer DNS
- D. Zmień nazwy rozszerzeń zainfekowanych plików

4. Dlaczego służby bezpieczeństwa odradzają płacenie okupu żądanego przez ransomware?

- A. Wpłacanie środków zachęca atakujących i nie gwarantuje dostarczenia klucza deszyfrującego
- B. Automatycznie unieważnia wszystkie firmowe polisy ubezpieczeniowe
- C. Automatycznie powiadamia e-mailem każdego klienta
- D. Uszkadza pozostałe pliki kopii zapasowych systemu

5. Czym jest plan awaryjnego odtwarzania systemów (DRP)?

- A. Ustrukturyzowany proces przywracania operacji i danych po naruszeniu bezpieczeństwa systemu
- B. Konfiguracja zapory sieciowej mapująca przychodzące porty sieciowe
- C. Schemat bazy danych z listą uprawnień administracyjnych użytkowników
- D. Protokół uwierzytelniania poczty e-mail odrzucający sfałszowane domeny

Punkt kontrolny 2: Wyzwanie – prawda czy fałsz

6 Pytanie 6

6. Ładunki ransomware mogą łatwo rozprzestrzeniać się na kopie zapasowe online podłączone do sieci.

- ◯ Prawda
- ◯ Fałsz

7 Pytanie 7

7. Zapłacenie okupu w kryptowalucie gwarantuje, że pliki zostaną pomyślnie odszyfrowane.

- ◯ Prawda
- ◯ Fałsz

8 Pytanie 8

8. Odłączenie zainfekowanych systemów od sieci pomaga powstrzymać rozprzestrzenianie się ransomware na sąsiednie systemy.

- ◯ Prawda
- ◯ Fałsz

9 Pytanie 9

9. Kryptografia symetryczna nigdy nie jest używana przez ransomware do szyfrowania nośników systemowych.

- ◯ Prawda
- ◯ Fałsz

10 Pytanie 10

10. Regularne testowanie procedur przywracania danych jest kluczową częścią odtwarzania po awarii.

- ◯ Prawda
- ◯ Fałsz

Punkt kontrolny 3: Wstawianie kluczowych terminów

Przeczytaj każde poniższe zdanie i uzupełnij lukę poprawnym terminem z banku słów.

1. Odmowę dostępu do plików lokalnych zapewnia kryptograficzne _____ .
2. Aktywnym złośliwym kodem uruchamianym w systemie jest _____ .
3. Odłączone kopie przechowywane poza siedzibą to bezpieczna _____ .
4. Aby powstrzymać rozprzestrzenianie złośliwego oprogramowania, potrzebna jest sieciowa _____ punktów końcowych.
5. Płatność w kryptowalucie żądana przez cyberprzestępców to _____ .
6. Przywracanie operacyjnych plików danych to _____ po awarii.

BANK SŁÓW

AWARIA IZOLACJA KOPIA OFFLINE ŁADUNEK ODZYSKIWANIE OKUP SZYFROWANIE TROJAN

Wpisz tutaj swoje odpowiedzi:

1.
2.
3.
4.
5.
6.

Punkt kontrolny 4: Dopasowywanie pojęć z zakresu bezpieczeństwa

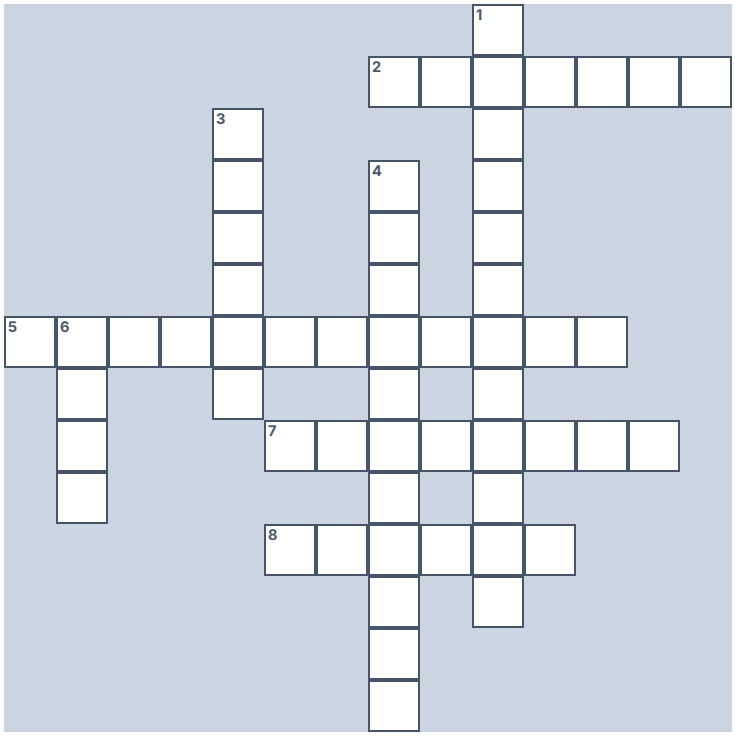
DOPASOWYWANIE DEFINICJI

Dopasuj każde pojęcie po lewej stronie do jego poprawnej definicji po prawej, wpisując odpowiednią literę (A-H) w edytowalne pole.

☐	1. SZYFROWANIE	A	Odłączenie zainfekowanych systemów sieciowych.
☐	2. ŁADUNEK	B	Złośliwy plik udający czysty.
☐	3. ZIMNA KOPIA ZAPASOWA	C	Kryptograficzne blokowanie plików.
☐	4. IZOLACJA	D	Poważne zakłócenie działania systemu.
☐	5. OKUP	E	Uruchamianie złośliwego oprogramowania.
☐	6. ODZYSKIWANIE	F	Odłączona kopia offline.
☐	7. KATASTROFA	G	Przywracanie bazy danych z kopii zapasowej.
☐	8. TROJAN	H	Kryptograficzne żądanie wypłaty klucza.

Punkt kontrolny 5: Krzyżówka

Rozwiąż krzyżówkę, wpisując litery w aktywne białe pola. Numery odpowiadają wskazówkom poniżej.



POZIOMO

2. Uruchamianie złośliwego oprogramowania. (7)

5. Odłączona kopia offline. (12)

7. Odłączanie zainfekowanych systemów sieciowych. (8)

8. Poważne zdarzenie zakłócające działanie systemu. (6)

PIONOWO

1. Przywracanie bazy danych z kopii zapasowej. (12)

3. Złośliwy plik udający czysty. (6)

4. Kryptograficzne blokowanie plików. (11)

6. Żądanie wypłaty w zamian za klucz kryptograficzny. (4)

Punkt kontrolny 5, wariant alternatywny: Dostępne wskazówki do krzyżówki

Użytkownicy czytników ekranu i klawiatury mogą wpisywać odpowiedzi do krzyżówki bezpośrednio w polach tekstowych poniżej.

POZIOMO

2 poziomo: Uruchamianie złośliwego oprogramowania. (7 liter):

5 poziomo: Odłączona kopia offline. (12 liter):

7 poziomo: Odłączanie zainfekowanych systemów sieciowych. (8 liter):

8 poziomo: Poważne zdarzenie zakłócające działanie systemu. (6 liter):

PIONOWO

1 pionowo: Przywracanie bazy danych z kopii zapasowej. (12 liter):

3 pionowo: Złośliwy plik udający czysty. (6 liter):

4 pionowo: Kryptograficzne blokowanie plików. (11 liter):

6 pionowo: Żądanie wypłaty w zamian za klucz kryptograficzny. (4 liter):

Punkt kontrolny 6: Ukryte słowa w wykreślance

Znajdź w poniższej siatce 8 kluczowych terminów słownictwa. Wyrazy mogą biec poziomo, pionowo lub po przekątnej.

E B A A B C Ó I Z Ł K Z L Y T
I L I D Q N K Z D I Ł Ń N L Q
N Ó R G N N Q O R S A T T F B
A N A Ś P O H L S B D W Ć Ś Ź
W A W V C Ż W A Ę L U G Ż S Ć
I J A N D Q Y C Ó C N U B Z A
K O Ż Ń Ć O L J A D E O D Y Ę
S R G I Ć K R A Q M K E I F S
Y T Ż Ś Ę U Q V E A A Q Ó R N
Z P T Y Q P K R T S Ć N Ź O B
D K O P I A O F F L I N E W Ę
O S Y X J A R Ż Z Z Ł F I A N
R K M M T O G P Q G Ż Ą O N V
F V B Ź S Ź B G M Ż G K O I P
Ń X C M Ż Ź F Z O X U L V E Ó

LISTA SŁÓW

SZYFROWANIE ŁADUNEK KOPIAOFFLINE IZOLACJA OKUP ODZYSKIWANIE AWARIA TROJAN

Punkt kontrolny 6, wariant alternatywny: Dostępne dopasowywanie słownictwa

Dopasuj każde z 8 pojęć z wykreślanki do jego poprawnej definicji, wpisując literę (A-H) w puste pole.

TERMINY ZE SŁOWNICZKA

- **A. SZYFROWANIE**
- **B. ŁADUNEK**
- **C. KOPIAOFFLINE**
- **D. IZOLACJA**
- **E. OKUP**
- **F. ODZYSKIWANIE**
- **G. AWARIA**
- **H. TROJAN**

DEFINICJE I POLA DOPASOWANIA

1. Odłączona kopia offline.
2. Złośliwy plik udający czysty.
3. Kryptograficzne blokowanie plików.
4. Żądanie wypłaty w zamian za klucz kryptograficzny.
5. Odłączanie zainfekowanych systemów sieciowych.
6. Poważne zdarzenie zakłócające działanie systemu.
7. Uruchamianie złośliwego oprogramowania.
8. Przywracanie bazy danych z kopii zapasowej.

Punkt kontrolny 7: Wyzwanie – pomieszane słowa

Rozszyfruj poniższe litery, aby odkryć kluczowe pojęcia i terminy związane z cyberbezpieczeństwem. Wpisz odpowiedzi w przygotowanych polach.

1. RWIZOASNYEF
2. EOAOKINPFLFI
3. POUK
4. ARAIAW
5. NKUDŁEA
6. JALCIAZO
7. WASODIENIZKY
8. ONTAJR

Zadanie dodatkowe: Myśl szybko

3 ODPOWIEDZI W KAŻDEJ KATEGORII. WYGRYWA OSOBA, KTÓRA PIERWSZA WYPEŁNI LISTĘ.

1	Informacje, których nigdy nie powinieneś udostępniać			
2	Urządzenia, które można zhakować			
3	Powody, dla których nie warto płacić okupu			
4	Bezpieczne nawyki, które możesz zacząć już dziś			
5	Narzędzia bezpieczeństwa, które znasz			
6	Sposoby na ochronę twoich kont			
7	Oznaki, że komputer jest zainfekowany			
8	Miejsca do przechowywania kopii zapasowej			
9	Pliki, których nigdy nie chcesz stracić			
10	Sposoby, w jakie rozprzestrzenia się ransomware			
11	Rzeczy do zrobienia w pierwszej godzinie ataku			
12	Osoby, z którymi należy się skontaktować podczas ataku			
13	Rzeczy, które ransomware może zablokować			
14	Słowa związane z cyberbezpieczeństwem			
15	Organizacje, które często padają ofiarą ataków			

Punkt kontrolny 8: Studia przypadków z cyberbezpieczeństwa

Zastosuj poznane pojęcia, aby rozwiązać poniższe scenariusze z życia wzięte.

STUDIUM PRZYPADKU 1: OGRANICZANIE ŁADUNKU RANSOMWARE W FIRMIE

👷

Scenariusz: Firmowa sieć lokalna została zaatakowana przez aktywny ransomware. Na kluczowych serwerach plików zaczęły pojawiać się pliki z rozszerzeniem .locked.

Pytanie do dyskusji: Opisz szczegółowo kroki powstrzymania i przedstaw protokół odzyskiwania danych.

STUDIUM PRZYPADKU 2: OCENA ARCHITEKTUR KOPII ZAPASOWYCH OFFLINE

👷

Scenariusz: Przedsiębiorstwo chce zaprojektować strategię tworzenia kopii zapasowych danych, która zmniejsza ryzyko naruszenia kopii zapasowych, nawet jeśli główna sieć lokalna zostanie całkowicie przejęta przez ransomware.

Pytanie do dyskusji: Zaprojektuj bezpieczny system skarbca na kopie zapasowe offline.

Punkt kontrolny 9: Odszyfruj szyfr

Specjalista ds. cyberbezpieczeństwa chroni zasoby sieciowe przed cyberprzestępcami. Użyj poniższego klucza liter i liczb, aby odszyfrować wiadomość, wpisując pasujące litery w puste miejsca.

KLUCZ SZYFROWANIA LITERA-LICZBA

A=1 Ą=2 B=3 C=4 Ć=5 D=6 E=7 Ę=8 F=9 G=10 H=11 I=12
J=13 K=14 L=15 Ł=16 M=17 N=18 Ń=19 O=20 Ó=21 P=22 Q=23 R=24
S=25 Ś=26 T=27 U=28 V=29 W=30 X=31 Y=32 Z=33 Ź=34 Ż=35

22 24 33 32 30 24 21 5

33 1 25 33 32 9 24 20 30 1 18 7 6 1 18 7 33

14 20 22 12 12 20 9 9 15 12 18 7

Odszyfrowana wiadomość:

WSKAZÓWKA: KAŻDA LICZBA OZNACZA POZYCJĘ TEJ LITERY W ALFABECIE (NP. 1 = A, 2 = B, 35 = Ż).

Punkt kontrolny 10: Podstawowe najczęściej zadawane pytania o cyberbezpieczeństwo (Część A)

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

Q1: Czym jest ransomware?

Ransomware to złośliwe oprogramowanie zaprojektowane tak, aby blokować dostęp do systemów komputerowych lub plików do czasu zapłacenia okupu.

Q2: Jak rozprzestrzenia się ransomware?

Przez załączniki w wiadomościach phishingowych, niezałatane luki w oprogramowaniu i przejęte systemy zdalnego dostępu. [1]

Q3: Dlaczego żąda się płatności w kryptowalucie?

Kryptowaluty, takie jak Bitcoin, oferują względną anonimowość, co utrudnia organom ścigania śledzenie środków.

Q4: Czy antywirus blokuje ransomware?

Tak, ale antywirus oparty na sygnaturach może zawieść wobec nowo utworzonych ładunków ransomware typu zero-day.

Q5: Czym jest kopia zapasowa odizolowana od sieci (air-gapped)?

Kopia zapasowa bez fizycznego ani logicznego połączenia z siecią główną, co chroni ją przed rozprzestrzenianiem się zagrożeń.

Punkt kontrolny 10: Podstawowe najczęściej zadawane pytania o cyberbezpieczeństwo (Część B)

Przejrzyj typowe pytania i odpowiedzi dotyczące ograniczania zagrożeń w sieci.

Q6: Czym jest podwójne wymuszenie (double extortion)?

Gdy atakujący nie tylko szyfrują pliki, ale też kradną wrażliwe dane, aby grozić publicznym wyciekiem w razie braku zapłaty.

Q7: Czym jest narzędzie deszyfrujące (decryptor)?

Narzędzie programowe zawierające klucz kryptograficzny potrzebny do przywrócenia zablokowanych plików do postaci zwykłego tekstu.

Q8: Jak wcześnie wykryć ransomware?

Przez monitorowanie systemów plików pod kątem nagłej, masowej modyfikacji i zmiany nazw plików.

Q9: Jaką rolę odgrywa ubezpieczenie?

Ubezpieczenie cybernetyczne może pomóc pokryć koszty odzyskiwania, ale warunki ochrony i zasady dotyczące płacenia okupu różnią się w zależności od polisy.

Q10: Czy powinienem zrestartować zainfekowany system?

Nie, ponowne uruchomienie może zniszczyć dowody w pamięci ulotnej; zamiast tego odizoluj urządzenie od sieci. [1]

Punkt kontrolny 10: Zaawansowane najczęściej zadawane pytania o bezpieczeństwo (Część C)

Poznaj zaawansowane aspekty techniczne ram bezpieczeństwa, analizy złośliwego oprogramowania i zgodności danych z przepisami.

Q1: Jak ransomware wykorzystuje szyfrowanie asymetryczne?

Używa klucza publicznego osadzonego w złośliwym oprogramowaniu do szyfrowania plików, a do ich odszyfrowania wymagany jest klucz prywatny atakującego.

Q2: Dlaczego stosuje się również szyfrowanie symetryczne?

Szyfrowanie symetryczne (jak AES) jest szybkie i może zaszyfrować ogromne bazy danych w kilka minut, podczas gdy klucze asymetryczne zabezpieczają klucz AES.

Q3: Czym jest segmentacja logiczna?

Podział sieci na izolowane strefy, co zapobiega rozprzestrzenianiu się złośliwego oprogramowania w poziomie ze stacji roboczych do serwerów rdzeniowych.

Q4: Czym jest pamięć WORM?

Nośniki typu Write-Once, Read-Many (jednokrotny zapis, wielokrotny odczyt), które uniemożliwiają edytowanie, nadpisywanie lub usuwanie danych kopii zapasowej przez ładunki ransomware.

Q5: Czym są kopie w tle (shadow copies)?

Lokalne migawki kopii zapasowych tworzone przez system Windows; ransomware zwykle usuwa je jako pierwsze za pomocą narzędzi administracyjnych.

Punkt kontrolny 10: Zaawansowane najczęściej zadawane pytania o bezpieczeństwo (Część D)

Poznaj zaawansowane aspekty techniczne ram bezpieczeństwa, analizy złośliwego oprogramowania i zgodności danych z przepisami.

Q6: Jak kradzież danych uwierzytelniających umożliwia ataki ransomware?

Atakujący kupują wykradzione loginy administratorów, aby logować się przez pulpity zdalne i ręcznie uruchamiać ransomware w całej sieci.

Q7: Czym jest próbne testowanie przywracania (dry-run restoration testing)?

Regularne przywracanie baz danych z kopii zapasowych w odizolowanych środowiskach testowych, aby sprawdzić, czy szybkość przywracania i integralność danych spełniają wskaźniki odtwarzania po awarii.

Q8: Jak wykrywanie i reagowanie na punktach końcowych (EDR) powstrzymuje ransomware?

Przez analizę zachowania procesów (np. szybkiego szyfrowania) i szybkie zawieszenie podejrzanej aplikacji.

Q9: Czym jest model ransomware jako usługa (RaaS)?

Model franczyzowy, w którym twórcy złośliwego oprogramowania wynajmują narzędzia do budowania ransomware partnerom w zamian za procent wypłat.

Q10: Jak niezałatane RDP wywołuje ransomware?

Wystawione na zewnątrz, niezałatane bramy Remote Desktop Protocol pozwalają atakującym łamać loginy metodą brute force i ręcznie uruchamiać złośliwe oprogramowanie.

Część 11: 10 faktów o cyberbezpieczeństwie z praktyki i spostrzeżeń

Przejrzyj prawdziwe fakty dotyczące naruszeń bezpieczeństwa, mechanizmów obronnych i standardów zgodności.

1. WGLĄD W BEZPIECZEŃSTWO

Twórcy ransomware często używają narzędzi takich jak vssadmin.exe do usuwania kopii w tle (shadow copies) systemu Windows i blokowania lokalnego przywracania. [1]

2. WGLĄD W BEZPIECZEŃSTWO

Symetryczne klucze AES-256 są zwykle używane do szyfrowania ładunków plików, które są następnie blokowane kluczami publicznymi RSA.

3. WGLĄD W BEZPIECZEŃSTWO

Odzyskiwanie po udanym ataku ransomware może trwać tygodnie, dlatego sprawdzone kopie zapasowe offline mają znaczenie.

4. WGLĄD W BEZPIECZEŃSTWO

FBI nie popiera płacenia okupu i ostrzega, że zapłata nie gwarantuje odzyskania jakichkolwiek danych. [2]

5. WGLĄD W BEZPIECZEŃSTWO

Plany odtwarzania po awarii (DRP) powinny określać Docelowy Czas Odtworzenia (RTO) i Docelowy Punkt Odtworzenia (RPO).

6. WGLĄD W BEZPIECZEŃSTWO

FBI zaleca kopie zapasowe, które są szyfrowane i niezmienne, czyli takie, których nie można zmienić ani usunąć. [3]

7. WGLĄD W BEZPIECZEŃSTWO

Twórcy ransomware stosują zaawansowane techniki obfuskacji, aby omijać tradycyjne skanery antywirusowe oparte na sygnaturach.

8. WGLĄD W BEZPIECZEŃSTWO

Segmentacja sieci ogranicza ruch boczny, pomagając powstrzymać rozprzestrzenianie się ransomware poza pierwszego zainfekowanego hosta. [3]

9. WGLĄD W BEZPIECZEŃSTWO

Wystawione na zewnątrz, słabo zabezpieczone usługi zdalne, takie jak Remote Desktop Protocol (RDP), są częstym punktem wejścia dla ransomware. [1]

10. WGLĄD W BEZPIECZEŃSTWO

CISA zaleca przechowywanie zaszyfrowanych kopii zapasowych offline, ponieważ wiele odmian ransomware wyszukuje i usuwa dostępne kopie zapasowe. [1]

Źródła i odnośniki techniczne

Przewodnik do nauki i interaktywne łamigłówki powstały na podstawie globalnych standardów NIST, OWASP i zgodności z przepisami o ochronie prywatności danych.

PUBLIKACJE NAUKOWE I BRANŻOWE

[1] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Klucz odpowiedzi: Punkt kontrolny 1 – test wielokrotnego wyboru

1 Pytanie 1

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Jaki jest główny mechanizm ataku ransomware? → Kryptograficzne szyfrowanie plików użytkownika w celu odmowy dostępu do systemu

2 Pytanie 2

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Czym jest kopia zapasowa offline (zimna)? → Kopia danych odłączona od sieci, aby chronić ją przed rozprzestrzenianiem się złośliwego oprogramowania

3 Pytanie 3

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

W jaki sposób zespoły bezpieczeństwa powinny izolować zainfekowane systemy podczas ataku ransomware? → Natychmiast odłącz kable sieciowe i wyłącz interfejsy bezprzewodowe

4 Pytanie 4

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Dlaczego służby bezpieczeństwa odradzają płacenie okupu żądanego przez ransomware? → Wpłacanie środków zachęca atakujących i nie gwarantuje dostarczenia klucza deszyfrującego

5 Pytanie 5

Poprawna odpowiedź: A

UWAGA DLA NAUCZYCIELA

Czym jest plan awaryjnego odtwarzania systemów (DRP)? → Ustrukturyzowany proces przywracania operacji i danych po naruszeniu bezpieczeństwa systemu

Klucz odpowiedzi: Punkt kontrolny 2 – prawda czy fałsz

6 **Pytanie 6** — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Ładunki ransomware mogą łatwo rozprzestrzeniać się na kopie zapasowe online podłączone do sieci.

7 **Pytanie 7** — **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

Fałsz: FBI ostrzega, że zapłata nie gwarantuje odzyskania żadnych danych. [2]

8 **Pytanie 8** — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Prawda: CISA zaleca odłączenie zainfekowanych hostów lub wyłączenie sieci, aby ograniczyć rozprzestrzenianie.

9 **Pytanie 9** — **Poprawna odpowiedź: Fałsz**

UWAGA DLA NAUCZYCIELA

Fałsz: ransomware zwykle szyfruje pliki szybkimi szyframi symetrycznymi, takimi jak AES.

10 **Pytanie 10** — **Poprawna odpowiedź: Prawda**

UWAGA DLA NAUCZYCIELA

Regularne testowanie procedur przywracania danych jest kluczową częścią odtwarzania po awarii.

Klucze słownictwa i kryteria oceny

Schemat oceniania dla nauczyciela: Przyznaj 1 punkt za każde poprawne dopasowanie (łącznie 8 pkt) i pojęcie w kontekście (łącznie 6 pkt).

PUNKT KONTROLNY 4: KLUCZ – DOPASOWYWANIE POJĘĆ

C 1. SZYFROWANIE	E 2. ŁADUNEK	F 3. ZIMNA KOPIA ZAPASOWA	A 4. IZOLACJA
H 5. OKUP	G 6. ODZYSKIWANIE	D 7. KATASTROFA	B 8. TROJAN

PUNKT KONTROLNY 3: KLUCZ – KLUCZOWE POJĘCIA

1 SZYFROWANIE	2 ŁADUNEK	3 KOPIA OFFLINE	4 IZOLACJA
5 OKUP	6 ODZYSKIWANIE		

PUNKT KONTROLNY 6, WARIANT ALTERNATYWNY: KLUCZ – DOPASOWYWANIE SŁÓW

1 C – KOPIAOFFLINE	2 H – TROJAN	3 A – SZYFROWANIE	4 E – OKUP
5 D – IZOLACJA	6 G – AWARIA	7 B – ŁADUNEK	8 F – ODZYSKIWANIE

UWAGI DO DYSKUSJI DLA NAUCZYCIELI

Kluczowe pojęcia:
Sprawdź, czy uczniowie potrafią własnymi słowami wyjaśnić pojęcia SZYFROWANIE, ŁADUNEK i ZIMNA KOPIA ZAPASOWA oraz podać przykład każdego z nich.

Studia przypadków:
Poproś uczniów, aby uzasadniali swoje zalecenia faktami z karty pracy, a nie przypuszczeniami.

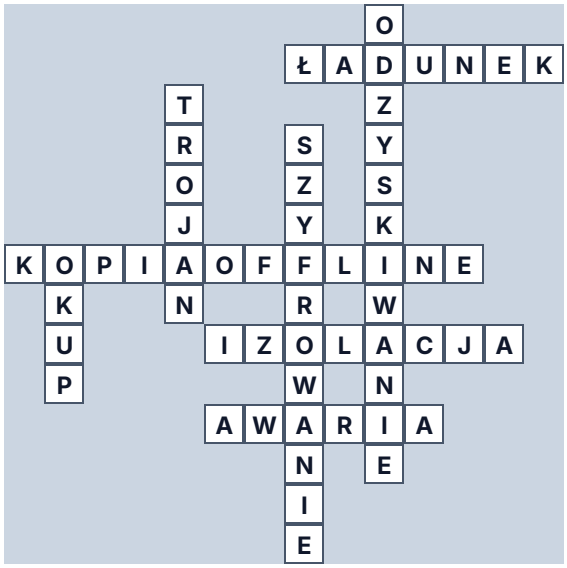
Ocena źródeł:
Niech uczniowie sprawdzą co najmniej jedno twierdzenie w źródłach z karty pracy; omówcie, dlaczego liczby, ceny i przepisy mogą się z czasem zmieniać.

Klucze do łamigłówek i uwagi dla nauczyciela

ROZWIĄZANIE WYSZUKIWANKI SŁOWNEJ

E	B	A	A	B	C	Ó	I	Z	Ł	K	Z	L	Y	T
I	L	I	D	Q	N	K	Z	D	I	Ł	Ń	N	L	Q
N	Ó	R	G	N	N	Q	O	R	S	A	T	T	F	B
A	N	A	Ś	P	O	H	L	S	B	D	W	Ć	Ś	Ź
W	A	W	V	C	Ż	W	A	Ę	L	U	G	Ż	S	Ć
I	J	A	N	D	Q	Y	C	Ó	C	N	U	B	Z	A
K	O	Ż	Ń	Ć	O	L	J	A	D	E	O	D	Y	Ę
S	R	G	I	Ć	K	R	A	Q	M	K	E	I	F	S
Y	T	Ż	Ś	Ę	U	Q	V	E	A	A	Q	Ó	R	N
Z	P	T	Y	Q	P	K	R	T	S	Ć	N	Ź	O	B
D	K	O	P	I	A	O	F	F	L	I	N	E	W	Ę
O	S	Y	X	J	A	R	Ż	Z	Z	Ł	F	I	A	N
R	K	M	M	T	O	G	P	Q	G	Ż	Ą	O	N	V
F	V	B	Ź	S	Ź	B	G	M	Ż	G	K	O	I	P
Ń	X	C	M	Ż	Ź	F	Z	O	X	U	L	V	E	Ó

ROZWIĄZANIE KRZYŻÓWKI



PRZEWODNIK DLA NAUCZYCIELA: ROZWIĄZANIA KRZYŻÓWKI

POZIOMO

2 poziomo: ŁADUNEK Uruchamianie złośliwego oprogramowania. (7 liter)

5 poziomo: KOPIAOFFLINE Odłączona kopia offline. (12 liter)

7 poziomo: IZOLACJA Odłączanie zainfekowanych systemów sieciowych. (8 liter)

8 poziomo: AWARIA Poważne zdarzenie zakłócające działanie systemu. (6 liter)

PIONOWO

1 pionowo: ODZYSKIWANIE Przywracanie bazy danych z kopii zapasowej. (12 liter)

3 pionowo: TROJAN Złośliwy plik udający czysty. (6 liter)

4 pionowo: SZYFROWANIE Kryptograficzne blokowanie plików. (11 liter)

6 pionowo: OKUP Żądanie wypłaty w zamian za klucz kryptograficzny. (4 liter)

Klucz do słów rozsypanych i rozwiązania szyfru

Klucz odpowiedzi do ćwiczenia z rozszyfrowywania słownictwa i Tajemniczego wyzwania szyfrowego.

KLUCZ DO ROZWIĄZANIA ANAGRAMÓW

1. RWIZOASNYEF — **SZYFROWANIE**
2. EOAOKINPFLFI — **KOPIAOFFLINE**
3. POUK — **OKUP**
4. ARAIAW — **AWARIA**
5. NKUDŁEA — **ŁADUNEK**
6. JALCIAZO — **IZOLACJA**
7. WASODIENIZKY — **ODZYSKIWANIE**
8. ONTAJR — **TROJAN**

KLUCZ DO WYZWANIA Z TAJNYM SZYFREM

"PRZYWRÓĆ ZASZYFROWANE DANE Z KOPII OFFLINE"

Klucz odpowiedzi do studiów przypadków

A Studium przypadku 1: Ograniczanie ładunku ransomware w firmie

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Firmowa sieć lokalna została naruszona przez aktywny ransomware. Kluczowe serwery plików zaczęły wyświetlać pliki z rozszerzeniem .locked.
- Zalecana strategia i rozwiązanie: Odłącz wszystkie zaatakowane serwery od sieci lokalnej. Zakończ aktywne sesje administracyjne. Przywróć niezainfekowane pliki z bezpiecznego, zablokowanego do zapisu systemu kopii zapasowych offline.

B Studium przypadku 2: Ocena architektur kopii zapasowych offline

Rozwiązanie dla nauczyciela

WYTYCZNE OCENIANIA

Odpowiedzi uczniów powinny obejmować następujące punkty:

- Analiza scenariusza: Firma chce zaprojektować strategię tworzenia kopii zapasowych, która zmniejsza ryzyko przejęcia kopii, nawet jeśli główna sieć lokalna zostanie całkowicie przejęta przez ransomware.
- Zalecana strategia i rozwiązanie: Wdróż pamięć masową typu WORM (write-once-read-many). Utwórz logiczną izolację (air gap), odłączając system kopii zapasowych od wszystkich sieci, i egzekwuj codzienną rotację fizycznych nośników.