Artur Markiewicz

RANSOMWARE W AKCJI

Przygotuj swoją firmę na atak cyberprzestępców

Helion

Redaktor prowadzący: Małgorzata Kulik

Projekt okładki: Studio Gravite/Olsztyn
Obarek, Pokoński, Pazdrijowski, Zaprucki

Grafika na okładce została wykorzystana za zgodą AdobeStock.com.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
helion.pl/user/opinie/metwfi
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

ISBN: 978-83-289-2922-7

Printed in Poland.

SPIS TREŚCI

Rozdział 15

REAGOWANIE NA INCYDENT: KLUCZOWE KROKI DLA FIRMY

Mimo wszelkich starań może dojść do incydentu.

W ogólnie przyjętych dobrych praktykach w cyberbezpieczeństwie wyróżnia się pięć kluczowych kroków: zidentyfikowanie, zabezpieczenie, detekcja, zareagowanie oraz przywrócenie (rysunek 15.1). Podejście to wywodzi się z ramowego modelu NIST Cybersecurity Framework 2.0 (CSF 2.0), który stanowi powszechnie uznany standard zarządzania ryzykami związanymi z cyberbezpieczeństwem i wspiera organizacje w budowaniu cyfrowej odporności. Model CSF 2.0 może być stosowany w każdej organizacji — niezależnie od wielkości czy branży — jako punkt odniesienia do budowy lub oceny programu bezpieczeństwa informacji.

Govern (zarządzaj) — zapewnienie nadzoru, polityk, odpowiedzialności i strategii w zakresie cyberbezpieczeństwa w całej organizacji. Nowy komponent dodany w wersji 2.0

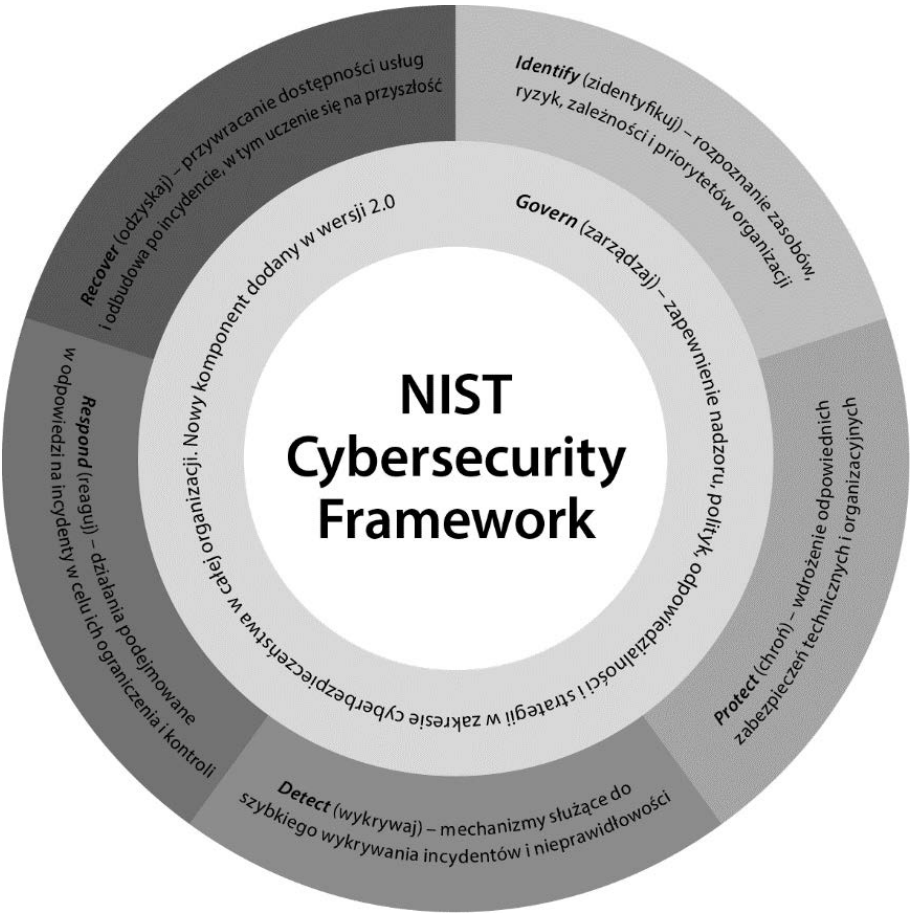
Identify (zidentyfikuj) — rozpoznanie zasobów, ryzyk, zależności i priorytetów organizacji

Protect (chroń) — wdrożenie odpowiednich zabezpieczeń technicznych i organizacyjnych

Detect (wykrywaj) — mechanizmy służące do szybkiego wykrywania incydentów i nieprawidłowości

Respond (reaguj) — działania podejmowane w odpowiedzi na incydenty w celu ich ograniczenia i kontroli

Recover (odzyskaj) — przywracanie dostępności usług i odbudowa po incydencie, w tym uczenie się na przyszłość



RYSUNEK 15.1. Kluczowe kroki w razie incydentu (*https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf*, s. 5)

Co robić po ataku?

- Odizoluj komputer od reszty sieci.
- Zrób zdjęcie ekranu z komunikatem o wymuszeniu, zgraj na osobny nośnik notkę z informacją o wymuszeniu (czasem jest to osobny plik) i garść zaszyfrowanych plików, które będą Twoimi próbkami.

- Nie resetuj komputera. Czasem da się odzyskać klucze z pamięci — lub wygenerować ponownie, jeśli znamy dokładny stan zegarów systemowych.
- Zresetuj poświadczenia, które mogły być nadużyte w ataku.
- Jeśli potrafisz, spróbuj zgrać samo ransomware.
- Zajrzyj na stronę nomoreransom.org — może będzie tam klucz do odszyfrowania.
- Zgłoś incydent do CERT Polska (incydent.cert.pl).
- Zgłoś incydent na policję lub bezpośrednio do prokuratury okręgowej.

Najogólniej można rzecz sprowadzić do trzech elementów:

- Opracuj plan odzyskiwania po incydencie.
- Twórz kopie zapasowe i przywracaj dane. Przed przywróceniem danych z kopii zapasowej sprawdź, czy jest ona wolna od złośliwego oprogramowania.
- Utrzymuj aktualną listę kontaktów do osób, które mogą być pomocne w reagowaniu na zdarzenie, określeniu aktualnej pozycji.

Przykładowa lista kroków

1. Rozpoznanie i zgłoszenie incydentu.

1.1. Zidentyfikuj i natychmiast zgłoś każdy podejrzany incydent do zespołu bezpieczeństwa IT.

1.2. Przeszkol pracowników w zakresie rozpoznawania i zgłaszania incydentów, które mogą mieć charakter zagrożenia cyberbezpieczeństwa.

1.3. Wdróż system zgłoszeń incydentów, który umożliwi szybkie powiadomienie zespołu IT o potencjalnych zagrożeniach.

2. Monitorowanie środowiska i wczesne ostrzeganie.

2.1. Stale monitoruj infrastrukturę IT za pomocą narzędzi do wykrywania anomalii i podejrzanych działań.

2.2. Wdróż narzędzia SIEM (*Security Information and Event Management*) oraz inne rozwiązania do automatycznego wykrywania zagrożeń i generowania alertów w czasie rzeczywistym.

2.3. Wdróż *Continuous Threat Exposure Management* (CTEM). To kompleksowy program, który umożliwia organizacji stałą identyfikację, priorytetyzację, walidację i naprawę luk w zabezpieczeniach.

3. Ocena skali i charakteru incydentu.

3.1. Zbadaj incydent, aby określić jego zakres, źródło i potencjalne konsekwencje.

3.2. Skorzystaj z narzędzi do monitorowania i analizy, aby dokładnie ocenić incydent oraz zidentyfikować naruszone systemy i dane.

4. Izolacja zainfekowanych systemów.

4.1. Odłącz zainfekowane urządzenia od sieci, aby zapobiec dalszemu rozprzestrzenianiu się zagrożenia.

4.2. Wprowadź procedury natychmiastowego izolowania zainfekowanych systemów, które mogą być aktywowane przez zespół IT.

5. Zabezpieczenie dowodów.

5.1. Zbierz i zabezpiecz dowody związane z incydentem, aby umożliwić ich analizę oraz podjęcie dalszych działań prawnych.

5.2. Ustal procedury zabezpieczania logów, zrzutów ekranu, wiadomości i innych istotnych danych.

6. Analiza przyczyny i punktu włamania.

6.1. Przeprowadź szczegółową analizę, aby zrozumieć, jak doszło do incydentu oraz jakie były jego przyczyny.

6.2. Współpracuj z ekspertami ds. bezpieczeństwa, aby zidentyfikować słabe punkty i mechanizmy ataku.

7. Eliminacja zagrożenia.

7.1. Usuń złośliwe oprogramowanie i napraw wszelkie luki w zabezpieczeniach, które zostały wykorzystane.

7.2. Zaktualizuj oprogramowanie, stosuj łatki bezpieczeństwa oraz wdrażaj dodatkowe zabezpieczenia tam, gdzie to konieczne.

8. Przywracanie systemów do normalnej pracy.

8.1. Przywróć zainfekowane systemy do pełnej operacyjności, zapewniając ich bezpieczeństwo.

8.2. Wdrażaj procedury przywracania danych z kopii zapasowych oraz przeprowadzaj testy systemów przed ponownym uruchomieniem.

9. Komunikacja z interesariuszami.

9.1. Informuj odpowiednie strony o incydencie, jego skutkach oraz podjętych działaniach.

9.2. Opracuj plan komunikacji, który uwzględnia pracowników, klientów, partnerów biznesowych oraz organy regulacyjne.

10. Przegląd i uczenie się na błędach.

10.1. Po zakończeniu incydentu przeanalizuj działania, aby wyciągnąć wnioski i wprowadzić ulepszenia w procedurach bezpieczeństwa.

10.2. Organizuj spotkania podsumowujące z udziałem wszystkich zaangażowanych stron, aby omówić, co poszło dobrze, a co można poprawić.

11. Aktualizacja i wdrożenie polityk bezpieczeństwa.

11.1. Na podstawie zebranych doświadczeń zaktualizuj polityki i procedury bezpieczeństwa, aby zapobiec przyszłym incydentom.

11.2. Wprowadź zmiany w politykach bezpieczeństwa, przeszkol pracowników oraz regularnie testuj nowe procedury, aby zapewnić ich skuteczność.

Więcej informacji dla specjalistów IT: The NIST Cybersecurity Framework (CSF) 2.0.

Kluczowe pytania, aby menedżer mógł skutecznie ocenić gotowość firmy na reagowanie na incydenty

1. Rozpoznanie i zgłaszanie incydentów.
    1.1. Czy pracownicy są przeszkoleni, aby rozpoznawać i zgłaszać incydenty cyberbezpieczeństwa?
    1.2. Czy mamy wdrożony system do szybkiego zgłaszania podejrzanych incydentów?
    1.3. Jak szybko zespół IT może otrzymać zgłoszenie o potencjalnym zagrożeniu?
2. Monitorowanie środowiska.
    2.1. Czy nasza infrastruktura IT jest stale monitorowana pod kątem anomalii i podejrzanych działań?
    2.2. Czy korzystamy z narzędzi do automatycznego wykrywania zagrożeń (np. SIEM) oraz systemów wczesnego ostrzegania?
    2.3. Jak często aktualizowane są te narzędzia i jak szybko reagują na nowe zagrożenia?
3. Ocena skali i charakteru incydentu.
    3.1. Czy nasz zespół IT ma narzędzia i umiejętności, aby szybko ocenić zakres incydentu i jego potencjalne konsekwencje?
    3.2. Jakie procedury mamy do zidentyfikowania naruszonych systemów i danych?
4. Izolacja zainfekowanych systemów.
    4.1. Czy mamy zdefiniowane procedury izolowania zainfekowanych systemów?
    4.2. Jakie technologie są dostępne do natychmiastowego odłączenia zagrożonych urządzeń od sieci?
    4.3. Jak szybko jesteśmy w stanie wprowadzić procedurę izolacji?

5. Zabezpieczenie dowodów.

5.1. Czy mamy opracowane procedury zbierania i zabezpieczania dowodów związanych z incydentami?

5.2. Jakie są nasze procedury w zakresie zabezpieczania logów, zrzutów ekranu i innych kluczowych danych?

6. Analiza przyczyny i punktu włamania.

6.1. Czy nasz zespół ma doświadczenie w analizie incydentów, aby zidentyfikować przyczynę i sposób włamania?

6.2. Czy współpracujemy z ekspertami ds. bezpieczeństwa w celu zidentyfikowania słabych punktów?

7. Eliminacja zagrożenia.

7.1. Czy mamy procedury usuwania złośliwego oprogramowania oraz naprawy luk w zabezpieczeniach?

7.2. Jak szybko po incydencie jesteśmy w stanie zastosować łatki bezpieczeństwa i wdrożyć dodatkowe środki ochrony?

8. Przywracanie systemów do normalnej pracy.

8.1. Czy mamy wdrożone procedury przywracania danych z kopii zapasowych?

8.2. Jakie są nasze procedury testowania systemów przed ich ponownym uruchomieniem po incydencie?

8.3. Jak długo trwa przywrócenie pełnej operacyjności systemów?

9. Komunikacja z interesariuszami.

9.1. Czy mamy plan komunikacji w przypadku incydentu, który obejmuje pracowników, klientów, partnerów i organy regulacyjne?

9.2. Jak szybko jesteśmy w stanie przekazać informacje o incydencie kluczowym interesariuszom?

10. Przegląd i uczenie się na błędach.

10.1. Czy regularnie analizujemy incydenty, aby wyciągać wnioski i wprowadzać ulepszenia w procedurach bezpieczeństwa?

10.2. Jak często organizujemy spotkania podsumowujące po incydentach z udziałem wszystkich zaangażowanych stron?

11. Aktualizacja polityk bezpieczeństwa.

11.1. Jak często aktualizujemy polityki i procedury bezpieczeństwa na podstawie doświadczeń z incydentów?

11.2. Czy przeszkoliliśmy pracowników z nowych procedur i czy regularnie testujemy ich skuteczność?

Te pytania pomogą menedżerowi ocenić stopień przygotowania firmy na incydenty cyberbezpieczeństwa oraz zapewnić, że organizacja jest w stanie skutecznie reagować i minimalizować szkody.

Kluczowe prompty do AI

Te prompty dla rozdziału „Reagowanie na incydent: kluczowe kroki dla firmy" mają na celu pomóc menedżerowi w efektywnym reagowaniu na incydenty związane z cyberbezpieczeństwem i bazują na najnowszych i sprawdzonych informacjach.

Kluczowe kroki reagowania na incydent

> „Jako menedżer chcę poznać aktualne kluczowe kroki, które firma powinna podjąć w odpowiedzi na incydent bezpieczeństwa, taki jak atak ransomware. Proszę o szczegółowy opis tych kroków wraz z odniesieniami do najnowszych źródeł".

Ocena gotowości firmy na incydenty

> „Pomóż mi jako menedżerowi ocenić gotowość mojej firmy na reagowanie na incydenty związane z cyberbezpieczeństwem. Proszę o najnowsze wytyczne i źródła dotyczące oceny i poprawy gotowości firmy na takie sytuacje".

Wdrożenie planu reagowania na incydent

> „Jakie są najlepsze praktyki wdrażania planu reagowania na incydenty w firmie? Jako menedżer chciałbym otrzymać aktualne informacje na ten temat, poparte źródłami, które wskazują na skuteczność tych działań".

Szkolenie zespołów reagowania na incydenty

> „Jakie szkolenia powinienem przeprowadzić, aby mój zespół był przygotowany do skutecznego reagowania na incydenty? Proszę o najnowsze rekomendacje oraz źródła".

Minimalizacja skutków incydentów

> „Jakie działania mogę podjąć jako menedżer, aby zminimalizować skutki incydentów cyberbezpieczeństwa? Proszę o aktualne informacje oraz najlepsze praktyki, poparte źródłami".

Cyberatak to kwestia czasu. Przygotuj się!

Jeśli chodzi o cyberbezpieczeństwo, żadna firma nie jest bezpieczna. Pytanie, które należy sobie zadać, nie brzmi: czy zostaniemy zaatakowani? Odpowiedź na nie jest bowiem oczywista: **tak, zostaniecie zaatakowani**. Właściwe pytania są takie:

- **Skąd będziemy wiedzieć, że zostaliśmy zaatakowani?**
- **Co wówczas zrobimy?**

Ten poradnik ma za zadanie zawczasu pomóc Ci na nie odpowiedzieć i wesprzeć Cię w momencie, w którym nastąpi atak typu ransomware. Polega on na blokowaniu pracownikom dostępu do urządzeń i plików, a następnie żądaniu okupu za jego przywrócenie.

Z książki dowiesz się między innymi:

- **Czym jest atak ransomware i jakie są jego możliwe konsekwencje**
- **Jakie taktyki stosują przestępcy**
- **Jak może wyglądać atak — na podstawie studiów przypadków**
- **Jak się zabezpieczyć, jeśli chodzi o sprzęt i ludzi**
- **W jaki sposób reagować na atak — z podziałem na role: od zarządu po szeregowego pracownika**

Helion
helion.pl
HELION S.A.
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!

ISBN 978-83-289-2922-7

Cena: 79,00 zł

Artur Markiewicz

Pasjonat cyberbezpieczeństwa z ponad 20-letnim doświadczeniem w branży IT, aktywny zawodowo od 1991 roku. W Trecom Group działa jako konsultant i trener, wspierając firmy, instytucje publiczne i sektor edukacji w budowaniu odporności na zagrożenia cyfrowe. Członek zarządu ISSA Polska, współtwórca projektów Cyfrowy Skaut i #ISSAPolskalocal, aktywnie zaangażowany w rozwój lokalnych społeczności i edukację w dziedzinie bezpieczeństwa informacji. Twórca platformy **cyberkurs.online**, na której prowadzi szkolenia dla użytkowników, liderów i zespołów technicznych — łącząc wiedzę technologiczną z empatią i systemowym podejściem. Autor licznych poradników, quizów i kampanii phishingowych służących działaniom edukacyjnym oraz testowym. Prelegent, konferansjer i uczestnik czołowych konferencji branżowych, takich jak Semafor, Confidence, Advanced Threat Summit, INSECON, KSC Forum czy Technology Risk Management Forum. Członek społeczności Toastmasters, w ramach której rozwija kompetencje komunikacyjne i przywódcze. Doradza organizacjom oraz osobom prywatnym w zakresie proaktywnego podejścia do bezpieczeństwa: przygotowania, monitorowania, reagowania na incydenty, edukacji, budowania świadomości, a także wspierania trenerów i prelegentów działających w tych obszarach.