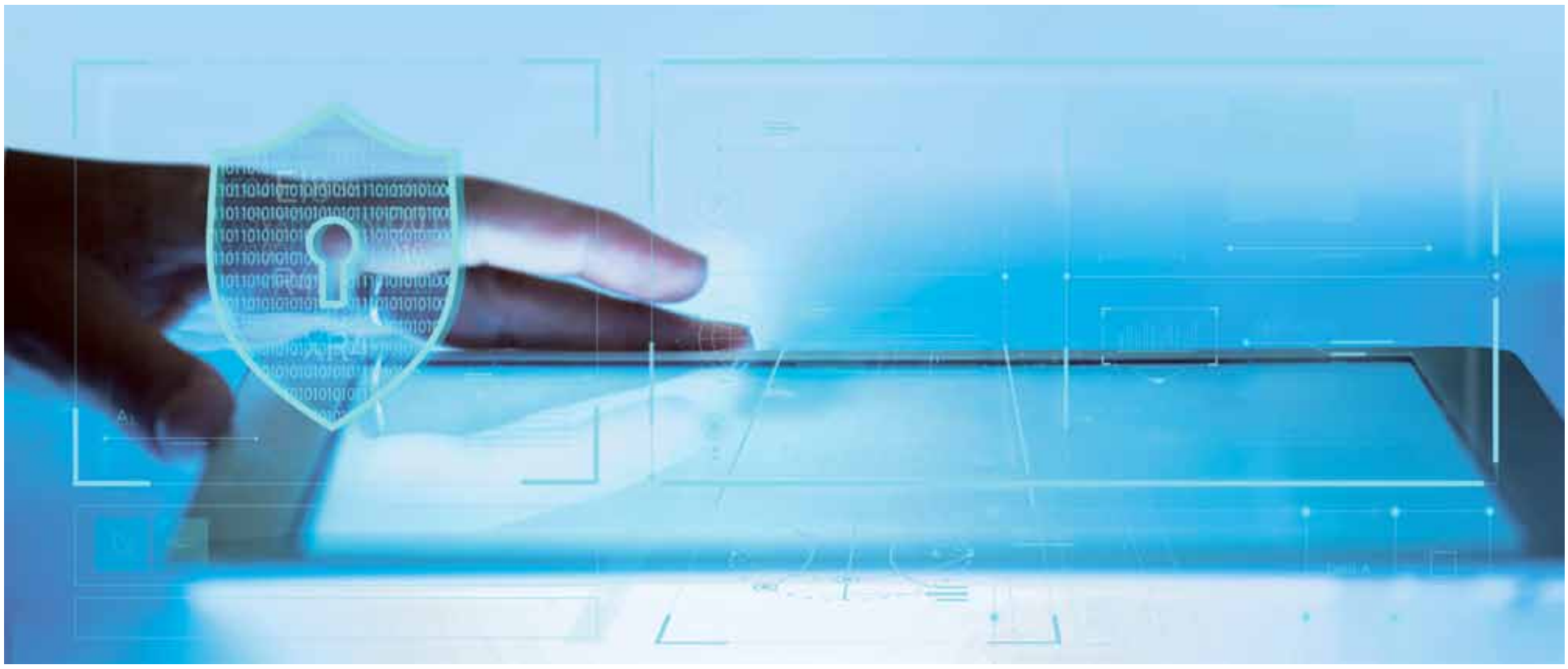
CYBERBEZPIECZEŃSTWO



Dlaczego odpowiedni system zarządzania ryzykiem jest tak ważny dla skutecznej walki z nadużyciami finansowymi?

Ochrona przed oszustwami to kluczowa kwestia, z którą detaliści muszą sobie radzić od dziesięcioleci. Widoczny obecnie szybki rozwój handlu elektronicznego zwiększył zapotrzebowanie na najbardziej skuteczne rozwiązania w zakresie bezpieczeństwa klientów i ich danych. Pandemia przyspieszyła proces cyfryzacji dla wielu firm, ponieważ odczuły one konieczność przeniesienia biznesu także do świata wirtualnego. Szybka transformacja wpłynęła również na zmiany w nawykach zachowań kupujących, które stały się kluczowym czynnikiem w budowaniu właściwych rozwiązań do zarządzania ryzykiem.

Jakub **Czerwiński**

wiceprezes ds. sprzedaży, Adyen

Nie oznacza to jednak, że przestępcy przestali atakować placówki fizyczne. Wręcz przeciwnie, obecnie oszustwa są obserwowane zarówno w świecie offline, jak i online. Według danych Adyen, 59 proc. sprzedawców detalicznych zaznacza, że poziom nieuczciwych transakcji w ich organizacji zdecydowanie wzrósł w stosunku do ubiegłego roku. Co więcej, w ciągu sześciu miesięcy dwóch na pięciu konsumentów zrezygnowało z zakupu po tym, jak ich karta kredytowa bądź debetowa została fałszywie odrzucona przez podejrzenie o oszustwo, a co piąty zetknął się z tym doświadczeniem cztery lub więcej razy w tym samym okresie. Łącznie wiąże się to z utraconą możliwością zysku na poziomie 197 mld funtów rocznie.

Kluczowe znaczenie

Oznacza to, że aby rozwijać się bezpiecznie, sprzedawcy detaliczni muszą dostarczać klientom to, co najlepsze z obu światów. Nowe rodzaje oszustw i działań mających na celu kradzież pieniędzy stały się bardziej rozbudowane, a narzędzia wykorzystywane do krzywdzących ruchów bardziej zaawansowane technologicznie. Coraz większą popularnością cieszą się internetowe sklepy i platformy handlowe, dlatego też mogą być one szczególnie narażone na oszustwa. Zarówno kupujący, jak i sprzedający są podatni na niebezpieczne praktyki. W miarę rozwoju oszustw, kluczowe znaczenie dla każdego rozwiązania w zakresie zarządzania bezpieczeństwem ma jak najszybsze ich wykrywanie, analizowanie i rozwiązywanie. Z drugiej strony szybkość i wygoda przy końcowej fazie zakupów oraz bezproblemowe korzystanie z technologii cyfrowych mają obecnie kluczowe znaczenie dla wielu firm.

Uzyskanie właściwej równowagi pomiędzy optymalizacją strategii ochrony przed oszustwami, bez widocznych zmian, masowych aktualizacji mailingowych lub spadku liczby prawdziwych zamówień, może stanowić niełatwe wyzwanie. Firmy ciężko pracują, aby zapewnić prawdziwym klientom bezproblemowe dokonywanie płatności, jednak przestępcy mają możliwość szybkiej adaptacji i atakowania firm dzięki wykorzystaniu swojej rozległej wiedzy technologicznej. Oczywiście zawsze istnieje pewien poziom ryzyka, które firmy muszą podjąć podczas prowadzenia działalności gospodarczej, ponieważ całkowite wyeliminowanie oszustw jest prawie niemożliwe. Jeśli chodzi o konwersję i zarządzanie oszustwami, najlepiej jest wypracować sposób na doprowadzenie do sytuacji, w której przedsiębiorca będzie czuł się komfortowo. Obciążanie klientów mnóstwem procesów weryfikujących może ich odstraszyć, ale jeśli właściciele firm podejdą to tego mądrze, prawdziwi klienci uznają pewien poziom zakłóceń za dopuszczalny, zwłaszcza jeśli chodzi o transakcje o wysokiej wartości. Był czas, kiedy wszyscy denerwowaliśmy się koniecznością ustawiania haseł posiadających minimum sześć liter, jedną cyfrę, dużą lub małą literę, ale to już dawno minęło.

Posiadać skuteczną strategię

Na pytanie, dlaczego posiadanie skutecznej strategii zarządzania ryzykiem jest tak ważne, odpowiedź jest prosta. Losowe dostosowywanie zasad i polityki, zamiana jednego modelu biznesowego na inny lub integracja z dodatkowymi podmiotami trzecimi w celu weryfikacji danych klientów jest opcją, ale zazwyczaj nie najbardziej efektywną i całkiem kosztowną. Co więcej, w większości przypadków, aby środki uwierzytelniania ryzyka zadziałały, zaangażowanych musi być wiele stron, od regulatorów i akceptantów, po handlowców i kupujących.

Wybór odpowiedniego partnera płatniczego może pomóc zminimalizować ryzyko, usprawnić proces i dostarczyć wyjątkowo ważnych danych. Zawsze staramy się zapewnić naszym klientom unikalne narzędzia do zapobiegania oszustwom oraz oparte na danych podejście do ich wykrywania, ograniczając pracę manualną i pomagając im uzyskać pełny wgląd w swoje transakcje płatnicze.

Ponieważ każdy kanał zakupowy niesie ze sobą własne ryzyko, ujednolicone rozwiązanie handlowe może okazać się bardzo pomocne. Jest to świetna opcja szczególnie dla sprzedawców detalicznych, ponieważ pomaga im ona w zarządzaniu ruchem w sklepach, aplikacjach mobilnych i w handlu elektronicznym – wszystko za pośrednictwem jednej platformy technologicznej. Ujednolicony system zwiększa wydajność, zapewnia stabilność, integralność i ostatecznie wyższe wskaźniki autoryzacji oraz lepszą wydajność – dzięki temu jest najlepszym narzędziem do zwalczania i zarządzania oszustwami płatniczymi. Wystarczy wyobrazić sobie sytuację, w której klient wchodzi do sklepu w Warszawie i kupuje na przykład parę butów, używając karty. Transakcja weryfikowana jest za pomocą kodu PIN (idealny scenariusz dla każdego oszusta, ponieważ odpowiedzialność przesunęła się na korzyść sprzedawcy). Tej samej nocy klient kupuje dodatkową parę skarpetek na stronie internetowej tego sklepu, przy czym adres IP kupującego rejestruje się zaledwie 10 mil od placówki, którą odwiedził kilka godzin wcześniej. Nawet jeśli klient korzysta z innej karty kredytowej przy zakupie online (co ze względu na brak historycznych danych o kupującym można uznać za większe ryzyko), prawdopodobieństwo, że zamówienie jest prawdziwe, jest dla sprzedawcy wyjątkowo wysokie.

Aby dotrzeć do bezpiecznej przystani, należy pamiętać o jednym czynniku, który odgrywa kluczową rolę nie tylko w codziennej działalności i międzynarodowej ekspansji, ale także w wykrywaniu oszustw. Złoty bilet na drodze do sukcesu stanowią informacje na temat profilu kupującego. Na przykład połączenie danych osobowych i historii zakupów klienta, który nabywa produkty zarówno w Internecie, jak i w fizycznym sklepie. Spójny system płatności jest w stanie błyskawicznie zidentyfikować, zarejestrować konto i połączyć dane w całej sieci omnichannel. Pozwala on na monitorowanie użytkowników w czasie rzeczywistym, co daje handlowcom pełną kontrolę nad tym, co dzieje się w ich sklepach lub na stronach internetowych. Posiadanie partnera, który współpracuje z wieloma handlowcami w różnych sektorach i regionach, daje właścicielom firm wiele korzyści. Mogą oni nie tylko uzyskać pełniejsze i dokładniejsze profile kupujących, ale także dostrzec znaki ostrzegawcze dzięki porównaniu danych z różnych miejsc i branż.

Skuteczne zarządzanie oszustwami polega na podejmowaniu solidnych decyzji opartych na danych, a nie pozostawianiu ich w sferze opinii i nieudanych prób. Zachowanie równowagi pomiędzy oferowaniem klientom bezproblemowych zakupów bez zakłócania ogólnego doświadczenia jest podstawą wizji naszego działania.

Cyberbezpieczeństwo kluczowym elementem dla zarządów firm, jak i rządów poszczególnych krajów w dobie digitalizacji

Cyfryzacja jest kluczem do dalszego rozwoju biznesu we wszystkich sektorach gospodarki. Niemniej po drugiej stronie mamy cyberprzestępczość, która jest coraz większym zagrożeniem. Te dwa elementy, wraz z postępującą digitalizacją zarówno podmiotów prywatnych, jak i państwowych, będą się ze sobą intensywnie ścierać.

Agnieszka **Zielińska**

dyrektor handlowy, Polcom

Kwestie cyberbezpieczeństwa powinny być kluczowym elementem zarówno dla zarządów firm, jak i rządów poszczególnych krajów w dobie digitalizacji. Jest to niezwykle istotne, ponieważ zgodnie z trendami na rynkach sukcesywnie rośnie liczba danych, które trzeba przetwarzać i odpowiednio zabezpieczyć. Co więcej, rodzi to też wymogi dotyczące bezpiecznego korzystania z Internetu. Wraz z coraz szerszym wykorzystaniem innowacji, w równym stopniu muszą więc postępować wymogi związane z zachowaniem bezpieczeństwa. Dotyczy to szczególnie odpowiedniego zabezpieczenia danych, w tym tożsamości klientów i obywateli.

Główne zagadnienie

Cyberbezpieczeństwo powinno być głównym zagadnieniem nie tylko na poziomie technicznym, ale też strategicznym we wszystkich podmiotach na rynku i instytucjach państwowych. Właśnie dlatego działania w zakresie bezpieczeństwa cyfrowego powinny być częścią wszystkich procesów na poszczególnych szczeblach organizacji władz lokalnych oraz centralnych. Wymaga to odpowiednich środków oraz wdrożenia rozwiązań technologicznych, np. chmury obliczeniowej, a także monitoringu zagrożeń i podatności w systemach informatycznych, rozwiązań proceduralno-organizacyjnych oraz zaangażowania ekspertów. Mówiąc o tych obszarach, nie można też nie wspomnieć o kompleksowym zarządzaniu incydentami bezpieczeństwa, ochronie przed sprofilowanymi atakami i szkodliwym oprogramowaniem oraz ochronie organizacji przed socjoatakami. Lista jak widać jest długa, podobnie jednak jak lista pomysłów cyberprzestępców na kolejne typy ataków.

W efekcie działań hakerów, a także zmieniającego się otoczenia biznesowego i konieczności coraz szybszego dostarczania przez firmy gotowych produktów na rynek, wiele podmiotów biznesowych rozważa zmianę swoich strategii w stronę bardziej zwinnych i elastycznych rozwiązań oraz proinnowacyjnego podejścia w działaniu. W tym celu wykorzystuje się cloud computing.

Skoncentrowani na bezpieczeństwie

Najcenniejsze dla rynku są bowiem rozwiązania pozwalające na szybkie dostosowanie technologii do wymagań zarówno pod kątem bezpieczeństwa, jak i strategii biznesowych oraz regulacji prawnych w sektorach nadzorowanych, takich jak np. bankowość.

Koncentracja profesjonalnego dostawcy usług cloudowych na cyberbezpieczeństwie jest nieporównywalnie wyższa, aniżeli jest to sobie w stanie zapewnić pojedynczy podmiot. Wyspecjalizowane data center zapewnia nie tylko odpowiednią jakość połączenia sieciowego, ale przede wszystkim odpowiedni poziom zabezpieczeń potwierdzony przez odpowiednie certyfikaty, np. ISO 27 001 oraz ISO 9001.

O możliwościach i poziomie zabezpieczeń chmury może świadczyć przykład Departamentu Obrony USA, który podał do publicznej wiadomości, że w ciągu 10 lat chce swoją infrastrukturę IT umieścić w chmurze. Pentagon na ten cel planuje przeznaczyć 10 mld dolarów. Co ciekawe, w chmurze od pewnego czasu swoje dane przechowuje już amerykańska Centralna Agencja Wywiadowcza (CIA).

O możliwościach i poziomie zabezpieczeń chmury może świadczyć przykład Departamentu Obrony USA, który podał do publicznej wiadomości, że w ciągu 10 lat chce swoją infrastrukturę IT umieścić w chmurze. Pentagon na ten cel planuje przeznaczyć 10 mld dolarów. Co ciekawe, w chmurze od pewnego czasu swoje dane przechowuje już amerykańska Centralna Agencja Wywiadowcza (CIA).

Safe Alert – synergia kompetencji daje przewagę

Badacze zagrożeń występujących w przestrzeni internetowej są zgodni co do tego, że częstotliwość i siła rażenia ataków cyberprzestępców przyjęły agresywnie zwyżkowy trend. Potężnym sprzymierzeńcem tej sytuacji jest covidowa rzeczywistość, która przeniosła pracę, pasje i życie codzienne wielu osób w wirtualne ramy. Biznes nie może pozostać obojętny na nowe, naglące potrzeby klientów w zakresie cyberbezpieczeństwa. Obserwując rosnące potrzeby rynku w tym zakresie, spółka BZ Group zaprojektowała i wdrożyła unikalną usługę, zapewniającą zdalną, komplementarną pomoc informatyka i prawnika w zakresie skutecznej redukcji skutków cyberataków lub dostępną jako wsparcie prewencyjne.

Joanna **Jurczak**

prezes zarządu, BZ Group

Codziennością stały się doniesienia o masowych przejęciach środków z kont bankowych, wyłudzenia danych, haseł, włamań na skrzynki e-mail, a nawet przechwytywaniu kont społecznościowych czy dostępów do stron www. Wskazane metody dają ogromne pole manewru hakerom w zakresie ich nielegalnego zysku, a ofiary narażone są na znaczne szkody. Zgodzić się można, że świadomość użytkowników sieci rośnie i ciągle dojrzewa, jednak cyberprzestępcy stosują coraz bardziej wyrafinowane metody, aby osiągnąć swoje cele. Cyberbezpieczeństwo stało się zatem nie tylko dobrem pożądanym, ale wręcz podstawowym, niezbędnym dla konsumentów oraz dla przedsiębiorców.

Usługa kompletna

Konsekwencje cyberataków nie znajdują się jedynie w katalogu ryzyk informatycznych. Ich negatywne skutki prawne, finansowe czy wizerunkowe mogą być również boleśnie odczuwalne. Z tego powodu w sytuacji niepożądanego zdarzenia w sieci sama pomoc informatyka nie jest wystarczająca. Podobnie nawet najbardziej fachowe doradztwo prawne czy pismo, które nie jest poparte merytorycznym i praktycznym wsparciem informatyka specjalisty, w celu zabezpieczenia dowodów przestępstwa czy zapewnienia optymalnej ochrony klienta w przyszłości, również jest niekompletne. Osobie poszkodowanej nie zależy przecież na połowicznym rozwiązaniu, poszukuje rozwiązania dostępnego od ręki, które kompleksowo rozwiąże jego problem.

Tak właśnie powstała idea Safe Alert. Połączenie kompetencji informatyczno-prawnych zapewniających klientowi praktyczną, wielowymiarową pomoc dostosowaną do jego aktualnej potrzeby w zakresie cyberbezpieczeństwa. Dodatkowo zdalna i wygodna forma usługi to możliwość szybkiej reakcji w sytuacji, gdy czas jest jednym z kluczowych elementów.

Must-have dla klientów

Sytuacja związana z COVID-19 niezaprzeczalnie działa w służbie cyberprzestępców. Osoby pracujące z domu stają się łatwiejszym celem do zhakowania niż pracownicy wykonujący swoje obowiązki w odpowiednio zabezpieczonym biurze. Nagląca potrzeba wsparcia w przypadku niebezpiecznego zdarzenia w sieci to motor wdrożenia dopasowanych do wymagań klientów rozwiązań. Poszerza się również grono odbiorców, którzy chcieliby prewencyjnie zabezpieczyć swoje dobra w sieci – tej grupie również jest dedykowana usługa Safe Alert.

Safe Alert działa na zasadzie specjalnej infolinii alarmowej (22 330 7720). Po weryfikacji dostępu do usługi, klient ustala z konsultantem zakres pomocy – w formie reakcji na cyberatak lub pomocy merytorycznej w zakresie prewencji. W przypadku ataku specjalista IT rozpoczyna zdalne zabezpieczenie dowodów przestępstwa, a prawnik opracowuje komplet rekomendacji prawnych. Dodatkowo specjaliści pomagają w wypełnieniu skomplikowanych formularzy, opracowania dokumentu reklamacji, wezwania do zaprzestania działań czy zawiadomienia organów ścigania. Natomiast jeśli klient chce podjąć działania prewencyjne, może skorzystać z interwencji i porad informatyka oraz fachowego doradztwa prawnika w aspekcie cyberbezpieczeństwa.

Cyberbezpieczeństwo jako usługa dodatkowa

Analizując dynamikę rozwoju usług powiązanych z zaspokojeniem potrzeby cyberbezpieczeństwa, prognozować można znaczący rozwój tego sektora rynku. Interesujące z perspektywy biznesowej staje się zapewnienie klientom dostępu do usług związanych z cyberbezpieczeństwem. Poczucie bezpieczeństwa i dostęp do praktycznej usługi dla klienta połączone z faktyczną korzyścią finansową dla partnera i elastyczny system wdrożenia to tylko niektóre zalety takiego rozwiązania.

Obecnie pakiet Safe Alert dostępny jest w ofercie dla naszych partnerów biznesowych, natomiast konsumenci i przedsiębiorcy mogą nabyć dostęp przez dedykowaną dla tego pakietu infolinię 22 330 7720 (więcej informacji na stronie: https://doradcainformatyczny.pl/safe-alert.html). BZ Group specjalizuje się w organizacji specjalistycznych zdalnych usług dodatkowych dla partnerów biznesowych z takich branż jak finansowa, benefitowa, medyczna czy edukacyjna.

Analizując dynamikę rozwoju usług powiązanych z zaspokojeniem potrzeby cyberbezpieczeństwa, prognozować można znaczący rozwój tego sektora rynku. Interesującym z perspektywy biznesowej staje się zapewnienie klientom dostępu do usług związanych z cyberbezpieczeństwem.

Materiał powstał przy współpracy z firmą BZ Group.

CYBERBEZPIECZEŃSTWO

Zachować podstawowe zasady cyberhigieny

Z Przemysławem Pazerą, Product Managerem w firmie Eaton, rozmawiała Joanna Zielińska.

Jakie kompetencje dyrektora ds. bezpieczeństwa pozwalają mu dbać o cyberbezpieczeństwo w firmie?
Cyberbezpieczeństwo to szeroka dziedzina obejmująca zarówno firmową sieć, jak i procesy przetwarzania informacji czy sprzęt. Dyrektor ds. bezpieczeństwa przede wszystkim dba o ochronę firmowych danych i zasobów. Zajmuje się oceną ryzyka i ustalaniem strategii, która pozwoli unikać zagrożeń. Na polskim rynku wciąż jest to dosyć nowa rola, dlatego nawet w większych firmach często sprawuje ją jedna osoba. CSO powinien łączyć kompetencje merytoryczne i techniczne z umiejętnościami miękkimi oraz rozumieniem biznesu. Z jednej strony konieczna jest stale aktualizowana, szeroka wiedza i nadążanie za dynamicznym rozwojem technologicznym, a także znajomość metod socjotechnicznych, na których w dużej mierze bazują ataki. Z drugiej strony niezbędne jest również zrozumienie ryzyka biznesowego oraz umiejętność negocjowania i sprawnego zarządzania zespołem, także w sytuacjach kryzysowych.

Przed czym, w kontekście cyberzagrożeń, muszą chronić się przedsiębiorstwa?
Cyberatak kojarzy się zazwyczaj z zainfekowanym przez wirusa komputerem lub kradzieżą haseł. Tymczasem może on przybrać bardzo różne formy, m.in. sabotażu poprzez sparaliżowanie krytycznych systemów, cyberszpiegostwa, a nawet fizycznego ataku. Przestępcy podrzucają na przykład zainfekowany pendrive pracownikowi lub podszywają się pod elektryka i w nieuprawniony sposób dostają do firmowych serwerów. Jednym z większych zagrożeń dla firm jest również ransomware, czyli złośliwe oprogramowanie blokujące dostęp do systemu lub szyfrujące zapisane w nim dane, a następnie żądające okupu za ich przywrócenie.

Źródło ryzyka stanowi m.in. stale rosnąca liczba urządzeń podłączonych do sieci, a także popularyzacja rozwiązań chmurowych. Najsłabszym ogniwem bardzo często okazuje się przy tym człowiek. Przestępcy stosują inżynierię społeczną i podstępem skłaniają pracowników do kliknięcia w złośliwy link lub załącznik, np. podając się za kolegę z zespołu czy wsparcie techniczne. Bardzo ważna jest więc edukacja kadry w zakresie podstawowych zasad cyberhigieny i zachowania ostrożności w sieci.

Dynamicznie zmieniające się metody przestępców oraz rozwój technologiczny sprawiają, że każda firma musi myśleć o cyberbezpieczeństwie kompleksowo – chronić zarówno sieć oraz oprogramowanie, jak i sprzęt czy serwery. Przypomina to nieustannie trwający mecz, w którym obydwie drużyny starają się wyprzedzić konkurenta o krok.

Jak radzić sobie w sytuacji, kiedy padliśmy ofiarą cyberprzestępstwa?
Niestety nie sposób zabezpieczyć się przed wszystkimi zagrożeniami, czego dowodzą przypadki ataków na największe banki i korporacje dysponujące wielowarstwową ochroną. Gdy firma padnie ofiarą cyberataku, powinna przede wszystkim przejąć inicjatywę i szybko zareagować: odłączyć zainfekowane urządzenia od sieci, zmienić hasła dostępu, przeskanować systemy i sieć lub poprosić o interwencję dostawcę usług IT. Zawsze należy też zgłosić taki przypadek odpowiednim służbom, przede wszystkim policji lub instytucji zajmującej się bezpieczeństwem teleinformatycznym. Można także powiadomić zespół CERT działający przy Naukowej i Akademickiej Sieci Komputerowej.
Bardzo ważne jest wyciągnięcie wniosków z ataku. O ile przed zagrożeniami trudno jest się w pełni ochronić, można zabezpieczyć się przed skutkami kolejnych incydentów. Warto zacząć od sprawdzenia procedur bezpieczeństwa danych i dostępu do informacji w firmie. Ważne, aby ograniczyć i kontrolować, kto i jakie informacje może oglądać, stosować politykę silnych haseł, używać programów szyfrujących dane. Skutecznym sposobem jest także regularne wykonywanie kopii zapasowych w chmurze oraz na niepodłączonych do sieci dyskach. Nawet jeśli przestępcy uda się zablokować czy usunąć dane, możliwe będzie ich łatwe odzyskanie.

Najsłabszym ogniwem bardzo często okazuje się człowiek. Przestępcy stosują inżynierię społeczną i podstępem skłaniają pracowników do kliknięcia w złośliwy link lub załącznik, np. podając się za kolegę z zespołu czy wsparcie techniczne. Bardzo ważna jest więc edukacja kadry w zakresie podstawowych zasad cyberhigieny i zachowania ostrożności w sieci.

Zagrożenia wobec infrastruktury fizycznej, czyli jakie cele stawiają sobie cyberprzestępcy?

Konwergencja systemów technik operacyjnych (OT) oraz środowisk IT sprawia, że infrastruktura krytyczna staje się podatna na cyberataki. Według badania Forrester Research, przeprowadzonego na zlecenie Fortinet, aż 80 proc. przedsiębiorstw doświadczyło w ciągu minionych dwóch lat incydentu związanego z naruszeniem bezpieczeństwa systemów OT. Takie sytuacje mogą mieć bardzo poważne konsekwencje dla funkcjonowania firmy, jej pracowników i klientów.

Jolanta **Malak**
dyrektor, Fortinet w Polsce

Korzyści i problemy
Połączenie systemów OT i IT jest opłacalne, ponieważ zapewnia skuteczniejsze monitorowanie krytycznych procesów przemysłowych. Pozwala też korzystać z danych pochodzących z urządzeń typu IIoT (ang. Industrial Internet of Things, przemysłowy Internet rzeczy), np. różnego rodzaju czujników. Mają one zastosowanie w takich branżach jak robotyka, ochrona zdrowia czy w procesach produkcyjnych, które są sterowane programowo. Integracja tych środowisk zapewnia też wyraźne oszczędności kosztów energii.
Możliwe zagrożenia bezpieczeństwa są podobne dla obu rodzajów systemów. Brak skutecznego planu ochrony dla technik operacyjnych sprawia, że systemy sterujące, takie jak ICS/SCADA, są narażone na cyberataki. Mogą one spowodować konsekwencje dalece wykraczające poza straty finansowe, utratę reputacji czy spadek zaufania do firmy. W skrajnych przypadkach może to nawet sprowadzić zagrożenie dla bezpieczeństwa publicznego, ludzkiego życia lub zdrowia.

Celem pieniądze lub zakłócenie działalności
Ataki na infrastrukturę krytyczną mogą być motywowane nie tylko chęcią zysku. Oczywiście cyberprzestępcy są oportunistami, działają tam, gdzie mogą liczyć na zyski. Są też świadomi, które przedsiębiorstwa mogą zapłacić np. okup w zamian za odszyfrowanie plików wcześniej zablokowanych przez oprogramowanie ransomware.
Należy jednak mieć na uwadze, że infrastruktura krytyczna może być także celem tych cyberprzestępców, którzy działają we współpracy z rządami bądź na ich zlecenie. Czasami staje się też obiektem zainteresowania tzw. haktywistów, którzy są motywowani ideologicznie lub politycznie, a ich celem jest zwracanie uwagi na wybrane kwestie polityczne lub społeczne czy też szkodzenie organizacjom lub przedsiębiorstwom, z których polityką się nie zgadzają.
W ostatnich latach jednym z najsłynniejszych ataków na infrastrukturę krytyczną był ten, który w 2015 r. spowodował przerwy w dostawie prądu w rejonie Iwano-Frankowska na Ukrainie. Do jego przeprowadzenia wykorzystano złośliwe oprogramowanie Black Energy. Nie można również zapomnieć o złośliwym narzędziu Stuxnet, które było jednym z pierwszych precyzyjnie ukierunkowanych ataków na systemy przemysłowe. Pojawił się na czołówkach gazet w 2010 r., gdy zaatakował przemysłowe systemy sterujące SCADA, a konkretnie programowalne sterowniki logiczne (PLC), które umożliwiają automatyzację procesów elektromechanicznych. Jako ciekawostkę można podać fakt, że od czasu, gdy Stuxnet zaatakował jedną z elektrowni jądrowych w Iranie, władze kraju zainwestowały wiele środków w rozwój własnej cyberarmii, która ma skutecznie konkurować z największymi cyberarmiami świata[1].

Kolejne wyzwania
Zabezpieczenie systemów przemysłowych to jedno z najważniejszych zadań zespołów OT. Pomimo świadomości tego problemu, działalność biznesowa jest coraz bardziej zagrożona, głównie dzięki rosnącym możliwościom, jakie mają cyberprzestępcy prowadzący bardziej wyrafinowane ataki. Dodatkowo w 2020 r. pojawia się kolejne wyzwanie stworzone przez COVID-19, między innymi większa liczba pracowników wykonujących zadania służbowe w domu i wdrożenie nowych narzędzi mających na celu wspieranie pracy zdalnej.

1. https://fortiguard.com/resources/threat-brief/2020/01/10/fortiguard-threat-intelligence-brief-january-10-2020

CYBERATAK? NAJLEPIEJ PRZEZ DYREKTORA, PRACOWNIKA I FIRMOWĄ DRUKARKĘ

Hakerzy stosują różne metody, próbując wykraść ważne dla nich dane, takie jak m.in. dane dostępowe do kont bankowych, numery PIN lub CVC kart kredytowych, szczegółowe dane osobowe czy – w przypadku whalingu (tj. ataku skierowanego przeciwko osobom piastującym wysokie stanowiska w organizacji) – wrażliwe dane firmowe. Nadal głównym, choć nie jedynym wektorem cyberataku są maile, a jedną z najpopularniejszych form ataki socjotechniczne, czyli takie, które bazują na skłonności człowieka do bezwiednego ulegania wpływom innym.

Tomasz **Szpikowski**

CEO, TestArmy Group

W raporcie firmy KPMG czytamy, że Internet rzeczy to jedna z trzech głównych sił napędowych transformacji biznesowej w ciągu najbliższych trzech lat. Tymczasem, mimo że zgodnie z szacunkami światowe wydatki na IoT rokrocznie rosną o ok. 15 proc., to na zabezpieczanie inteligentnych urządzeń nadal przeznaczany jest zaledwie ułamek tej kwoty – ok. 0,2 proc. To niepokojące, bo jak alarmują eksperci, dobry firewall czy monitoring infrastruktury sieciowej to obecnie zbyt mało, aby mówić o efektywnej ochronie przed cyberzagrożeniami. Jeżeli firma chce korzystać z inteligentnych urządzeń, a przy tym eliminować ryzyko skutecznie przeprowadzanych cyberataków, konieczna jest dokładna analiza wszystkich wykorzystywanych przez nią systemów, zarówno tych fizycznych, jak i wirtualnych.

Połowa urządzeń IoT ma luki w systemach bezpieczeństwa. W tym drukarka prezesa znanej firmy

Aby udowodnić ryzyko związane z korzystaniem z nieodpowiednio zabezpieczonych urządzeń podłączanych do sieci, eksperci z TestArmy CyberForces przeprowadzili dwa testy penetracyjne. W pierwszym zbadali poziom zabezpieczeń popularnych sprzętów IoT dostępnych w sklepach. W drugim podjęli próbę włamania się do systemu znanej korporacji obracającej setkami tysięcy danych osobowych pochodzących ze zgód marketingowych. Wyniki obu testów dały do myślenia:

• połowa przebadanych urządzeń IoT posiada luki w systemach bezpieczeństwa.

Pod lupą naszych ekspertów od cyberbezpieczeństwa znalazły się popularne urządzenia wykorzystywane w smart firmach i smart domach, m.in. inteligentne przełączniki i włączniki światła, inteligentne żarówki, programowalne termostaty, słuchawki czy lampki na USB. Okazało się, że aż 5 na 10 z przetestowanych urządzeń IoT posiadało dziury w oprogramowaniu. Złamanie systemu i dostanie się do sieci bezprzewodowej, do której były podłączone, zajmowało ekspertom nie więcej niż kilkadziesiąt minut (ok. 30 minut w przypadku najtańszych urządzeń).

• Drukarka otwiera dostęp do wrażliwych danych i… gabinetu prezesa

W ramach drugiego testu sprawdziliśmy, czy urządzenia, z których korzysta jednym ze znanych na rynku korporacji, zajmująca się przetwarzaniem wrażliwych danych osobowych pochodzących ze zgód marketingowych, są odpowiednio zabezpieczone. Podczas zaplanowanych testów infrastruktury bezpieczeństwa nasi eksperci odkryli, że firmowy system posiada lukę pozwalającą na uzyskanie zdalnego połączenia z bezprzewodową, zintegrowaną z laptopami pracowników drukarką. Odkryli też możliwość podłączenia się do firmowych kamer bezpieczeństwa, sterowania nimi, a nawet odbierania obrazu na żywo, co pozwala podejrzeć np. wprowadzane przez pracowników 6-cyfrowe kody do zamków magnetycznych drzwi wejściowych do biur. Po wykryciu tych błędów zostały one naprawione, a system uszczelniony.

Dostać się do firmowej sieci można nie tylko przez urządzenia

Wysoce rozwinięte technologiczne kraje mają wiele sposobów na to, aby radzić sobie z cyberzagrożeniami wynikającymi z rozwoju cyfrowych technologii uzależniających. Za dobry przykład mogą posłużyć Niemcy, gdzie służby na bieżąco publikują informacje ostrzegające przed ryzykownymi technologiami lub wręcz zakazują stosowania niektórych z nich, jak np. szpiegujących smartwatchów.

Tymczasem cyberprzestępcy są kreatywni, atakując nie tylko częściej, ale wykorzystując do tego trudne do przewidzenia sposoby. Same praktyki OSINT (Open Source Intelligence, wywiad źródeł jawnych) i zbierania informacji na temat celu ataku istnieją od dekad. Problem z ich wykrywaniem nasilił się jednak, gdy do równania wprowadzone zostały aplikacje z potencjałem uzależniającym. Psychologiczne zjawiska wpływające na zachowanie użytkowników prowadzą do sytuacji, w których nawet przeszkoleni dyrektorzy korporacji padają ofiarą ataków socjotechnicznych. Przemęczeni i w ciągłym pośpiechu, chcą osiągnąć cel jak najszybciej, jednocześnie pozostając produktywnymi. Ich umysł ignoruje czerwone flagi, które normalnie pojawiają się u osób niebędących uzależnionymi od używania danego medium.

Czasem więc wystarczy e-mail w znajomej sprawie czy z niepokojącą informacją, np.: „czy widziałeś kompromitujące wpisy na temat swojej córki w Internecie?", aby w przypływie emocji kliknąć w link podany w mailu i nie zauważyć, że zamiast zostać przekierowanym na rzeczywistą stronę, ofiara trafia na stronę kontrolowaną przez atakującego. Witryna wygląda tak samo jak znana strona i wymaga logowania.

W sytuacji, w której człowiek nie jest pod ciągłym wpływem czynnika uzależniającego, mógłby zadać sobie pytanie: „dlaczego muszę się logować, skoro jeszcze 15 minut temu korzystałem z aplikacji, będąc zalogowanym i nie było żadnego problemu?". Jednak ofiara chce jak najszybciej dostać się do zniesławiających danych. Loguje się, wchodzi na stronę i faktycznie widzi informację o tym, że jego córka wzięła udział w nietypowej imprezie będąc na wakacjach we Włoszech. Pliki są do pobrania, załączone w archiwum zip. Historia brzmi wiarygodnie, bo rzeczywiście córka była w tym konkretnym terminie w tej właśnie lokalizacji. Ufa więc informacji i pobiera archiwum zip. W środku nie ma nic, oprócz złośliwego kodu, który wykonuje się w momencie wypakowania plików docx.

Niepewna ofiara ataku może zgłosić się do swojego działu IT z prośbą o pomoc, podejrzewając, że pakiet MS Office nie działa, bo zdjęcia nie mogły się otworzyć. Taka reakcja byłaby pożądana, ponieważ daje IT szansę na analizę i rozpoznanie ataku. Umożliwia wywołanie odpowiednich mechanizmów odpowiedzi na incydent bezpieczeństwa, powstrzymanie ataku i ochronę przed kompromitacją danych ofiary i jego firmy.

W pesymistycznym dla bezpieczeństwa biznesu scenariuszu ofiara uznaje, że była to marna prowokacja, ociera pot z czoła i wraca do swoich codziennych zadań. W tym czasie złośliwe oprogramowanie umożliwia cyberprzestępcom dostęp do wewnętrznej infrastruktury firmy oraz portali. Na tym skandal się nie kończy, gdyż zdobyte dane logowania, oprócz ataku na firmę, zostają wykorzystane do eskalacji uderzenia poprzez faktyczny atak na prywatne życie ofiary, wydobycie historii rozmów prowadzonych przez media społecznościowe i szantaże.

Prosty atak rozgrywający się w zaledwie kilka minut doprowadza więc do ogromnych strat dla biznesu i osoby, która w wyniku braku odpowiedniej edukacji padła jego ofiarą!

Nasuwa się pytanie, skąd przestępca zdobył informacje pozwalające mu stworzyć scenariusz ataku? O ile zaatakowany dyrektor czy pracownik przechodzi proste programy edukacji bezpieczeństwa w swojej korporacji, o tyle jego rodzina już nie. Przejrzenie ich profili w mediach społecznościowych i wyciągnięcie potrzebnych danych to dla hakera kwestia minut. Niestety jest to bardzo powszechny i niebezpieczny wektor ataku, często pomijany w programach edukacji osób zajmujących kierownicze stanowiska.

Inną, bardzo popularną metodą stosowaną przez cyberprzestępców jest tzw. CEO Froud, czyli oszustwo „na prezesa". Jak wygląda schemat takiego ataku? Rzecz zaczyna się od uzyskania dostępu do e-maila prezesa, z którego wysyłane są zlecenia przelewów. Gdy cyberprzestępca zyska taki dostęp, ma pełne spektrum możliwości.

• Gdy włamanie dotyczy firmy współpracującej z zagranicznym dostawcą, może wykorzystać długą relację biznes–dostawca. Mając dostęp do historii przelewów, może wysyłać e-mailem prośby o zmianę rachunku, na który kierowane są pieniądze. Ponieważ adres e-mail będzie łudząco podobny, odbiorca prawdopodobnie nie będzie podejrzewać, że cała sytuacja jest oszustwem.

• Gdy włamanie dotyczy firmy zlecającej duże ilości przelewów, podstawiony „dyrektor" może zlecić własnym pracownikom czy instytucji finansowej obsługującej firmę przesłanie środków na podany numer konta.

• Gdy włamanie dotyczy firmy współpracującej z zewnętrznym doradcą podatkowym lub adwokatem, przestępca może wysłać prośbę o wypełnienie papierów podatkowych, do których ma dostęp, albo o przekazanie szczegółowych i poufnych danych pracowników.

Potrzebna ciągła i kreatywna edukacja!

Takie proste przykłady ataków są tylko wierzchołkiem góry lodowej. Choć fenomen cyfrowych technologii uzależniających wzbudza coraz większe zainteresowanie ze strony psychologów i socjologów, minie jeszcze sporo czasu, zanim rezultaty badań będą wiarygodne w stopniu, który nie tylko pozwoli odeprzeć aktualne ataki, ale przygotować się na przyszłościowe zagrożenia, wynikające np. z faktu tracenia umiejętności utrzymania koncentracji na konkretnym zadaniu.

Być może dojdziemy do poziomu rozproszenia, w którym będziemy padać ofiarą ataków socjotechnicznych, na które nie zareagujemy nawet po fakcie. Zwyczajnie nie będziemy pamiętać, że w ogóle wykonaliśmy jakąś czynność online, która mogła wygenerować ryzyko skompromitowania naszych danych. Może też ze względu na otaczającą nas technologię będziemy coraz lepiej uczyć się zarządzania chaosem i łatwiej będzie nam rozpoznawać ataki, które są wynikiem odchylenia od tego, do czego jesteśmy na co dzień przyzwyczajeni.

Dlatego teraz, bardziej niż kiedykolwiek wcześniej, istotna jest ciągła i kreatywna edukacja osób mających dostęp do krytycznych danych, czyli ludzi pełniących kluczowe role w swoich firmach czy powiązanych z bezpieczeństwem państwa. Ataków możemy spodziewać się coraz więcej, ale ich siła tkwi nie w ilości, ale w mnogości wektorów, wykorzystywanych przez kreatywnych hakerów na trudne do przewidzenia sposoby.

CYBERBEZPIECZEŃSTWO

WALKA Z RANSOMWARE,
jednym z największych współczesnych zagrożeń dla biznesu

Szkody, które może wyrządzić przedsiębiorstwom ransomware, są oszałamiające. Przedsiębiorstwa, posiadające poczucie, że nie mają wyboru i muszą płacić cyberprzestępcom za odblokowanie ich plików, mogą nie tylko stracić pieniądze, ale także narażają na szwank swoją reputację. Zgodnie z raportem opracowanym przez Cybersecurity Ventures przewiduje się, że w 2021 r. globalne koszty powstałe w wyniku działania ransomware wzrosną o 20 mld dolarów.

Rick **Vanover**
Senior Director, Product Strategy, Veeam

Podczas gdy najlepszą odpowiedzią na atak szyfrujący firmowe dane jest prewencja, w całym krajobrazie zagrożeń nie zawsze jest to możliwe. To samo badanie Cybersecurity Ventures przewiduje, że w 2021 r. co 11 sekund jakaś firma padnie ofiarą ataku typu ransomware. W ostatecznym rozrachunku prawie wszystkie systemy komputerowe są podatne na złamanie, tak więc firmy muszą być przygotowane na funkcjonowanie w rzeczywistości nieustannych ataków i posiadać plan awaryjny na wypadek najgorszego.
Posiadanie kopii zapasowych dostępnych offline oraz przechowywanie ich, między innymi, poza siedzibą firmy, a także utrzymywanie zdolności do szybkiego odzyskiwania danych po awarii może pomóc przedsiębiorstwom odzyskać dane zaszyfrowane przez atakujących. Zarówno ryzyko, jak i scenariusze takich ataków są jednak zróżnicowane, dlatego też przedsiębiorstwa potrzebują odpowiedniego planu działania oraz pewności, że informacje z kopii zapasowych nie zostaną wykorzystane przeciwko nim, np. nie są już zainfekowane.

Krajobraz zagrożeń ewoluuje
W dzisiejszych czasach obserwuje się rosnącą fragmentację w rodzajach ataków wymuszających okup. Szefowie działów bezpieczeństwa (CSO) kojarzą tego typu haracz głównie z szyfrowaniem danych. Oznacza to, że złośliwe oprogramowanie uzyskuje dostęp do poufnych lub krytycznych danych i szyfruje je. Umowa w takim scenariuszu polega na tym, że firma płaci okup w zamian za pliki, które mają być odszyfrowane i przywrócone do ich oryginalnej, użytecznej postaci. Nie jest to jednak jedyne zagrożenie dla CSO, które należy rozważyć. W innych przypadkach cyberataki będą polegać na rozsyłaniu poufnych danych poza firmę, zamiast je szyfrować. W tym wypadku zapłacenie okupu ma na celu zapobieżenie publicznemu wyciekowi potencjalnie wrażliwych danych.
Różne modele i scenariusze działań przestępców utrudniają konsekwentną obronę przed wciąż zmieniającym się spektrum zagrożeń. Złotą zasadą dla organizacji jest posiadanie szczegółowej wiedzy, co jest normalnym zachowaniem w ramach ich własnej infrastruktury IT. Można to osiągnąć poprzez ciągłe monitorowanie danych i przechowywanie ich w chmurze, a także poprzez wykorzystanie analiz sieci, systemów operacyjnych i aplikacji. Zwiększona świadomość tego, jak wygląda bezpieczny stan rzeczy, może sprawić, że podejrzane i złośliwe działania będą łatwiejsze do wykrycia, co znacznie przyspieszy czas reakcji.
Mądre wykorzystanie szyfrowania jest równie dobrym pomysłem. Jeśli złośliwe oprogramowanie nie może zobaczyć danych, trudniej będzie wykorzystać je przeciwko nam. Zgodnie z raportem Duo Privacy in the Internet Trends, 87 proc. ruchu w sieci jest szyfrowane, a liczba ta stale rośnie. Jednak nadal ciężko określić, jaki odsetek danych w przedsiębiorstwach jest zaszyfrowany. Z danych zebranych przez Zscaler's IoT in the Enterprise wynika, że 91,5 proc. ruchu w sieciach IoT przedsiębiorstw nie jest w żaden sposób zaszyfrowane. Te mocno kontrastujące ze sobą dane wskazują na istnienie znacznej różnicy między sposobem, w jaki przedsiębiorstwa z reguły wykorzystują szyfrowanie, w porównaniu z platformami internetowymi i dostawcami usług.

Czy kopie zapasowe są wartościowym celem dla cyberprzestępców?
Jednym z obszarów, w którym szyfrowanie jest niezbędne do wzmocnienia ochrony organizacji zarówno przed żądaniami okupu, jak i przed zagrożeniami wewnętrznymi, jest wdrożenie szyfrowania nearline kopii zapasowych danych. W raporcie Veeam 2019 Cloud Data Management stwierdzono, że ponad dwie trzecie organizacji tworzy kopie zapasowe swoich danych. Choć jest to oczywiście dobra wiadomość, to nietrudno wyobrazić sobie, jaki ogromny potencjał szantażu mają cyberprzestępcy, jeśli chodzi o uzyskanie dostępu do kopii zapasowych całej infrastruktury cyfrowej organizacji.
Biorąc pod uwagę fakt, że cyberprzestępcy wykorzystujący oprogramowanie ransomware poszukują danych, to teoretycznie mogą znaleźć wszystko, czego potrzebują, w kopiach bezpieczeństwa. Mogą one mieć różną postać: od dysków systemowych i wymiennych dysków twardych po urządzenia taśmowe offline i kopie zapasowe w chmurze. Niezależnie od tego, którą opcję wybierze firma, samo repozytorium kopii zapasowych musi być chronione przed atakiem za pomocą bardzo odpornego typu nośnika. W przeciwnym razie istnieje ryzyko, że próbując zapewnić ciągłość działania, firmy mogą tworzyć skarbiec słabo zabezpieczonych danych, które mogłyby zostać wykorzystane przeciwko nim.
W przypadku niektórych ryzykownych działań można zwiększyć bezpieczeństwo poprzez szyfrowanie kopii zapasowych na każdym kroku. Historycznie, szyfrowanie kopii zapasowych było doskonałym pomysłem, gdy nośniki opuszczały siedzibę firmy lub gdy dane były przesyłane przez Internet. Biorąc pod uwagę rozpowszechnienie współczesnych zagrożeń w cyberprzestrzeni, szyfrowanie musi odbywać się bliżej samego procesu tworzenia kopii zapasowych. Najskuteczniejszą techniką jest jednak odporność danych zapisanych w kopii zapasowej.

Zabezpieczanie kopii zapasowych danych
Dochodzimy do ważnego tematu ultraodpornej pamięci masowej do tworzenia kopii zapasowych – jednej z najbardziej efektywnych form przechowywania danych, która jest odporna na ataki ransomware. Istnieje przynajmniej kilka sposobów, w jaki organizacje mogą osiągnąć taki poziom ochrony, aby ich kopie zapasowe danych nie stały się przysłowiowymi tylnymi drzwiami dla cyberprzestępców.
Pierwszym z nich jest wykorzystanie taśm offline, które są bardzo skuteczną formą nośnika odseparowanego od sieci Internet. Taśmy są często uważane za staromodną i nieefektywną technologię przechowywania danych, ale nie można ich pobić, jeśli chodzi o tworzenie wysoce przenośnych, bezpiecznych i niezawodnych kopii zapasowych, dodatkowo o niskim koszcie. Podobnie jak w przypadku taśm, wymienne dyski również mają cechę offline, która polega na tym, że nie są w sieci, chyba że są akurat odczytywane lub zapisywane. To sprawia, że są one preferowaną opcją, jeśli chodzi o ograniczanie widoczności kopiowanych plików dla agentów złośliwego oprogramowania.
Niezmienne kopie zapasowe w chmurze, takie jak choćby tryb zgodności pamięci masowej AWS S3 do blokowania obiektów oznaczają, że dane kopii zapasowych przechowywane w chmurze nie mogą zostać usunięte przez ransomware, złośliwych administratorów ani nawet przypadkowo. Tego typu rozwiązanie jest dostępne w chmurze publicznej AWS S3, jak również w wielu kompatybilnych z S3 systemach pamięci masowej (zarówno lokalnych, jak i w ramach oferty publicznej). Ponadto nasze rozwiązanie zapewnia ochronę, dzięki której kopie zapasowe danych mogą być przechowywane całkowicie poza zasięgiem klientów. Jest ona dostarczana przez dostawcę usług i pomaga użytkownikom końcowym chronić się przed ransomoware, zagrożeniami wewnętrznymi i przypadkowym usunięciem danych.
Szefowie działów bezpieczeństwa stale zmagają się z rozsądnym kompromisem pomiędzy wygodą a bezpieczeństwem. Dziś przedsiębiorstwa przechodzą transformację cyfrową i mają wielorakie potrzeby inwestycyjne, zatem ochrona przed oprogramowaniem ransomware jest krytyczna dla zapewnienia ciągłości działania. Tworzenie lokalnych kopii zapasowych oraz w trybie offline może pomóc złagodzić skutki działania oprogramowania tego typu. W połączeniu z odpowiednimi rozwiązaniami w zakresie bezpieczeństwa i szkoleniami pracowników niezwykle odporne kopie zapasowe do zarządzania danymi w chmurze mogą dać organizacjom pewność, że są dobrze chronione nawet w stale zmieniającym się środowisku zagrożeń.

Zwiększona świadomość tego, jak wygląda bezpieczny stan rzeczy, może sprawić, że podejrzane i złośliwe działania będą łatwiejsze do wykrycia, co znacznie przyspieszy czas reakcji.