Metody tworzenia firmy odpornej na cyberprzestępcę i ataki typu **ransomware**

Autor Artur Markiewicz

Metody tworzenia firmy odpornej na cyberprzestępcę i ataki typu **ransomware**

Autor Artur Markiewicz

Spis treści

Spis tabel

Spis rysunków

Licencja

📅 **Data publikacji:** 23.02.2025

I. Wstęp

Twoi ludzie nie są winni temu, że firma nie jest bezpieczna.

Szukanie winnych u ludzi to ślepa uliczka.

Winne są procesy lub ich brak.

Winny jest poziom wiedzy i ścieżki jej zdobywania.

Winna jest trójka: lenistwo, niekompetencja, pazerność.

Lenistwo to robienie czegoś najkrótszą drogą, żeby było widać efekt. To zaniechanie robienie czegoś innego. W zakresie cyberbezpieczeństwa to nie stosowanie się do procedur, do dobrych praktyk. To ignorowanie czerwonych flag, które powiewają w komunikacie przestępcy. To także prokrastynacja, czekanie na mityczny poniedziałek, żeby zacząć coś robić.

Niekompetencja nie wynika z człowieka, a z deficytu wiedzy. Ludzie unikają wiedzy, bo wymaga uczenia się czegoś nowego (**lenistwo**).

To także brak szerokiego myślenia, ograniczanie się do wycinka, w którym człowiek czuje się dobrze. W zakresie cyberbezpieczeństwa zrobienie jednej rzeczy dobrze nie oznacza, że cały łańcuch będzie wytrzymały. Niekompetencja ma swoje źródło w galopującej rzeczywistości, gdzie czasem trudno jest nadrobić braki wiedzy. Materia do zrozumienia jest spora, a każdy punkt łączy się, zależy od czegoś innego.

Wiedza niezbędna do zapewnienia poziomu cyberbezpieczeństwa nie towarzyszyła nam w naturalnej ścieżce edukacji (do teraz nie

towarzyszy).

Pazerność to apetyty na duże zyski małym wysiłkiem energetycznym. To towarzyszy przestępcy. Ma on relatywnie wysoki zwrot z inwestycji przy bardzo mały wkładzie pracy.

Firmy, systemy, ludzie są słabo zabezpieczeni (**niekompetencja**), nie przestrzegają zasad (**lenistwo**), co daje bardzo nisko wiszące owoce.

Łatwiej może być kogoś okraść (okup z ataku ransomware) niż podobne pieniądze zarobić w legalny sposób.
Firmy często zdobywają nowe rynki w bardzo agresywny sposób, nie uwzględniając potrzeby cyberbezpieczeństwa takich operacji.

Każdy nowy proces, każda zmiana potrzebuje dostosowania środków bezpieczeństwa. W praktyce to dynamiczna analiza zagrożeń.

Dowolne proporcje tych zjawisk, tworzą przestrzeń, która jest, na którą można nałożyć dobre praktyki i podnieść poziom bezpieczeństwa.

Ludzie branży cyberbezpieczeństwa, specjaliści infoSEC, są od tego, żeby być tuż przed firmą i odgarniać zagrożenia, które są znane i przewidywalne. Są niczym **pług śnieżny**, który jest tuż przed pociągiem pędzącym swoim torem w śnieżną pogodę.

Maszynista, pasażerowie nie odpowiadają za to, że śnieg pada, nie mają na niego wpływu. Jak zignorują i nie zrobią z tym nic, nie dojadą do celu. Ludzie branży są od tego, żeby owe **przeszkody usuwać z drogi** firmy.

Te przeszkody tam są.

Przestępcy są, działają, mają swoje sposoby i techniki.

Korzystają z luk, niedoskonałości, błędów, ignorancji, lenistwa, niekompetencji ludzi, firm, technologii.

Nie mamy wpływu na ich motywację, **mamy wpływ na** to co z tym zrobimy.

O tym jest ten poradnik.

Wiele poradników powstało po to by były, by je wypchnąć na rynek, zarobić, zrobić i zapomnieć.

Chciałbym, żeby ten poradnik był stosowany i manager mógł do niego wracać.

Treść pisałem tak by była uniwersalna w kontekście tego co jest dziś i co da się przewidzieć w przyszłości :)

Fundamenty powstały na bazie moich doświadczeń, dokumentów, z którymi pracuję.

Zagadnienia merytoryczne są opisane spłyconym językiem.

Nie jest odbiorcą poradnika specjalista inżynier, lecz specjalista, który chce by procesy biznesowe, dane w firmie były bezpieczne.

Manager opiekujący się biznesem nie może dziś ignorować cyberbezpieczeństwa, traktować go jako zła koniecznego.

Zaopiekowanie się tematach ochrony biznesu jest elementem odpowiedzialności za biznes.

Obowiązkiem jest wiedzieć kto wie więcej, kto co zrobił i co planuje robić.

Obowiązkiem jest narzucić kierunek.

Obowiązkiem jest wiedzieć co ma być chronione.

Deficyty wiedzy o tym jak się coś chroni jest zrównoważony właściwymi pytaniami, nadaniem kierunku i przekazaniem obszaru do specjalistów.

To co będzie pokryte środkami bezpieczeństwa zależy od analizy ryzyka i odpowiedzi co i przed czym chronić.

Poradnik był pisany w kontekście ochrony przed atakami ransomware, które mają swoja specyfikę, ale dokładnie te same rady mogą jednocześnie chronić przed wieloma innymi źródłami problemów.

Stawiam zawsze na profilaktykę, która rozpoczyna się od takich materiałów. Przygotowanie się na przewidywalne zagrożenia to analiza ryzyka, stosowanie odpowiednich zabezpieczeń.

Te zagrożenia, które nie były bezpośrednio analizowane najczęściej mogą być pokryte posiadanymi zabezpieczeniami, a nawet jeśli nie, to drogą, którą przebyła organizacja pomoże i będzie wsparciem w

reagowaniu na to co nie było przewidziane.

Nawet w najczarniejszym scenariuszu może być moment zapanowania nad konsekwencjami, opanowaniem sytuacji i wyciągnięciem z niej lekcji.

Zarządzanie kryzysowe, procedury przywracania, plan ciągłości działanie, ciągłe doskonalenie będą pomocne w wielu sytuacjach.

Najgorsza sytuacja to bycie w mitycznym, życzeniowym, myśleniu, że nam się nic nie stanie, ataki nas nie spotkają, a nawet jeśli to nie mamy nic do stracenia.

Pytania:

1. *Czy będziemy zaatakowani?*

2. Kiedy będziemy zaatakowani?

Nie mają znaczenia, bo kiedyś będziemy.

Inne kolejne pytania są ważniejsze:
3. Skąd będziemy wiedzieli, że jesteśmy zaatakowani?

4. Co wówczas zrobimy?

Pomocny w udzieleniu odpowiedzi na te pytania jest ten poradnik.

Od odpowiedzi co to ten atak ransomware, poprzez możliwe konsekwencje, studium przypadków, taktyk przestępców, role zarządu i co powinni wiedzieć, przez mapowanie ryzyk, środki zabezpieczające, rolę szkoleń, kopie zapasowe, kategoryzację danych, na planie ciągłości działania i sposobie reagowania na incydenty kończąc.

Dodatkowo słownik, sugestie innych działań i źródła wiedzy.

Poradnik możesz czytać po kolei, wybranymi rozdziałami lub pytaniami managera co do zakresu (najczęściej ostatni punkt rozdziału).

W poradniku znajdziesz także prompty do AI (model językowy, "sztuczna inteligencja") czyli narzędzia, które może być twoim źródłem aktualnej wiedzy.

II. Korzystanie z AI do efektywnego wykorzystania z tego poradnika

Wprowadzenie promptów AI do tego poradnika ma na celu zwiększenie samodzielności managerów w obszarze cyberbezpieczeństwa oraz ułatwienie pracy z przedstawionymi tu materiałami. Prompty te zostały zaprojektowane tak, aby wspierać managerów w budowaniu kontekstu, znajdowaniu najlepszych rad, wytycznych oraz sposobów stosowania środków bezpieczeństwa w ich firmach.

Kluczowe założenia:

- **AI nie zna tego poradnika**: Wszystkie prompty są skonstruowane tak, aby AI korzystała z najnowszej, sprawdzonej wiedzy dostępnej w jej bazie danych, a nie z treści poradnika. Zapewnia to, że generowane odpowiedzi są aktualne, rzetelne i dostosowane do bieżących standardów oraz praktyk w obszarze cyberbezpieczeństwa.
- **Podawanie źródeł**: Każda odpowiedź generowana przez AI powinna zawierać odniesienie do źródeł, z których pochodzi informacja. Dzięki temu managerowie mogą być pewni, że otrzymują dane oparte na sprawdzonych i wiarygodnych informacjach, co jest kluczowe w podejmowaniu decyzji związanych z bezpieczeństwem firmy.
- **Budowanie kontekstu**: Prompty są zaprojektowane tak, aby pomagały managerom w tworzeniu kontekstu specyficznego dla ich firmy. Dzięki temu możliwe jest lepsze dostosowanie strategii i działań do unikalnych potrzeb organizacji, co zwiększa skuteczność wdrożonych środków ochronnych.

Aby ułatwić tworzenie spersonalizowanych promptów, które będą odpowiadały na konkretne potrzeby Twojej firmy, proponujemy skorzystanie z poniższego Master Promptu. To narzędzie pozwoli Ci na budowanie kolejnych promptów, które AI będzie mogła wykorzystać do generowania szczegółowych rekomendacji i odpowiedzi.

Master Prompt:

```
"Używając najnowszych i sprawdzonych informacji dostępnych w
Twojej bazie danych, pomóż mi zbudować listę szczegółowych
promptów do AI, które dostosują pytania, strategie ochrony
oraz studium przypadków do specyfiki mojej firmy w branży
[branża]. Jestem managerem, który nie jest ekspertem
technicznym, więc proszę o podanie odpowiedzi w sposób
zrozumiały, unikając nadmiernie technicznego języka. Proszę
również o podanie źródeł, na których opierają się te
odpowiedzi, oraz uwzględnienie najlepszych praktyk w
obszarze cyberbezpieczeństwa."
```

Struktura Dokumentu i Gdzie Znaleźć Prompty

W całym dokumencie znajdziesz różne sekcje, w których umieszczone zostały prompty AI. Są one dostosowane do poszczególnych tematów, takich jak:

- **Kluczowe pytania dla managera**: W każdej sekcji zawierającej kluczowe pytania znajdziesz prompt, który pomoże Ci dostosować te pytania do specyfiki Twojej firmy. AI wygeneruje odpowiedzi oparte na najnowszej wiedzy, uwzględniając źródła, z których ta wiedza pochodzi.
- **Studium przypadków**: Każde studium przypadku zawiera prompt, który pomoże Ci przenieść lekcje z analizowanych przypadków na grunt Twojej organizacji. AI dostarczy wskazówki, jak dostosować wnioski do Twojej branży, korzystając z aktualnych informacji i najlepszych praktyk.
- **Strategie ochrony i reagowania na incydenty**: W tych rozdziałach znajdziesz prompty wspierające tworzenie lub optymalizację strategii ochrony, bazując na najlepszych dostępnych praktykach. AI pomoże w dostosowaniu tych strategii do specyficznych wymagań Twojej firmy, jednocześnie podając źródła, na których się opiera.

Każdy z tych promptów, podobnie jak Master Prompt, zakłada, że AI nie ma dostępu do tego konkretnego poradnika, ale korzysta z najnowszych i sprawdzonych informacji, zawsze podając źródła, na których się opiera. Dzięki temu możesz być pewien, że otrzymane rekomendacje są aktualne i wiarygodne, co pozwala na ich efektywne wdrożenie w Twojej firmie.

III. Co to jest atak typu Ransomware

Przewaga konkurencyjna dzięki inwestycjom w cyberbezpieczeństwo

W dzisiejszym dynamicznie zmieniającym się środowisku biznesowym, cyberbezpieczeństwo stało się kluczowym elementem budowania przewagi konkurencyjnej.

Firmy, które inwestują w zaawansowane środki ochrony przed cyberzagrożeniami, zyskują nie tylko bezpieczeństwo swoich danych, ale także zaufanie klientów i partnerów biznesowych.

W dobie rosnącej liczby ataków ransomware i innych zagrożeń, klienci coraz częściej wybierają firmy, które mogą zagwarantować im bezpieczeństwo ich danych. Inwestycje w cyberbezpieczeństwo przekładają się na większą lojalność klientów, co w efekcie prowadzi do wzrostu przychodów i umocnienia pozycji rynkowej.

Wsparcie zewnętrzne jako klucz do skutecznej ochrony

Wdrożenie skutecznych środków ochrony przed cyberzagrożeniami może być skomplikowane i wymagać specjalistycznej wiedzy. Dlatego warto skorzystać z usług zewnętrznych ekspertów i firm specjalizujących się w cyberbezpieczeństwie. Profesjonalne firmy oferują szeroki zakres usług, od audytów bezpieczeństwa, przez testy penetracyjne, aż po zarządzanie incydentami i odzyskiwanie danych.

Dzięki wsparciu zewnętrznych ekspertów, organizacje mogą szybko i skutecznie wdrożyć niezbędne środki ochrony, minimalizując ryzyko ataków i ich potencjalne konsekwencje. Współpraca z doświadczonymi partnerami w zakresie cyberbezpieczeństwa pozwala firmom skupić się na swojej podstawowej działalności, jednocześnie mając pewność, że ich dane są chronione na najwyższym poziomie.

Atak typu ransomware to rodzaj cyberprzestępstwa, w którym złośliwe oprogramowanie (ransomware) infekuje komputer lub sieć, blokując dostęp do systemów lub danych poprzez szyfrowanie ich.

Celem atakującego jest **wymuszenie od ofiary okupu** w zamian za klucz deszyfrujący, który umożliwi odzyskanie dostępu do zasobów.

Ransomware może przenikać do systemu za pośrednictwem różnych metod, takich jak phishingowe e-maile zawierające zainfekowane załączniki, luki w zabezpieczeniach oprogramowania, złośliwe reklamy na stronach internetowych lub zainfekowane urządzenia USB.

Po skutecznym zainfekowaniu systemu ransomware zaczyna szyfrować pliki użytkownika, zmieniając ich rozszerzenia i **uniemożliwiając do nich dostęp**. W momencie, gdy proces szyfrowania jest zakończony, ofiara otrzymuje wiadomość z żądaniem okupu, zwykle w formie kryptowaluty, takiej jak Bitcoin, która zapewnia anonimowość transakcji.

W wiadomości często znajdują się instrukcje dotyczące płatności oraz groźby, że jeśli **okup nie zostanie zapłacony w określonym czasie, klucz deszyfrujący zostanie zniszczony, co spowoduje utratę danych na zawsze**.

Dodatkowo przestępcy grożą ujawnieniem pozyskanych danych.

Oprócz tradycyjnych ataków ransomware, które polegają na szyfrowaniu danych i żądaniu okupu za ich odszyfrowanie, coraz częściej pojawiają się bardziej złożone i groźne formy tego cyberprzestępstwa.

W atakach typu "doxware" lub "leakware" przestępcy nie tylko blokują dostęp do danych, ale także **grożą ich ujawnieniem lub sprzedażą** wrażliwych informacji, jeśli okup nie zostanie zapłacony.

Ten rodzaj ataku jest szczególnie niebezpieczny dla firm przechowujących poufne dane klientów, dane medyczne, informacje finansowe czy tajemnice handlowe.

Groźba publicznego ujawnienia takich informacji może prowadzić do ogromnych strat reputacyjnych, prawnych i finansowych, które mogą znacznie przewyższyć koszty samego okupu.

Tego rodzaju ataki podkreślają znaczenie kompleksowej ochrony danych i systemów oraz konieczność szybkiego i zdecydowanego reagowania na incydenty.

Skutki ataku ransomware mogą być katastrofalne dla ofiar, w tym przedsiębiorstw, instytucji publicznych oraz osób prywatnych.

Oprócz bezpośrednich strat finansowych związanych z opłatą okupu, ofiary mogą ponieść dodatkowe koszty związane z przestojami operacyjnymi, przywracaniem systemów, analizą śledczą oraz wzmocnieniem zabezpieczeń, aby zapobiec przyszłym atakom.

Ponadto, atak ransomware może prowadzić do utraty reputacji oraz zaufania klientów, co ma długoterminowe negatywne skutki dla działalności organizacji.

Dlatego tak ważne jest wdrażanie skutecznych środków zapobiegawczych i edukowanie użytkowników na temat zagrożeń cyberbezpieczeństwa.

Pochodzenie: ransom - okup, ware - końcówka od "software" czyli oprogramowanie - oprogramowanie służące do wyłudzania okupu.

Konsekwencje ataku typu Ransomware:

Konsekwencje operacyjne:

- Zatrzymanie działania firmy;
- Zakłócenie działalności operacyjnej;
- Utrata lub zaszyfrowanie krytycznych danych;

- Ujawnienie i wyciek poufnych informacji;
- Koszty związane z odzyskiwaniem danych;

Konsekwencje finansowe:

- Wymuszenie okupu;
- Utrata przychodów;
- Wzrost kosztów ubezpieczenia cyberbezpieczeństwa;
- Spadek wartości rynkowej firmy;
- Kary finansowe i zwiększenie kontroli regulacyjnych;

Konsekwencje reputacyjne:

- Utrata reputacji;
- Utrata zaufania klientów;
- Zagrożenie przyszłej współpracy z partnerami;

Konsekwencje prawne:

- Potencjalne działania prawne;

Przeciwdziałanie:

- Postępowanie wg procedur;
- Korzystanie z dobrych praktyk;
- Aktualizacja systemów;
- Szkolenia.

Przeciwdziałanie opiera się na wielu elementach, które sprowadzają się do postępowania wg procedur, korzystania z dobrych praktyk, aktualizacji systemów, szkoleniach.

Pytania managera dotyczące konsekwencji ataku typu ransomware:

1. Konsekwencje operacyjne
   1.1. Jakie mogą być skutki zatrzymania działania firmy w wyniku ataku ransomware?
   1.2. W jaki sposób atak ransomware może zakłócić naszą działalność operacyjną?
   1.3. Jakie krytyczne dane mogą zostać utracone lub zaszyfrowane w wyniku ataku?
   1.4. Jakie poufne informacje mogą zostać ujawnione lub wycieknięte w wyniku ataku?
   1.5. Jakie będą koszty związane z odzyskiwaniem danych po ataku ransomware?
2. Konsekwencje finansowe
   2.1. Jakie mogą być koszty wymuszenia okupu przez cyberprzestępców?

Szkolenia i edukacja pracowników

Opis

Regularne szkolenia z cyberbezpieczeństwa mają na celu zwiększenie świadomości pracowników i zapobieganie błędom, które mogą prowadzić do ataków ransomware. Szkolenia powinny łączyć teorię z praktyką, pomagając pracownikom rozpoznawać i unikać zagrożeń, takich jak phishing czy złośliwe oprogramowanie, oraz je zgłaszać.
Działy IT, kierownictwo organizacji powinny patrzeć holistycznie, uwzględniać najlepsze praktyki.

Cel edukacji pracowników w kontekście cyberbezpieczeństwa

Edukacja pracowników w zakresie cyberbezpieczeństwa ma na celu zwiększenie odporności organizacji na zagrożenia, takie jak ataki typu ransomware; W zależności od grupy docelowej, cele edukacji różnią się pod względem obszarów wiedzy, nawyków, umiejętności, stosowania procedur oraz zdolności do działania proaktywnego i reaktywnego;

1. Pracownicy
   1.1. Obszar wiedzy:
      1.1.1. Cel: Zapewnienie podstawowej wiedzy na temat zagrożeń i metod ochrony, takich jak rozpoznawanie phishingu i innych prób oszustwa;
      1.1.2. Cel: Zrozumienie jak działają cyberprzestępcy, jakie mają cele i sposoby;
      1.1.3. Cel: Przegląd przykładów kampanii przestępczych;
      1.1.4. Cel: Zrozumienie, jakie rodzaje danych są najbardziej narażone na ataki i dlaczego ich ochrona jest kluczowa dla organizacji;
      1.1.5. Cel: Znajomość regulacji prawnych dotyczących ochrony danych oraz konsekwencji prawnych i finansowych wynikających z ich naruszenia;
   1.2. Nawyki:
      1.2.1. Cel: Wyrabianie nawyków bezpiecznego korzystania z systemów informatycznych, np. stosowanie różnych haseł do różnych usług, unikania klikania w podejrzane linki;
      1.2.2. Cel: Zbudowanie nawyków pozwalających określić co jest podejrzane;
      1.2.3. Cel: Zgłaszanie zdarzeń, które mogą wywołać negatywny wpływ na firmę;
      1.2.4. Cel: Utrwalanie nawyku regularnego sprawdzania autentyczności e-maili i komunikatów, zanim podejmie się jakiekolwiek działania;
   1.3. Umiejętności:
      1.3.1. Cel: Umożliwienie pracownikom skutecznego korzystania z narzędzi firmowych, takich jak rozwiązania związane z uwierzytelnianiem wieloskładnikowym i systemy do zarządzania hasłami;
      1.3.2. Cel: Szkolenie pracowników w zakresie korzystania z narzędzi do szyfrowania danych i komunikacji;
      1.3.3. Cel: Rozwój umiejętności rozpoznawania prób socjotechnicznych i innych form inżynierii społecznej stosowanej przez cyberprzestępców;
   1.4. Stosowanie i budowanie procedur:

1.4.1. Cel: Zrozumienie i przestrzeganie firmowych polityk bezpieczeństwa oraz umiejętność zgłaszania podejrzanych zdarzeń;
1.4.2. Cel: Umiejętność identyfikowania luk w aktualnych procedurach bezpieczeństwa i proponowania ulepszeń;
1.4.3. Cel: Zdolność do koordynacji działań z innymi zespołami w firmie, aby zapewnić, że polityki bezpieczeństwa są jednolicie stosowane i aktualizowane;

1.5. Działania proaktywne:
1.5.1. Cel: Motywowanie pracowników do aktywnego monitorowania potencjalnych zagrożeń i zgłaszania ich zespołowi IT;
1.5.2. Cel: Podkreślenie, że cyberbezpieczeństwo to odpowiedzialność każdego pracownika, a nie tylko zespołu IT;
1.5.3. Cel: Współpraca z działem IT nakierowana na budowanie propracowniczych procedur wspierających ich pracę i jednocześnie zapewniających odpowiedni poziom cyberbezpieczeństwa;
1.5.4. Cel: Angażowanie się w regularne szkolenia i aktualizowanie wiedzy na temat nowych zagrożeń i metod ochrony;
1.5.5. Cel: Zachęcanie pracowników do zgłaszania podejrzanych zachowań i zdarzeń, nawet jeśli nie mają pewności co do ich charakteru;

1.6. Umiejętności reagowania:
1.6.1. Cel: Przygotowanie pracowników do szybkiej reakcji na incydenty, takie jak wyciek danych, poprzez odpowiednie zgłoszenie i podjęcie działań zgodnych z procedurami;
1.6.2. Cel: Szkolenie w zakresie szybkiego izolowania zagrożenia, aby minimalizować jego wpływ na organizację;
1.6.3. Cel: Przygotowanie do współpracy z działem IT oraz zespołem zarządzania kryzysowego w sytuacji incydentu, aby zapewnić skuteczne i szybkie rozwiązanie problemu;

2. Kierownictwo
2.1. Obszar Wiedzy:

Potencjalne sposoby przekazu

- Szkolenia stacjonarne: Warsztaty i prezentacje prowadzone przez specjalistów z zakresu cyberbezpieczeństwa;
- E-learning: Kursy online z interaktywnymi modułami, dostępne w dowolnym czasie;
- Webinary: Sesje na żywo z możliwością zadawania pytań i interakcji z prowadzącymi;
- Materiały informacyjne: Infografiki, ulotki i broszury dostarczane drogą elektroniczną lub w formie papierowej;
- Symulacje ataków: Praktyczne ćwiczenia, takie jak symulowane ataki phishingowe, które uczą rozpoznawania zagrożeń w rzeczywistych warunkach;
- Newslettery: Regularne wiadomości e-mail z poradami i aktualizacjami dotyczącymi cyberbezpieczeństwa;
- Filmy edukacyjne: Krótkie filmy instruktażowe ilustrujące kluczowe zasady i zagrożenia;
- Sesje Q&A: Regularne spotkania, podczas których pracownicy mogą zadawać pytania i rozwiewać wątpliwości dotyczące cyberbezpieczeństwa.

Potencjalne tematy

- Podstawy cyberbezpieczeństwa;
- Rozpoznawanie phishingu;
- Bezpieczne korzystanie z e-maila i internetu;
- Ochrona danych osobowych;
- Procedury zgłaszania incydentów;
- Bezpieczne zarządzanie hasłami.

Sposoby oceny wiedzy

- Testy online po szkoleniach;
- Symulacje phishingowe;
- Ankiety oceniające świadomość zagrożeń;
- Ocena zachowań pracowników w codziennej pracy.

Pytania managera dotyczące szkoleń i edukacji

1. Jakie są kluczowe cele projektu szkoleniowego?
2. Jakie grupy pracowników wymagają najbardziej intensywnych szkoleń?
3. Jakie narzędzia lub metody szkoleniowe będą najbardziej efektywne?
4. Jak monitorujemy postępy i skuteczność tych szkoleń?
5. Jakie są nasze plany na szkolenia odświeżające?
6. Kto będzie tworzył plany szkoleniowe?
7. O ile liczba zgłaszanych incydentów bezpieczeństwa zwiększyła się od czasu wprowadzenia szkoleń?
8. Jakie zmiany w środowisku pracy zostały zauważone po wdrożeniu programu szkoleniowego?

Rady pomagające przeciwdziałać na atak typu ransomware

1. Używaj oprogramowania antywirusowego przez cały czas;
2. Utrzymuj komputery i wszystkie elementy środowiska w pełni zaktualizowane;
3. Blokuj dostęp do stron z ransomware;
4. Zezwalaj tylko na autoryzowane aplikacje;
5. Ogranicz korzystanie z urządzeń prywatnych;
6. Używaj standardowych kont użytkowników;
7. Unikaj korzystania z aplikacji osobistych;
8. Uważaj na nieznane źródła;
9. Włącz drugi składnik logowania;
10. Ogranicz dostęp do zasobów za pośrednictwem sieci, zwłaszcza ograniczając RDP;
11. Testuj backupy;
12. Realizuj szkolenia.

Zmniejsz prawdopodobieństwo, że złośliwa zawartość dotrze do Twoich sieci.

1. Wyłącz środowiska skryptowe i makra;
2. Skonfiguruj swoje systemy tak, aby aktywnie sprawdzały zawartość. Zezwalaj tylko na określone typy plików, blokując witryny, aplikacje, protokoły itp., które są znane jako złośliwe;
3. Rozważ filtrowanie ruchu sieciowego, wdrożenie zasad monitorowania oraz blokowania nielegalnego lub złośliwego ruchu przed dotarciem do sieci;
4. Zaimplementuj reguły czarnej/białej listy oparte na kanałach analizy zagrożeń działających na żywo, aby uniemożliwić użytkownikom dostęp do złośliwych stron internetowych, złośliwych adresów IP, phishingowych adresów URL, anonimowych serwerów proxy, sieci Tor i innych usług anonimizacji, itp.

Kluczowe prompty do AI

Te prompty dla rozdziału "Rady Pomagające Przeciwdziałać Atakowi Typu Ransomware" mają na celu pomóc managerowi w opracowaniu i wdrożeniu strategii zapobiegania atakom ransomware, bazując na najnowszych i sprawdzonych informacjach.

Skuteczne środki zapobiegawcze przeciw ransomware

"Jako manager, chcę dowiedzieć się, jakie są najnowsze i najbardziej skuteczne środki zapobiegawcze, które moja firma może wdrożyć, aby uniknąć ataku typu ransomware. Proszę o informacje poparte odpowiednimi źródłami."

Edukacja pracowników w zakresie ransomware

"Jak mogę jako manager skutecznie edukować pracowników na temat zagrożeń związanych z ransomware i sposobów zapobiegania takim atakom? Proszę o aktualne materiały edukacyjne i źródła, które można wykorzystać."

Monitorowanie i wykrywanie zagrożeń ransomware

"Jakie są najlepsze praktyki w zakresie monitorowania i wykrywania zagrożeń typu ransomware w mojej firmie? Proszę o aktualne narzędzia i źródła potwierdzające ich skuteczność."

Przygotowanie firmy na potencjalny atak ransomware

"Jak mogę jako manager przygotować firmę na potencjalny atak ransomware, aby zminimalizować jego skutki? Proszę o zalecenia i źródła dotyczące najnowszych strategii przygotowawczych."

Odzyskiwanie danych po ataku ransomware

"Jakie są najlepsze praktyki w zakresie odzyskiwania danych po ataku ransomware? Jako manager, chciałbym otrzymać aktualne informacje na ten temat, poparte odpowiednimi źródłami."

Pytania managera o kopie zapasowe

Oto kilka pytań biznesowych, które manager może zadać zespołom IT na temat strategii tworzenia kopii zapasowych 3-2-1

1. Kto jest odpowiedzialny za zarządzanie i nadzorowanie całego procesu tworzenia kopii zapasowych?
2. Kto wykonuje poszczególne operacje związane z tworzeniem, przechowywaniem i testowaniem kopii zapasowych, i jakie są ich obowiązki?
3. Jak często są wykonywane kopie zapasowe w ramach strategii 3-2-1 i jak szybko możemy przywrócić dane w przypadku incydentu?
4. Jakie procesy zapewniają, że przynajmniej jedna kopia zapasowa jest przechowywana poza siedzibą firmy lub w chmurze, a także jak weryfikujemy integralność i dostępność tych kopii?
5. Czy wszystkie krytyczne dane biznesowe i systemy są objęte strategią 3-2-1, jak identyfikujemy te zasoby oraz jak strategia ta integruje się z naszym planem DRP?
6. Jakie środki są podejmowane w celu ochrony kopii zapasowych przed naruszeniami bezpieczeństwa, w tym ransomware?
7. Jak często testujemy kopie zapasowe, aby upewnić się, że mogą być skutecznie przywrócone w sytuacji awaryjnej, i jakie są koszty utrzymania oraz skalowania strategii 3-2-1?
8. Jakie ryzyka mogą zakłócić naszą strategię 3-2-1 i jak zapewniamy zgodność tej strategii z wymogami regulacyjnymi?
9. Jakie są nasze docelowe RPO (Recovery Point Objective) dla różnych systemów i danych oraz jak strategia 3-2-1 wspiera osiągnięcie tych celów?
10. Jak możemy współpracować, aby określić realistyczne RTO (Recovery Time Objective) dla kluczowych systemów, oraz jak strategia 3-2-1 może pomóc w spełnieniu tych oczekiwań?
11. Czy obecne procesy backupu są zgodne z naszymi założeniami dotyczącymi RPO i wspierają cele biznesowe dotyczące RTO, oraz jakie są plany ich optymalizacji?

Przykładowe mierniki działań ochronnych

1. Średni czas wykrycia (Mean Time to Detect, MTTD): Czas, jaki upływa od momentu rozpoczęcia ataku do jego wykrycia. Krótszy czas wykrycia oznacza szybszą reakcję na zagrożenia.
2. Średni czas reakcji (Mean Time to Respond, MTTR): Czas, jaki upływa od momentu wykrycia ataku do podjęcia działań naprawczych. Szybsza reakcja może zminimalizować szkody.
3. Liczba incydentów bezpieczeństwa: Całkowita liczba zgłoszonych i potwierdzonych incydentów bezpieczeństwa w określonym okresie. Mniejsza liczba incydentów może świadczyć o skuteczniejszych środkach ochrony.
4. Procent incydentów wykrytych wewnętrznie: Odsetek incydentów wykrytych przez wewnętrzne systemy monitorowania w porównaniu do tych zgłoszonych przez zewnętrzne źródła. Wyższy procent wykryć wewnętrznych może świadczyć o skuteczności systemów monitorowania.
5. Czas przestoju systemu: Łączny czas, przez jaki systemy były niedostępne z powodu incydentów bezpieczeństwa. Krótszy czas przestoju oznacza lepszą odporność systemów.
6. Koszt incydentów bezpieczeństwa: Całkowity koszt związany z incydentami bezpieczeństwa, w tym koszty naprawy, utraty danych, przestojów i potencjalnych kar. Niższe koszty mogą świadczyć o skuteczniejszych środkach ochrony.
7. Procent pracowników przeszkolonych w zakresie bezpieczeństwa: Odsetek pracowników, którzy przeszli szkolenia z zakresu cyberbezpieczeństwa. Wyższy procent przeszkolonych pracowników może zmniejszyć ryzyko incydentów wynikających z błędów ludzkich.
8. Phishing Click Rate (Wskaźnik kliknięć w phishing): Procent pracowników, którzy kliknęli w symulowane phishingowe e-maile podczas testów. Niższy wskaźnik oznacza wyższą świadomość zagrożeń.
9. Incident Reporting Rate (Wskaźnik zgłaszania incydentów): Liczba zgłoszonych incydentów bezpieczeństwa przez pracowników. Wyższy wskaźnik może świadczyć o większej czujności i świadomości zagrożeń.

10. Time to Report (Czas zgłoszenia): Średni czas, jaki upływa od momentu zauważenia incydentu do jego zgłoszenia. Krótszy czas oznacza szybszą reakcję na potencjalne zagrożenia.
11. Training Completion Rate (Wskaźnik ukończenia szkoleń): Procent pracowników, którzy ukończyli obowiązkowe szkolenia z zakresu cyberbezpieczeństwa. Ważne jest, aby nie tylko ukończyli szkolenie, ale także zrozumieli jego treść.
12. Knowledge Retention Rate (Wskaźnik retencji wiedzy): Procent pracowników, którzy zachowali wiedzę zdobytą podczas szkoleń, mierzony poprzez okresowe testy wiedzy. Wyższy wskaźnik oznacza skuteczniejsze szkolenia.
13. Reduction in Security Incidents (Redukcja incydentów bezpieczeństwa): Spadek liczby incydentów bezpieczeństwa po wdrożeniu programów szkoleniowych. To bezpośredni wskaźnik skuteczności szkoleń.
14. Employee Feedback (Opinie pracowników): Opinie pracowników na temat jakości i przydatności szkoleń, zbierane poprzez ankiety. Pozytywne opinie mogą świadczyć o skuteczności programów szkoleniowych.
15. Behavioral Change Rate (Wskaźnik zmiany zachowań): Procent pracowników, którzy zmienili swoje zachowania na bardziej bezpieczne po ukończeniu szkoleń. Może to być mierzone poprzez obserwacje i analizy zachowań pracowników przed i po szkoleniu.
16. Security Policy Adherence Rate (Wskaźnik przestrzegania polityki bezpieczeństwa): Procent pracowników, którzy przestrzegają polityk i procedur bezpieczeństwa po ukończeniu szkoleń. Wyższy wskaźnik oznacza lepsze zrozumienie i wdrożenie polityk bezpieczeństwa.
17. Simulated Attack Success Rate (Wskaźnik sukcesu symulowanych ataków): Procent symulowanych ataków, które zostały skutecznie zidentyfikowane i zneutralizowane przez pracowników. Niższy wskaźnik oznacza wyższą skuteczność szkoleń.

Te mierniki mogą pomóc w ocenie skuteczności działań związanych z cyberbezpieczeństwem i identyfikacji obszarów wymagających poprawy.

Pytania managera o mierniki i doskonalenie

1. Monitorowanie i raportowanie:
   1.1. Jakie metryki i wskaźniki wykorzystujemy do monitorowania skuteczności naszych działań ochronnych?
   1.2. Jak często raportujemy wyniki dotyczące bezpieczeństwa do wyższej kadry zarządzającej?
2. Ciągłe doskonalenie:

   2.1. Jakie procesy mamy wdrożone, aby stale doskonalić nasze podejście do ochrony przed ransomware?
   2.2. Jak zbieramy i analizujemy feedback od pracowników na temat naszych polityk i procedur bezpieczeństwa?

Odpowiedzi na te pytania pomogą managerowi lepiej zrozumieć obecną sytuację, zidentyfikować luki i obszary do poprawy oraz skutecznie wdrożyć i monitorować strategie ochrony przed ransomware w organizacji.

To tylko fragmenty...

Więcej w poradniku w pełnej wersji Patronite i BuyCoffee.to

Scenariusz 5: Przejęcie kont administratorów

Kontekst:

Firma padła ofiarą ataku, w wyniku którego atakujący przejęli konta administratorów. Atakujący uzyskali dostęp do sieci firmy poprzez wyłudzenie danych uwierzytelniających phishingową wiadomością e-mail kierującą na fałszywy panel logowania, a następnie eskalowali swoje uprawnienia.

Pytania:

Rozpoznanie ataku:

- Jakie sygnały wskazują na możliwy atak phishingowy?
- W jaki sposób zespół mógł wykryć próbę wyłudzenia danych uwierzytelniających?
- Czy w firmie istnieje procedura raportowania podejrzanych wiadomości e-mail? Jak została ona wdrożona?

Ochrona przed phishingiem:

- Jakie środki ochrony przed phishingiem są wdrożone w firmie?
- Czy pracownicy zostali odpowiednio przeszkoleni w zakresie rozpoznawania ataków phishingowych?
- Jakie techniczne mechanizmy są zastosowane, aby uniemożliwić użytkownikom dostęp do fałszywych stron logowania?

Eskalacja uprawnień:

- Jakie mechanizmy zapobiegania eskalacji uprawnień są zaimplementowane w firmie?
- Jakie kroki należy podjąć w przypadku wykrycia nieautoryzowanej eskalacji uprawnień?
- Jak często są przeprowadzane audyty uprawnień użytkowników, zwłaszcza kont administratorów?

Reakcja na incydent:

- Jakie działania podjęto, gdy zidentyfikowano przejęcie konta administratora?
- Czy zespół odpowiedzialny za reagowanie na incydenty miał dostęp do odpowiednich narzędzi i informacji, aby skutecznie zareagować na incydent?
- Jakie procedury zostały uruchomione w celu odcięcia atakującego od sieci?

Zarządzanie dostępem:

- Czy zasady zarządzania dostępem do kont administratorów były przestrzegane?
- Czy konta administratorów są chronione dodatkową warstwą zabezpieczeń, taką jak uwierzytelnianie wieloskładnikowe (MFA)?
- Jakie mechanizmy monitorowania dostępu do kont administratorów są wdrożone?

Komunikacja i eskalacja:

- Jakie kroki komunikacyjne zostały podjęte po zidentyfikowaniu incydentu?
- Jakie procedury eskalacji zostały uruchomione wewnątrz zespołu, aby natychmiast zaangażować odpowiednie osoby do rozwiązania problemu?
- Jakie informacje były przekazywane kierownictwu oraz innym zainteresowanym stronom w trakcie incydentu?

Zabezpieczenie i analiza post-mortem:

- Jakie środki zostały podjęte w celu zabezpieczenia dowodów cyfrowych po incydencie?
- Jakie działania naprawcze zostały zidentyfikowane po analizie incydentu?
- Czy przeprowadzono analizę przyczynową, aby zrozumieć, jak atakujący uzyskali dostęp i jakie luki pozwoliły na eskalację uprawnień?

Odzyskiwanie i zapobieganie:

- Jakie kroki zostały podjęte w celu przywrócenia normalnej pracy systemów po incydencie?
- Jakie długoterminowe zmiany w politykach bezpieczeństwa zostały wdrożone po incydencie, aby zapobiec podobnym zdarzeniom w przyszłości?
- Czy wprowadzono dodatkowe procedury zabezpieczające lub szkolenia dla pracowników w wyniku tego incydentu?

Wnioski managera

1.
2.
3.
4.
5.

Wnioski uczestników

1.
2.
3.
4.
5.

IV. Źródła

- Dobre praktyki w zakresie zapobiegania i reagowania na ataki typu **Ransomware –** KNF https://www.knf.gov.pl/?articleId=89342&p_id=18
- **Poradnik Ransomware** CERT Polska https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf
- **Stop Ransomware** CISA https://www.cisa.gov/stopransomware
- CISA **Tabletop Exercise Packages** https://www.cisa.gov/resourceshttps://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packagestools/services/cisa-tabletop-exercise-packages
- **Cyber, Cyber... – 88 – Ransomware – co robić po ataku?** Fundacja Bezpieczna Cyberprzestrzeń - lut 7, 2020, Podcast https://www.cybsecurity.org/pl/cyberhttps://www.cybsecurity.org/pl/cyber-cyber-88-ransomware-co-robic-po-ataku/cyber-88-ransomware-co-robic-po-ataku/
- Działania zapobiegawcze dla firm https://www.nomoreransom.org/pl/prevention-advice-for-businesses.html
- Projekt pomagający pozyskaniu kluczy deszyfrujących https://www.nomoreransom.org/pl/index.html
- NIST Risk Management Framework https://csrc.nist.gov/projects/risk-management/about-rmf
- The NIST Cybersecurity Framework (CSF) 2.0 https://www.nist.gov/cyberframework https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- NIST IR 8374 Ransomware Risk Management: A Cybersecurity Framework Profile https://csrc.nist.gov/pubs/ir/8374/final
- https://www.cisa.gov/stopransomware/ransomware-guide
- Email Attacks – Prevention Guide | Cyber Security Hotline 1300 CYBER1
- Access control lists
- Macro Security for Microsoft Office
- Network segmentation and separation
- Securing PowerShell in the Enterprise

V. Autor dokumentu

Artur Markiewicz

Konsultant cyberbezpieczeństwa

WWW: https://cyberkurs.online/

LI: https://www.linkedin.com/in/artur-markiewicz/

- Lider, trener, konsultant.
- Cyber Security Consultant w Trecom,
- Członek Zarządu ISSA Polska,
- Członek Zespołu Cyfrowy Skaut,
- Lider projektu #ISSAPolskalocal.

Realizuje i koordynuje projekty IT dla biznesu, edukacji czy administracji publicznej.

LICENCJA