W JAKI SPOSÓB ORGANIZACJE BRONIĄ SIĘ PRZED CYBERATAKAMI .ZARZĄDZANIE CYBER RYZYKIEM

Ryzyka cybernetyczne to stale zmieniające się zagrożenie dla zdolności organizacji do osiągania celów i wykonywania podstawowych funkcji. Cyberbezpieczeństwo to nie tylko kwestia informatyczna, ale wieloaspektowe wyzwanie, które wymaga podejścia do zarządzania w skali całego przedsiębiorstwa. Chociaż całkowita ochrona przed zagrożeniami cybernetycznymi jest nieosiągalna, najlepszą praktyką jest podejście oparte na ryzyku, które wdraża kompleksową strategię unikania, łagodzenia, akceptowania lub przenoszenia ryzyka stwarzanego przez zagrożenia cybernetyczne. Tradycyjne podejście do traktowania cyberbezpieczeństwa jako budowania większych ścian, takich jak zapory ogniowe i oprogramowanie antywirusowe – choć nadal konieczne, ale już nie wystarcza. Aby w pełni rozpoznać czynniki ryzyka cybernetycznego, organizacje muszą wiedzieć, jak transformacja pracy cyfrowej wpływa na ich środowisko operacyjne. Bazując na różnych analizach branżowych, rosnące tempo technologiczne tworzy następujące zmiany i wyzwania, które bezpośrednio wiążą się z cyberryzykiem.

Czynniki przyspieszające

* „Inteligentne" urządzenia i usługi powodujące niezamierzone konsekwencje i masę danych, zwiększające podatność na eksploatację; ludzie często odsunięci od procesów decyzyjnych;

* Media społecznościowe i BYOD (Bring Your Own Device), z pracownikami, klientami, obywatelami „zawsze włączonymi" i dzielącymi się informacjami – nie doceniając w pełni wpływu na prywatność i poufność;

* Przy jeszcze większej liczbie podłączonych urządzeń cyberprzestępcy będzie jeszcze łatwiej dostać się do wektora ataku;

* Przyjęcie przetwarzania mobilnego spowodowało zatarcie granic organizacyjnych, a dział IT zbliża się do użytkownika i oddala od organizacji oraz

* Organizacje umieszczające więcej danych w chmurze i ze stronami trzecimi; atrakcyjne, ale niebezpieczne, z utratą kontroli, zwiększonymi zagrożeniami i nieoczekiwaną łącznością - tworzy złożony ekosystem.

Zagrożenia cybernetyczne stają się coraz poważniejsze, ponieważ technologia nadal ewoluuje szybciej niż wysiłki na rzecz skutecznego zarządzania ryzykiem i jego kontroli. Forbes ogłosił na początku 2016 r. prognozę, że do 2019 r. koszty cyberprzestępczości osiągną 2 biliony USD. Wymagane jest całościowe podejście do zarządzania ryzykiem cybernetycznym w całej organizacji, jej sieci, łańcuchach dostaw i większym ekosystemie. Na przykład organizacje muszą ustanowić i utrzymywać odpowiednie ramy zarządzania i zarządzania ryzykiem, aby identyfikować i eliminować zagrożenia związane z sieciami i usługami komunikacyjnymi. Zarządzanie ryzykiem cybernetycznym to złożony problem, wymagający zaangażowania kadry kierowniczej, stałego zarządzania, technik zarządzania ryzykiem, korelacji zagrożeń, współpracy w całej organizacji oraz przyjęcia nowego biznesowego modelu operacyjnego. Ostatecznym celem zarządzania ryzykiem cybernetycznym jest budowanie odporności cybernetycznej, w której systemy i operacje organizacji są zaprojektowane do wykrywania zagrożeń cybernetycznych i reagowania na zdarzenia cybernetyczne w celu zminimalizowania zakłóceń biznesowych i strat finansowych.

DALSZE ROZWAŻANIE

16 korporacyjnych zagrożeń cyberbezpieczeństwa, na które trzeba się przygotować

1) Nieuwzględnienie podstaw cyberbezpieczeństwa

2) Niezrozumienie, co generuje korporacyjne zagrożenia cyberbezpieczeństwa

3) Brak polityki cyberbezpieczeństwa

4) Myląca zgodność z cyberbezpieczeństwem

5) Czynnik ludzki – najsłabsze ogniwo

6) Polityka Bring Your Own Device (BYOD) i chmura

7) Ograniczenia w zakresie finansowania, talentów i zasobów

8) Brak szkolenia w zakresie bezpieczeństwa informacji

9) Brak planu naprawczego

10) Ciągle ewoluujące ryzyko

11) Starzejąca się infrastruktura

12) korporacyjna nieelastyczność

13) Brak odpowiedzialności

14) Trudności w integracji źródeł danych

15) Trzymanie się reaktywnego sposobu myślenia

16) Rozłączenie między wydatkami a wdrażaniem

ZNACZENIE PROGRAMU ZARZĄDZANIA CYBERRYZYKIEM

Nieautoryzowany dostęp do systemów i danych organizacji może spowodować nieodwracalne szkody dla jej działalności, reputacji i wartości. Zakres i dotkliwość wpływu cyberataku będą zależeć od charakteru ataku oraz zdolności organizacji do reagowania i minimalizowania jego skutków. Naruszenia cyberbezpieczeństwa wpływają nie tylko na wyniki finansowe organizacji, ale także na jej reputację, markę i własność intelektualną. Przykłady biznesowego efektu cyberataku obejmują:

* Utrata danych osobowych, takich jak dane kontaktowe klienta lub dane bankowe, lub wrażliwych danych osobowych, takich jak informacje o pacjencie

* Niezdolność do działania i prowadzenia działalności, takiej jak atak DDoS, który przytłacza serwery poczty e-mail organizacji

* Utrata klientów i biznesu z obniżeniem zadowolenia i utrzymania klientów

* Uszkodzenie wartości organizacji prowadzące do spadku cen akcji.

Tradycyjny model bezpieczeństwa informacji, oparty na zgodności i zorientowany na granicę, nie jest przeznaczony do rozwiązywania współczesnych, coraz bardziej wyrafinowanych cyberataków. Ponadto koszty walki z cyberzagrożeniami gwałtownie wzrosły, ponieważ organy regulacyjne koncentrują się na tym, jak dobrze instytucje finansowe bronią się przed tymi zagrożeniami. Rosnące wyrafinowanie i częstotliwość cyberataków jest głównym powodem do niepokoju ze względu na możliwość zakłócenia i zniszczenia systemów i informacji. Według badań Protiviti, najbardziej znaczące poziomy ryzyka cyberbezpieczeństwa zgłaszane organizacjom obejmowały bezpieczeństwo danych, utratę reputacji, wyciek danych i naruszenie zgodności. Dalsze badania wskazują, że utrata reputacji, przerwy w działalności i odszkodowania za utratę danych klientów to trzy główne przyczyny strat ekonomicznych.

Na przykład naruszenie danych Target w 2014 r. było jednym z największych w historii. Dane osobowe około 70 milionów osób mogły zostać naruszone. Poinformowano, że kosztowało to firmę znacznie ponad 100 milionów USD, nie licząc szkody dla reputacji i utraty biznesu, po czym dyrektor generalny firmy opuścił stanowisko.

10 najczęstszych zagrożeń związanych z cyberbezpieczeństwem wysyłanych do organizacji

1) Bezpieczeństwo danych (informacje o firmie)

2) Uszkodzenie marki/reputacji

3) Wyciek danych (dane osobowe pracownika)

4) Naruszenie przepisów i zgodności

5) Wirusy i złośliwe oprogramowanie

6) Przerwana ciągłość działania

7) Strata finansowa

8) Utrata własności intelektualnej

9) Utrata produktywności pracowników

10) Zniesławienie pracownika

Zarządzanie ryzykiem cybernetycznym definiuje się jako:

„Skoordynowane zarządzanie inteligencją, technologią i operacjami biznesowymi w celu skutecznego zarządzania zasobami informacji biznesowych organizacji w celu zapobiegania niepożądanym konsekwencjom. Jest to proces, dzięki któremu firma chroni swoje krytyczne aktywa i reputację przed zewnętrznymi i wewnętrznymi zagrożeniami ze strony osób lub organizacji, ale nie ogranicza się to do środków technicznych. Coraz częściej instytucje finansowe powinny teraz postrzegać zarządzanie ryzykiem cybernetycznym jako integralny aspekt zarządzania ich działalnością i kontrolowania ryzyka".

Ze względu na rozmiar, złożoność i ciągłą ewolucję wektorów ataków nie ma prostego i uniwersalnego podejścia do zarządzania ryzykiem związanym z cyberbezpieczeństwem. Jednak kluczowe jest, aby gdzieś zacząć, aby ustalić punkt odniesienia dla identyfikacji krytycznych komponentów, które muszą zostać włączone do podejścia do zarządzania ryzykiem cybernetycznym. Skuteczne i odpowiednie ramy to podstawa, od której należy zacząć. Ramy cyberbezpieczeństwa to zestaw działań w zakresie cyberbezpieczeństwa, pożądanych wyników i odpowiednich odniesień, które są wspólne dla wszystkich sektorów infrastruktury krytycznej. Struktura jest centralnym elementem programu zarządzania ryzykiem cybernetycznym, pomagając w:

* Identyfikacja i priorytetyzacja ekspozycji na ryzyko w organizacji

* Oszacowanie potencjalnego wpływu biznesowego i określenie możliwych konsekwencji

* Dopasowanie wszystkich aspektów cyberzagrożeń do biznesu

* Ocena dojrzałości obecnego programu cyberbezpieczeństwa w celu zidentyfikowania obszarów wymagających poprawy

* Zbieranie informacji w celu tworzenia testów porównawczych z innymi organizacjami

Wykazano, że podstawowe zarządzanie ryzykiem informacyjnym zapobiega nawet 85% cyberataków, co pozwala organizacjom skoncentrować się na zarządzaniu wpływem pozostałych 15%. Organizacje powinny rozważyć zastosowanie następujących podstawowych procedur bezpieczeństwa w celu zmniejszenia zagrożeń cybernetycznych w tych kluczowych obszarach. Kluczowe elementy skutecznego programu zarządzania ryzykiem cybernetycznym, takie jak definiowanie ról i obowiązków, wdrażanie standardów/najlepszych praktyk w zakresie cyberbezpieczeństwa, ustalanie procesu reagowania na cyberataki oraz uwzględnianie zakresu ubezpieczenia cybernetycznego, omówiono w kolejnych sekcjach.

Zarządzanie ryzykiem informacyjnym: Stwórz skuteczną strukturę zarządzania i określ swój apetyt na ryzyko – tak jak w przypadku każdego innego ryzyka. Utrzymuj zaangażowanie zarządu w cyberryzyko. Opracuj wspierające zasady zarządzania ryzykiem informacyjnym.

Praca w domu i pracy mobilnej : Opracuj politykę pracy mobilnej i przeszkol personel, aby się do niej stosował. Zastosuj bezpieczną kompilację linii bazowej do wszystkich urządzeń. Chroń dane zarówno podczas przesyłania, jak i w spoczynku.

Edukacja i świadomość użytkowników: Opracuj zasady bezpieczeństwa użytkowników obejmujące dopuszczalne i bezpieczne korzystanie z systemów organizacji. Stwórz program szkolenia personelu. Utrzymuj świadomość użytkowników na temat zagrożeń cybernetycznych.

Zarządzanie incydentami: ustal zdolność reagowania na incydenty i odzyskiwania po awarii. Twórz i testuj plany zarządzania incydentami. Zapewnij specjalistyczne szkolenie zespołowi zarządzania incydentami. Zgłaszaj incydenty kryminalne organom ścigania.

Zarządzanie uprawnieniami użytkowników : ustal procesy zarządzania kontami i ogranicz liczbę kont uprzywilejowanych. Ogranicz uprawnienia użytkowników i monitoruj aktywność użytkowników. Kontroluj dostęp do dzienników aktywności i audytu.

Kontrola nośników wymiennych : Utwórz zasady kontroli dostępu do nośników wymiennych. Ogranicz rodzaje i wykorzystanie mediów. Przeskanuj wszystkie nośniki w poszukiwaniu złośliwego oprogramowania przed zaimportowaniem do systemu firmowego.

Monitorowanie: ustal strategię monitorowania i opracuj polityki wspierające. Stale monitoruj wszystkie systemy i sieci informacyjne. Analizuj dzienniki pod kątem nietypowej aktywności, która może wskazywać na atak.

Bezpieczna konfiguracja : Zastosuj poprawki bezpieczeństwa i upewnij się, że zachowana jest bezpieczna konfiguracja wszystkich systemów informatycznych. Utwórz inwentarz systemu i zdefiniuj kompilację bazową dla wszystkich urządzeń informacyjnych.

Ochrona przed złośliwym oprogramowaniem : opracuj odpowiednie zasady i utwórz zabezpieczenia przed złośliwym oprogramowaniem, które mają zastosowanie i są odpowiednie dla wszystkich obszarów działalności. Skanuj w poszukiwaniu złośliwego oprogramowania w całej organizacji.

Bezpieczeństwo sieci: Chroń sieci przed zewnętrznymi i wewnętrznymi atakami. Zarządzaj granicami sieci. Odfiltruj nieautoryzowany dostęp i złośliwą zawartość. Monitoruj i testuj zabezpieczenia.

ROLE I OBOWIĄZKI

Chociaż zaangażowanie wyższego szczebla kierowniczego ma kluczowe znaczenie dla powodzenia programów cyberbezpieczeństwa organizacji, wraz z jasnym łańcuchem odpowiedzialności, dobrze wyszkolony personel stanowi pierwszą linię obrony przed cyberatakami. Skuteczne szkolenie pomaga

zmniejszyć prawdopodobieństwo pomyślnego ataku, zapewniając pracownikom o dobrych intencjach wiedzę pozwalającą uniknąć nieumyślnego stania się wektorami ataku (na przykład poprzez niezamierzone pobranie malware).

ODPOWIEDZIALNOŚĆ ZARZĄDU

Problem potęguje fakt, że wiele zarządów nadal postrzega cyberbezpieczeństwo jako kwestię IT. Taka percepcja nie tylko zwiększa potencjalne narażenie organizacji na ataki, ale także poszerza lukę komunikacyjną między osobami odpowiedzialnymi za ochronę przedsiębiorstwa a tymi, których obowiązki polegają na zapewnieniu zwrotu inwestorom i udziałowcom oraz utrzymywaniu silnego ładu korporacyjnego. Temat cyberbezpieczeństwa musi przejść z domeny informatyka do kadry kierowniczej i zarządu. Dyrektor generalny i zarząd powinni przejąć ostateczną odpowiedzialność za program cyberbezpieczeństwa, taki jak ogólny program zwalczania oszustw. Zagrożenia cybernetyczne powinny być regularnie omawiane z dyrektorem generalnym i zarządem, ponieważ cyberzagrożenia należą do najważniejszych zagrożeń biznesowych, z jakimi borykają się obecnie organizacje. Zarządy są teraz odpowiedzialne za to, że dyrektorzy muszą postrzegać cyberbezpieczeństwo jako kwestię ryzyka w całym przedsiębiorstwie, którą należy rozpatrywać z perspektywy strategicznej, wielofunkcyjnej i ekonomicznej. PwC zidentyfikowało następujące powody, dla których rady nadzorcze powinny aktywnie nadzorować kwestie związane z cyberbezpieczeństwem. Możliwość zaszkodzenia reputacji – na rynku, wśród akcjonariuszy i partnerów - nigdy nie należy lekceważyć. Kwestia cyberbezpieczeństwa musi zostać skierowana do sali konferencyjnej, gdzie może zająć należne jej miejsce jako zasadniczy element ogólnej strategii zarządzania ryzykiem w organizacji.

Siedem powodów, dla których cyberbezpieczeństwo jest problemem nadzoru zarządu

1) Wpływ cyberbezpieczeństwa ma charakter systemowy. Incydenty mogą mieć wpływ na globalne operacje organizacji, nawet jeśli punkt ryzyka znajduje się tysiące mil stąd.

2) Skutki finansowe mogą być znaczące i mogą obejmować kosztowne pozwy zbiorowe, które mogą odzwierciedlać odpowiedzialność powierniczą Rady za zachowanie wartości finansowej firmy.

3) Wraz z ewolucją przepisów zgodność staje się coraz trudniejsza i coraz bardziej kosztowna. Na przykład unijna dyrektywa o ochronie danych zawiera propozycję kar w wysokości do 5% globalnych przychodów firmy. Stanowi to również podstawę do sporów cywilnych.

4) IoT przyniósł nowe zagrożenia, w tym narażenie kontroli przemysłowych i systemów inteligentnych budynków, które mogą powodować ekstremalne ryzyko i ogromne szkody fizyczne.

5) Ubezpieczenie cyberbezpieczeństwa należy traktować jako regulacyjne zabezpieczenie przed zagrożeniami cybernetycznymi. Komisja ds. ryzyka powinna zadawać pytania dotyczące pokrycia odpowiedzialności dyrektorów i urzędników, ogólnej odpowiedzialności handlowej, wcześniejszych działań oraz ubezpieczenia mienia i następstw nieszczęśliwych wypadków.

6) Przeciwnicy, tacy jak państwa narodowe i przestępczość zorganizowana, współpracują ze sobą, aby atakować organizacje w celach takich jak sabotaż gospodarczy, kradzież tajemnic handlowych, pranie pieniędzy, terroryzm oraz operacje wojskowe i wywiadowcze.

7) Cyberataki mogą skutkować znacznymi stratami finansowymi i szkodzić reputacji marki, zakłócając cele strategiczne organizacji, takie jak planowana fuzja lub przejęcie, wprowadzenie nowego produktu lub umowa biznesowa z potencjalnym klientem

SPONSORING NA POZIOMIE C

Chociaż wszyscy są odpowiedzialni za cyberbezpieczeństwo, najbardziej skuteczne jest podejście odgórne i wielofunkcyjne. Zespół zarządzający powinien uznać swoją przywódczą rolę w ustalaniu odpowiedniego tonu i struktury umożliwiającej cyberodporność w całej organizacji. Na przykład zespół musi być bezpośrednio zaangażowany w nadawanie tonu na szczycie, przeglądanie i zatwierdzanie polityk, budowanie świadomości, inwestowanie w zasoby i ułatwianie nowych programów. Powinny zostać utworzone komisje nadzorcze złożone z kadry kierowniczej wyższego szczebla i członków zarządu, aby zapewnić przestrzeganie wiodących praktyk w całej organizacji. Ostatnie badanie Instytutu Ponemone sugeruje, że cyberbezpieczeństwo stanie się przewagą konkurencyjną i priorytetem na poziomie C w oparciu o karne przewidywania ekspertów ds. cyberbezpieczeństwa. Ankieta z 2015 r. Fortune 500 CEO wykazała, że cyberbezpieczeństwo znalazło się na drugim miejscu, gdy dyrektorów generalnych zapytano o największe wyzwania ich firm. Próby wykrywania i reagowania na ataki są utrudnione ze względu na ich stale ewoluujący charakter, ponieważ sprawcy szybko znajdują nowe sposoby ich wykonania. Firmy próbujące dorównać tej szybkości w opracowywaniu metod zapobiegania i reagowania są czasami ograniczone przez słabe zrozumienie ryzyka, brak talentu technicznego i nieodpowiednie możliwości w zakresie bezpieczeństwa. Chociaż dyrektorzy generalni martwią się rosnącym ryzykiem cybernetycznym, własność i odpowiedzialność za cyberryzyko jest mniej jasna. Chociaż jest wielu właścicieli na poziomie „C" (CISO, CFO, CEO, CRO i Risk Management), każdy z nich ma inne, ale powiązane interesy i niestety często nie integruje ryzyka ani nie efektywnie współpracuje przy jego zarządzaniu. W związku z tym kluczowe znaczenie ma jasne określenie ról i obowiązków związanych z cyberryzykiem. PwC sugeruje zorganizowanie następujących grup, w tym komitetu zarządzania ryzykiem cybernetycznym, komitetu nadzoru nad ryzykiem cybernetycznym oraz zespołu operacyjnego ds. ryzyka cybernetycznego w celu przeprowadzenia silnego procesu zarządzania ryzykiem cybernetycznym.

Grupa : Kluczowi gracze : Obowiązki

Komitet ds. Zarządzania Ryzykiem Cybernetycznym:

* Dyrektor operacyjny (COO)

* Dyrektor ds. Ryzyka (CRO)

* Szef ochrony

* Kierownicy firm i obszarów funkcjonalnych (takich jak

* Planowanie ciągłości działania, prawne, ryzyko/regulacja) :

- Współpracuj z liderami wyższego szczebla w celu opracowania strategii cyberryzyka.

- Zdecyduj, które zasoby informacyjne są niezbędne.

- Ustala budżet na cyberryzyko.

- Monitoruj pozycję organizacji w zakresie cyberryzyka i raportuj o tym starszym liderom i radzie dyrektorów.

- Przeglądanie raportów z zespołów ds. nadzoru i operacji w zakresie cyberryzyka oraz pomoc w ustaleniu priorytetów pojawiających się zagrożeń cybernetycznych.

- Zrewiduj strategię, aby dostosować program w miarę ewolucji krajobrazu zagrożeń cybernetycznych.

Komitet Nadzoru nad Ryzykiem Cybernetycznym:

* Zespół ds. technologii informatycznych

* Zespół wsparcia biznesowego

* Zespoły biznesowe :

- Oceń aktywne zagrożenia, przed którymi stoi organizacja, stojące za nimi osoby i zasoby, którym zagrażają.

- Oceń skuteczność zespołu operacyjnego.

- Identyfikuj nowe zagrożenia i poprawiaj, pokaż, czy zasoby informacyjne są chronione.

- Określ, w jaki sposób zmiany biznesowe wpływają na obszar cybernetyczny, w tym nowe oferty usług, dostawców, dostawców lub partnerów biznesowych.

- Monitoruj stan poprawek i zmiany konfiguracji na krytyczne systemy.

- Nadzoruj programy szkoleniowe dla pracowników.

- Przejrzyj nowe wymagania prawne i dotyczące zgodności.

Zespół ds. Operacji Ryzyka Cybernetycznego:

* Menedżerowie z doświadczeniem operacyjnym w zakresie sieci, bezpieczeństwa informacji, oszustw i bezpieczeństwa korporacyjnego

* Centrum operacji bezpieczeństwa :

- Działaj jako pierwsza linia obrony do wykrywania i reagowania na zdarzenia cybernetyczne

- Kompiluj informacje w czasie rzeczywistym ze wszystkich grup monitorujących cyberzagrożenia.

- Tworzy raporty dla komitetów nadzoru nad ryzykiem cybernetycznym i komitetów zarządzających, w tym takie elementy, jak: liczba i rodzaj zdarzeń cybernetycznych, początek i czas trwania zdarzeń, które aktywa były celem ataków, rodzaje prób oszustwa, porównanie zdarzeń cybernetycznych z trendami w branży, incydenty i raporty reakcji, oceny zagrożeń i raporty wywiadowcze

Do codziennego wdrażania, zarządzania ryzykiem i kontroli wiele firm wyznacza jednego dyrektora na poziomie C, często Chief Technology Officer (CTO), który nadzoruje strategię i jej wdrażanie. Osoba wybrana do tej roli powinna mieć bezpośredni dostęp oraz regularną i otwartą komunikację z prezesem i zarządem. Pomoże to stworzyć środowisko, w którym anomalię cyberbezpieczeństwa można szybko zidentyfikować, natychmiast zaadresować, udokumentować i zgłosić odpowiednim stronom. W szczególności kierownictwo wykonawcze powinno podjąć następujące kroki w celu stworzenia programu zarządzania ryzykiem cybernetycznym, aby chronić swoje strumienie przychodów, procesy biznesowe, aktywa, obiekty, markę i reputację:

Uwagi dla kadry kierowniczej we wdrażaniu programu zarządzania ryzykiem cybernetycznym

Akcja: Kroki

Ustanowienie zarządzania ryzykiem cybernetycznym

• Określ, kto w organizacji powinien być zaangażowany w rozwój programu zarządzania ryzykiem cybernetycznym

• Ustanowienie międzyorganizacyjnego komitetu kadry kierowniczej wyższego szczebla

• Skonfiguruj procesy operacyjne i strukturę raportowania

• Połącz się z innymi programami ryzyka, takimi jak usuwanie skutków awarii, ciągłość działania i zarządzanie kryzysowe

Zrozum cybergranicę organizacyjną

• Zidentyfikuj wszystkie lokalizacje, w których przechowywane są, przesyłane i udostępniane jego dane

• Rozważ nowe obszary, takie jak big data, analityka i media społecznościowe

Zidentyfikuj krytyczne procesy biznesowe i aktywa

• Określ, co składa się na ich najcenniejsze strumienie przychodów, procesy biznesowe, aktywa i obiekty

• Określ, gdzie się znajdują i kto ma do nich dostęp

Zidentyfikuj cyberzagrożenia

• Ustanowienie solidnej funkcji analizy zagrożeń opartej na współdzielonej inteligencji, danych i badaniach ze źródeł wewnętrznych i zewnętrznych.

Popraw gromadzenie, analizę i raportowanie informacji

• Upewnij się, że zespół ds. operacji związanych z ryzykiem cybernetycznym obsługuje trzy podstawowe funkcje w celu budowania niezawodnych funkcji analizy zagrożeń cybernetycznych i technicznych. Są to: zbieranie i zarządzanie, przetwarzanie i analizowanie oraz raportowanie i działanie.

Planuj i odpowiadaj

• Zaplanuj i przygotuj reakcję na zdarzenia cybernetyczne, określając, kto powinien podjąć działania, jakie są jego obowiązki i co powinien zrobić

• Często powracaj do technik gromadzenia danych wywiadowczych, wykorzystuj i aktualizuj opcje ubezpieczenia cybernetycznego oraz aktualizuj technologie cyberbezpieczeństwa

EY sugeruje, aby liderzy biznesowi rozważyli, czy ramy cyberbezpieczeństwa organizacji mogą odpowiedzieć na następujące problemy,

* Ryzyko regulacyjne

Jak rządy i regulatorzy zareagują na rosnące zagrożenie ryzykiem informacyjnym?

* Wstrząsy geopolityczne

Jaka jest ekspozycja naszej organizacji na te wstrząsy? Jak responsywna jest nasza organizacja IT?

* Ryzyko reputacji

Jak cyberatak wpłynąłby na naszą reputację i markę?

* Awarie kontroli

Czy luki lub słabości w naszych mechanizmach kontroli IT i zabezpieczeniach mogą być czynnikami przyczyniającymi się do tego?

* Ryzyko informacji

W jaki sposób nasza organizacja zajmie się kluczowymi obszarami ryzyka związanymi z bezpieczeństwem, odpornością i wyciekiem danych?

* Ekspansja na rynkach wschodzących

Czy zwiększenie zasięgu naszej firmy zwiększa wyzwanie ciągłości biznesowej?

* Przekształcanie firmy

Jak bardzo zmieni się nasz profil ryzyka informacyjnego?

* Ryzyko regulacyjne

Jak rządy i regulatorzy zareagują na rosnące zagrożenie ryzykiem informacyjnym?

* Centra usług wspólnych

Czy korzystanie z usług stron trzecich lub centrów usług wspólnych zwiększy ryzyko dla naszego bezpieczeństwa i zaopatrzenia w IT?

* Bezpieczeństwo IP i danych

Czy nasza organizacja jest zabezpieczona przed wyciekiem danych, utratą i nieuczciwymi pracownikami?

* Akwizycje i integracja

Jak skuteczne są inwestycje naszej organizacji, jeśli nie jesteśmy w stanie?

zintegrować informacje należące do przejmowanej firmy?

* Uderzając w nagłówki

Haktywiści są z natury ideologiczni. W jaki sposób kwestie takie jak polityka podatkowa, płace i zarządzanie środowiskiem mogą spowodować, że nasza firma stanie się celem cybernetycznym?

ŚWIADOMOŚĆ I ZAANGAŻOWANIE PRACOWNIKÓW

Chociaż dyrektor generalny i zarząd, nadający ton podnoszeniu bezpieczeństwa, są odpowiedzialni za zapewnienie, że firma zaprojektuje i wdroży skuteczny program cyberbezpieczeństwa, cyberzagrożenia i działania łagodzące są w gestii całego przedsiębiorstwa; wszyscy mają do odegrania kluczową rolę. Poniższa tabela zawiera szczegółowe obowiązki według działu.

Dział : Obowiązki

Poziom wykonawczy :

* Opracuj solidną strategię cyberbezpieczeństwa

* Upewnij się, że informacje wysokiej jakości są odbierane i przyswajane

* Wdrażaj programy zwiększające świadomość bezpieczeństwa użytkowników

* Wspieraj wydatki na bezpieczeństwo oparte na strategii

Prawny :

* Śledź ewoluujące środowisko cyberregulacyjne

* Monitoruj decyzje podejmowane przez regulatorów w odpowiedzi na incydenty cybernetyczne

* Bądź świadomy czynników, które mogą unieważnić ubezpieczenie cybernetyczne

Audyt i ryzyko:

* Zapewnij dokładne zrozumienie i pokrycie zagrożeń technologicznych

* Przeprowadź wstępne badanie due diligence w celu ograniczenia ryzyka związanego ze stronami trzecimi

* Zajmij się ryzykiem związanym z systemami operacyjnymi (niefinansowymi) * Zajmij się podstawowymi problemami audytu IT

IT

* Przeprowadź kryminalistyczne oceny gotowości

* Bądź świadomy zmieniającego się krajobrazu zagrożeń i wektorów ataków

* Testuj plany reagowania na incydenty

* Wdrażaj skuteczne procesy monitorowania

* Zastosuj nowe strategie, w tym symulacje cyberataków, grywalizację szkoleń i sesji uświadamiających dotyczących bezpieczeństwa oraz analizę danych dotyczących bezpieczeństwa.

W całej organizacji należy odnotować i uszczegółowić szeroki zakres indywidualnych obowiązków. Globalne badanie PwC sugeruje, że firmy, które prowadzą program świadomości bezpieczeństwa, znacznie obniżają średnie straty finansowe wynikające z incydentów cyberbezpieczeństwa. Wiele organizacji intensywnie inwestuje w środki kontroli technicznej, aby chronić swoje systemy komputerowe i dane. Jednak większość tych technicznych mechanizmów kontrolnych staje się bezużyteczna, ponieważ pracownicy nie mają szkolenia w zakresie świadomości cyberbezpieczeństwa. Pracownicy podejmują ryzyko online, a to znacznie zwiększa ryzyko cybernetyczne dla ich organizacji. Ryzykowne działania pracowników obejmują otwieranie podejrzanych wiadomości e-mail, brak ochrony poufnych informacji przechowywanych lub przesyłanych z ich komputerów. Badanie 2015 Cyber Threat Defense Report Survey pokazuje, że niska świadomość bezpieczeństwa wśród pracowników pozostaje największym czynnikiem hamującym ochronę przed cyberzagrożeniami. Pracownicy powinni być informowani o dobrych praktykach w zakresie cyberbezpieczeństwa i rozumieć, że odgrywają kluczową rolę w ochronie zasobów informacyjnych ich organizacji. Kanadyjska Organizacja Regulacyjna Przemysłu Inwestycyjnego (IIROC) zasugerowała, aby organizacje rozważyły następujące zalecenia dotyczące świadomości i szkoleń w zakresie cyberbezpieczeństwa.

Zalecenia dotyczące świadomości i szkoleń w zakresie cyberbezpieczeństwa

• Wdrażanie polityk obejmujących dopuszczalne i bezpieczne korzystanie z systemów komputerowych.

• Obowiązek szkolenia i świadomości cyberbezpieczeństwa dla wszystkich pracowników. Szkolenie może odbywać się w klasie, online lub za pośrednictwem wideo i powinno odbywać się co roku. Ataki hakerskie (np. phishing e-mailowy) często są wymierzone w kadrę kierowniczą, dlatego ważne jest, aby uczestniczyli oni również w szkoleniu z zakresu cyberbezpieczeństwa.

• Upewnij się, że wszyscy pracownicy rozumieją swoje role i obowiązki w zakresie cyberbezpieczeństwa.

• Użytkowników należy poinstruować, aby nie otwierali podejrzanych wiadomości e-mail ani nie klikali podejrzanych linków, niezależnie od źródła.

• Użytkowników należy poinstruować, aby nie podłączali urządzeń do sieci, chyba że mają ku temu uzasadniony powód biznesowy lub nie korzystają z wcześniej zatwierdzonych urządzeń.

• Użytkownicy powinni być poinstruowani, aby postępować zgodnie z dobrymi praktykami dotyczącymi haseł.

• Użytkownicy powinni rozumieć niebezpieczeństwa i bezpieczne korzystanie z zewnętrznych nośników (pamięć USB i CD).

• Użytkownicy nie powinni pobierać ani instalować nieautoryzowanych aplikacji, ponieważ mogą one zawierać złośliwą zawartość.

• Użytkownicy powinni zrozumieć, że wobec personelu, który nie przestrzega zasad świadomości cyberbezpieczeństwa i polityk bezpieczeństwa, zostaną nałożone odpowiednie sankcje.

• Metody kształcenia ustawicznego dla kadry kierowniczej mogą zawierać filmy lub seminaria internetowe, które edukują użytkowników i dzielą się obowiązkową wiedzą.

EY sugeruje, aby pracownicy byli dokładnie przeszkoleni w zakresie rodzajów zagrożeń, których należy szukać, zarówno wewnętrznych, jak i zewnętrznych w organizacji, a także odpowiedniego reagowania na każdy incydent. Zagrożenia bezpieczeństwa mogą obejmować wszystko, od podejrzanych wiadomości e-mail wysyłanych do pracowników, zwłaszcza pracowników na wrażliwych stanowiskach, po naruszenia systemów zarządzania zasobami ludzkimi i danymi finansowymi, zaawansowane trwałe zagrożenia i nieautoryzowany dostęp do niepublicznej własności intelektualnej i wrażliwych danych klientów. Szkolenie w zakresie świadomości bezpieczeństwa informacji powinno odbywać się w sposób ciągły, z kwartalną aktualizacją i częstymi testami zdolności pracowników do zrozumienia i identyfikacji potencjalnych zagrożeń. Najlepiej przygotowane organizacje zdają sobie sprawę, że odpowiedzialność za odpieranie cyberataków nie pozostaje już w domenie IT. Jest to kwestia dotycząca całego przedsiębiorstwa i wymaga poczucia odpowiedzialności pracowniczej za bezpieczeństwo informacji.

EY sugeruje, aby pracownicy byli gruntownie edukowani na temat rodzajów zagrożeń, których należy szukać, zarówno wewnętrznych, jak i zewnętrznych w organizacji, a także odpowiedniego reagowania na każdy incydent. Zagrożenia bezpieczeństwa mogą obejmować wszystko, od podejrzanych wiadomości e-mail wysyłanych do pracowników, zwłaszcza pracowników na wrażliwych stanowiskach, po naruszenia systemów zarządzania zasobami ludzkimi i danymi finansowymi, zaawansowane trwałe zagrożenia i nieautoryzowany dostęp, po niepubliczną własność intelektualną i wrażliwe dane klientów. Szkolenie w zakresie świadomości bezpieczeństwa informacji powinno odbywać się w sposób ciągły, z kwartalną aktualizacją i częstymi testami zdolności pracowników do zrozumienia i identyfikacji potencjalnych zagrożeń. Najlepiej przygotowane organizacje zdają sobie sprawę, że odpowiedzialność za odpieranie cyberataków nie pozostaje już w domenie IT. Jest to kwestia dotycząca całego przedsiębiorstwa i wymaga poczucia odpowiedzialności pracowniczej za bezpieczeństwo informacji.

AUDYT WEWNĘTRZNY

Na całym świecie liderzy audytu wewnętrznego robią postępy w kierunku doskonałości, wykazując, że wgląd biznesowy, specjalistyczna wiedza techniczna i umiejętności w zakresie relacji są cennym zasobem we wspieraniu zarządzania organizacją, zarządzania ryzykiem i celów strategicznych. Członkowie zarządu, kadra kierownicza i kierownictwo w dużej mierze polegają na swoich funkcjach audytu wewnętrznego, aby zapewnić usługi zapewniające i doradcze, które pomagają organizacji monitorować i wzmacniać jej kulturę oraz alarmować, gdy coś może być nie tak. Ponadto w obliczu trwającej transformacji biznesowej coraz więcej interesariuszy poszukuje informacji od swoich grup audytu wewnętrznego, obejmujących nie tylko zagrożenia związane ze strategią długoterminową, ale

także siłę środków cyberbezpieczeństwa oraz zagrożenia związane z transformacją cyfrową i technologią mobilną. Według Instytutu Audytorów Wewnętrznych (IIA) przewidywany wzrost liczebności i budżetu personelu audytu wewnętrznego w wielu częściach świata odzwierciedla uznanie i wsparcie dla podnoszącej wartości audytu wewnętrznego przez kierownictwo i zarządy oraz umożliwia działom audytu wewnętrznego zwiększyć czas poświęcony na krytyczne obszary, takie jak zapewnienie zarządzania ryzykiem i strategie biznesowe. Cyberbezpieczeństwo odnosi się do środków podjętych w celu ochrony danych firmy w systemach komputerowych przed utratą, zniszczeniem, nieautoryzowanym dostępem lub niewłaściwym wykorzystaniem przez niezamierzone strony. Według Protiviti, Internal Audit Capabilities and Needs Survey, znaczny wzrost z roku na rok liczby organizacji w USA, które obecnie uwzględniają zagrożenia cyberbezpieczeństwa w rocznym planie audytu. Prawie trzy na cztery (73%) organizacji ocenia ryzyko cyberbezpieczeństwa w ramach rocznego planu audytu, w porównaniu z zaledwie połową (53%) organizacji w 2015 r. Wynik ten wskazuje na wyższy poziom zainteresowania i obaw organizacji dotyczących cyberzagrożeń teraz spotykają się codziennie. Ponadto wiele organizacji prawdopodobnie znajduje się pod wpływem swoich zewnętrznych audytorów, którzy wzmagają kontrolę nad programem cyberbezpieczeństwa kierownictwa, napędzanym przez obecne środowisko cyberzagrożeń oraz obowiązki informacyjne Komisji Papierów Wartościowych i Giełd USA. Według IIA głównymi powodami audytu cyberbezpieczeństwa jest to, że cyberbezpieczeństwo zostało słusznie ocenione jako wysokie, oraz że CAE poruszył tę kwestię podczas procesu planowania audytu, pokazując, że liderzy audytu wewnętrznego mogą być katalizatorem dla organizacji, która przeprowadza audyt. właściwy nacisk na coraz większe znaczenie cyberbezpieczeństwa. Audyt wewnętrzny zapewnia holistyczne podejście do identyfikowania obszarów, w których organizacja może być podatna na ataki od testowania zasad BYOD po przegląd umów z podmiotami zewnętrznymi pod kątem zgodności z protokołami bezpieczeństwa. Audyt wewnętrzny może również zapewnić zapewnienie skuteczności zarządzania IT. Na podstawie wyników globalnego badania IIA działy audytu wewnętrznego, które przeprowadzają audyt cyberbezpieczeństwa, zaczynają świadczyć swoim organizacjom szeroki zakres cennych usług. Na przykład najczęstsze usługi obejmują ocenę kontroli dotyczących procesu przetwarzania, przechowywania i/lub transportu danych systemów podłączonych do Internetu, przegląd planu ciągłości działania oraz ocenę procesu oceny ryzyka cyberbezpieczeństwa. Zgodnie z wynikami ankiety Protiviti, ISO 27000, GTAG 16 (Data Analysis Technologies), oraz Przewodnik po ocenie ryzyka informatycznego (GAIT) są najczęściej uznawane za najważniejsze priorytety przez audyt wewnętrzny w latach 2007–2016. Ponieważ ZAW dostrzegają znaczenie zapewnienia jasności w zakresie ryzyka informatycznego, rozumieją potrzebę audytu wewnętrznego w celu wykorzystania tego informacje w ramach programu audytu i działań na rzecz organizacji. Na przykład CAE uznały, że na szczycie swojej listy priorytetów znalazły się big data i analiza biznesowa.

Lista priorytetów CAE

- Big Data/Business Intelligence
- ISO 31000 (zarządzanie ryzykiem)
- ISO 9000 (Zarządzanie jakością i zapewnienie jakości)
- GTAG 17 – Audyt zarządzania IT
- Audyt kultury korporacyjnej

W oparciu o wyniki globalnego badania IIA, działy audytu wewnętrznego świadczą szeroki zakres cennych usług związanych z dużymi danymi, takich jak ocena kontroli dostępności, użyteczności, integralności lub bezpieczeństwa danych; ocena ryzyka związanego z wykorzystaniem big data; oraz

ocenę dokładności dużych zbiorów danych. Poniższa tabela przedstawia dalsze priorytety według wielkości firmy:

Najważniejsze priorytety audytu wewnętrznego według wielkości firmy

Małe < 1 mld USD : Średnie 1 mld USD-9 mld USD : Duże > 10 mld USD

Ramy bezpieczeństwa NIST: ISO 27000: Transformacja biznesowa/cyfrowa

ISO 27000: Aplikacja mobilna: Big Data/Business Intelligence

Big Data/Business Intelligence: NIST Cybersecurity Framework: Standardy rachunkowości w chmurze

Transformacja biznesowa/cyfrowa : GTAG 16 : GTAG 16

Internet rzeczy : Internet rzeczy : Przetwarzanie w chmurze

Ponieważ kwestie technologiczne dominują na liście priorytetów audytorów wewnętrznych, audyt wewnętrzny nadal postrzega analitykę danych i audyt oparty na technologii jako istotne priorytety. Audyt wewnętrzny w coraz większym stopniu wykorzystuje w swojej pracy analitykę danych i inne technologie. Badanie przeprowadzone w 2015 r. przez praktyków Globalnego Audytu Wewnętrznego przeprowadzonego przez wspólny organ wiedzy wykazało, że pięciu na dziesięciu respondentów testuje całe populacje zamiast próbkowania, wykorzystując eksplorację danych i analizę danych w celu monitorowania ryzyka i kontroli, a także identyfikacji oszustw i nie tylko. W przypadku odpowiednich zasobów i wsparcia audyt wewnętrzny rozwinie umiejętności i perspektywę świadczenia usług przeglądu i zapewnienia w zakresie cyberbezpieczeństwa. Istnieje sześć kluczowych obszarów kluczowych dla przygotowania cybernetycznego. Oto jak audyt wewnętrzny może przyczynić się do każdego z nich:

Jak audyt wewnętrzny może pomóc w przygotowaniu cybernetycznym

Zakres: Cel

Governance & Processes: Identyfikowanie luk w politykach i procedurach wdrożonych w organizacji dotyczących bezpieczeństwa informacji i infrastruktury IT oraz związanych z nimi ryzyk, takie jak przegląd polityk cyberbezpieczeństwa i testowanie skuteczności operacji bezpieczeństwa.

Przegląd bezpieczeństwa architektury sieci i analiza behawioralna: Oceń, czy architektura bezpieczeństwa obsługuje progi ryzyka organizacji, jednocześnie wspierając kluczowe cele biznesowe, takie jak przegląd architektury bezpieczeństwa i urządzeń oraz procedury logowania.

Proaktywny, zaawansowany, uporczywy przegląd zagrożeń: ogranicz ryzyko wycieku informacji i podsłuchiwania oraz przewiduj oczekiwane ataki i zagrożenia, na które może być narażona sieć, takie jak przeprowadzanie analizy przyczyn źródłowych, dogłębna inspekcja pakietów i identyfikacja złośliwego oprogramowania.

Baseline Security Review: Identyfikuj zagrożenia bezpieczeństwa w sieci, takie jak testowanie komponentów sieciowych związanych z bezpieczeństwem i przeprowadzanie analiz podatności.

Identyfikacja i reakcja na cyberataki: Oceń procedury i procesy, które umożliwiają wykrywanie i zgłaszanie incydentów cyberataków, takie jak przegląd zespołu reagowania oraz procesy raportowania i badania.

Identyfikacja i łagodzenie luk w zabezpieczeniach : pomaga wykryć wykorzystywaną lukę i związaną z nią aplikację, aby można było zastosować odpowiednią poprawkę do zainfekowanej części, np. zidentyfikować wykorzystywane aplikacje.

Oprócz ochrony i wykrywania, audyt wewnętrzny odgrywa kluczową rolę we wspieraniu komitetu audytu w nadzorowaniu cyberbezpieczeństwa. Na przykład regularne oceny przeprowadzane przez audyt wewnętrzny odgrywają ważną rolę w dostarczaniu komitetowi audytu kompleksowej oceny mocnych i słabych stron organizacji. CAE są w wyjątkowej sytuacji, aby edukować członków zarządu i komisji rewizyjnej na temat różnorodnych wysiłków organizacji w walce z cyberzagrożeniami

Najważniejsze działania w zakresie cyberbezpieczeństwa dla CAE i audytu wewnętrznego

• Współpracuj z zarządem zarządu w celu opracowania strategii i polityk i cyberbezpieczeństwa

• Zidentyfikuj i wykorzystaj możliwości poprawy zdolności organizacji do identyfikowania, oceny i ograniczania ryzyka cyberbezpieczeństwa do akceptowalnego poziomu.

• Uznaj, że ryzyko cyberbezpieczeństwa jest nie tylko zewnętrzne – oceniaj i ograniczaj potencjalne zagrożenia, które mogą wynikać z działań pracownika lub partnerów biznesowych.

• Wykorzystanie relacji z komitetem audytu i radą do (a) podniesienia świadomości i wiedzy na temat cyberzagrożeń; oraz b) zapewnić, aby rada pozostawała w wysokim stopniu zaangażowana w kwestie cyberbezpieczeństwa i była na bieżąco informowana o zmieniającym się charakterze ryzyka cyberbezpieczeństwa.

• Zapewnienie formalnego włączenia ryzyka cyberbezpieczeństwa do planu audytu.

• Rozwijanie i aktualizowanie wiedzy na temat wpływu nowych technologii i trendów na firmę oraz jej profil ryzyka cyberbezpieczeństwa.

• Oceń program cyberbezpieczeństwa organizacji pod kątem NIST Cybersecurity Framework, uznając, że ponieważ ramy nie sięgają poziomu kontroli, Twój program cyberbezpieczeństwa może wymagać dodatkowych ocen IS 27001 i 27002.

• Poszukuj możliwości poinformowania kierownictwa, że w odniesieniu do cyberbezpieczeństwa najsilniejsze możliwości prewencyjne wymagają połączenia bezpieczeństwa ludzkiego i technologicznego – uzupełniającego połączenia edukacji, świadomości, czujności i narzędzi technologicznych.

• Podkreśl, że monitorowanie cyberbezpieczeństwa i reagowanie na incydenty cybernetyczne powinny być priorytetem najwyższego kierownictwa — jasny protokół eskalacji może pomóc w uzasadnieniu (i utrzymaniu) tego priorytetu.

• Rozwiązanie problemu niedoborów personelu i zasobów w zakresie IT/kontroli oraz braku narzędzi technologicznych, które mogą utrudniać skuteczne zarządzanie ryzykiem cyberbezpieczeństwa.

Silna funkcja audytu wewnętrznego, która jest odpowiednio wyposażona i przeszkolona, jest jednym z najważniejszych narzędzi dostępnych dla zarządów, komitetów audytu, kadry kierowniczej i kierownictwa podczas tworzenia i udoskonalania strategii, polityk i protokołów w celu zapewnienia całościowej ochrony organizacji przed zagrożeniami cybernetycznymi .

STANDARDY CYBERBEZPIECZEŃSTWA

Wykorzystuje kompleksowy program zarządzania ryzykiem cybernetycznym, standardy branżowe i najlepsze praktyki w celu ochrony systemów i wykrywania potencjalnych problemów. Jest wspierany

przez procesy informowane o aktualnych zagrożeniach i umożliwia szybką reakcję i naprawę. Chociaż wymagania dotyczące zgodności pomagają ustalić dobry poziom bezpieczeństwa cybernetycznego w celu wyeliminowania znanych luk w zabezpieczeniach, nie rozwiązują one odpowiednio nowych i dynamicznych zagrożeń ani nie przeciwdziałają wyrafinowanym przeciwnikom. Stosowanie podejścia opartego na ryzyku do stosowania standardów i praktyk w zakresie bezpieczeństwa cybernetycznego pozwala na bardziej kompleksowe i efektywne kosztowo zarządzanie ryzykiem cybernetycznym niż same działania w zakresie zgodności. Na podstawie ankiety Dimensional Research przyjęcie standardów bezpieczeństwa jest powszechną praktyką, ponieważ 84% organizacji korzysta z ram bezpieczeństwa. Przyjęcie standardów bezpieczeństwa jest normą, że bankowość i finansowanie (88%), technologie informacyjne (87%), rząd (86%) i produkcja (83%) mają wskaźniki przyjęcia standardów bezpieczeństwa powyżej 80%. Edukacja i opieka zdrowotna są tylko nieznacznie w tyle (odpowiednio 77% i 61%). Standardy cyberbezpieczeństwa istnieją od kilkudziesięciu lat, ponieważ użytkownicy i dostawcy współpracowali na wielu forach krajowych i międzynarodowych. Standardy cyberbezpieczeństwa to techniki ogólnie określone w publikowanych materiałach, które mają na celu ochronę cyberśrodowiska użytkownika lub organizacji poprzez zmniejszenie ryzyka, w tym zapobieganie lub łagodzenie cyberataków. Opublikowane materiały składają się z kolekcji narzędzi, polityk, koncepcji bezpieczeństwa, zabezpieczeń, wytycznych, metod zarządzania ryzykiem, działań, szkoleń, najlepszych praktyk i technologii. W poniższych sekcjach omówiono najważniejsze z powszechnie uznanych standardów cyberbezpieczeństwa.

ISO/IEC 27001:2013

System zarządzania bezpieczeństwem informacji (ISMS) zachowuje poufność, integralność i dostępność informacji poprzez zastosowanie procesu zarządzania ryzykiem i daje zainteresowanym stronom pewność, że ryzyko jest odpowiednio zarządzane. Na ustanowienie i wdrożenie SZBI w organizacji mają wpływ potrzeby i cele organizacji, wymagania bezpieczeństwa, stosowane procesy oraz wielkość i struktura organizacji. Oczekuje się, że wszystkie te wpływające czynniki będą się zmieniać w czasie. Dlatego ważne jest, aby SZBI był częścią i był zintegrowany z procesami organizacji i ogólną strukturą zarządzania oraz aby bezpieczeństwo informacji było brane pod uwagę przy projektowaniu procesów, systemów informatycznych i kontroli. W październiku 2013 r. Międzynarodowa Organizacja Normalizacyjna (ISO) i Międzynarodowa Komisja Elektrotechniczna (IEC), wyspecjalizowany system ogólnoświatowej normalizacji, opublikowały wersję normy ISO/IEC 27001:2013. Oficjalny tytuł normy to Technologia informacyjna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, który jest częścią rosnącej rodziny norm ISO/IEC 27000. Ta najnowsza wersja normy ISO/IEC 27001 kładzie większy nacisk na pomiar i ocenę skuteczności SZBI organizacji, a także dodano nową sekcję dotyczącą outsourcingu, która odzwierciedla fakt, że wiele organizacji polega na stronach trzecich w zakresie dostarczania niektórych aspektów IT. Ogólnie rzecz biorąc, najnowsza wersja pomaga zachować jej znaczenie dla wyzwań współczesnego biznesu i zapewnia zgodność z zasadami zarządzania ryzykiem zawartymi w ISO 31000. Opiera się na strukturze wysokiego poziomu (Annex SL), która jest powszechna ramy dla wszystkich zmienionych i przyszłych norm systemu zarządzania ISO, w tym ISO 9001:2015 i ISO 14001:2015.

Klauzula: Kluczowe wymagania

4 . Kontekst Organizacji:

* Zidentyfikuj wszystkie zewnętrzne i wewnętrzne problemy istotne dla organizacji i jej informacji lub informacji powierzonych przez strony trzecie;

* Ustal wszystkie zainteresowane strony i interesariuszy oraz ich znaczenie dla informacji;

* Określ wymagania dla zainteresowanych stron, które mogą obejmować zobowiązania prawne, regulacyjne i/lub umowne;

* Zdefiniuj zakres SZBI powiązany z kierunkiem strategicznym organizacji, podstawowymi celami i wymaganiami stron zainteresowanych oraz

* Zademonstruj w organizacji ustanowienie, wdrożenie, utrzymanie i ciągłe doskonalenie SZBI w odniesieniu do standardu

5. Przywództwo

Najwyższe kierownictwo wykazuje przywództwo i zaangażowanie poprzez:

* Ustanowienie SZBI i polityki bezpieczeństwa informacji oraz

* Zapewnienie, że polityka bezpieczeństwa informacji jest zgodna ze strategicznym kierunkiem organizacji, że są one udostępniane, komunikowane, utrzymywane i rozumiane przez wszystkie strony

6. Planowanie

Ta klauzula:

* Przedstawia, w jaki sposób i organizacja planuje działania w celu zajęcia się ryzykiem związanym z informacją;

* Koncentruje się na tym, jak organizacja radzi sobie z ryzykiem bezpieczeństwa informacji i musi być proporcjonalna do potencjalnego wpływu, jaki mają, oraz

* Omów potrzebę ustanowienia celów bezpieczeństwa informacji, a norma definiuje właściwości, jakie muszą mieć cele bezpieczeństwa informacji.

7. Wsparcie

Ta klauzula koncentruje się na uzyskaniu odpowiednich zasobów i właściwych

istniejąca infrastruktura:

* Cały personel powinien być świadomy polityki bezpieczeństwa informacji oraz tego, w jaki sposób przyczynia się do jej skuteczności i konsekwencji nieprzestrzegania;

* Komunikacja wewnętrzna i zewnętrzna związana z bezpieczeństwem informacji i SZBI jest odpowiednio komunikowana

* Określ poziom udokumentowanych informacji niezbędnych do kontroli ISMS

8. Operacja

Ta klauzula dotyczy wykonania planów i procesów, które są przedmiotem poprzednich klauzul, takich jak:

* Zajmowanie się realizacją ustalonych działań i osiągnięciem celów bezpieczeństwa informacji;

* W uznaniu zwiększonego wykorzystania funkcji zlecanych na zewnątrz, procesy te również muszą być identyfikowane i kontrolowane oraz

* Zajmowanie się wykonywaniem ocen ryzyka bezpieczeństwa informacji w zaplanowanych odstępach czasu

9. Ocena wydajności

Ta klauzula dotyczy monitorowania, mierzenia, analizowania i oceny ISMS w celu zapewnienia, że jest skuteczny i taki pozostanie.

10. Poprawa

* Jak organizacja reaguje na niezgodności, podejmuje działania, koryguje je i radzi sobie z konsekwencjami;

* W jaki sposób organizacja wyeliminuje przyczyny takich niezgodności, aby nie występowały one gdzie indziej oraz

* Wykazać ciągłe doskonalenie ISMS

Od publikacji wersji z 2005 roku, a wraz z jej aktualizacją w 2013 roku, liczba przyznanych certyfikatów ISO/IEC 27001 z roku na rok wzrasta. Na przykład na podstawie corocznego badania ISO dotyczącego certyfikacji systemów zarządzania w 2015 r. wydano łącznie 27 536 certyfikatów dla ISO 27001, co stanowi wzrost o 20% w stosunku do ubiegłego roku. Wyraźnie widać tendencję do wzrostu w ostatnich latach.

BRANŻA KART PŁATNICZYCH. STANDARD BEZPIECZEŃSTWA DANYCH

Według PwC, Global State of Information Security Survey 2016, sektorem, który odnotował największy wzrost aktywności cyberprzestępczości w 2015 roku, był handel detaliczny, podczas gdy usługi finansowe – wciąż jeden z najbardziej atakowanych sektorów – ustabilizowały się, przy bardzo niewielkim wzroście pod względem liczba ataków w ciągu ostatnich trzech lat. Firmy zajmujące się sprzedażą detaliczną i dobrami konsumenckimi stoją w obliczu zagrożeń cybernetycznych głównie ze strony cyberprzestępców podobnych do korporacyjnych, którzy chcą uzyskać konto finansowe i inne dane klientów, na których mogą zarabiać. Ci cyberprzestępcy mogą atakować systemy punktów sprzedaży lub bazy danych klientów w celu przechwytywania danych uwierzytelniających użytkownika, przechowywanych danych finansowych, przechowywanych informacji umożliwiających identyfikację osób i podobnych zbiorów danych. Badanie firm w Stanach Zjednoczonych i Europie ujawnia działania, które mogą narazić dane posiadaczy kart na ryzyko, że:

* 81% numerów kart płatniczych sklepu

* 73% dat ważności kart płatniczych w sklepie

* 71% przechowuje kody weryfikacyjne kart płatniczych

* 57% przechowuje dane klienta z paska magnetycznego karty płatniczej

* 16% przechowuje inne dane osobowe

Według PrivacyRights.org od stycznia 2005 naruszono ponad 510 milionów rekordów zawierających poufne informacje. Luki w zabezpieczeniach sprzedawców mogą pojawić się niemal wszędzie w ekosystemie przetwarzania kart, w tym w urządzeniach w punktach sprzedaży; komputery osobiste lub serwery; bezprzewodowe hotspoty lub aplikacje do zakupów internetowych; w papierowych systemach przechowywania; oraz niezabezpieczone przesyłanie danych posiadaczy kart do dostawców usług. Luki mogą nawet obejmować systemy obsługiwane przez dostawców usług i agentów rozliczeniowych, czyli instytucje finansowe, które inicjują i utrzymują relacje z akceptantami akceptującymi karty płatnicze. Payment Card Industry Security Standards Council (PCI SSC) ustanowiła wymagania techniczne i operacyjne w celu ochrony danych posiadaczy kart. Standardy mają

zastosowanie do wszystkich podmiotów, które przechowują, przetwarzają lub przesyłają dane posiadaczy kart, wraz z wytycznymi dla twórców oprogramowania oraz producentów aplikacji i urządzeń wykorzystywanych w tych transakcjach. Standardy bezpieczeństwa PCI obejmują standard bezpieczeństwa danych PCI (DSS), wymagania dotyczące bezpieczeństwa transakcji PIN (PTS) oraz standard bezpieczeństwa danych aplikacji płatniczych (PA-DSS).

Przegląd standardów bezpieczeństwa PCI

PCI Data Security Standard (DSS): PCI DSS ma zastosowanie do wszystkich podmiotów, które przechowują, przetwarzają i/lub przesyłają dane posiadaczy kart. Obejmuje techniczne i operacyjne komponenty systemu zawarte lub połączone z danymi posiadacza karty. Sprzedawca, który akceptuje lub przetwarza karty płatnicze, musi przestrzegać PCI DSS. Organizacje uczestniczące obejmują handlowców, banki wydające karty płatnicze, procesory, programistów i innych dostawców.

Wymagania dotyczące bezpieczeństwa transakcji PIN (PTS) : PCI PTS (dawniej PCI PED) to zestaw wymagań bezpieczeństwa skoncentrowanych na charakterystyce i zarządzaniu urządzeniami używanymi do ochrony kodów PIN posiadaczy kart i innych czynnościach związanych z przetwarzaniem płatności. Wymagania dotyczą producentów, których muszą przestrzegać przy projektowaniu, produkcji i transporcie urządzenia do podmiotu, który je wdraża. Instytucje finansowe, podmioty przetwarzające, sprzedawcy i usługodawcy powinni używać wyłącznie urządzeń lub komponentów przetestowanych i zatwierdzonych przez PCI SSC.

Standard bezpieczeństwa danych aplikacji płatniczych (PA-DSS): PA-DSS jest przeznaczony dla twórców oprogramowania i integratorów aplikacji płatniczych, które przechowują, przetwarzają lub przesyłają dane posiadaczy kart w ramach autoryzacji lub rozliczenia, gdy te aplikacje są sprzedawane, dystrybuowane lub licencjonowane stronom trzecim . Większość marek kart zachęca sprzedawców do korzystania z aplikacji płatniczych przetestowanych i zatwierdzonych przez PCI SSC.

PCI DSS na całym świecie ma zastosowanie do podmiotów takich jak American Express, Discover Financial Services, JCB International, MasterCard Worldwide i Visa Inc., które przechowują, przetwarzają lub przesyłają dane posiadaczy kart. Składa się z 12 wymagań, które odzwierciedlają najlepsze praktyki bezpieczeństwa. Te wymagania określają ramy bezpiecznego środowiska płatności.

Standard bezpieczeństwa danych PCI

Cele: Wymagania PCI DSS

Zbuduj i utrzymuj bezpieczną sieć:

1) Zainstaluj i utrzymuj konfigurację zapory sieciowej w celu ochrony danych posiadaczy kart

2) Nie używaj dostarczonych przez dostawcę wartości domyślnych haseł systemowych i innych parametrów bezpieczeństwa

Chroń dane posiadacza karty:

3) Chroń przechowywane dane posiadacza karty

4) Szyfruj transmisję danych posiadacza karty w otwartych sieciach publicznych

Prowadź program zarządzania lukami w zabezpieczeniach:

5) Używaj i regularnie aktualizuj oprogramowanie lub programy antywirusowe

6) Opracuj i utrzymuj bezpieczne systemy i aplikacje Wdrażaj silne środki kontroli dostępu:

7) Ograniczenie dostępu do danych posiadacza karty przez potrzeby biznesowe

8) Przypisz unikalny identyfikator każdej osobie z dostępem do komputera

9) Ogranicz fizyczny dostęp do danych posiadacza karty

Regularnie monitoruj i testuj sieci:

10) Śledź i monitoruj cały dostęp do zasobów sieciowych i danych posiadaczy kart

11) Regularnie testuj systemy i procesy bezpieczeństwa

Utrzymuj politykę bezpieczeństwa informacji:

12) Utrzymuj politykę dotyczącą bezpieczeństwa informacji dla całego personelu

DALSZE ROZWAŻANIE

Wiele naruszeń miało miejsce w systemach PCI, które spełniały lub przekraczały jego standard. Może to wynikać z wielu powodów, ale z naszego doświadczenia wynika, że opiera się głównie na karcie z paskiem magnetycznym, która jest łatwiejsza do sklonowania i trudniejsza do kontrolowania niż układ scalony, standard kart EMV2 z obsługą chipów, stosowany w Europie, Kanadzie i Ameryce Łacińskiej. Skradzione numery kont i inne dane są mniej opłacalne dla kart EMV, a tym samym mniej atrakcyjne dla złodziei stosujących podejście skimmer. Grzywny nakładane przez Radę Standardów Bezpieczeństwa PCI mogą być znaczne.

RAMY CYBERBEZPIECZEŃSTWA NIST

NIST Cybersecurity Framework to dobrowolne wytyczne oparte na istniejących standardach, wytycznych i praktykach dla organizacji infrastruktury krytycznej w celu lepszego zarządzania i zmniejszania ryzyka cyberbezpieczeństwa. Wersja 1.0 Ram, wydana w 2014 r., została przygotowana przez Narodowy Instytut Standardów i Technologii (NIST) przy dużym udziale sektora prywatnego. Ponad 3000 osób z różnych gałęzi przemysłu, środowisk akademickich i rządowych wzięło udział w warsztatach i seminariach internetowych w całym kraju pomogło w opracowaniu Ram. Ramy zostały opracowane w odpowiedzi na rozporządzenie wykonawcze 13636, które określa obowiązki departamentów i agencji federalnych w zakresie pomocy w poprawie cyberbezpieczeństwa infrastruktury krytycznej. Ramy umożliwiają organizacjom - niezależnie od wielkości, stopnia ryzyka cyberbezpieczeństwa lub zaawansowania cyberbezpieczeństwa – stosowanie zasad i najlepszych praktyk zarządzania ryzykiem w celu poprawy bezpieczeństwa i odporności infrastruktury krytycznej. Ponadto Ramy nie są specyficzne dla branży, wspólna taksonomia standardów, wytycznych i praktyk również nie jest specyficzna dla danego kraju. Organizacje spoza USA mogą również wykorzystywać Ramy do wzmocnienia własnych wysiłków w zakresie cyberbezpieczeństwa, a Ramy mogą przyczynić się do opracowania wspólnego języka współpracy międzynarodowej w zakresie cyberbezpieczeństwa infrastruktury krytycznej. Ramy obejmują oparte na ryzyku zestawienie wytycznych, które mogą pomóc organizacjom w identyfikowaniu, wdrażaniu i ulepszaniu praktyk w zakresie cyberbezpieczeństwa oraz tworzą wspólny język dla wewnętrznej i zewnętrznej komunikacji w kwestiach związanych z cyberbezpieczeństwem. W szczególności zapewnia mechanizm oceny, który umożliwia organizacjom:

* Określ ich obecne możliwości cyberbezpieczeństwa;

* Ustaw indywidualne cele dla stanu docelowego i

* Stwórz plan ulepszania i utrzymywania programów cyberbezpieczeństwa.

Ostatnie ankiety i badania sugerują, że organizacje przyjmują ramy bezpieczeństwa jako inicjatywę w ramach najlepszych praktyk lub w celu spełnienia wymagań umownych lub regulacyjnych. Wiele organizacji, niezależnie od branży, rozważało przyjęcie NIST Framework w celu ustanowienia swojego systemu zarządzania bezpieczeństwem informacji, co pokazują następujące statystyki:

• Badanie Zdolności i Potrzeb Audytu Wewnętrznego Protiviti 2016: około 71% wewnętrznych działów audytu oceniło programy cyberbezpieczeństwa swoich organizacji pod kątem NIST Framework, jeśli cyberbezpieczeństwo jest uwzględnione w planie audytu.

• Raport Gartner Inc. 2016: NIST Framework został przyjęty przez 30% amerykańskich organizacji, z przewidywanym wykorzystaniem 50% do 2020 roku.

• Trendy badań wymiarowych w przyjęciu ram bezpieczeństwa 2016: Przyjęcie ram NIST może osiągnąć 43% do końca 2016 r.

Struktura jest często wyróżniana jako nie standard techniczny lub zestaw kontroli bezpieczeństwa, ale raczej bardziej holistyczne narzędzie do zarządzania ryzykiem, które wyróżnia się w wielu obszarach.

Wartości ram

* Zapewnienie nadrzędnych wskazówek, które mogą kształtować polityki korporacyjne i walidować strategie zarządzania ryzykiem;

* Zaoferuj szablon dla dyrektorów i urzędników korporacyjnych, aby ocenić stan cyberbezpieczeństwa ich organizacji, dojrzałość programu i ryzyko szczątkowe;

* Wykorzystywane do budżetowania korporacyjnego poprzez mapowanie planowanych inwestycji i map drogowych projektów do poszczególnych funkcji lub kategorii;

* Zapewnij wspólny język do komunikowania postawy organizacji w zakresie cyberbezpieczeństwa zewnętrznym interesariuszom, takim jak audytorzy, ubezpieczyciele i organy regulacyjne;

* Standardy nakładkowe, takie jak ISO/IEC 27001 i NIST SP 800-53, które można wykorzystać jako dodatkowe narzędzie bez dodatkowych kosztów poniesionych podczas dodawania, przechodzenia do nowego standardu i

* Zmniejszenie ryzyka prawnego wynikającego z tego, że obejmuje wiele praktyk związanych z cyberbezpieczeństwem, które są kluczowe w procesach konsumenckich i działaniach organów ścigania

KRYTYCZNE KONTROLE BEZPIECZEŃSTWA

Centrum Bezpieczeństwa w Internecie (CIS) zajmuje się zwiększaniem gotowości i reagowania na cyberbezpieczeństwo wśród podmiotów sektora publicznego i prywatnego. Kierowane przez CIS Krytyczne kontrole bezpieczeństwa CIS („Kontrole CIS”), skierowane do użytkowników IT na całym świecie, stanowią priorytetowy zestaw cyberpraktyk stworzone w celu powstrzymania dzisiejszych najbardziej rozpowszechnionych i niebezpiecznych cyberataków, takich jak włamanie do karty kredytowej, kradzież identyfikacji, oprogramowanie ransomware, kradzież własności intelektualnej, utrata prywatności, odmowa usługi. Kontrole są dostosowane i mapowane na wszystkie główne struktury, takie jak NIST Cybersecurity Framework i seria ISO 27000 lub przepisy, takie jak PCI, HIPAA i FISMA, są zatwierdzane przez społeczność wiodących światowych ekspertów. Według CIS organizacje, które stosują tylko pięć pierwszych kontroli CIS, mogą zmniejszyć ryzyko cyberataku o około 85%. Wdrożenie wszystkich 20 kontroli CIS zwiększa redukcję ryzyka do około 94%:

• CSC 1: Wykaz autoryzowanych i nieautoryzowanych urządzeń

• CSC 2: Spis autoryzowanego i nieautoryzowanego oprogramowania

• CSC 3: Bezpieczne konfiguracje sprzętu i oprogramowania na urządzeniach mobilnych, laptopach, stacjach roboczych i serwerach

• CSC 4: Ciągła ocena i naprawa podatności

• CSC 5: Kontrolowane korzystanie z uprawnień administracyjnych

• CSC 6: Utrzymanie, monitorowanie i analiza dzienników audytu

• CSC 7: Ochrona poczty e-mail i przeglądarki internetowej

• CSC 8: Ochrona przed złośliwym oprogramowaniem

• CSC 9: Ograniczenie i kontrola portów sieciowych, protokołów i usług

• CSC 10: Możliwość odzyskiwania danych

• CSC 11: Bezpieczne konfiguracje urządzeń sieciowych, takich jak zapory, routery i przełączniki

• CSC 12: Obrona granic

• CSC 13: Ochrona danych

• CSC 14: Dostęp kontrolowany w oparciu o potrzebę wiedzy

• CSC 15: Bezprzewodowa kontrola dostępu

• CSC 16: Monitorowanie i kontrola konta

• CSC 17: Ocena umiejętności bezpieczeństwa i odpowiednie szkolenie w celu wypełnienia luk

• CSC 18: Bezpieczeństwo oprogramowania aplikacji

• CSC 19: Reagowanie i zarządzanie incydentami

• CSC 20: Testy penetracyjne i ćwiczenia Czerwonej Drużyny

Przykłady pięciu najlepszych kontroli CIS

CIS Controls: Najważniejsze informacje o szczegółowych kontrolach

CSC1: Spis autoryzowanych i nieautoryzowanych urządzeń

1,1

Wdróż zautomatyzowane narzędzie do wykrywania inwentaryzacji zasobów i użyj go do stworzenia wstępnej inwentaryzacji systemów podłączonych do publicznych i prywatnych sieci organizacji.

1.2

Jeśli organizacja dynamicznie przypisuje adresy za pomocą protokołu DHCP, należy wdrożyć rejestrowanie serwera protokołu dynamicznej konfiguracji hosta (DHCP) i wykorzystać te informacje do usprawnienia inwentaryzacji zasobów.

1,3

Upewnij się, że wszystkie zakupy sprzętu automatycznie aktualizują system inwentaryzacji, gdy nowe, zatwierdzone urządzenia są podłączane do sieci.

CSC 2: Spis autoryzowanego i nieautoryzowanego oprogramowania

2,1

Opracuj listę autoryzowanego oprogramowania i wersji wymaganych w przedsiębiorstwie dla każdego typu systemu, w tym serwerów, stacji roboczych i laptopów różnego rodzaju i zastosowań.

2.2

Wdróż technologię białej listy aplikacji, która umożliwia systemom uruchamianie oprogramowania tylko wtedy, gdy znajduje się ono na białej liście i uniemożliwia uruchamianie całego innego oprogramowania w systemie.

2,3

Wdrażaj narzędzia do inwentaryzacji oprogramowania w całej organizacji, obejmujące każdy z używanych systemów operacyjnych, w tym serwery, stacje robocze i laptopy.

CSC 3: Bezpieczne konfiguracje sprzętu i oprogramowania na urządzeniach mobilnych, laptopach, stacjach roboczych i serwerach

3.1

Stwórz standardowe bezpieczne konfiguracje swoich systemów operacyjnych i aplikacje.

3.2

Postępuj zgodnie z uderzonym zarządzaniem konfiguracją, budując bezpieczny obraz, który jest używany do tworzenia wszystkich nowych systemów wdrażanych w przedsiębiorstwie.

3,3

Przechowuj obrazy wzorcowe na bezpiecznie skonfigurowanych serwerach, zweryfikowanych za pomocą narzędzi do sprawdzania integralności, które umożliwiają ciągłą inspekcję i zarządzanie zmianami, aby zapewnić, że możliwe są tylko autoryzowane zmiany w obrazie.

CSC 4: Ciągła ocena podatności i działania naprawcze

4.1

Uruchamiaj zautomatyzowane narzędzia do skanowania podatności na wszystkie systemy w sieci co tydzień lub częściej i dostarczaj priorytetowe listy najbardziej krytycznych podatności każdemu odpowiedzialnemu administratorowi systemu wraz z ocenami ryzyka, które porównują skuteczność administratorów systemu i działów w zmniejszaniu ryzyka.

4.2

Koreluj dzienniki zdarzeń z informacjami ze skanowania luk w zabezpieczeniach, aby osiągnąć dwa cele. Po pierwsze, personel powinien sprawdzić, czy aktywność zwykłych narzędzi do skanowania podatności jest rejestrowana. Po drugie, personel powinien być w stanie skorelować zdarzenia wykrycia ataku z wcześniejszymi wynikami skanowania luk w zabezpieczeniach.

CSC 5: Kontrolowane korzystanie z uprawnień administracyjnych

5.1

Zminimalizuj uprawnienia administracyjne i używaj kont administracyjnych tylko wtedy, gdy są one wymagane.

5.2

Używaj zautomatyzowanych narzędzi do inwentaryzacji wszystkich kont administracyjnych i sprawdzaj, czy każda osoba z uprawnieniami administracyjnymi na komputerach stacjonarnych, laptopach i serwerach jest autoryzowana przez kierownika wyższego szczebla.

WYKRYWANIE I ODPOWIEDŹ NA CYBERATAKI

Organizacje coraz częściej akceptują fakt, że nie są w stanie zapobiec wszystkim cyberatakom. Trudność w zapobieganiu atakom nie jest równa trudności w identyfikacji i skutecznym ich łagodzeniu. Biorąc pod uwagę rodzaje luk wykorzystywanych przez atakujących i ich metody, wiele ataków i włamań nie jest od razu wykrywanych. Na przykład niektóre są rozpoznawane dopiero po miesiącach, aw niektórych przypadkach po latach. Należy położyć nacisk na usprawnienie mechanizmów wczesnego wykrywania, reagowania i odzyskiwania, aby łagodzić i lepiej zarządzać konsekwencjami ograniczającymi szkody i zapewniającymi ciągłość działania.

WYKRYWANIE

Żadna organizacja nie może się chronić bez zrozumienia, przed czym się chroni. Pierwszym działaniem, jakie każda organizacja powinna podjąć, jest zrozumienie specyfiki cyberzagrożeń, z jakimi się boryka. Cyberoszustwa są coraz powszechniejsze i dotykają wszystkich sektorów gospodarki, od handlu detalicznego i usług finansowych po opiekę zdrowotną i edukację. Cyberataki stają się coraz bardziej destrukcyjne, ponieważ są coraz bardziej publiczne i widoczne. Chociaż zapobieganie, takie jak kontrolowanie dostępu za pomocą zapory ogniowej, haseł i podobnych środków, nadal ma kluczowe znaczenie, nacisk kładzie się na odchodzenie od samej prewencji i zwracanie się na pytania, jak reagować na włamania i ograniczać powodowane przez nie szkody. Według EY, Global Information Security Survey 2015, 36% organizacji twierdzi, że jest mało prawdopodobne, aby były w stanie wykryć wyrafinowany cyberatak. To niepokojące, biorąc pod uwagę, że poziom zaawansowania stale rośnie. Cyberprzestępcy często wykazują pewne zachowania lub cechy, które mogą sugerować jako znaki ostrzegawcze lub czerwone flagi. Czynnikiem krytycznym jest to, że jest to zgłaszane odpowiednim stronom, które są w stanie w razie potrzeby podjąć odpowiednie działania na czas. EY wymienia następujące przykłady wskaźników, które radar powinien być wykrywany:

Wskaźniki potencjalnych działań związanych z oszustwami cybernetycznymi

* Bardzo widoczne ataki bez oczywistego celu: np. DDoS; skradzione szczegóły, ale bez oczywistego ich wykorzystania

* Nieoczekiwane ruchy cen akcji

* Nowe produkty wprowadzone przez konkurencję, które są niesamowicie podobne do Twoich badań i rozwoju oraz własności intelektualnej i trafiają na rynek tuż przed Twoim – wskazując na kradzież własności intelektualnej oraz znajomość Twojej strategii rozwoju i harmonogramu

* Zakłócenie fuzji i przejęć (M&A): konkurencyjne oferty, które wykazują podobieństwa i mogą wykazywać świadomość poufnych planów; Celem fuzji i przejęć są incydenty cybernetyczne (np. skradzione IP)

* Nietypowe zachowanie klientów lub spółek joint venture: pamiętaj, że nie zawsze mogą to być prawdziwi klienci lub partnerzy, ponieważ cyberprzestępcy mogą dołączyć do organizacji, aby uzyskać łatwiejszy dostęp do Twoich systemów i danych

* Nietypowe zachowanie pracowników: menedżerowie personelu muszą być bardziej świadomi zmian w zachowaniu, zwłaszcza gdy ci pracownicy pracują w bardziej wrażliwych obszarach

* Zakłócenia operacyjne, ale bez wyraźnej przyczyny

* Dziwactwa w systemach przetwarzania płatności lub zamówień

* Bazy danych klientów lub użytkowników zawierające niespójne informacje

DALSZE ROZWAŻANIE

Wykrycie naruszenia

Niezwykle ważne jest skrócenie odstępu między skutecznym wykrywaniem a reakcją – i jak najszybsze przerwanie szkodliwych skutków dla działalności. Po wezwaniu służb ratowniczych ds. kryzysu i cyberbezpieczeństwa, oto kilka kroków, które możesz podjąć:

1) Zdobądź podstawowe fakty dotyczące naruszenia i dowiedz się, czy nadal trwa. Wraz ze wzrostem złożoności sieci trudno jest określić, w jaki sposób wrogi podmiot mógł wejść do sieci. Wyrafinowane narzędzia do kryminalistyki i analizy danych – niektóre z nich są dostępne od ekspertów zewnętrznych, a inne od organów ścigania – mają kluczowe znaczenie na tym etapie.

2) Weź pod uwagę, że wykryty atak może czasami maskować głębsze wtargnięcia do Twojej organizacji, a w niektórych sytuacjach wykrycie naruszenia i rozpoczęcie ograniczania szkód może zająć tygodnie, a nie godziny.

3) Zdecyduj, czy iw jakim zakresie dążyć do zaangażowania organów ścigania i czy właściwa agencja jest lokalna czy federalna. Należy wziąć pod uwagę wiele czynników, które będą się różnić w zależności od rodzaju i skali ataku. Jest to istotna kwestia, biorąc pod uwagę, że prawie połowa respondentów wątpi w zdolność rządu do prowadzenia dochodzeń w sprawie cyberprzestępczości.

4) Rozważ ryzyko wtórne. Na przykład zwykłe naruszenie wiadomości e-mail może ujawnić tajemnice przeciwnikom. Jeśli sieci zostaną naruszone, a firma korzysta z usług telefonii VOIP/sieciowej, istnieje prawdopodobieństwo, że telefony również zostaną naruszone.

5) Wreszcie, gdy dochodzi do naruszenia, pamiętaj, że dochodzenie cybernetyczne jest nadal zasadniczo dochodzeniem i nadal obowiązują zasady dochodzenia karnego. Koncentrując się na zatrzymaniu trwającego ataku i powrocie do sieci, ważne jest, aby nieumyślnie nie zniszczyć dowodów, które mogłyby pomóc w tym dochodzeniu – i w zapobieganiu kolejnemu atakowi. Definicja standardów zawodowych zostałaby zmodyfikowana w celu dodania standardów i praktyk dotyczących systemów cyberbezpieczeństwa.

ZARZĄDZANIE REAGOWANIEM NA INCYDENTY

Nawet dobrze broniona organizacja w pewnym momencie doświadczy incydentu cybernetycznego. Planowanie i przygotowywanie się na incydent cyberbezpieczeństwa może być jednym z największych wyzwań, przed jakimi stoi każda organizacja, zwłaszcza gdy wystąpi incydent cyberbezpieczeństwa, kierownictwo musi podjąć działania i złagodzić je tak szybko, jak to możliwe – wszelkie zagrożenia dla poufności, integralności i dostępności zasoby informacyjne organizacji. Chociaż cyberzagrożenia rosną z roku na rok, przygotowania biznesowe nie dotrzymują kroku, ponieważ tylko cztery na dziesięć (37%)

organizacji posiada plan reagowania na incydenty cybernetyczne, jak wynika z globalnego badania przeprowadzonego przez PwC w 2016 roku. Biorąc pod uwagę częste stosowanie przez hakerów technik dywersyjnych, niewystarczająco skoordynowana reakcja ogranicza zdolność organizacji do zidentyfikowania i zbadania wszystkich obszarów, które faktycznie zostały naruszone. Organizacja musi być przygotowana na radzenie sobie z incydentami, które mogą pochodzić z różnych źródeł zagrażających zasobom informacyjnym, w tym cyberprzestępcom, konkurentom przemysłowym, hakerom, hakerom i pracownikom. Aby sprostać rzeczywistości, gotowość cybernetyczną należy traktować jako test warunków skrajnych organizacji. Gdy zabezpieczenia sieciowe zostaną przeniknięte, organizacja musi mieć jasny pomysł, jak prawidłowo i szybko reagować. Aby szybko zareagować i zminimalizować skutki, organizacja powinna regularnie wycinać swój udokumentowany plan reagowania na incydenty cybernetyczne w całym podmiocie. Działania wczesnej reakcji mogą ograniczyć lub nawet zapobiec możliwym uszkodzeniom. Kluczowym elementem przygotowania reakcji na incydenty cybernetyczne jest planowanie we współpracy z całym kierownictwem, liderami biznesowymi, planistami ciągłości, operatorami systemów, radcą prawnym i sprawami publicznymi. Obejmuje integrację polityk i procedur reagowania na incydenty cybernetyczne z istniejącymi planami odzyskiwania po awarii i ciągłości działania. Kanadyjska Organizacja Regulacyjna Branży Inwestycyjnej (IIROC) zasugerowała, że przy wdrażaniu zarządzania incydentami cybernetycznymi organizacje powinny wziąć pod uwagę następujące cele.

Cele zarządzania incydentami cyberbezpieczeństwa

• Unikaj incydentów związanych z cyberbezpieczeństwem, zanim się pojawią

• Zminimalizuj wpływ incydentów cyberbezpieczeństwa na poufność, dostępność lub integralność usług, zasobów informacyjnych i operacji branży inwestycyjnej

• Ograniczaj zagrożenia i luki w zabezpieczeniach w miarę występowania incydentów cyberbezpieczeństwa

• Poprawa koordynacji i zarządzania incydentami cyberbezpieczeństwa w branży inwestycyjnej

• Zmniejszenie bezpośrednich i pośrednich kosztów spowodowanych incydentami cyberbezpieczeństwa

• Zgłaszaj ustalenia kierownictwu wykonawczemu

Proaktywne planowanie reakcji na incydenty rozpoczyna się od wykrycia naruszeń, koncentrując się na domenie logowania i monitorowania platformy. Większość systemów ma wiele urządzeń, które rejestrują różne rodzaje aktywności. Na przykład dzienniki zapory i dzienniki aplikacji przechowują informacje o tym, kto się loguje, kto zmienia dane, jakie rekordy przegląda i inne informacje. Po wykryciu przychodzi odpowiedź. W jaki sposób organizacja odzyskuje siły po incydencie? W jaki sposób organizacja ogranicza szkody i powstrzymuje wszelkie nielegalne działania, które nadal toczą się w sieci? Pytania te są krytycznymi elementami planu reagowania na incydenty cyberbezpieczeństwa, który obejmuje również plan komunikacji w celu informowania stron bezpośrednio dotkniętych; inni interesariusze, tacy jak członkowie zarządu, sprzedawcy i klienci; i wreszcie świat zewnętrzny. Plan reagowania na incydenty cyberbezpieczeństwa powinien odzwierciedlać branżę, wielkość organizacji i inne czynniki, takie jak ogólne ramy cyberbezpieczeństwa, ponieważ żaden model nie pasuje do wszystkich sytuacji. Zazwyczaj zarys planu reagowania na incydenty składa się z następujących podstawowych kroków sugerowanych przez Crowe Horwath LLP.

Proaktywne planowanie reagowania na incydenty

1) Inwentaryzacja i zrozumienie danych, które mają być chronione.

2) Inwentaryzacja i klasyfikacja incydentów.

3) Zrozum znane zagrożenia i monitoruj nowe.

4) Zidentyfikuj interesariuszy i zespół reagowania na incydenty — komunikacja korporacyjna, prawnicy, zgodność, linie biznesowe, IT i zewnętrzni partnerzy kryminalistyczni.

5) Skonfiguruj centrum dowodzenia.

6) Opracowanie i wdrożenie strategii powstrzymywania i badania.

7) Opracowanie i wdrożenie strategii ochrony dowodów.

8) Opracuj i wdroż plan komunikacji dla klientów, mediów, regulatorów i innych interesariuszy.

9) Przeprowadź sekcję zwłok i zastosuj wyciągnięte wnioski.

Organizacje mogą być przytłoczone potencjalnie ogromną ilością danych. Dlatego nawiązanie relacji z organizacjami udostępniającymi informacje cybernetyczne ma kluczowe znaczenie dla agregacji danych i filtrowania fałszywych alarmów. Organizacje wymiany i analizy informacji (ISAO), których celem jest pomoc firmom w dzieleniu się informacjami o zagrożeniach między sobą oraz z sektorem publicznym, już wykazują znaczne postępy. Liczne podmioty z sektora publicznego i prywatnego utworzyły ISAO lub ogłosiły takie plany. Przykłady obejmują między innymi Commonwealth of Virginia ISAO, The Legal Services ISAO, Retail Industry ISAO, The National Credit Union ISAO oraz Maritime & Port Security Information Sharing and Analysis Organization. Według PwC większość organizacji twierdzi, że współpraca zewnętrzna pozwala im udostępniać i otrzymywać bardziej przydatne informacje od partnerów z branży, a także od centrów wymiany i analizy informacji (ISAC). Wiele osób zgłasza również, że udostępnianie informacji poprawiło ich świadomość zagrożeń i inteligencję. Według PwC, ISAO zapewniają wyjątkowo potężny model udostępniania informacji o cyberbezpieczeństwie, z następującymi potencjalnymi korzyściami.

Jak ISAO poprawiają perspektywy udostępniania informacji

* Tworzenie zaufanej i połączonej sieci, która znacznie wzmacnia możliwości poszczególnych organizacji w zakresie identyfikowania i ograniczania zagrożeń cybernetycznych.

* Szybkie dostarczanie praktycznych informacji o zagrożeniach cybernetycznych w celu wsparcia wymiernych ulepszeń w zakresie cyberbezpieczeństwa.

* Obniżenie kosztów i barier wejścia w zakresie udostępniania informacji dotyczących cyberbezpieczeństwa.

* Usprawnienie i uproszczenie zarządzania informacjami, analizą i inteligencją w zakresie cyberbezpieczeństwa.

* Kwalifikowanie członków do ochrony prawnej przed niektórymi działaniami odpowiedzialności, antymonopolowymi i regulacyjnymi.

* Pomoc w spełnieniu lub przekroczeniu rosnących oczekiwań organów regulacyjnych w zakresie ograniczania ryzyka cybernetycznego w czasach, gdy kierownictwo firmy jest coraz bardziej pociągane do odpowiedzialności za naruszenia.

* Przekształcenie modeli biznesowych w zakresie wymiany informacji w celu zwiększenia ekonomii skali.

Stany Zjednoczone nie są jedynym krajem, który podkreśla siłę partnerstwa. Na przykład UE zatwierdziła dyrektywę w sprawie bezpieczeństwa sieci i informacji, która określa podobne cele. Dyrektywa wymaga, aby państwa członkowskie utworzyły zespół reagowania na incydenty związane z bezpieczeństwem komputerowym (CSIRT) oraz aby przedsiębiorstwa w infrastrukturze krytycznej powiadamiały organy krajowe o wystąpieniu incydentów cybernetycznych. Nakazuje również przedsiębiorstwom utworzenie grupy współpracy w celu ułatwienia wymiany informacji o ryzyku. W Wielkiej Brytanii cztery duże banki utworzyły Sojusz ds. Obrony Cybernetycznej, aby współpracować z brytyjską Krajową Jednostką ds. Cyberprzestępczości. Ta branżowo-rządowa grupa ma na celu umożliwienie bankom wymiany aktualnych informacji na temat technik inteligencji i reagowania na zagrożenia cybernetyczne.

CYBER UBEZPIECZENIE

RYNEK UBEZPIECZEŃ CYBER W SKRÓCIE

Ubezpieczenia cybernetyczne to jeden z najszybciej rozwijających się sektorów na rynku ubezpieczeniowym, ponieważ wykorzystanie technologii stało się tak powszechne. Błędy w zabezpieczeniach w dzisiejszej gospodarce opartej na informacjach mogą spowodować znaczne długoterminowe wydatki dla dotkniętych nimi organizacji i poważnie zaszkodzić zaufaniu konsumentów i reputacji marki. Celowanie w zasoby elektroniczne może wywrzeć istotny wpływ na całą organizację i prawdopodobnie jej partnerów, gdy wrażliwe informacje o klientach, własność intelektualna, a nawet kontrola kluczowych maszyn są coraz bardziej zagrożone cyberatakiem. Według Allianz Global Corporate & Specialty wzrost nastąpi w miarę nabywania przez organizacje ubezpieczenia cybernetycznego w szerszym zakresie i wielkości. W miarę wzrostu świadomości ryzyka będą coraz częściej badać swoje możliwości przeniesienia ryzyka. Na przykład sektory, które przechowują duże ilości danych osobowych, takie jak opieka zdrowotna i handel detaliczny, lub sektory opierające się na zdigitalizowanych operacjach procesów technologicznych, takich jak logistyka, produkcja i telekomunikacja, obecnie najczęściej kupują ubezpieczenie cybernetyczne. Rośnie również zainteresowanie wśród instytucji finansowych oraz sektorów energii, usług użyteczności publicznej i transportu, napędzane rosnącymi zobowiązaniami wynikającymi z wzajemnych połączeń. Rynek ubezpieczeń cybernetycznych jest obecnie szacowany na około 2 miliardy USD składki na całym świecie, przy czym rynek ubezpieczeń cybernetycznych w USA stanowi około 90%. Wśród wielu wczesnych użytkowników znalazły się firmy świadczące usługi finansowe, sprzedawcy detaliczni i organizacje opieki zdrowotnej z dużą ilością informacji umożliwiających identyfikację osoby ze względu na obowiązkowe przepisy dotyczące powiadamiania o naruszeniu danych. Dlatego rynek ubezpieczeń cybernetycznych rozwijał się znacznie szybciej w USA niż w UE. Jednak rynek europejski nadrabia zaległości, ponieważ unijne ogólne rozporządzenie o ochronie danych (RODO) wymaga szybkiego powiadamiania organów nadzorczych o naruszeniach ochrony danych osobowych. Rynek ubezpieczeń cybernetycznych rośnie w tempie dwucyfrowym rok do roku i może osiągnąć ponad 20 miliardów dolarów w ciągu najbliższych 10 lat.

Dlaczego ubezpieczenie cybernetyczne?

* Wzrasta częstotliwość naruszeń prywatności.

* Zagrożenia i luki w zabezpieczeniach stają się dramatycznie gorsze.

* Ponad 40 stanów uchwaliło przepisy dotyczące prywatności w odpowiedzi na częstotliwość naruszeń prywatności.

* Ład korporacyjny wymaga, aby organizacje zajmowały się ryzykiem związanym z technologią informacyjną.

* Akcjonariusze oczekują, że ich inwestycja jest chroniona przed niekorzystnymi wahaniami rynku.

* Korporacje notowane na giełdzie i duże korporacje prywatne mogą doświadczyć sporów akcjonariuszy z powodu niewłaściwego zarządzania ryzykiem cybernetycznym.

* Adwokatura powodów staje się bardziej aktywna w prowadzeniu sporów zbiorowych.

* Umowy mogą wymagać ubezpieczenia cybernetycznego.

* Ubezpieczenie cybernetyczne może złagodzić wpływ finansowy na firmę.

UTRATA FINANSOWA NARUSZENIA BEZPIECZEŃSTWA/PRYWATNOŚCI

Według niedawnego badania Ponemon przeprowadzonego na 252 organizacjach, w USA odnotowano najwyższy łączny średni koszt cyberprzestępczości na poziomie 15 mln USD, a próba rosyjska wykazała najniższy średni koszt w wysokości 2,4 mln USD. Niemcy, Japonia, Australia i Rosja odnotowały niewielki spadek kosztów cyberprzestępczości w ciągu ostatniego roku. Wynik ten jest jednak spowodowany różnicami kursowymi w ciągu ostatniego roku wynikającymi z silnego dolara amerykańskiego w stosunku do innych walut lokalnych. W związku z tym, biorąc pod uwagę różnice kursowe, w rzeczywistości następuje wzrost netto całkowitych kosztów cyberprzestępczości. Zgodnie z raportem The Cost of Cybercrime wydanym przez brytyjski gabinet, poniżej wymieniono główne obszary, które mogą mieć wpływ na strukturę kosztów rządu lub organizacji:

* Koszty w oczekiwaniu na cyberprzestępczość: Środki bezpieczeństwa, takie jak instalacja oprogramowania antywirusowego, koszty ubezpieczenia i utrzymanie standardów bezpieczeństwa IT.

* Koszty będące konsekwencją cyberprzestępczości: Straty pieniężne dla organizacji, takie jak brak ciągłości działania i straty spowodowane kradzieżą IP.

* Koszty reakcji na cyberprzestępczość: płacenie grzywien i odszkodowań dla ofiar kradzieży tożsamości oraz koszty związane z dochodzeniem w sprawie przestępstwa.

* Koszty pośrednie związane z cyberprzestępczością: koszty wynikające z utraty reputacji organizacji i utraty zaufania do transakcji cybernetycznych

Przedstawione poniżej koszty cyberprzestępczości odnoszą się zarówno do radzenia sobie z cyberprzestępczością jako kosztem wewnętrznym (np. wykrywanie, odzyskiwanie i reagowanie na incydent), jak i konsekwencjami cyberataku jako konsekwencjami zewnętrznymi (np. przerwanie działalności i utrata przychodów). we wszystkich krajach.

Ramy kosztów dla cyberprzestępczości

Centra działalności związanej z kosztami wewnętrznymi: Konsekwencje i koszty zewnętrzne

• Wykrycie : • Utrata lub kradzież informacji

• Dochodzenie i eskalacja : • Przerwa biznesowa

• Przechowywanie : • Uszkodzenie sprzętu

• Powrót do zdrowia : • Utrata przychodów

• Odpowiedź ex post

Wśród organizacji reprezentowanych w tym badaniu Ponemon zakłócenia biznesowe stanowią największy składnik kosztów (39%). Koszt zakłócenia działalności biznesowej obejmuje zmniejszoną produktywność pracowników i awarie procesów biznesowych, które mają miejsce po cyberataku. Utrata informacji i przychodów wynosi odpowiednio 35% i 21%. Badanie pokazuje również, że firmy wydają najwięcej na wykrywanie i odzyskiwanie. Działania w zakresie wykrywania i odzyskiwania cyberprzestępczości stanowią 53% całkowitych kosztów działalności wewnętrznej. Za nimi plasują się koszty hermetyzacji i badania (odpowiednio 16% i 14%).

Jaka jest strata finansowa w wyniku naruszenia bezpieczeństwa/prywatności?

* Koszt obrony i/lub rozstrzygnięcia sporu z klientami lub pracownikami w związku z kradzieżą tożsamości.

* Koszt obrony i/lub rozstrzygnięcia sporu z bankami w celu odzyskania wartości ponownego wydania kart kredytowych lub nieuczciwych transakcji.

* Koszt obrony i/lub rozstrzygnięcia dochodzeń regulacyjnych i sądowych.

* Koszt odpowiedzi na przepisy regulacyjne.

* Koszt obrony i/lub rozliczenia nieautoryzowanego dostępu lub nieuprawnionego użycia.

* Koszt obrony i/lub rozstrzygnięcia zarzutów, że złośliwy kod (np. wirusy) spowodował szkody w danych lub systemach komputerowych osób trzecich.

* Koszt obrony i/lub rozstrzygnięcia zarzutów, że system komputerowy ubezpieczonego odmówił stronie trzeciej możliwości przeprowadzania transakcji.

* Koszt obrony i/lub rozstrzygnięcia sporu z klientami lub pracownikami w związku z kradzieżą tożsamości.

ROLA CYBER UBEZPIECZEŃ

Stale ewoluujący krajobraz ryzyka cybernetycznego powoduje zainteresowanie ubezpieczeniami cybernetycznymi jako jednym uzupełniającym elementem zarządzania ryzykiem cybernetycznym. Zaawansowani technicznie przeciwnicy zawsze znajdą nowe sposoby na obejście zabezpieczeń cybernetycznych. Dlatego zaawansowane technologie cyberbezpieczeństwa nie powstrzymają wszystkich cyberataków. Według globalnego badania EY, 56% respondentów twierdzi, że jest „mało prawdopodobne lub wysoce nieprawdopodobne", aby ich organizacja była w stanie wykryć wyrafinowany atak. Wiele organizacji uświadomiło sobie, że cyberatak jest nieunikniony. Nie jest to kwestia „czy" to się stanie, ale „kiedy". Organizacje mogą być chronione przed następującymi zagrożeniami w przypadku utraty lub incydentu związanego z cyberbezpieczeństwem dzięki swoim polisom ubezpieczeniowym (z ubezpieczeniem premium/premium plus).

Obszary ryzyka cyberbezpieczeństwa

* Ochrona prywatności i naruszenia danych

* Pokrycie kosztów przerwania działalności i przywrócenia

* Ochrona roszczeń dotyczących bezpieczeństwa sieci

* Ochrona roszczeń z tytułu odpowiedzialności za media

* Pokrycie kosztów regulacyjnych

* Grzywny ustawowe i kary pokrywają

* Koszty powiadomień

* Koszty odpowiedzi

* Ochrona przed kradzieżą hakera

* Ochrona komunikacji kryzysowej

* Pokrycie usług konsultanta

* Płatności elektroniczne

* Okładka cyberwymuszenia

Organizacje mogą wdrożyć szereg środków ryzyka w celu zapobiegania, wykrywania i kontroli reagowania w celu utrzymania zagrożeń cybernetycznych na akceptowalnym poziomie. Nie da się być w 100% bezpiecznym, nawet jeśli istnieje solidne podejście do zarządzania ryzykiem cybernetycznym. Chociaż ubezpieczenie cybernetyczne nie zastępuje dobrego cyberbezpieczeństwa, odgrywa kluczową rolę jako część holistycznej strategii zarządzania ryzykiem, tworząc drugą linię obrony w celu złagodzenia incydentów cybernetycznych. Ubezpieczenie cybernetyczne może zapewnić ochronę w najgorszym przypadku, umożliwiając organizacjom przeniesienie części ryzyka związanego z incydentami cybernetycznymi na swojego dostawcę ubezpieczeń. Z tego powodu wiele firm kupuje ubezpieczenia cybernetyczne, aby złagodzić finansowe skutki cyberprzestępczości, gdy się one pojawią. Oprócz ograniczania ryzyka finansowego związanego z cyberprzestępczością, organizacje, które kupują ubezpieczenie, mogą lepiej zrozumieć swoją gotowość do cyberprzestępczości. Ubezpieczyciele wymagają bowiem dokładnej oceny aktualnych możliwości i ryzyka jako warunku zakupu polisy. Oceny te mogą pomóc organizacjom w lepszym przewidywaniu narażeń prawnych i regulacyjnych, kosztów reakcji i potencjalnych szkód dla marki związanych z zagrożeniami cyberbezpieczeństwa.

UWAGI DOTYCZĄCE WYSTARCZAJĄCEGO POKRYCIA

W wielu przypadkach tradycyjna ochrona ubezpieczeniowa nie obejmuje pełnego zakresu zagrożeń i potencjalnych strat, jakie niosą ze sobą cyberryzyka. Na początku XXI wieku ubezpieczyciele zaczęli oferować polisy ubezpieczeniowe ukierunkowane na ochronę przed stratami finansowymi wynikającymi z naruszenia bezpieczeństwa danych. Obecnie własne produkty ubezpieczeniowe obejmują niszczenie danych, ataki typu „odmowa usługi", kradzież i wyłudzenia; mogą również obejmować koszty reagowania na incydenty i działań naprawczych, dochodzenia i audytu cyberbezpieczeństwa. Organizacje muszą być świadome wpływu, jaki incydent cybernetyczny może mieć na ich łańcuch dostaw, odpowiedzialności, jaką mogą ponieść, jeśli nie mogą dostarczyć swoich produktów na czas lub jeśli stracą dane klientów, wszelkich przepisów jurysdykcyjnych, które mogą mieć zastosowanie. Inne kluczowe obszary ochrony obejmują powiadomienia o prywatności, zarządzanie kryzysowe, dochodzenia kryminalistyczne, przywracanie danych i przerwy w działalności. Typowa ochrona oferowana obecnie w ramach polityki cybernetycznej może obejmować:

Przykłady ubezpieczenia cybernetycznego

Ubezpieczenie strony pierwszej:

Zatrudnianie profesjonalnej odpowiedzi:

• Adwokaci doradzający

• Firmy public relations

• Firmy zarządzania kryzysowego

• Firmy zajmujące się informatyką śledczą

Koszty powiadomienia:

• Koszty bezpośrednie, w tym drukowanie/wysyłka

• Usługi monitorowania kredytów dla dotkniętych osób

Koszty administracyjne ochrony:

• Szkolenie pracowników

• Tworzenie portali informacyjnych

• Tworzenie bezpieczeństwa i reagowania na incydenty

• Rekompensata ubezpieczonemu za utracony dochód w wyniku naruszenia

• Przywracanie utraconych danych

Ubezpieczenie strony trzeciej:

• Koszt obrony regulacyjnej, w tym grzywny i odszkodowanie karne

• Koszt obrony przed sporami

• Odszkodowania sądowe

Kierownictwo powinno określić rodzaj i zakres ubezpieczenia, który najlepiej służy interesom organizacji, aby zapewnić, że ubezpieczenie jest dostosowane do pełnego zakresu potencjalnego narażenia, na jakie incydent cybernetyczny naraziłby organizację. Kierownictwo powinno również rozważyć ochronę z mocą wsteczną. Naruszenia cybernetyczne mogą trwać miesiące, a nawet lata bez wykrycia, dlatego organizacje powinny wziąć pod uwagę, że mogły już paść ofiarą niewykrytego naruszenia w momencie, gdy szukają ochrony. W niektórych przypadkach ubezpieczyciele mogą chcieć zapewnić ochronę z mocą wsteczną do dwóch lat przed sporządzeniem polisy. Funkcja ta jest jednak w dużym stopniu zależna od unikalnego profilu ryzyka potencjalnego ubezpieczonego i charakteru istniejącego wcześniej programu cyberbezpieczeństwa. Ponadto, dokonując przeglądu potencjalnych ubezpieczycieli, należy mieć świadomość, że:

* Rynek ubezpieczeń cybernetycznych znajduje się głównie w fazie kształtowania, w której polisy różnią się znacznie od jednego dostawcy do drugiego;

* Zasięg może być niewystarczający w niektórych obszarach, takich jak kradzież własności intelektualnej, uszczerbek na reputacji i awarie infrastruktury cybernetycznej;

* Dane aktuarialne są ograniczone dla ubezpieczycieli w celu dostosowania składek na podstawie tego, które środki bezpieczeństwa i produkty są najskuteczniejsze, oraz

*Ubezpieczenia cybernetyczne mogą przewidywać wyłączenia, nakładać limity lub dodawać klauzule chroniące ubezpieczyciela przed wyższymi zagrożeniami, takimi jak niewykonanie usług dostawcy usług w chmurze, niezaszyfrowane urządzenia zawierające dane osobowe lub inne wrażliwe dane oraz awarie oprogramowania komputerowego spowodowane błędami programowania ;

Wiele dużych firm próbuje uzyskać polisy o wartości 80-100 mln USD, podczas gdy mniejsze firmy decydują się na polisy o wartości 10 mln USD. Według PwC nie ma jednego uniwersalnego zalecenia dotyczącego polityki, aby przedsiębiorcy rozumieli, że nie będą w stanie ubezpieczyć pełnego ryzyka straty, ponieważ rynek po prostu nie ma jeszcze podaży. Przy ustalaniu zakresu ubezpieczenia kierownictwo powinno wziąć pod uwagę następujące czynniki:

• Wielkość spółki

• Sektor przemysłowy

• Rodzaje gromadzonych, przetwarzanych i przechowywanych danych

• Naruszenie informacji prawnie zobligowanych do ochrony

• Dojrzałość kontroli bezpieczeństwa

• Tolerancja ryzyka

PRZYKŁAD Z PRAWDZIWEGO ŚWIATA

Przykłady roszczeń z tytułu odpowiedzialności za bezpieczeństwo

• Haker przeniknął do witryny zakupów online i ukradł 300 000 numerów kart kredytowych klientów. Serwis spotkał się z roszczeniami klientów o nieautoryzowane obciążenia kart kredytowych.

• Firmy, które nieświadomie rozpowszechniają robaka, wirusa lub inny szkodliwy plik za pośrednictwem poczty e-mail na osoby trzecie, mogą ponosić odpowiedzialność tych osób trzecich za dochody utracone w wyniku przeciążenia przez wirusa sieci komputerowych osób trzecich.

• Niezadowolony pracownik uszkodził dane w systemie firmy, który został wykorzystany do uaktualnienia produktu już dostępnego na rynku. Korupcja spowodowała szkody dla klientów próbujących unowocześnić produkt, a także opóźnienia, przekroczenia kosztów itp., skutkując stratą w wysokości 50 milionów dolarów.

Przykłady roszczeń z tytułu odpowiedzialności za prywatność

• Operator internetowej tablicy ogłoszeń wytoczył pozew przeciwko parze, która zamieściła na tablicy wiele niegrzecznych i zawierających groźby wiadomości. Para złożyła pozew wzajemny, twierdząc, że użycie przez operatora plików cookie stanowi naruszenie, konwersję i naruszenie prywatności.

• Właściciel firmy został pozwany po tym, jak złodzieje tożsamości byli w stanie:

uzyskać osobiste informacje konsumenckie klientów ze śmietnika wyrzuconych plików.

Przykłady roszczeń z tytułu odpowiedzialności za media elektroniczne

• Powód, odrzucony kandydat na szeryfa hrabstwa, twierdził, że właściciel strony internetowej zezwolił na publikowanie zniesławiających treści na swojej stronie internetowej, co spowodowało, że przegrał wybory.

• Właściciele materiału wideo pozwali właściciela witryny o naruszenie praw autorskich, twierdząc, że witryna transmitowała materiał do transmisji internetowej bez zezwolenia. Pojawił się problem dotyczący tego, czy strona, od której właściciel witryny uzyskał nagranie, faktycznie posiadała prawa do nagrania wideo do przeniesienia.

• Powód pozwał magazyn internetowy, twierdząc, że opublikował jego zdjęcie bez pozwolenia.