

Artur Markiewicz

0 0
1 1 0011 011100101011 0 1
0 10010001100101010011111 01 0 0
1 1110011111001100000101111011 11 0 10 1
0 1100111001010011100011000010001100 0 1 0
1 100110111000011011000111000110111001 0 100 0
0 10111110000110010111001011000001000 01 1 0 1 0
1 1100 1011101101100100110011111001111100 0 1 0
0 0011100110111011110101100111000 10 0 1 0 0 1 0 0
1 01011010 1001001001 01001 00 0 1 1 0 101 0 0
0 110 00110 00 000 101 100101 1 0 1 1 0 0 1 0
0 001 101 0 010 1110001010001110000 0 1 1 0 0 0 1
0 00100101010010010011000 1011110110 1 1 1 1 1
0 0000 0 0 1 0 0 000000 011010 0 0 0 100 1 0
0 000 1 1 100 000 1000 1
0 11 1 0 10 1 1
0 011 0 0 1
0 110 100110 111 1
1 1010 10001011 0 1 0
0 1011101 0011 010 10 0
110100101 001111 1 1 0 0 0
011 0 1010111000101011 1 1 1 1 0 0
0 0010 1 111 110101 1 1 0 1
1 1 0100 1 01
1 0 10 00011 10 1 0 1 0
1 1 100 0011101 0 1 1
1 0 1 0 0101010 0 0 1 0
0 11 1 0 0 0 0
0 0 0 1110 0 0 0 0 0
1 0 0 10 00 00100 1 1
1 000 1 00 1 0 1 0 1 1 1 011 0
0 1011011 1 0 0 1 0 00 0110 0 0 1 0 1011 0 1 0
0101000011011 0 1 0 0 1 1 11001 11 010
001000 0010000 1 1 0 111 011011 1 0 011 1 1 1 1
01111 010 1 1 00 110010 1 1 01 11010
0000 1 1 0 01 101 0 0 0 0 1100 0
1 0 1 0 1 1 1
110 0 1 0 0 0
11000 0 11100
1 10 0 1101
1 1 0 1101
0

RANSOMWARE W AKCJI

Przygotuj swoją firmę na atak cyberprzestępców

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiejkolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz wydawca dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz wydawca nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

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

Copyright © Helion S.A. 2025

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

SPIS TREŚCI

WSTĘP	13
ROZDZIAŁ 1. UŻYWANIE AI W CELU EFEKTYWNEGO WYKORZYSTANIA TEGO PORADNIKA	17
Kluczowe założenia	17
Master prompt	18
Struktura poradnika i miejsca, w których możesz znaleźć prompty	18
ROZDZIAŁ 2. ATAK TYPU RANSOMWARE	20
Przewaga konkurencyjna dzięki inwestycjom w cyberbezpieczeństwo	20
Wsparcie zewnętrzne jako klucz do skutecznej ochrony	20
Konsekwencje ataku typu ransomware	22
Pytania menedżera dotyczące konsekwencji ataku typu ransomware	23
Kluczowe prompty do AI	25
<i>Zrozumienie mechanizmów ataku ransomware</i>	25
<i>Analiza zagrożeń związanych z ransomware'em</i>	25
<i>Rozpoznawanie sygnałów ataku ransomware</i>	25
<i>Ochrona firmy przed ransomware'em</i>	25
<i>Edukacja pracowników na temat ransomware'u</i>	25
ROZDZIAŁ 3. STUDIUM PRZYPADKU. ATAK RANSOMWARE NA FIRMĘ XYZ	26
Tło	26
Opis ataku	26
Działania podjęte przez firmę	26

RANSOMWARE W AKCJI

Wnioski	28
Podsumowanie	28
Przykłady innych firm	28
<i>Konsekwencje zapłacenia okupu</i>	28
<i>Brak kopii zapasowych i odbudowa systemów</i>	29
<i>Skuteczność zaawansowanych narzędzi ochrony</i>	29
Kluczowe prompty do AI	30
<i>Analiza przypadku ataku ransomware</i>	30
<i>Wyciąganie wniosków z analizy przypadku</i>	30
<i>Dostosowanie strategii obrony na podstawie studium przypadku</i>	30
<i>Ocena skuteczności reakcji firmy XYZ na atak ransomware</i>	31
<i>Nauka na błędach innych firm</i>	31

ROZDZIAŁ 4. ZESTAWIENIE TAKTYK DZIAŁANIA ATAKUJĄCYCH 32

Kolejność działań przestępców	33
Kluczowe prompty do AI	35
<i>Identyfikacja taktyk cyberprzestępców</i>	36
<i>Analiza zagrożeń wynikających z taktyk atakujących</i>	36
<i>Opracowanie strategii obrony przed taktykami atakujących</i>	36
<i>Monitorowanie i wykrywanie taktyk atakujących</i>	36
<i>Szkolenie zespołu w zakresie obrony przed taktykami atakujących</i>	36

ROZDZIAŁ 5. ZAANGAŻOWANIE ZARZĄDU 37

Korzyści z inwestowania w cyberbezpieczeństwo	37
Konsekwencje braku działań	38
Przykłady zaangażowania zarządu	38
Kluczowe pytania, jakie może zadać menedżer, aby mógł skutecznie ocenić poziom zaangażowania zarządu	39
<i>Co powinien wiedzieć menedżer (minimum)</i>	39
<i>Co powinien wiedzieć menedżer (optimum)</i>	40

Spis treści

<i>Jak zakomunikować wdrożenie</i>	50
<i>Co powinien wiedzieć menedżer</i>	50
<i>Lista pytań, które menedżer powinien zadać</i>	51
Kluczowe prompty do AI	55
<i>Budowanie świadomości zarządu na temat cyberzagrożeń</i>	55
<i>Prezentacja zagrożeń i strategii zarządowi</i>	55
<i>Zaangażowanie zarządu w decyzje dotyczące cyberbezpieczeństwa</i>	56
<i>Edukacja zarządu w zakresie cyberbezpieczeństwa</i>	56
<i>Monitorowanie zaangażowania zarządu</i>	56

ROZDZIAŁ 6. BUDOWANIE STRATEGII OCHRONY PRZED CYBERZAGROŻENIAMI

<i>Cel strategii ochrony przed cyberzagrożeniami</i>	57
<i>Znaczenie strategii dla organizacji</i>	57
Ocena obecnej sytuacji	58
<i>Identyfikacja zagrożeń</i>	58
<i>Ocena istniejących środków technicznych i procedur zabezpieczających</i>	58
<i>Analiza przeszłych incydentów cyberbezpieczeństwa</i>	58
<i>Wyniki testów kopii zapasowych i planów ciągłości działania</i>	58
Określenie celów	59
<i>Cele w zakresie cyberbezpieczeństwa na najbliższy rok</i>	59
<i>Przewidywane nowe zagrożenia i wyzwania</i>	59
<i>Standardy i najlepsze praktyki do wdrożenia</i>	59
Planowanie działań	59
<i>Konkretnie działania mające na celu minimalizację ryzyka cyberzagrożeń</i>	59
<i>Szkolenia i warsztaty z zakresu cyberbezpieczeństwa dla pracowników</i>	60
<i>Procedury reagowania na incydenty</i>	60
Ocena dotychczasowych osiągnięć	60
<i>Wdrożone środki techniczne i procedury zabezpieczające</i>	60
<i>Szkolenia z zakresu cyberbezpieczeństwa</i>	60
<i>Zarządzanie incydentami cyberbezpieczeństwa i wyniki działań</i>	61

RANSOMWARE W AKCJI

Opracowanie pomysłów na przyszłość	61
<i>Nowe technologie i narzędzia do wdrożenia</i>	61
<i>Innowacyjne podejścia w procedurach reagowania na incydenty</i>	61
<i>Dodatkowe środki zabezpieczające</i>	61
Monitorowanie i rozliczanie postępów	62
<i>Metryki i wskaźniki do monitorowania skuteczności działań</i>	62
<i>Częstotliwość audytów i testów zabezpieczeń</i>	62
<i>Procedury raportowania postępów zarządowi</i>	62
<i>Mechanizmy zapewniające ciągłe doskonalenie strategii i procedur</i>	62
Wyciąganie wniosków i doskonalenie	63
<i>Wnioski z dotychczasowych działań i obszary wymagające poprawy</i>	63
<i>Działania zwiększające świadomość pracowników na temat zagrożeń</i>	63
<i>Procedury reagowania na podejrzone aktywności w przyszłości</i>	63
Przykładowy plan strategii	63
Pytania dla menedżera dotyczące strategii	64
Kluczowe prompty do AI	66
<i>Tworzenie kompleksowej strategii ochrony</i>	66
<i>Analiza aktualnych zagrożeń cybernetycznych</i>	66
<i>Wdrożenie strategii ochrony</i>	67
<i>Integracja strategii ochrony z innymi procesami</i>	67
<i>Monitorowanie skuteczności strategii ochrony</i>	67

ROZDZIAŁ 7. MAPOWANIE RYZYKA 68

Identyfikacja i analiza ryzyka	68
Proces mapowania ryzyka	68
Elementy, które mogą być wynikiem mapowania ryzyka	70
Przykładowy harmonogram wdrożenia mapowania ryzyka	71
Przykładowa tabela analizy ryzyka	72
Przykładowa lista ryzyk związanych z cyberbezpieczeństwem	74
Pytania menedżera do IT i osób odpowiedzialnych za zgodność dotyczące mapowania ryzyka	75

Spis treści

Kluczowe prompty do AI	76
<i>Identyfikacja zagrożeń cybernetycznych</i>	76
<i>Ocena ryzyka w cyberbezpieczeństwie</i>	76
<i>Priorytetyzacja ryzyk w organizacji</i>	76
<i>Tworzenie planu zarządzania ryzykiem</i>	77
<i>Monitorowanie i aktualizacja mapy ryzyka</i>	77
Ćwiczenie. Analiza ryzyka	77
ROZDZIAŁ 8. ŚRODKI ZABEZPIECZAJĄCE (TECHNICZNE, ORGANIZACYJNE, PROCESOWE)	82
Środki techniczne	83
<i>Przykłady środków technicznych</i>	83
Środki organizacyjne	84
<i>Przykłady środków organizacyjnych</i>	84
Środki procesowe	85
<i>Przykłady środków procesowych</i>	86
<i>Środki bezpieczeństwa jako usługa</i>	88
Model biznesowy środków bezpieczeństwa	90
Kluczowe pytania do menedżera dotyczące wyboru i wdrożenia środków zabezpieczających	91
Kluczowe prompty do AI	95
<i>Wybór odpowiednich środków technicznych</i>	95
<i>Zarządzanie organizacyjnymi środkami zabezpieczającymi</i>	95
<i>Procesy wspierające cyberbezpieczeństwo</i>	95
<i>Integracja środków zabezpieczających</i>	96
<i>Monitorowanie skuteczności środków zabezpieczających</i>	96
ROZDZIAŁ 9. SZKOLENIA I EDUKACJA PRACOWNIKÓW	97
Cel edukacji pracowników w kontekście cyberbezpieczeństwa	97
Sugerowany terminarz	104
Przykładowy podział na grupy	105

RANSOMWARE W AKCJI

Potencjalne sposoby przekazu	106
Potencjalne tematy	106
Sposoby oceny wiedzy	107
Pytania menedżera dotyczące szkoleń i edukacji	107
Kluczowe prompty do AI	108
<i>Tworzenie programów szkoleniowych z zakresu cyberbezpieczeństwa</i>	108
<i>Regularność i zakres szkoleń</i>	109
<i>Metody angażowania pracowników w szkolenia</i>	109
<i>Ocena skuteczności szkoleń</i>	109
<i>Dostosowanie szkoleń do zmieniających się zagrożeń</i>	109

ROZDZIAŁ 10. RADY POMAGAJĄCE PRZECIWDZIAŁAĆ ATAKOWI TYPU RANSOMWARE 110

Zmniejsz prawdopodobieństwo, że złośliwa zawartość dotrze do Twoich sieci	111
Kluczowe prompty do AI	111
<i>Skuteczne środki zapobiegawcze przeciw ransomware'owi</i>	111
<i>Edukacja pracowników w zakresie ransomware'u</i>	111
<i>Monitorowanie i wykrywanie zagrożeń typu ransomware</i>	112
<i>Przygotowanie firmy na potencjalny atak ransomware</i>	112
<i>Odzyskiwanie danych po ataku ransomware</i>	112

ROZDZIAŁ 11. KOPIE ZAPASOWE 113

Reguła 3-2-1	114
Zasada backupu 3-2-1-1-0	114
Parametry RTO i RPO	114
<i>RPO (Recovery Point Objective)</i>	114
<i>RTO (Recovery Time Objective)</i>	115
Przykład zasady backupu 3-2-1-1-0 dla firmy usługowej z 200 pracownikami	115
<i>Elementy zasady 3-2-1-1-0</i>	115
<i>Przykładowa implementacja dla firmy usługowej</i>	116
Pytania menedżera o kopie zapasowe	117

Spis treści

Potencjalne odpowiedzi na pytania dla przykładowej firmy	118
<i>Kontekst przykładowej firmy</i>	118
<i>Potencjalne odpowiedzi na pytania dotyczące strategii tworzenia kopii zapasowych 3-2-1</i>	118
Kluczowe prompty do AI	121
<i>Tworzenie skutecznych kopii zapasowych</i>	121
<i>Reguła 3-2-1 dla kopii zapasowych</i>	121
<i>Odyskiwanie danych z kopii zapasowych</i>	121
<i>Automatyzacja tworzenia kopii zapasowych</i>	122
<i>Testowanie kopii zapasowych</i>	122
ROZDZIAŁ 12. KATEGORYZACJA DANYCH	123
Klucz do efektywnej strategii DRP i RTO	123
Przykładowe kategoryzacje danych z uwzględnieniem RTO, RPO i polityk backupowych	124
Współpraca z działami biznesowymi w zakresie kategoryzacji danych	126
Przykładowy harmonogram kategoryzacji danych	126
Kluczowe pytania biznesowe dotyczące kategoryzacji danych	127
Kluczowe prompty do AI	128
<i>Tworzenie kategorii danych</i>	128
<i>Zarządzanie ryzykiem związanym z danymi</i>	128
<i>Wdrożenie polityki kategoryzacji danych</i>	128
<i>Monitorowanie i aktualizacja kategorii danych</i>	129
<i>Integracja kategoryzacji danych z innymi procesami</i>	129
ROZDZIAŁ 13. BUSINESS IMPACT ANALYSIS (BIA) – ANALIZA WPŁYWU NA BIZNES	130
Kluczowe informacje o BIA	131
Kluczowe pytania dla menedżera dotyczące BIA	131
Kluczowe prompty do AI	132
<i>Przeprowadzenie analizy BIA</i>	132
<i>Ocena ryzyka i jego wpływu na biznes</i>	132

RANSOMWARE W AKCJI

<i>Zarządzanie wynikami BIA</i>	133
<i>Integracja analizy BIA z innymi procesami</i>	133
<i>Aktualizacja i monitorowanie BIA</i>	133

ROZDZIAŁ 14. BUSINESS CONTINUITY PLANNING (BCP) I DISASTER RECOVERY PLANNING (DRP) **134**

Business Continuity Planning (BCP)	134
Disaster Recovery Planning (DRP)	134
Spodziewane wyniki dotyczące BCP i DRP	135
Przykładowy harmonogram wdrożenia polityk BCP i DRP	135
Pytania działów biznesowych do działów IT i zgodności	137
Kluczowe prompty do AI	138
<i>Tworzenie planu BCP</i>	138
<i>Wdrażanie DRP w organizacji</i>	138
<i>Ocena gotowości planów BCP i DRP</i>	138
<i>Testowanie i aktualizacja planów BCP i DRP</i>	139
<i>Integracja BCP i DRP z ogólną strategią firmy</i>	139

ROZDZIAŁ 15. REAGOWANIE NA INCYDENT: KLUCZOWE KROKI DLA FIRMY **140**

Co robić po ataku?	141
Przykładowa lista kroków	142
Kluczowe pytania, aby menedżer mógł skutecznie ocenić gotowość firmy na reagowanie na incydenty	145
Kluczowe prompty do AI	147
<i>Kluczowe kroki reagowania na incydent</i>	147
<i>Ocena gotowości firmy na incydenty</i>	147
<i>Wdrożenie planu reagowania na incydent</i>	148
<i>Szkolenie zespołów reagowania na incydenty</i>	148
<i>Minimalizacja skutków incydentów</i>	148

ROZDZIAŁ 16. ZGODNOŚĆ Z NORMAMI, WYTYCZNYMI, DOBRYMI PRAKTYKAMI **149**

Najważniejsze standardy i normy	152
<i>RODO (rozporządzenie o ochronie danych osobowych)</i>	152
<i>ISO/IEC 27001</i>	153
<i>NIST Cybersecurity Framework (NIST CSF)</i>	153
<i>NIST SP 800-53</i>	153
<i>CIS Controls</i>	153
<i>NIS2</i>	153
<i>DORA (Digital Operational Resilience Act)</i>	154
<i>Ustawa o krajowym systemie cyberbezpieczeństwa (UoKSC)</i>	154
Kluczowe prompty do AI	154
<i>Aktualne normy i wytyczne w cyberbezpieczeństwie</i>	154
<i>Ocena zgodności firmy z najlepszymi praktykami</i>	154
<i>Wdrażanie zgodności z normami w organizacji</i>	155
<i>Zarządzanie ryzykiem w kontekście zgodności z normami</i>	155
<i>Monitorowanie i raportowanie zgodności</i>	155

ROZDZIAŁ 17. PODSUMOWANIE I WNIOSKI **156**

Przykładowe mierniki działań ochronnych	156
Pytania menedżera o mierniki i doskonalenie	158
Kluczowe prompty do AI	159
<i>Kluczowe wnioski dla cyberbezpieczeństwa firmy</i>	159
<i>Wnioski dotyczące skuteczności obecnych strategii</i>	159
<i>Sugestie dalszych kroków w zakresie cyberbezpieczeństwa</i>	159

ROZDZIAŁ 18. PROPOZYCJA ĆWICZEŃ SYMULACYJNYCH **160**

Ćwiczenie 1. Symulacja reagowania na incydenty bezpieczeństwa w firmie	160
<i>Instrukcja przeprowadzenia symulacji</i>	161
<i>Przykładowe scenariusze</i>	162

RANSOMWARE W AKCJI

Ćwiczenie 2. Mapowanie ryzyka	164
<i>Kontekst</i>	164
<i>Cel ćwiczenia</i>	164
<i>Zadania</i>	164
<i>Pytania do uczestników</i>	165
Ćwiczenie 3. Wyciek danych z firmy	165
<i>Kontekst</i>	165
<i>Pytania</i>	165
Ćwiczenie 4. Zaszyfrowanie strony	166
<i>Kontekst</i>	166
<i>Pytania</i>	166
Ćwiczenie 5. Atak na systemy SCADA/ICS	167
<i>Kontekst</i>	167
<i>Cel ćwiczenia</i>	167
<i>Pytania</i>	167
Ćwiczenie 6. Zaszyfrowanie danych	169
<i>Kontekst</i>	169
<i>Pytania</i>	169
Ćwiczenie 7. Przejęcie kont administratorów	170
<i>Kontekst</i>	170
<i>Pytania</i>	170
DODATEK A. ELEMENTY DO DAŁSZEJ PRACY W FIRMIE	173
DODATEK B. SŁOWNIK PODSTAWOWYCH POJĘĆ	175
DODATEK C. ŹRÓDŁA	181
DODATEK D. O AUTORZE	183

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

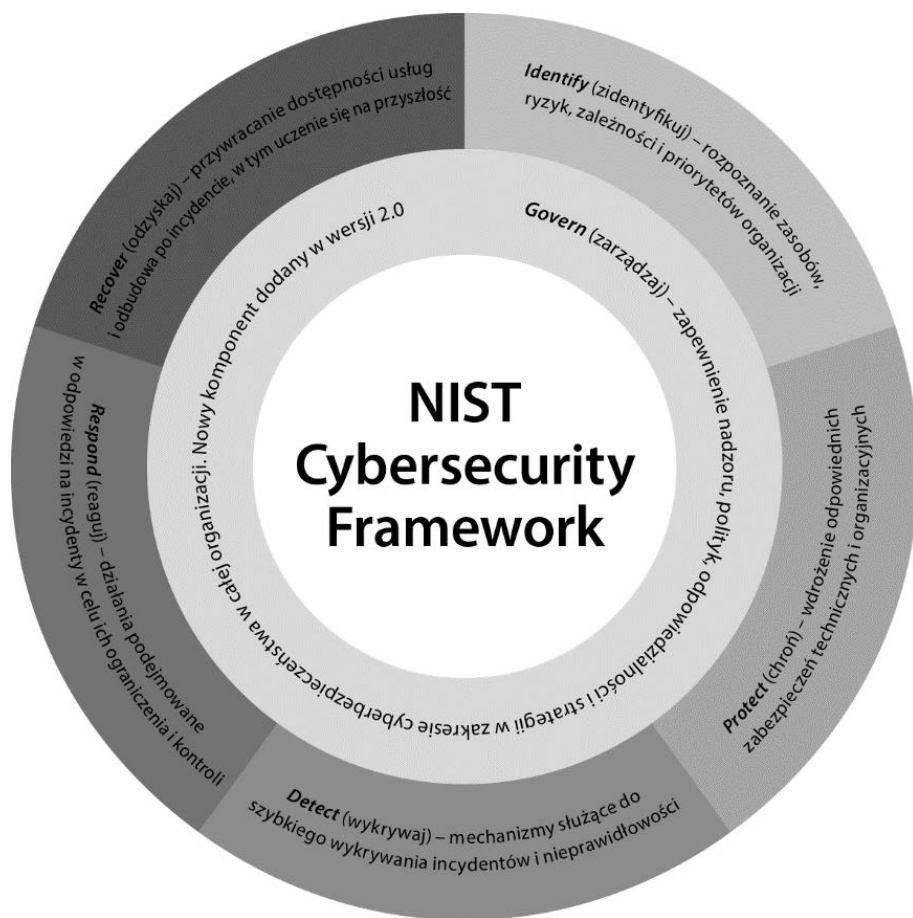
Protect (chronić) — wdrożenie odpowiednich zabezpieczeń technicznych i organizacyjnych

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

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

Reagowanie na incydent: kluczowe kroki dla firmy

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



RYSUNEK 15.1. Kluczowe kroki w radzie 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.

RANSOMWARE W AKCJI

- 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 ostrzeżenie.

- 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 incydem, 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 incydom.
- 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?

Reagowanie na incydent: kluczowe kroki dla firmy

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”.

PROGRAM PARTNERSKI

— GRUPY HELION —



1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA
Helion

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



KOD KORZYŚCI
Siegij po więcej! ▶





helion.pl



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

ISBN 978-83-289-2922-7



9 788328 929227

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.

