Zadanie 3 Zostań CYBERBOHATEREM Szkoły! Zadanie należy wykonać do 25 listopada 2026r.

Przeczytaj uważnie dwie sytuacje problemowe i odpowiedz na poniższe pytania. Nie musisz przepisywać treści pytań, wystarczy napisać: np. Ransomware Zadanie 1 Ad1 itd.

Sytuacja problemowa 1

W poniedziałek rano pracownik szkolnego sekretariatu otworzył wiadomość e-mail zatytułowaną **„Pilne! Aktualizacja dokumentacji uczniów”.** Po otwarciu załącznika komputer zaczął działać wolniej, a po kilku minutach na ekranie pojawił się komunikat o zaszyfrowaniu plików. Wkrótce okazało się, że:

- nie można otworzyć dokumentów uczniów;
- część plików zmieniła rozszerzenia;
- szkolny serwer plików przestał działać prawidłowo;
- na ekranie pojawiło się żądanie zapłaty okupu;
- nie wiadomo czy wyciekły dane uczniów i pracowników szkoły;
- nie wiadomo, czy kopie zapasowe są bezpieczne.

Dyrektor prosi uczniów o przygotowanie planu reagowania na incydent.

Polecenia dla uczniów

Zadanie 1. Analiza ataku 10 pkt.

1. Wyjaśnij na podstawie definicji oraz zaistniałej sytuacji, czym jest ransomware.
2. Wskaż prawdopodobny sposób, w jaki doszło do infekcji.
3. Wyjaśnij, dlaczego atakujący żądają okupu.
4. Wskaż trzy potencjalne skutki ataku dla szkoły.

Zadanie 2. Reagowanie na incydent 10 pkt.

Uporządkuj działania szkoły od najpilniejszego do najmniej pilnego i uzasadnij swój wybór:

- Sprawdzić bezpieczeństwo kopii zapasowych.
- Zawiadomić służby.
- Odizolować zainfekowane komputery od sieci.
- Poinformować jednostki administracyjne szkoły o zaistniałym problemie.
- Zgłosić incydent administratorowi IT i dyrekcji.
- Zapłacić okup, aby szybko odzyskać pliki.
- Zabezpieczyć dowody i ustalić zakres incydentu.
- Przywrócić systemy po usunięciu zagrożenia.

Zaznacz działania, które powinny znaleźć się w planie. Następnie ustal ich kolejność w odpowiedzi pisemnej. Jeżeli uważacie, że to nie wszystkie działania, to proszę dopisać swoje pomysły.

Zadanie 3. Opracowanie planu ochrony 5 pkt.

Zaproponuj pięć rozwiązań, które pomogą szkole ograniczyć ryzyko podobnego ataku w przyszłości. Uwzględnij m.in. kopie zapasowe, aktualizacje oprogramowania, hasła i szkolenia użytkowników.

Zadanie 4. Decyzja zespołu 5 pkt.

Czy szkoła powinna zapłacić okup? Przedstaw dwa argumenty przemawiające przeciwko płatności lub za płatnością. Zaproponuj alternatywny sposób odzyskania danych.

Zadanie 5. Komunikat 5 pkt.

Napisz krótki komunikat dla uczniów i rodziców informujący o incydencie. Nie wywołuj paniki i nie podawaj niepotwierdzonych informacji.

Sytuacja problemowa 2

Szkoła korzysta z platformy internetowej, na której uczniowie sprawdzają oceny, pobierają materiały i przesyłają zadania.

W poniedziałek o godzinie 8:00 platforma nagle przestaje działać. Uczniowie nie mogą się zalogować, nauczyciele nie mają dostępu do materiałów, a administrator zauważa ogromny wzrost liczby połączeń z serwerem.

Po wstępnej analizie okazuje się, że serwer otrzymuje tak wiele żądań, że nie jest w stanie obsługiwać prawidłowo zwykłych użytkowników.

Administrator podejrzewa atak DDoS (Distributed Denial of Service)!

Zadanie 1. Rozpoznaj zagrożenie 10 pkt.

1. Wyjaśnij na podstawie definicji oraz zaistniałej sytuacji czym jest atak DDoS?
2. Jakie objawy wskazują na możliwy atak DDoS?
3. Jaki jest główny cel takiego ataku?
4. Czym DDoS różni się od ransomware?
5. Czy atak DDoS musi oznaczać kradzież danych? Uzasadnij odpowiedź.

Zadanie 2. Podejmij decyzję 5 pkt.

Jesteście zespołem administratorów szkolnej platformy. Wybierzcie trzy najważniejsze działania, które należy podjąć. Wybór uzasadnij.

1. Przeanalizować ruch sieciowy i potwierdzić, czy występuje atak.
2. Skontaktować się z dostawcą hostingu lub usług sieciowych.
3. Zastosować dostępne mechanizmy ochrony przed DDoS i filtrowania ruchu.
4. Wyłączyć wszystkie zabezpieczenia serwera.
5. Opublikować hasła administratorów, aby uczniowie mogli pomóc.
6. Przygotować tymczasowy sposób przekazywania materiałów uczniom.

Zadanie 3. Zaprojektuj zabezpieczenia 5 pkt.

Zaproponuj cztery sposoby, dzięki którym szkoła może lepiej przygotować się na atak DDoS. Uwzględnij ochronę techniczną, współpracę z dostawcą usług oraz komunikację z uczniami.

Zadanie 4. Przygotuj komunikat 5 pkt.

Napisz krótką informację dla uczniów, w której:

- wyjaśnisz, dlaczego platforma jest niedostępna;
- poinformujesz, co szkoła robi w tej sytuacji;
- wskażesz alternatywny sposób przesyłania prac domowych.

Bonus 15 pkt.

Przygotuj schemat postępowania po wykryciu jednego z prezentowanych ataków. Schemat ma pokazywać kolejność działań od infekcji do bezpiecznego przywrócenia sytemu. Możesz go wykonać w formie plakatu, prezentacji multimedialnej lub schematu blokowego.