Miesięcznik
Ubezpieczeniowy

ISSN 1732-2413 • WSZYSTKO, CO TRZEBA WIEDZIEĆ O RYNKU UBEZPIECZEŃ • TOM 17 I NUMER 9 I WRZESIEŃ 2020 • 3 WRZEŚNIA 2020

W NUMERZE:

BI w centrum uwagi

dystrybucja, produkty, konstrukcja, oczekiwania rynkowe

Bartosz Grześkowiak o konsolidacji/Cyfrowa obsługa/Utrata wartości handlowej

Skuteczna ochrona przed cyberatakami

Wraz z pandemią Covid-19 dla firm szczególnie ważne stały się kwestie bezpieczeństwa IT. Początkowo priorytetem było szybkie umożliwienie na szeroką skalę pracy zdalnej, przy jednoczesnym zachowaniu poufności, integralności i dostępności usług dla klientów. Teraz konieczne jest sprawdzenie bezpieczeństwa wprowadzanych zmian i dostosowanie strategii ochrony danych. – Dariusz Smoleń, Rafał Domański, Oskar Sokoliński

Ujawnienie wycieku danych czy wypłata odszkodowań na fikcyjne konta w wyniku działań cyberprzestępców to ogromne zagrożenie dla wizerunku ubezpieczyciela. Z kolei w nowej, pandemicznej rzeczywistości szybko odnaleźli się cyberprzestępcy, chcący wykorzystać słabsze bezpieczeństwo sieci i komputerów domowych. Jak podaje Google, każdego dnia w kwietniu odnotowano ponad 18 milionów przypadków zidentyfikowanego złośliwego oprogramowania i wiadomości phishingowych, związanych z sytuacją pandemiczną (Źródło: Threat Analysis Group, „Findings on COVID-19 and online security threats," blog.google). Atakujący próbują wykorzystywać także luki w zabezpieczeniach powstałe ze względu na zmianę sposobu pracy. Jak wskazują analizy, od początku pandemii ponad 80% firm odnotowało kilka lub więcej prób cyberataku, co jest ogromnym wzrostem względem czasów sprzed pandemii (Źródło: *The Exabeam 2020 State of the SOC Report,* Exabeam).

LUDZIE I PROCESY

Bezpieczeństwo informacji i ochrona przed cyfrowymi zagrożeniami to nie tylko aspekty technologiczne, ale przede wszystkim ludzie i procesy. Dlatego, żeby skutecznie odpowiadać na ostatnie wyzwania związane z cyberbezpieczeństwem, należy uwzględnić wszystkie te trzy wymiary, a kluczowa kwestia ludzi dotyczy zarówno aspektów bezpieczeństwa pracowników, jak i klientów.

Bardzo ważnym aspektem bezpieczeństwa jest świadomość zagrożeń wśród pracowników. Nawet przy najlepszej kontroli technologii, pracownicy pracujący w domu muszą nadal kierować się rozsądkiem, aby zachować bezpieczeństwo informacji. Dodatkowy stres związany z pandemią, może zwiększyć ich podatność na ataki socjotechniczne. Niektórzy pracownicy mogą częściej niż w biurze podejmować działania, które otwierają ich na zagrożenia, takie jak odwiedzanie złośliwych witryn internetowych, w normalnych warunkach blokowanych przez sieci biurowe. Budowanie świadomości wśród pracowników wymaga kilku działań ze strony zespołów ds. bezpieczeństwa. Podstawą jest efektywna komunikacja. Niestety, w dobie pandemii, ostrzeżenia dotyczące cyberbezpieczeństwa mogą się zagubić wśród komunikatów związanych z kryzysem. Zespoły zajmujące się tym obszarem mogą jednak stosować niekonwencjonalne metody. Przykładem może być ustanowienie dwukierunkowych kanałów komunikacji, które pozwolą użytkownikom publikować i przeglądać pytania, zgłaszać incydenty w czasie rzeczywistym i dzielić się najlepszymi praktykami. Może to być także umieszczanie ogłoszeń w postaci komunikatów pojawiających się po zablokowaniu ekranu w służbowych komputerach.

Kolejnym ważnym aspektem jest treść komunikacji i koncertowanie się na przekazywaniu pracownikom wskazówek o tym, jak postępować, zamiast wskazywać na to, czego nie robić. Mówienie pracownikom, aby nie korzystali z ogólnodostępnych narzędzi (takich jak internetowe mapy), które mogą im wydawać się niezbędne, może przynieść efekt przeciwny do zamierzonego. Zamiast tego zespoły ds. bezpieczeństwa powinny wyjaśniać korzyści, takie jak bezpieczeństwo i podniesienie produktywności, wynikające z używania zatwierdzonych w firmie narzędzi. Także kampanie symulujące działania phishingowe są jednym ze sposobów na pokazanie, a tym samym przygotowanie pracowników na potencjalną próbę ataku w sieci.

Dodatkowo warto zidentyfikować i monitorować grupy użytkowników wysokiego ryzyka, w tym pracowników mających styczność z poufnymi danymi. Wychwytywanie w porę nietypowych zachowań (takich jak nietypowe wzorce przepustowości lub zbiorcze pobieranie danych przedsiębiorstwa), które mogą wskazywać na naruszenia bezpieczeństwa za pośrednictwem ich komputerów, może uchronić przed wyciekiem danych.

PODRÓŻ KLIENTA

Czynnik ludzki to nie tylko pracownicy, ale także interakcje z klientem. Od wybuchu epidemii cyberprzestępcy mają

Dr Dariusz Smoleń,
starszy konsultant w warszawskim biurze McKinsey. Wspiera klientów z sektora ubezpieczeniowego.

Rafał Domański,
partner lokalny w warszawskim biurze McKinsey. Wspiera klientów z sektora ubezpieczeniowego.

Oskar Sokoliński,
partner lokalny w warszawskim biurze McKinsey. Wspiera klientów z sektora ubezpieczeniowego.

więcej możliwości działania, wykorzystując luki w zabezpieczeniach związane z tożsamością konsumenta i kontrolą zarządzania dostępem. Tymczasem klienci oczekują łatwiejszej obsługi cyfrowej, w tym szybkiego uwierzytelniania i logowania, a także interaktywności - np. przy zakupie polis czy samolikwidacji drobnych szkód komunikacyjnych online. Firmy, które będą w stanie to wszystko zaoferować przy zachowaniu wysokich standardów bezpieczeństwa, mogą zdobyć lojalność klientów. Aby ograniczyć ryzyka, organizacje muszą poznać ścieżki poruszania się klientów po portalach. Chodzi o odpowiednio zdefiniowane osobowości konsumentów, z których każda ma przypisane cechy, zachowanie, postawy i określone problemy, z którymi się mierzy (ang. *pain points*). Katalog osobowości użytkowników i podróży konsumenta (ang. *customer journey*) powinien być wystarczająco obszerny, aby objąć jak najwięcej rzeczywistych użytkowników portalu.

Następnie dla kluczowych ścieżek tj. najczęściej występujących profili klientów i ich interakcji (np. zgłoszenie szkody) należy zdefiniować potencjalne ryzyka i zabezpieczenia. Ustalając wśród nich priorytety, analizuje się ścieżki klientów, przyjmując perspektywę cyberprzestępcy. W ramach takich analiz powstają mapy „podróży napastnika", podobnie jak mapy podróży użytkowników. Odzwierciedlają one, jak cyberprzestępca może wykorzystać słabości systemu, a następnie pomagają zdefiniować nowe mechanizmy kontroli. Na rysunku 1. przedstawiono przykładową analizę ścieżki dla klienta korzystającego z portalu ubezpieczeniowego.

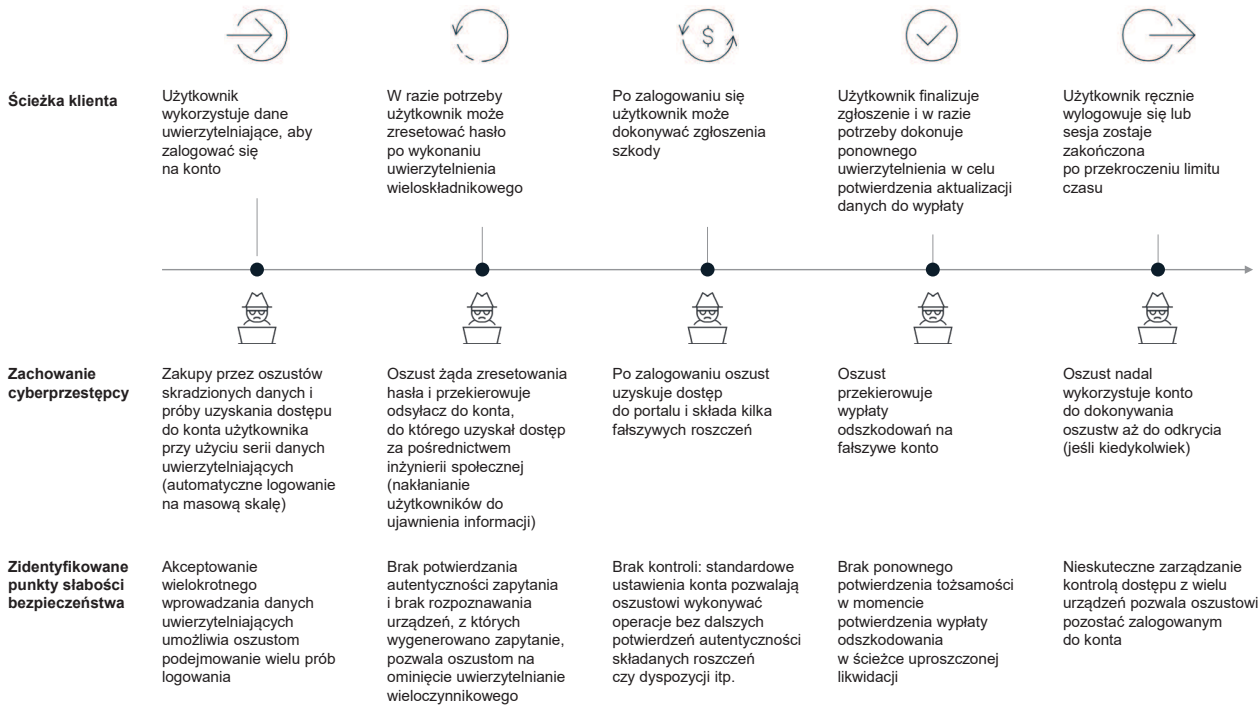
Przy tworzeniu zabezpieczeń, należy jednak pamiętać o zachowaniu równowagi pomiędzy bezpieczeństwem a łatwością obsługi przez klienta. W przypadku obsługi szkód, zbyt radykalne zabezpieczenia sprawią, że klient nie skorzysta z opcji uproszczonej ścieżki likwidacji. Z kolei zbyt luźne zasady mogą otworzyć furtkę dla wypłat fikcyjnych odszkodowań lub realizacji odszkodowań na fałszywe konta. Znalezienie kompromisu wymaga wielokrotnego powtarzania analiz bezpieczeństwa oraz testów A/B sprawdzających doświadczenia i odczucia klientów.

KORZYSTANIE Z TECHNOLOGII

Kolejnym ważnym dla bezpieczeństwa aspektem, szczególnie przy pracy zdalnej na szeroką skalę, jest technologia. Obszarem, który nie wymaga istotnych nakładów, a pomaga szczególnie w czasie dynamicznych zmian, jest przyspieszanie cyklu wdrażania poprawek dla krytycznych systemów. Skrócenie cykli aktualizacji systemów, choćby takich jak wirtualne sieci prywatne (VPN) czy interfejsy w chmurze, pomoże szybko eliminować luki wkrótce po ich wykryciu.

Ważnym elementem wymagającym wysiłku jest skalowanie uwierzytelniania wieloskładnikowego, szczególnie istotnego przy dostępie do sieci i krytycznych aplikacji. Szybkie zwiększenie skali korzystania z tego rodzaju uwierzytelnienia może być trudne. Jednak kilka praktyk sprawia, że wdrażanie takiej usługi jest łatwiejsze w zarządzaniu. Jedną z nich jest nadanie priorytetu użytkownikom, którzy mają podwyższone uprawnienia (tacy jak administratorzy domen oraz twórcy aplikacji) i pracują z krytycznymi systemami (na przykład osoby obsługujące przelewy pieniężne). Pilotażowe wdrożenia na niewielką skalę dla tych użytkowników umożliwią zespołom ds. cyberbezpieczeństwa wyciąganie wniosków i wykorzystywanie ich do kształtowania szerszych planów wdrożeniowych, pozwalając w pierwszej kolejności zabezpieczyć krytyczne obszary. Może to także ułatwić przyśpieszenie wdrażania rozwiązań chmurowych, które ułatwiają pracownikom pracę z domu.

Rys. 1. Analiza potencjalnych ryzyk dla klienta zgłaszającego szkodę za pomocą portalu ubezpieczeniowego

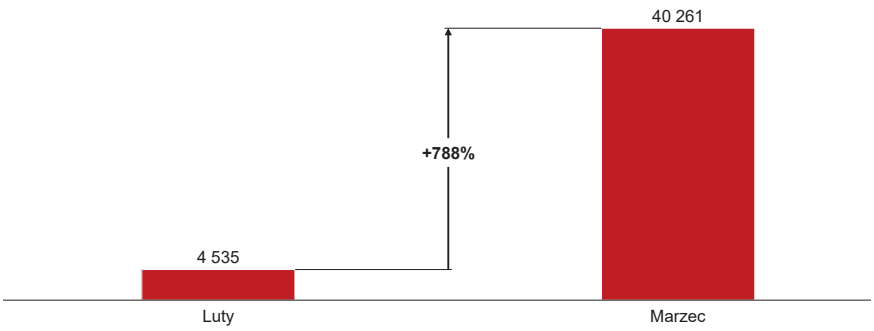


Zmiany dotyczyć mogą również procesów biznesowych. Niewiele z nich jest zaprojektowanych do obsługi pracy z domu na szeroką skalę, więc większości brakuje odpowiednich elementów sterujących. Na przykład pracownik, który nigdy nie wykonywał pracy zdalnej wysokiego ryzyka i nie skonfigurował sieci VPN, może nie być w stanie tego zrobić. W takich przypadkach konieczne jest wzmocnienie narzędzi wspierających pracę zdalną. Na czas wzmożonego zapotrzebowania, podczas gdy wyjątkowo duża liczba pracowników instaluje i konfiguruje podstawowe narzędzia bezpieczeństwa, serwisy pomocy technicznej i bezpieczeństwa wymagają zwiększonej dostępności.

Zdefiniowania może wymagać także podejście do zabezpieczania dokumentów fizycznych. W biurze pracownicy często mają łatwy dostęp do bezpiecznych mechanizmów udostępniania dokumentów w wersji elektronicznej, a także niszczarek i bezpiecznych pojemników na materiały drukowane. W domu, wrażliwe informacje mogą trafić do kosza lub zostać przekazane niezabezpieczoną drogą (np. prywatnym mailem). Konieczne jest ustalenie norm dotyczących przesyłania dokumentów elektronicznych oraz przechowywania i niszczenia fizycznych kopii.

Przy prawie sześciokrotnym wzroście liczby złośliwych maili i oprogramowania w trakcie pandemii (Źródło: *COVID-19 Cybercrime Analysis Report*, Interpol) warto także rozszerzyć zakres działań monitorujących całą organizację, w szczególności danych i punktów końcowych.

Rys. 2. Wzrost liczby złośliwych maili i oprogramowania zaklasyfikowanych jako wysokiego ryzyka, luty-marzec 2020, Interpol



Źródło: Interpol, raport:COVID-19 Cybercrime Analysis Report – August 2020.

Podstawowe mechanizmy ochrony wewnętrznej sieci, takie jak serwery proxy, bramy internetowe, systemy wykrywania włamań lub systemy zapobiegania włamaniom, nie zabezpieczą użytkowników pracujących z domu, poza siecią firmową i bez połączenia do sieci VPN. W zależności od stosowanych zabezpieczeń organizacje, które nie wymagają korzystania z sieci VPN lub wymagają jedynie jej dostępu do ograniczonego zestawu zasobów, mogą pozostać w dużej mierze niezabezpieczone. Konsekwentnie wraz ze wzrostem monitorowania potrzebne jest także dostosowanie protokołów reagowania na incydenty. W przypadku incydentów cybernetycznych pracownicy muszą wiedzieć, jak je zgłaszać. Ponadto liderzy ds. cyberbezpieczeństwa powinni przygotować procesy tak, aby odpowiedzi na napływające zgłoszenia nie utknęły w martwym punkcie, chociażby z powodu braku dostępności w danej chwili osoby decydującej o działaniach, czy ze względu na skokowy wzrost zgłoszeń.

© Fotolia

FIRMA JAKO EKOSYSTEM

Analizując procesy, warto spojrzeć na swoją firmę jak na ekosystem. Niemal każda organizacja korzysta z usług kontrahentów i zewnętrznych dostawców, a większość z nich integruje systemy informatyczne i udostępnia dane stronom trzecim, zarówno tym, z którymi firma ma podpisane odpowiednie umowy, jak i tym, z którymi takich umów nie ma. Kiedy organizacje oceniają, które mechanizmy kontroli należy rozszerzyć na pracowników, aby zabezpieczyć nowe protokoły pracy z domu, powinny zrobić to samo dla użytkowników i połączeń stron trzecich, które prawdopodobnie będą zarządzać podobnymi zmianami w swoich operacjach i protokołach bezpieczeństwa. Nawet najsilniejsza kontrola technologii nie zastąpi zdrowego rozsądku pracowników pracujących w domu. W ostatnich miesiącach zapewnienie możliwości pracy zdalnej i utrzymanie sieci obsługujących klientów były niezbędne do zapewnienia ciągłości działania. Organizacje redefiniując swoje podejście do cyberbezpieczeństwa, potrzebują elastyczności w określaniu priorytetów zgodnie z potrzebami biznesowymi. Oczywiście będą się one różnić w zależności od sytuacji firmy. Spowolnienie gospodarcze spowodowane skutkami pandemii w wielu firmach może ograniczyć apetyty na inwestycje w cyberbezpieczeństwo. Jednak w przypadku większości ubezpieczycieli ostatnie miesiące to istotny wzrost ruchu w internecie, stąd potrzebne może okazać się dodatkowe zabezpieczenie nowych kanałów online na dużą skalę. Podniesienie rangi kwestii cyberbezpieczeństwa oraz weryfikacja strategii jest podstawowym działaniem. Brak właściwej ochrony danych klientów może skutkować nieodwracalnymi stratami wizerunkowymi oraz finansowymi. ❑