CYBERBEZPIECZEŃSTWO

Uważność to podstawa

Kluczowe jest zwrócenie uwagi na dwa aspekty – zmniejszenie powierzchni ataku oraz zwiększenie świadomości zagrożeń wśród pracowników każdego szczebla. Upraszczając zagadnienie, mogę wskazać dwie główne taktyki, które mają do dyspozycji atakujący.

Leszek **Tasiemski**

VP of Products, WithSecure

Pierwsza z nich zakłada wykorzystanie luki w zabezpieczeniach. Może nią być na przykład źle skonfigurowane urządzenie sieciowe lub zapomniany serwer bez zainstalowanych aktualizacji. Obecnie coraz częściej jest to też nieprawidłowo skonfigurowany fragment infrastruktury w chmurze. Co do zasady, im mniej urządzeń i usług działa, zwłaszcza z dostępem z publicznej sieci, tym łatwiej utrzymać infrastrukturę w stanie zaktualizowanym i dobrze skonfigurowanym. Atakujący ma wtedy węższe pole manewru. Chcąc zabezpieczać się przed atakami, firmy powinny więc stosować strategię określaną mianem ograniczania powierzchni ataku.

Ryzyko ataku, którego nie da się wyeliminować

Drugą metodą stosowaną przez hakerów jest wykorzystanie nieuwagi użytkownika. Najczęściej atak przybiera formę phishingu, czyli wiadomości (nie zawsze jest to email), które przypominają realną korespondencję i nakłaniają do kliknięcia w link, otwarcia załącznika czy podania hasła. W realnym świecie nawet grupy APT często używają phishingu jako wektora ataku i robią to z przerażającą skutecznością. Nasze własne badania pokazują, że ponad 30 proc. użytkowników otwiera linki w mailach phishingowych.

Ryzyka tego rodzaju ataku nie da się wyeliminować, ale można ograniczyć jego skutki poprzez edukowanie użytkowników. Ważne jest zachęcanie pracowników do raportowania podejrzanych wiadomości (zwłaszcza jeśli zdarzyło im się kliknąć w link lub pobrać załącznik) oraz włączenie wieloskładnikowego uwierzytelnienia, dzięki czemu przejęte hasło będzie bezużyteczne, ponieważ atakujący nie będzie miał dostępu do drugiego składnika, np. jednorazowego kodu. Należy pamiętać, że wiadomości phishingowe coraz częściej są przesyłane również w mediach społecznościowych.

Zabezpieczenia przed cyberatakami powinny być dostosowane do dojrzałości technologicznej danej firmy. Czasami spotykamy się z sytuacją, kiedy firma wdraża bardzo skomplikowane systemy wykrywania incydentów, ale nie jest w stanie interpretować generowanych alertów, ani właściwie na nie reagować.

Korzystanie z urządzeń prywatnych w pracy, a cyberbezpieczeństwo

Pandemia spowodowała, że spora część z nas zaczęła regularnie lub na stałe pracować z miejsc innych niż biuro. Oznacza to, że klasyczny model firmowej „sieci-twierdzy" ostatecznie odchodzi do lamusa. Używamy coraz bardziej różnorodnych urządzeń, które łączą się z coraz bardziej zróżnicowanymi platformami. Działom IT trudno jest wyznaczyć wyraźną granicę między infrastrukturą firmową a domową pracownika czy dostawcy usługi chmurowej. Współczesne modele zabezpieczeń powinny być dynamiczne i niezwiązane z połączeniem sieciowym czy topologią tej sieci.

W przypadku prywatnych urządzeń, zazwyczaj telefonów i tabletów, ważna jest możliwość zdalnego zarządzania ich bezpieczeństwem – oczywiście z poszanowaniem prywatności przechowywanych na nich danych. Podłączając prywatne urządzenie do firmowych zasobów, konieczne jest wymuszenie pewnych ustawień bezpieczeństwa, takich jak szyfrowanie pamięci czy blokada ekranu. Urządzenie może też być odcięte od firmowych zasobów, jeśli nie zostało zaktualizowane lub zostały złamane zabezpieczenia systemu operacyjnego (jailbreak). Ważne jest zachowanie równowagi między zapewnieniem bezpieczeństwa danych a prywatnością użytkownika. Widzimy na rynku wyraźny trend rozwiązań typu Zero-Trust, gdzie uprawnienia do zasobów są przyznawane dynamicznie, na podstawie spełnienia kryteriów bezpieczeństwa i uwierzytelnienia danego użytkownika. W nowym paradygmacie nie ma więc znaczenia czy urządzenie jest firmowe czy prywatne. Istotne jest zastosowanie tych samych, spójnych polityk bezpieczeństwa i zasad dostępu za każdym razem gdy urządzenie ma mieć dostęp do korporacyjnych danych.

Chronić się przed zagrożeniami opartymi na bogatych zasobach (APT)

Grupy APT to zorganizowane zespoły hakerskie zazwyczaj wyposażone w dobrą infrastrukturę oraz bezpośrednio powiązane z rządami poszczególnych krajów. Mają dostęp do nieujawnionych luk bezpieczeństwa (o-days) w oprogramowaniu wykorzystywanym przez ofiary oraz narzędzia, które umożliwiają łatwe ich wykorzystanie.

Ataki ze strony APT są najtrudniejsze do wykrycia i powstrzymania. Najskuteczniejsze z nich nigdy nie zostały wykryte, a te, o których wiemy, dotyczą największych na świecie firm czy organizacji rządowych, które dysponują ogromnymi budżetami na zabezpieczenia. Najczęstsze motywy działania APT to szpiegostwo (polityczne i technologiczne), sabotaż, dezinformacja i manipulacja.

Ze względu na szerokie użycie luk o-days (wady oprogramowania, do których producent jeszcze nie udostępnił łatki), całkowite zabezpieczenie przed APT nie jest możliwe. Aby zwiększyć szansę na wczesne wykrycie i zablokowanie ataku, ważne jest warstwowe podejście do zabezpieczeń. Jeśli wcześniejsze warstwy, na przykład oprogramowanie EPP, nie będą w stanie zablokować ataku, kolejną szansą jest jego wczesne wykrycie poprzez analizę aktywności w systemach. Oczywiście nie można zapominać o podstawach – ograniczanie powierzchni ataku, likwidowanie podatności oraz implementacja uwierzytelniania wieloskładnikowego. Jeżeli te działania nie zatrzymają ataku, to na pewno go utrudnią.

Przeanalizować model zagrożeń dla danej organizacji

Warto przeanalizować model zagrożeń dla danej organizacji i zastanowić się jakie dane czy typ dostępu są istotne z punktu widzenia potencjalnego ataku. Na przykład, dla dostawcy energii prawdopodobnie najważniejsze będzie zabezpieczenie systemów sterowania i monitorowania sieci przesyłowej (sabotaż), podczas gdy producent mikroprocesorów najprawdopodobniej najpilniej musi strzec swojej własności intelektualnej (szpiegostwo). Kiedy krytyczne dane i systemy zostaną zidentyfikowane, należy szczególnie skupić się na ograniczaniu dostępu do nich (wtedy nawet przejęcie konta użytkownika przez aktora APT nie da hakerom dostępu do danych) oraz monitorowaniu aktywności, oraz anomalii w kluczowych obszarach.

Grupy APT rutynowo używają phishingu, żeby zdobyć pierwotny dostęp do systemów. Później, wykorzystując go, rozszerzają swój atak i eskalują uprawnienia. Krytyczne jest wdrożenie MFA (uwierzytelniania wieloskładnikowego) oraz podnoszenie świadomości kadry w zakresie wyłapywania i raportowania prób phishingu.

Ważną taktyką wykorzystywaną przez APT są także ataki na łańcuch dostaw (supply chain attack). Przykładem może być niedawny atak na wiele urzędów oraz dużych firm w USA poprzez dostawcę technologii używanej przez te instytucje (SolarWinds). W tego typu atakach APT uzyskują dostęp do systemów poprzez atak na inne systemy, których używają ich rzeczywiste cele. Atakując łańcuch dostaw, hakerzy uzyskują efekt skali – łamiąc zabezpieczenia jednej firmy, umieszczają implant w jej produkcie, a po jakimś czasie mają dostęp do systemów większości klientów, którzy korzystają z zainfekowanego systemu lub łączą się z nim.

Lew ING na straży bezpieczeństwa

ING Hubs Poland dostarcza usługi cyberbezpieczeństwa dla całej Grupy ING. To bardzo odpowiedzialne zadanie, z którego firma wywiązuje się każdego dnia. Wszystko po to, aby dane, w tym pieniądze klientów, były dobrze strzeżone.

Katarzyna **Fulek-Szajkowska**

Firmy, które działają w ramach Grupy ING są partnerami biznesowymi ING Hubs Poland. Bez względu na strefę czasową dane tych instytucji finansowych są strzeżone przez polską spółkę – globalne centrum usług dla Grupy ING. Oznacza to, że pracownicy zlokalizowani w Polsce 24 godziny na dobę, siedem dni w tygodniu monitorują bezpieczeństwo wszystkich podmiotów wraz z centrami danych. Jest to ok. 100 osób, które zajmują się wykrywaniem cyberataków.

Biały haker – dobry haker

W obronie przeciw atakom ze strony przestępców jest też drugi filar, który stanowią tzw. Biali hakerzy. Czym się zajmują? Włamywaniem się do systemów bankowych firmy, dla której pracują. Chodzi o to, aby sprawdzić, czy systemy te są szczelne, a jeśli nie, aby zawczasu zlikwidować wszelkie możliwości dostania się do wewnątrz. Dzięki temu wiadomo, jaki jest stan bezpieczeństwa firmy poddawanej takim testom. Pentesterzy (czyli biali hakerzy, z ang. penetration tester) sugerują także, co można poprawić, aby system był odpowiednio zabezpieczony.

– W ING opracowaliśmy procedurę, która zobowiązuje nas do tego, aby każda aplikacja została poddana co najmniej jednemu testowi bezpieczeństwa IT w roku. Wymóg ten dotyczy także testów CyberSec po każdej, dużej zmianie – mówi Przemysław Wolek, dyrektor Pionu Bezpieczeństwa Cybernetycznego ING Hubs Poland – wątpię, aby rekomendacja Unii Europejskiej poszła dalej – dodaje.

Zidentyfikuj się

Trzecim filarem bezpieczeństwa, którym zajmuje się ING Hubs Poland jest zarządzanie dostępami i tożsamością. 55 tysięcy pracowników ING na całym świecie mają dostępy do sieci wewnętrznej i różnych systemów. Każdy z nich musi się „wylegitymować", zanim otrzyma dostęp do konkretnego systemu.

Każdy z pracowników ING musi przechodzić obowiązkowe, cykliczne szkolenia dotyczące m.in. cyberbezpieczeństwa. Każdy otrzymuje od czasu do czasu wiadomość e-mail, na którą musi odpowiednio reagować poprzez zgłoszenie phishingu. To tylko jeden z przykładów dbałości o świadomość cyberbezpieczeństwa wśród pracowników Grupy ING.

Inwestycja w bezpieczeństwo

W bezpieczeństwo trzeba inwestować. Technologia jest rozwiązaniem, ale podobnie jak człowiek ma pewne ułomności. Człowiek ulega zmęczeniu lub po wykonaniu zbyt wiele razy podobnego zadania po prostu nie jest w stanie wyłapać drobne odstępstwa od normy. W związku z tym tacy pracownicy rotują na swoich stanowiskach po to, aby zawsze mieć świeży umysł. Technologia nie rotuje – technologia się rozwija. W czym wyraża się jej niedoskonałość? W tym, że reaguje alarmem, który niekoniecznie jest zasadny. W tym momencie wkracza człowiek, który weryfikuje zasadność alarmu.

– Ważnym i rozsądnym kierunkiem jest automatyzowanie pewnych zadań, na razie jednak są one stosowane raczej jako wsparcie, niż działanie odrębne „oddane" maszynie. – mówi Przemysław Wolek.

Inwestycja w bezpieczeństwo to nie tylko wyłożenie pieniędzy (niemałych) na technologię. To także ogromne inwestycje na pozyskanie i utrzymanie, a także rozwój pracowników – specjalistów najwyższej klasy.

– Im więcej mamy potencjalnych zagrożeń z zewnątrz wynikających chociażby z sytuacji geopolityczne, tym więcej pracowników potrzebujemy. Warto podkreślić, że nie tylko ING Hubs Poland – mówi Przemysław Wolek. – To oznacza potężny drenaż rynku pracy, a zatem mniejszą dostępność odpowiednich specjalistów. W związku z tym trzeba mieć to coś, co przyciąga i utrzymuje wewnątrz firmy talenty – dodaje.

Pracowników przyciągają na pewno wynagrodzenie, możliwość rozwoju i… ciekawe zadania. W przypadku pracy w cyberbezpieczeństwie to może być na przykład odparcie ataków cyberprzestępców. A zagrożenia są coraz bardziej wyrafinowane. Bo nie do końca chodzi tylko o pieniądze.

> Dobrze jest pamiętać, że o bezpieczeństwo trzeba dbać na wiele sposobów. Jest też ono w gestii zarówno pracowników banków, jak i ich klientów. Wtedy i tylko wtedy nasze pieniądze są bezpieczne.

Ciemna strona mocy

Kim jest i czego chce cyberprzestępca. Istnieją na świecie przestępcy, którzy po prostu piorą nielegalnie zdobyte środki finansowe – tym zajmuje się pion przeciwdziałania praniu pieniędzy. Tu stosowane są inne mechanizmy niż w przypadku przestępców, którzy chcą wykraść dane. Ci wykorzystują dane do tego, aby okraść klienta banku czy instytucji finansowej. Jednak są także tacy przestępcy, których celem jest zniszczenie danych.

– Te osoby nie mają nic do stracenia. Włamują się do systemów bankowych po to, aby zniszczyć przechowywane tam dane. Nie chcą ich wykorzystywać w żaden sposób. Co gorsza, oni w ogóle nie przejmują się konsekwencjami, jakie im grożą – mówi Przemysław Wolek.

Zniszczenie danych jest chyba największym zagrożeniem dla systemu finansowego. Nie da się bowiem ich odzyskać, a odbudowanie zniszczonej wiedzy – to czas i pieniądze.

Dobrze jest pamiętać, że o bezpieczeństwo trzeba dbać na wiele sposobów. Jest też ono w gestii zarówno pracowników banków, jak i ich klientów. Wtedy i tylko wtedy nasze pieniądze są bezpieczne.

Cyber Mocni dbają o bezpieczeństwo Twojego dziecka w sieci

Cyber Mocni to oddolna inicjatywa ekspertów ING Hubs Poland, na co dzień związanych z szeroko rozumianym cyberbezpieczeństwem. Projekt kierowany jest do dzieci i młodzieży. Ma pomóc im zrozumieć, że internet to fantastyczne narzędzie, ale bywa też niebezpieczne.

Cyber Mocni ostrzegają młodych internautów, na co uważać w sieci oraz jak zachowywać się w internecie, by być mniej podatnym na działania przestępców.

– Stale edukuje się dorosłych, a świadomość cyberzagrożeń należy budować od najmłodszych lat. Stąd też postanowiliśmy wyjść z projektem do dzieci i młodzieży, dla których zagłębienie się w wirtualny świat to coś zupełnie normalnego. A przecież najmłodsi mogą nie zdawać sobie sprawy, że oprócz rozrywki, nauki i przyjemności w sieci mogą czekać na nich zagrożenia. Tak powstał projekt Cyber Mocni – informuje Kamila Juszczyk, Business Control Specialist w ING Hubs Poland, współorganizatorka projektu.

Formuła Cyber Mocnych

Do tej pory, ze względu na pandemię, projekt był realizowany w formie zdalnych webinarów. Aktualnie Cyber Mocni (nierzadko w towarzystwie lwa Leosia) odwiedzają dzieci w szkołach i przedszkolach.

– W ciągu roku przeszkoliliśmy ponad 600 dzieci! Zdecydowaliśmy się zmienić formułę zdalną na realne spotkania, aby jeszcze lepiej krzewić zachowania i postawy dzieci – i to od najmłodszych lat. Szkolenia realizujemy na terenie Katowic i okolicznych miast, a od niedawna także w Warszawie. Zachęcamy do kontaktu z nami poprzez wiadomość e-mail na adres: cybermocni@ing.com, aby umówić spotkanie w szkole lub przedszkolu – dodaje Karolina Sieruga, Business Control Specialist w ING Hubs Poland, współorganizatorka projektu.

Jakie tematy pokrywają szkolenia Cyber Mocnych?

- Książę z bajki – czyli kto tak naprawdę jest po drugiej stronie monitora?
- Bezpieczeństwo aplikacji mobilnych – jak świadomie z nich korzystać i nie dać się oszukać?
- Hejt w internecie – jak się go ustrzec?
- Księżniczka czy żaba – co mówią o nas zdjęcia, które publikujemy?
- Piraci nie tylko z Karaibów – czyli jak nie naruszać praw autorskich?
- Świat finansów – jak go ogarnąć?

Tematy szkoleń dopasowywane są odpowiednio do grup wiekowych. Przeznaczone są przede wszystkim dla dzieci w wieku przedszkolnym oraz uczniów klas 1-8 szkoły podstawowej.

Zadbajmy wspólnie o bezpieczeństwo naszych dzieci w sieci. Z Cyber Mocnymi można skontaktować się pod adresem mailowym: cybermocni@ing.com.

MATERIAŁ PARTNERA

CYBERBEZPIECZEŃSTWO
– krok, którego nie możesz pominąć przenosząc biznes do świata cyfrowego

Cyfrowa transformacja to cel większości organizacji, które chcą działać efektywnie, budować przewagę konkurencyjną i móc w ogóle funkcjonować na rynku. Teraz to już reakcja na teraźniejszość, a nie patrzenie w przyszłość.

Rafał **Barański**

CEO, braf.tech

Dla jednych będzie to dostosowanie środowiska pracy do modelu zdalnego czy hybrydowego, inni w świecie cyfrowym upatrują nowe dla siebie kanały dystrybucji produktów czy usług, a jeszcze kolejna grupa dostrzega możliwości ze stosowania bardziej zaawansowanych technologii w różnych obszarach swojego biznesu. To, co jeszcze 5 lat temu było wymieniane jako trend technologiczny – AI, uczenie maszynowe, blockchain, IoT, chmura obliczeniowa – staje się lub już jest, codziennością wielu firm.

Wieloaspektowość tematu

Jednak, aby na tej drodze do digitalizacji ustrzec się pułapek i problemów i aby działanie było w pełni świadome, konieczne jest uwzględnienie wszystkich aspektów. Jednym z kluczowych jest bezpieczeństwo. Digitalizacja ułatwia prowadzenie procesów biznesowych niezależnie od pory dnia i lokalizacji, zapewnia szeroki dostęp do zasobów i danych, otwiera organizacje na świat. Jednocześnie jednak tworzy nowe zagrożenia, bo przecież inni również mogą starać się zdobyć do tego dostęp. Nie jest to oczywiście nic nowego, ale wiele osób, zwłaszcza w przypadku mniejszych organizacji o tym zapomina.

Kamienie milowe na osi czasu cyfrowej transformacji

Kamieniem milowym na osi czasu cyfrowej transformacji był rok 2020 i pandemia. Masowe wprowadzenie pracy zdalnej pokazało, że większość firm nie była na to gotowa właśnie pod kątem bezpieczeństwa czy możliwości posiadanej infrastruktury informatycznej. Wtedy organizacje zaczęły przechodzić na chmurę, digitalizować procesy wewnętrzne i zewnętrzne i wchodzić do świata online ze swoimi usługami. Jak można było przypuszczać, wszystko zbiegło się z gigantycznym wzrostem liczby ataków cybernetycznych – wg McAfee i FireEye było ich o 81 proc. więcej w 2020 r. w stosunku do 2019 r. Nic więc dziwnego, że wzrosło też zapotrzebowanie na systemy ochrony oraz specjalistów w tym zakresie.

Zadba o kwestie ochrony systemów i infrastruktury

Cyberbezpieczeństwo to bardzo obszerny obszar IT, który z roku na rok jeszcze bardziej się rozrasta, bo pojawiają się nowe technologie, które wpływają na procesy w firmach, ale także nowe zagrożenia i formy ataku. Przede wszystkim trzeba zacząć od ludzi. W zależności od wielkości organizacji i stopnia zaawansowania technologicznego przedsiębiorstwo powinno posiadać osobę lub zespół, który zadba o kwestie ochrony systemów i infrastruktury. W mniejszych podmiotach często jest to administrator systemów lub mały zespół IT zajmujący się podstawowymi operacjami z zakresu obsługi infrastruktury i oprogramowania. Jeśli posiadają oni odpowiednie kompetencje i świadomość zagrożeń to może okazać się to wystarczające. Jednak większe firmy, jak i te wykorzystujące technologie w większej liczbie procesów, powinny jednak szukać specjalistów o konkretnym doświadczeniu i umiejętnościach z zakresu cybersecurity, a to obecnie jest dużym wyzwaniem. Alternatywą jest oczywiście outsourcing ekspertów lub całej usługi od wyspecjalizowanej firmy, co zapewni pewien poziom bezpieczeństwa w tym aspekcie.

Pod kontrolą

Kolejnym punktem obowiązkowym jest audyt i strategia bezpieczeństwa. Firma musi poznać sytuację wyjściową, określić, które procesy i systemy są krytyczne z punktu widzenia ich biznesu, które punkty styku są zabezpieczone, a gdzie może potencjalnie dojść do groźnych incydentów, a następnie stworzyć strategię na bazie tej wiedzy. Sposobów wykorzystania technologii, jak i ochrony jest bardzo wiele i każdy z nich to osobny przypadek. W obecnych czasach nawet proste rozwiązania dają pewien poziom zabezpieczenia. Istotnym elementem jest np. sposób logowania do systemów i aplikacji – weryfikacja wieloskładnikowa (MLA – Multi – Level Authentication) jest bardzo prosta do implementacji i to absolutnie podstawowa rzecz, którą większość dostawców rozwiązań stosuje. Można do tego wykorzystać kody przesyłane na urządzenie mobilne, specjalne aplikacje np. Microsoft czy Google Authenticator, ale też rozwiązania biometryczne. Jeśli organizacja jest duża i wykorzystuje wiele aplikacji, to warto pomyśleć o systemie, który pozwoli kontrolować, kto ma do nich dostęp i na jakim poziomie. Ważne, aby nim odpowiednio zarządzać, bo czasem źródłem incydentów bezpieczeństwa są pracownicy. Takim rozwiązaniem są systemy lasy IAM (Identity Access Management), np. SaraNext stworzony przez braf.

> Człowiek zawsze stanowił najsłabsze ogniowo i pomimo starań specjalistów próbujących wyeliminować luki i automatyzować pewne procesy, bardzo trudno zminimalizować jego wpływ.

tech i stosowany w dużych organizacjach zatrudniających ponad 150 000 osób. Bardzo wiele firm zaczęło stosować w ostatnim czasie rozwiązania chmurowe – migrowało swoje systemy krytyczne czy aplikacje, przechowują tam swoje dane, wykorzystują produkty SaaS (Software as a Service) w procesach biznesowych czy BaaS (Backup as a Service), aby zabezpieczyć się przed utratą ciągłości działania systemów i utratą danych. To dobry pomysł, bo często efektywny kosztowo, ale też same zabezpieczenia natywne są na wystarczającym poziomie, np. dostawcy cloud wymagają każdorazowej weryfikacji tożsamości urządzeń podłączonych do chmurowej sieci. Oczywiście są też bardzo zaawansowane rozwiązania np. systemy oparte o sztuczną inteligencję i uczenie maszynowe, które monitorują środowisko IT w czasie rzeczywistym, rozpoznają zagrożenia, przewidują ataki i podejmują odpowiednie kroki lub informują osobę odpowiedzialną za bezpieczeństwo. To bardzo wyrafinowane systemy, ale miejmy świadomość, że po drugiej stronie barykady przestępcy również stosują takie technologie.

Od cyfrowej transformacji nie ma odwrotu

Na koniec element niezwykle ważny i często pomijany, czyli czynnik ludzki. Do wielu zagrożeń bezpieczeństwa dochodzi w wyniku błędów, zaniedbań, braku wiedzy, a czasem celowego działania pracowników. Człowiek zawsze stanowił najsłabsze ogniowo i pomimo starań specjalistów próbujących wyeliminować luki i automatyzować pewne procesy, bardzo trudno zminimalizować jego wpływ. Jak sobie z tym radzić? Polityka bezpieczeństwa, edukacja, budowanie świadomości zagrożeń i monitorowanie. Większość zdarzeń ma charakter nieintencjonalny i może wynikać z niższego poziomu kompetencji cyfrowych, gorszego dnia, ale też trzeba pamiętać, że metody stosowane przez hakerów są coraz sprytniejsze.

Cyberbezpieczeństwo to kwestia niezwykle złożona i nie ma tu jednej recepty, która ochroni firmę. Podstawa to świadomość zagrożeń i pewne zasoby kompetencji, które można zbudować w firmie lub powierzyć specjalistom z zewnątrz. Od cyfrowej transformacji nie ma odwrotu.

Firmy atrakcyjnym celem dla hakerów, czyli jak zabezpieczyć się przed cyberatakiem

Ryzyko cyberataku dotyczy wszystkich, także mniejszych firm, które mogą go nawet w pierwszym momencie nie zauważyć. To właśnie dla nich skutki działalności cyberprzestępców mogą być najpoważniejsze. Z naszych analiz wynika, że im mniejsza firma, tym dłużej atakujący są w stanie penetrować jej zasoby. W niektórych przypadkach to nawet 51 dni.

Grzegorz **Nocoń**

inżynier systemowy w firmie Sophos

W Polsce aż 8 na 10 ataków ransomware kończy się zaszyfrowaniem firmowych danych. Połowa przedsiębiorstw, których dane zaszyfrowano, zapłaciła przestępcom, nawet jeśli miała inną możliwość odzyskiwania informacji, jak na przykład odtworzenie kopii zapasowych. Firmy płaciły przestępcom średnio 670 tys. zł. Powodów, dla których przedsiębiorstwa płacą okup, może być kilka: niekompletne kopie zapasowe, obawa przed wyciekiem skradzionych informacji, presja, aby jak najszybciej przywrócić działalność. Przywracanie danych za pomocą kopii zapasowych może być trudne i czasochłonne, wiele firm myśli więc, że zapłacenie okupu będzie szybsze. Niestety nie ma gwarancji, że dane zostaną odszyfrowane, a cyberprzestępcy zwrócą pozyskane nielegalnie dane.

Zwracać uwagę na wszystkie aspekty ochrony

Biorąc pod uwagę to, jakie zagrożenia czyhają na firmę, trzeba zwracać uwagę na wszystkie aspekty ochrony: wykorzystywane technologie i oprogramowanie, korzystanie z wiedzy specjalistów, ale też edukację pracowników. Zatrudnieni również mogą stać się celem przestępców, dlatego tak ważne jest przeprowadzanie szkoleń z zakresu firmowych procedur bezpieczeństwa oraz zasad cyberhigieny.

Nie zawsze udaje się ustalić, jak atakujący uzyskali dostęp do firmowej sieci. Dlatego specjaliści do spraw cyberbezpieczeństwa powinni zachować czujność i na bieżąco łatać luki, zwłaszcza w powszechnie używanym oprogramowaniu. Nie mniej istotne jest wdrożenie modelu bezpieczeństwa „zero trust", czyli kontrola dostępu do newralgicznych danych, zabezpieczanie usług umożliwiających pracę zdalną i stosowanie wieloskładnikowego uwierzytelniania. Ważne są również regularne kontrole bezpieczeństwa oraz inwestowanie w wysokiej jakości zabezpieczenia. Najlepszą ochroną jest aktywne „polowanie" na zagrożenia i identyfikowanie atakujących jeszcze zanim dostaną się do sieci. Jeśli nie jest to możliwe w ramach istniejących struktur, warto rozważyć skorzystanie z usług zewnętrznych ekspertów.

Przede wszystkim trzeba też pamiętać, że należy być gotowym na najgorszy scenariusz. Przywracanie systemu po ataku to skomplikowany proces. Firma w takiej sytuacji może być wyłączona na wiele tygodni, co generuje ogromne koszty. Dlatego konieczne jest przygotowanie się na taką ewentualność: tworzenie kopii zapasowych, określenie priorytetów oraz ćwiczenie przywracania danych, a także ścieżki informowania odpowiednich osób o incydencie, aby jak najszybciej wznowić pracę.

Świadomi zagrożeń?

W 2020 r. 27 proc. polskich przedsiębiorstw otwarcie przyznawało, że nie uważa się za potencjalny cel dla hakerów. Rok później odsetek ten zmalał do zaledwie 3 proc., co najlepiej świadczy o tym, jak zwiększyła się świadomość zagrożenia cyberatakami. Z raportu Sophos wynika, że już trzy na cztery polskie firmy miały styczność ze złośliwym oprogramowaniem ransomware. To poważny problem, o którym nie tylko się słyszy, ale coraz częściej odczuwa „na własnej skórze". Ponad połowa ankietowanych przez nas przedsiębiorstw jest zdania, że działania cyberprzestępców są bardziej złożone i dotkliwsze niż w poprzednich latach.

Należy jednak zaznaczyć, że Polska jest nie tylko w europejskiej, ale i w światowej czołówce pod względem odsetka dużych firm posiadających polisę od cyberataku – ma ją aż 97 proc. z nich. W 9 na 10 przypadków wykupione ubezpieczenie obejmuje odszkodowanie za skutki zainfekowania oprogramowaniem ransomware.

Wyraźnie zwiększone zainteresowanie cyberbezpieczeństwem – i działaniami na jego rzecz – wyraźnie widać wśród specjalistów IT w firmach. Sprawy mają się jednak inaczej wśród osób zajmujących najwyższe stanowiska. Z naszych najnowszych badań wynika, że ponad połowa z nich deklaruje, że w firmie stosowana jest polityka cyberbezpieczeństwa. Jednak 28 proc. przyznało, że w ich przedsiębiorstwach takowych się nie stosuje, a prawie co piąty badany nie wie, jaka jest obowiązująca w jego firmie polityka cyberbezpieczeństwa.

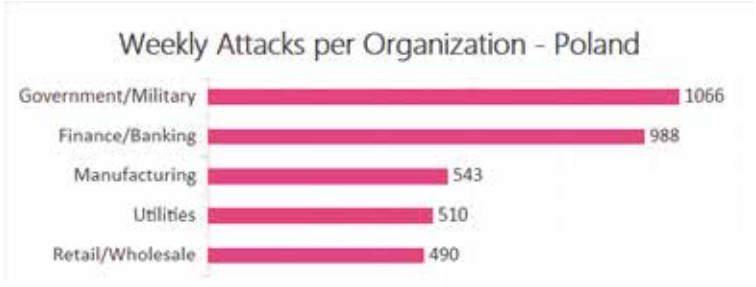
Hakerzy celują w polskie wojsko i administrację!

W ostatnim półroczu polski sektor rządowo-wojskowy doświadczył średnio 1066 ataków cybernetycznych w tygodniu (na pojedynczą sieć!). Niemal równie często atakowane są firmy z sektora finansowo-bankowego (988 ataków na organizację w tygodniu). Obecnie wartości te mogą być jeszcze wyższe, ze względu na potężny, ponad 50 proc., przyrost ataków w ostatnich tygodniach – ostrzegają eksperci firmy Check Point Software.

Już kolejny kwartał utrzymywany jest trzeci stopień alarmowy CRP (CHARLIE-CRP), wprowadzony w celu przeciwdziałania zagrożeniom w cyberprzestrzeni. Stopień CHARLIE–CRP dotyczy bezpieczeństwa cyberprzestrzeni i jest trzecim z czterech stopni alarmowych określonych w ustawie o działaniach antyterrorystycznych. Stopień ten jest wprowadzany w przypadku wystąpienia zdarzenia potwierdzającego prawdopodobny cel ataku o charakterze terrorystycznym w cyberprzestrzeni albo uzyskania wiarygodnych informacji o planowanym zdarzeniu.

W obliczu wysokiego zagrożenia

Wysokie zagrożenie dla kluczowych instytucji w kraju – zarówno publicznych, jak i prywatnych – potwierdzają dane udostępnione przez Check Point Software Technologies, firmę specjalizującą się w bezpieczeństwie cybernetycznym. W ostatnich sześciu miesiącach najczęściej atakowanymi organizacjami były te z sektora rządowo-wojskowego. Doświadczały one średnio 1066 ataków w tygodniu. I to na pojedynczą placówkę! Drugim najczęściej obieranym przez cyberprzestępców celem jest sektor finansowo-bankowy z 988 atakami. Eksperci firmy Check Point wskazują również, że cyberprzestępcy chętnie atakują również polskie firmy z sektora wytwórczego (543), użyteczności publicznej (510) oraz hurt i detal (490 ataków w tygodniu na pojedynczą organizację). Zaznaczają, jednak, że dziś wyniki te mogą być jeszcze wyższe, w ostatnich pięciu tygodniach zaobserwowali bowiem niespodziewany, 50-proc. wzrost cyberataków na polskie organizacje.



Wiele z przeprowadzanych ataków, dzięki zaawansowanym systemom bezpieczeństwa i zespołom reagowania, nie osiąga swoich celów. Te, które przełamały mniej sprawne zabezpieczenia, często nie są ujawniane lub… są poza świadomością zespołów IT. Cyberprzestępcy przez wiele miesięcy mogą inwigilować sieć firmową, ukrywając swoją obecność i czekając na najlepszy moment na ujawnienie. Rezultatem może być zaszyfrowanie danych i wniesienie żądania opłacenia okupu za ich odszyfrowanie. Hakerzy działający na zlecenie innych podmiotów mogą z kolei po cichu wykradać dokumentację, która okazałaby się istotna z punktu widzenia konkurencji. Szpiegostwo przemysłowe działa bowiem również w cyberprzestrzeni. Niestety, wiele z polskich firm wciąż nie posiada bardziej zaawansowanych systemów ani wykwalifikowanego personelu nadzorującego bezpieczeństwo sieciowe. Organizacje, które nie posiadają zasobów na zbudowanie silnego zespołu reagowania, mogą jednak skorzystać z usług zewnętrznych integrujących bezpieczeństwo – np. Check Point Horizon, oferujący również 24-godzinny kontakt z wyspecjalizowanymi analitykami.

Ataki to codzienność. Do gry włączają się haktywiści

W lipcu specjaliści ds. bezpieczeństwa zaobserwowali kampanię hakerską skierowaną przeciwko czołowym firmom z Polski, Czech oraz innych europejskich krajów. Cyberprzestępcy, najprawdopodobniej z północnokoreańskiej grupy APT37, wykorzystali w swoich działaniach malware Konni, będący trojanem zdalnego dostępu. Rok wcześniej, za sprawą tego samego narzędzia, inwigilowane były firmy rosyjskie.

Ataki hakerskie coraz częściej służą również prowadzonym równolegle działaniom wojennym. Cyberwojna to zjawisko, które na dobre zagościło w naszej świadomości za sprawą konfliktu w Ukrainie. Hakerzy walczą w sieci po obu stronach, nie tylko na ścisłe zlecenie rządu, ale będąc częścią ruchu haktywistycznego, przed którym w jednym ze swoich raportów przestrzegali analitycy Check Point Research. Ich orężem są nie tylko złośliwe programy, ale również fakenewsy oraz wszelka dezinformacja pojawiająca się od wielu lat w sieci.

Przykładem działań na rzecz wojny był lipcowy atak DDoS na polską Policję, prawdopodobnie przeprowadzony przez rosyjskojęzyczną grupę Killnet, która w maju 2022 r. wypowiedziała wojnę krajom wspierającym Ukrainę, w tym Polsce. Kilka miesięcy wcześniej zaatakowany został jeden z serwisów informacyjnych Wirtualnej Polski. Hakerzy umieścili na stronie hasło „Ukraina musi przegrać".

Kiedyś incydenty, dziś spustoszenie: ewolucja cyberataków w sektorze finansowym

W ciągu ostatnich lat kartele cyberprzestępcze rozpleniły się po całej Europie. Co gorsza, zajęły pozycję i wytoczyły przeciwko nam znacznie większe działa niż kiedykolwiek.

Piotr **Kraś**

menadżer zespołu architektów, VMware

Prężnie działające grupy hakerów funkcjonują obecnie na wzór wielonarodowych korporacji i są wykorzystywane przez konwencjonalne syndykaty przestępcze do wspierania ich nielegalnej działalności, takiej jak wymuszenia i pranie brudnych pieniędzy. Profesjonalne i zorganizowane jak nigdy dotąd, cieszą się również większą protekcją i strumieniem funduszy ze strony niektórych państw, które, choć głośno tego nie mówią, widzą w nich swoją tajną broń.

Według badań przeprowadzonych przez brytyjski gabinet Wielka Brytania doświadcza corocznie największej liczby takich przestępstw w Europie, zaraz za nią plasuje się Francja. Uwzględniając te fakty jako tło dla współczesnych zagrożeń, VMware przeprowadził wywiady ze 130 liderami ds. bezpieczeństwa finansowego i sieciowego z całego świata. Celem było przygotowanie 5. edycji raportu na temat napadów na nowoczesne banki. Tegoroczne wyniki powinny być ostrzeżeniem dla całej branży — napastnicy cele zmieniają jak rękawiczki, a skala spustoszeń jest przerażająca.

Napięcie geopolityczne rozprzestrzenia się w cyberprzestrzeni

Ataki wymierzone w sektor finansowy często doprowadzają do całkowitej zagłady – w ten sposób napastnicy zacierają ślady, przez co utrudniają podjęcie jakichkolwiek działań organom ścigania. Z naszego raportu wynika, że 63 proc. instytucji finansowych doświadczyło zwiększonej liczby ataków destrukcyjnych, co stanowi wzrost o 17 proc. w stosunku do ubiegłego roku. Tego typu incydenty polegają między innymi na szyfrowaniu plików, usuwaniu danych, niszczeniu dysków twardych, przerywaniu połączeń lub implementacji złośliwego kodu.

Przykładowo, przy okazji inwazji Rosji na Ukrainę byliśmy świadkami wypuszczenia złośliwego oprogramowania o nazwie HermeticWiper. Ten malware potrafi ominąć zabezpieczenia systemu Windows i uzyskać dostęp do wielu niskopoziomowych struktur danych na dysku, fragmentować pliki i nadpisywać je, aby później uniemożliwić ich odzyskanie.

Należy podkreślić, że większość respondentów naszego badania stwierdziła, że to właśnie Rosja stanowi największe zagrożenie dla działalności ich organizacji.

Rok RAT – szczury z dark webu

Instytucje finansowe nie były odpowiednio przygotowane na niedawne odrodzenie się oprogramowania ransomware. 74 proc. liderów ds. bezpieczeństwa finansowego doświadczyło jednego lub więcej ataków tego rodzaju w ciągu ostatniego roku, a 63 proc. ofiar zapłaciło okup. Te statystyki są zatrważające.

Jednym z powodów, dla którego tradycyjne organizacje przestępcze zostały stałymi klientami dark webu, jest dobrze zaopatrzony ekosystem z gotowymi do użycia zestawami wirusów. Co więcej, tacy cyberzłoczyńcy jak grupa Conti, maksymalnie

ułatwili swoim współpracownikom przeprowadzanie ataków ransomware na krytyczne branże, takie jak branża finansowa. W tej organizacji zwykli programiści zarabiają około 1500-2000$ miesięcznie, a członkowie negocjujący płatności okupu mogą brać udział w podziale zysków.

Analiza techniczna zawarta w najnowszym raporcie VMware Threat Analysis Unit pokazuje, jak rozprzestrzenia się oprogramowanie ransomware i jak narzędzia zdalnego dostępu (Remote Access Tools) ułatwiają napastnikom przejmowanie kontroli nad systemami. Ransomware i narzędzia RAT to toksyczna kombinacja, która pozwala atakującym utrzymać się w środowisku i ustanowić serwery pośrednie, które mogą być wykorzystane do atakowania kolejnych systemów.

Gdy cyberprzestępcy uzyskają wymagany dostęp, zazwyczaj starają się go spieniężyć, wykorzystując do wymuszeń (w tym podwójnych i potrójnych) dane ofiary lub wykorzystując dostęp do zasobów/usług chmurowych do wydobywania kryptowalut (cryptojacking).

Manipulowanie rynkami finansowymi

Cyberkartele zdały sobie sprawę, że najcenniejszym aktywem instytucji finansowych są niepubliczne informacje rynkowe. 2/3 liderów, doświadczyło ataków, których celem były strategie handlowe. 25 proc. z nich przyznało, że w ich wypadku chodziło o dane rynkowe.

Jesteśmy świadkami ewolucji od napadu na bank do szpiegostwa gospodarczego. Cyberprzestępcy biorą na cel informacje lub strategie korporacyjne, które – gdy tylko zostaną podane do publicznej wiadomości – mogą wpłynąć na kurs akcji firmy. Ci poinformowani mogą wyprzedzić rynek i wykorzystać posiadaną wiedzę przy transakcjach handlowych. Z przeprowadzonego badania wynika, że 44 proc. ataków Chronos było wymierzonych w pozycje rynkowe. Dotyczy to manipulacji znacznikami czasu, co jest niepokojące, biorąc pod uwagę, jak krytyczną rolę odgrywa czas na rynkach finansowych.

Obrona jest najlepszym atakiem

Dlatego bezpieczeństwo stało się najważniejszą kwestią wśród liderów sektora finansowego. Zgodnie z wynikami naszego raportu, większość instytucji finansowych planuje w tym roku zwiększyć swój budżet zabezpieczenia o 20-30 proc., uznając rozszerzone wykrywanie i reagowanie (Extended Detection and Response: XDR) za swój najistotniejszy priorytet inwestycyjny w tej dziedzinie.

Jako specjaliści od bezpieczeństwa wiemy, że silna obrona to najlepszy atak — za standardową czynność powinno się przyjąć cotygodniowe wyszukiwanie zagrożeń. Dzielenie się spostrzeżeniami dotyczącymi potencjalnych czy zaobserwowanych zagrożeń, pomogłoby zespołom bezpieczeństwa w wykrywaniu anomalii behawioralnych, ponieważ agresorzy mogą potajemnie utrwalać się w infrastrukturze organizacji. Obecnie tylko 51 proc. instytucji finansowych przeprowadza takie czynności raz w tygodniu. Mam nadzieję, że liczba ta zwiększy się w przyszłorocznym raporcie, ponieważ działania typu threat hunting mają wiele zalet, nie tylko pozwalają na wykrycie śladów włamania, ale także stanowią źródło informacji o zagrożeniach.

Biorąc pod uwagę dzisiejszy ewoluujący krajobraz zagrożeń, cyberbezpieczeństwo stało się imperatywem dla ochrony marki. Zaufanie i wiara bezpieczeństwo usług finansowych zależy od umiejętnego unikania, łagodzenia i reagowania na współczesne zagrożenia cybernetyczne. Podczas gdy organy zarządzające ustanawiają nowe regulacje i wymierzają wysokie kary, przyszedł czas, by branża przejęła inicjatywę i wyprzedziła o krok internetowych przestępców.

Usługi MDR - skuteczna ochrona przed cyberatakami

Ochrona danych jeszcze nigdy nie była tak ważna ani nie stanowiła większego wyzwania. Cyberataki stają się coraz bardziej wyrafinowane i ukierunkowane, a tradycyjne rozwiązania bezpieczeństwa już nie wystarczają.

Zbigniew **Kniżewski**

Chief Executive Officer, Cyber360

Niestety, wiele firm nadal nie do końca wie, w jaki sposób podejść do tematu cyberbezpieczeństwa w organizacji, łudząc się, że ten problem ich nie dotyczy lub że ich dotychczasowe sposoby i zabezpieczenia działają bez zarzutu.

Statystyki jednak nie kłamią i pokazują, że problem jest bardzo realny. Według IBM, ataki hakerskie wykrywane są średnio dopiero po 212 dniach. To ponad pół roku nieuprawnionego dostępu do danych! W roku 2020, w sieci hoteli Mariott wykryto cyberatak, który kosztował organizację utratę danych ponad 5 milionów klientów – i utratę zaufania, być może na zawsze.

Zarządzać zagrożeniami

Rozwiązaniem tego problemu są dostępne na rynku usługi MDR (Managed Detection and Response). MDR zapewnia całodobowe monitorowanie i wykrywanie zagrożeń, a także możliwości reagowania na incydenty. Dlaczego takie podejście daje lepszą ochronę? Ponieważ obejmuje wszystkie aspekty cyberbezpieczeństwa, a dzięki wdrożeniu MDR, organizacja może analizować i usuwać potencjalne incydenty w ramach infrastruktury, serwerów, czy urządzeń, na różnych segmentach sieci przez całą dobę. Co ważne zarządzanie zagrożeniami jest ułatwione dzięki stałemu monitoringowi środowiska klienta i analizie danych w celu identyfikacji potencjalnych incydentów. Usługa działa bez przerwy, a taka konfiguracja pozwala firmom skupić się na swojej działalności, bez konieczności martwienia się o kwestie bezpieczeństwa danych. MDR jest działaniem proaktywnym. Oznacza to, że potencjalne zagrożenia są identyfikowane i usuwane, zanim zdążą wyrządzić jakiekolwiek szkody. MDR to usługi 360 stopni, które wykorzystują najnowocześniejszą technologię i najnowsze informacje dotyczące bezpieczeństwa, aby wyprzedzać nie tylko potencjalne ataki, ale i trendy związane z nowymi zagrożeniami. Zarówno przedsiębiorstwa, które mają już wdrożone częściowe procesy cyberbezpieczeństwa, jak i te, które nie mają strategii reagowania na cyberataki, mogą w pełni wykorzystać benefity MDR w organizacji.

Monitorowanie zagrożeń 24/7 nie powinno już być traktowane jako opcjonalne, a podejście oparte na usługach MDR daje największe szanse na odparcie coraz bardziej zaawansowanych, internetowych ataków. To nowoczesne rozwiązanie, które każda firma powinna posiadać, aby chronić swoje dane, procesy i operacje biznesowe.

Potrzeby konsumentów, a odpowiedź firm w świetle zmieniających się oczekiwań

Konsumenci jasno mówią co myślą o zagrożeniu, jakim jest rosnąca liczba oszustw w związku z popularyzacją handlu przez Internet. Według tegorocznego Adyen Retail Report, 52 proc. Polaków twierdzi, że przedsiębiorstwa powinny mocniej chronić klientów przed oszustwami podczas zakupów. Co na to biznes? Okazuje się, że luka między wymaganiami i dostarczanymi usługami rośnie, zamiast się zmniejszać.

Jakub **Czerwiński**

VP CEE, Adyen

Wraz z procesem transformacji cyfrowej pojawiają się nowe zagrożenia, a cyberoszuści podejmują coraz odważniejsze kroki, by śledzić firmy i ich klientów nie tylko w przestrzeni fizycznej, ale i w świecie wirtualnym – szczególnie jeśli pod uwagę weźmiemy krajobraz dzisiejszego handlu. Chcący pozostać na czele peletonu sprzedawcy coraz mocniej otwierają się nowe kanały mobilne, czy sprzedaż przy użyciu mediów społecznościowych. Konsumenci przedstawiają przy tym swoje oczekiwania dość jasno, jednak nie wszyscy przedsiębiorcy potrafią na nie odpowiedzieć. W tegorocznym Adyen Retail Report polscy sprzedawcy przyznają, że próby wyłudzeń wzrosły w zeszłym roku o 33 proc.
Dla kontrastu, tyle samo konsumentów zezwoli sprzedawcy na przechowywanie i wykorzystywanie danych pod warunkiem zapewnienia bezpieczeństwa i ochrony prywatności, a jak powszechnie wiadomo, to właśnie dane o kliencie są kluczem do sukcesu marki. Niestety, ponad połowa Polaków (52 proc.) nadal jest zdania, że sprzedawcy muszą zrobić więcej, aby chronić konsumentów przed oszustwami związanymi z płatnościami (średnia światowa to 49 proc.).
Takie dane wskazują na pewien zastój w rozwoju relacji klient – marka, jednak z drugiej strony widocznie podkreślają, które aspekty powinny się zmienić, by poziom usług, jakiego oczekują klienci, wzrósł. Właściwe przygotowanie e-sklepu ma kluczowe znaczenie w zwalczaniu tego typu działalności. Gdzie szukać odpowiedzi?

Era przestępczości 4.0 versus SI
Ruch na stronie i zgromadzone dane powinny być stale monitorowane i analizowane, by upewnić się, że nie utworzyły się żadne otwarte luki, które mogą zagrażać klientom. Należy uważnie obserwować wszelkiego rodzaju zagrożenia, ataki i podejrzane działania oraz niezwłocznie reagować w przypadku ich wystąpienia. Warto współpracować z wiarygodnymi firmami, które pomagają w przetwarzaniu płatności i utrzymywaniu bezpieczeństwa danych swoich klientów.
Coraz większą rolę w wykrywaniu oszustw w transakcjach, eliminacji nadużyć i zwalczaniu kradzieży tożsamości odgrywają zaawansowane algorytmy – według badań Adyen ich pomocy szuka już 41 proc. polskich firm. Coraz bardziej widoczna staje się bowiem np. aktywność testerów kart, którzy wykorzystują w swoich działaniach boty lub skrypty. Odpowiednie rozwiązanie oparte na algorytmach sztucznej inteligencji i uczeniu maszynowym może ich jednak łatwo zidentyfikować, m.in. poprzez wykrycie nieprawidłowości w transakcjach poddanych analizie w niewielkim przedziale czasowym. Dzięki dodatkowym danym i elastycznemu systemowi ryzyka, firmy są w stanie wykorzystać dokładniejsze profile kupujących, aby zrozumieć ich regularne zachowania i to, jak różnią się one po przejęciu konta przez niepożądaną osobę. By stworzyć stabilny kontekst, brane są pod uwagę setki powiązanych ze sobą parametrów, nawet jeśli kupujący zmieni urządzenie czy sieć. System sygnalizuje nietypowe zachowanie użytkownika, wskazując ryzyko wystąpienia nadużycia.
Wykorzystując możliwości technologii wspierających bezpieczeństwo transakcji, właściciele zyskują przewagę w zakresie przewidywania i zapobiegania oszustwom, a także wiedzę na temat środowiska ryzyka w celu szybkiego wykrywania anomalii. Wszystko zachodzi przy maksymalnym ograniczeniu manualnych działań i pełnej przejrzystości transakcji. W świecie napędzanym przez e-zakupy to obecnie jeden z najważniejszych elementów zabezpieczających rozwój e-commerce.

Patrząc w przód
Odpowiednia strategia przeciwdziałania oszustwom wymaga uwagi i skupienia – losowo dobierane zasady, ciągłe zmiany w modelach biznesowych lub integracja z dodatkowymi partnerami mogą nie tyle podważyć zaufanie klientów, ile odebrać to zaufanie raz na zawsze. Należy pamiętać, że przestępcy dostosowują się do otoczenia niczym kameleon i potrafią płynnie poruszać się po krawędzi. Jednocześnie, co ważne, weryfikacja użytkowników lub przeprowadzanych transakcji nie powinna odbywać się kosztem ich interakcji z firmą – w przeciwnym razie powrót konsumentów do wybranych usług może być obarczony dużym ryzykiem. Przedsiębiorcy zawsze powinni zachować czujność i zadbać o to, by wybrać jak najlepsze podejście, które finalnie zapewni klientom niepodważalne bezpieczeństwo.
Analiza najnowszych danych dotyczących polskiego krajobrazu handlowego powinna stanowić dla nich istotną wskazówkę. Ze względu na to, że kwestie płatności – ich bezpieczeństwa, opcji wyboru i szybkości – są tak istotne dla kupujących, e-handel powinien jeszcze bardziej zainwestować w ten obszar działalności.

Cyberbezpieczeństwo kluczowym elementem wspierającym biznes podczas cyfrowej transformacji

Wraz z rozszerzaniem przez przedsiębiorstwa zakresu swoich sieci, m.in. na lokalizacje zdalne i domowe biura pracowników, wrosło znaczenie cyberbezpieczeństwa jako strategicznie ważnego obszaru. Zapewnienie ochrony infrastrukturze IT oraz gromadzonym i przetwarzanym w niej danym nie jest już sprawą wyłącznie działów informatycznych. Wraz z postępem cyfrowej rewolucji zagadnienia te stały się kwestią kluczową dla działalności operacyjnej firm czy ich wizerunku, co jest szczególnie istotne w branży finansowej.

Jolanta **Malak**

dyrektorka Fortinet w Polsce

Jak podkreślają eksperci, obecnie należy zadawać sobie pytanie: nie czy, ale kiedy firma zostanie zaatakowana przez cyberprzestępców. Mają oni do dyspozycji coraz nowocześniejsze narzędzia, bazujące na sztucznej inteligencji i wyposażone w mechanizmy automatyzacji. Dodatkowo, niektóre z nich mogą być wykorzystywane nawet przez początkujących i mało wprawnych technicznie przestępców. Jest to możliwe, ponieważ w darknecie można znaleźć wiele złośliwych narzędzi, dostępnych w modelu usługowym. Tymczasem infrastruktura IT w firmach jest coraz bardziej złożona, często zabezpieczana przez wiele niewspółpracujących ze sobą rozwiązań ochronnych. Ponadto przedsiębiorstwa często skarżą się na obecność luki kompetencyjnej, wskazując na rynkowy brak odpowiedniej liczby specjalistów ds. cyberbezpieczeństwa.

W wielu przedsiębiorstwach osoby zajmujące się bezpieczeństwem IT muszą brać odpowiedzialność za wykrywanie coraz bardziej wyrafinowanych i szkodliwych cyberataków. Tymczasem zazwyczaj do dyspozycji mają zestaw złożonych i odizolowanych od siebie narzędzi ochronnych. Taka sytuacja często doprowadza do powstawania luk w zabezpieczeniach, co z kolei skutkuje kradzieżą danych, pieniędzy lub kosztownym przestojem w działalności firmy, a w dalszej konsekwencji – problemami prawnymi i wizerunkowymi.

Cyberbezpieczeństwo zyskuje na znaczeniu

Na szczęście od pewnego czasu osoby zarządzające przedsiębiorstwami zdają się rozumieć, że cyberbezpieczeństwo jest obszarem o krytycznym znaczeniu dla firm. Z pewnością na zrozumienie tego stanu wpłynęła pandemia COVID-19, w trakcie której zaistniała nagła konieczność zabezpieczenia środowiska pracy zdalnej. Według badania dotyczącego zachowania ciągłości biznesowej w firmach w Polsce przeprowadzonego przez Fortinet w 2020 r., aż 88 proc. ankietowanych przyznało, że cyberbezpieczeństwo jest dla zarządu priorytetowe lub przynajmniej istotne.

Wśród działań, które miałyby poświadczyć, że tak w istocie jest, wymieniano m.in. nacisk na przeprowadzanie przeglądów procesów bezpieczeństwa oraz zwiększenie budżetu na rozwiązania ochronne, jak i szkolenia dla pracowników. Zarządy firm chciały też mieć lepszy wgląd w sytuację dotyczącą stanu bezpieczeństwa, stąd też wzrosły ich oczekiwania co do częstotliwości raportowania działań związanych z bezpieczeństwem IT.

Spójna architektura ochronna na ratunek

Zmiana podejścia osób zarządzających firmami musi jednak iść w parze ze zmianą myślenia na temat stosowanych w firmach zabezpieczeń. Architektura ochronna powinna wspierać procesy związane z cyfrową transformacją, jakie zachodzą w przedsiębiorstwach. Dlatego należy odchodzić od zabezpieczeń bazujących na punktowych rozwiązaniach zabezpieczających, często niewspółpracujących ze sobą, na rzecz skonsolidowanej i zautomatyzowanej platformy ochronnej. Jej poszczególne elementy powinny ze sobą współpracować i zapewniać wysoki poziom bezpieczeństwa dla całego środowiska IT: sieci, urządzeń końcowych, aplikacji, chmury i centrów danych.

Dzięki możliwości wzajemnej komunikacji rozwiązania działające w ramach zintegrowanej platformy ochronnej pozwalają na automatyzację procesów, co z kolei pozwala szybciej identyfikować zagrożenia. Systemy bazujące na sztucznej inteligencji oraz uczeniu maszynowym, często wbudowane w zintegrowane platformy ochronne, zapewniają identyfikowanie złośliwych narzędzi, ich analizę oraz reagowanie na nie w czasie rzeczywistym, co pozwala zminimalizować ryzyko wystąpienia incydentu naruszenia bezpieczeństwa sieci.

Należy zadbać o wiedzę pracowników

Cyfrowa transformacja sprawia również, że każdy z pracowników firmy staje się współodpowiedzialny za zachowanie bezpieczeństwa IT. Dlatego też osoby decyzyjne w przedsiębiorstwach powinny dbać o to, aby personel miał zapewnioną aktualną wiedzę na temat cyberzagrożeń w sieci.

Regularnie powinny być przeprowadzane szkolenia dotyczące cyberhigieny, a ich uczestnicy powinni rozumieć, jakie są podstawowe zasady dotyczące bezpiecznego poruszania się w cyfrowej przestrzeni, jak rozpoznać próbę ataku z wykorzystaniem technik manipulacyjnych (np. phishing), jakie są podstawowe zasady dotyczące tworzenia i przechowywania silnych haseł, korzystania z wieloskładnikowej weryfikacji dostępu do kont itd. Ważne jest także, aby firma posiadała opracowaną politykę bezpieczeństwa, w tym określone procedury mówiące, jak pracownicy powinni się zachować w przypadku zauważenia incydentu dotyczącego bezpieczeństwa IT.

Podsumowując: aby proces cyfrowej transformacji był dla firmy zyskowny, przyczyniał się do jej rozwoju, ale jednocześnie był bezpieczny, należy zadbać o odpowiedni poziom i zakres rozwiązań ochronnych oraz zainwestować w wiedzę i umiejętności pracowników.

Korzystanie z prywatnych urządzeń w pracy, a cyberbezpieczeństwo

Praca zdalna i hybrydowa wpłynęły na zwiększenie się skali zjawiska BYOD (Bring Your Own Device), które polega na wykonywaniu pracy za pomocą urządzeń prywatnych, np. smartfonów czy tabletów. Jednak jednocześnie wzrosło ryzyko cyberataków na prywatny sprzęt, który po połączeniu z firmową siecią może stać się dla przestępców bramą wejściową do całego systemu przedsiębiorstwa.

Wojciech **Ciesielski**

menedżer ds. sektora finansowego, Fortinet

Nie wszystkie firmy są w stanie zapewnić swoim pracownikom odpowiednie narzędzia, takie jak komputery, laptopy czy telefony, do wykonywania pracy spoza biura. Z kolei sprzęt prywatny nie zawsze wyposażony jest w odpowiednie systemy zabezpieczenia danych, co powoduje, że podczas wykorzystywania go do pracy dane służbowe stają się narażone na ataki cyberprzestępców. Jednak, jak wskazują eksperci Fortinet, to błędy ludzkie najczęściej powodują wycieki poufnych informacji. Dotyczy to również sektora finansowego i zatrudnionych w nim pracowników.

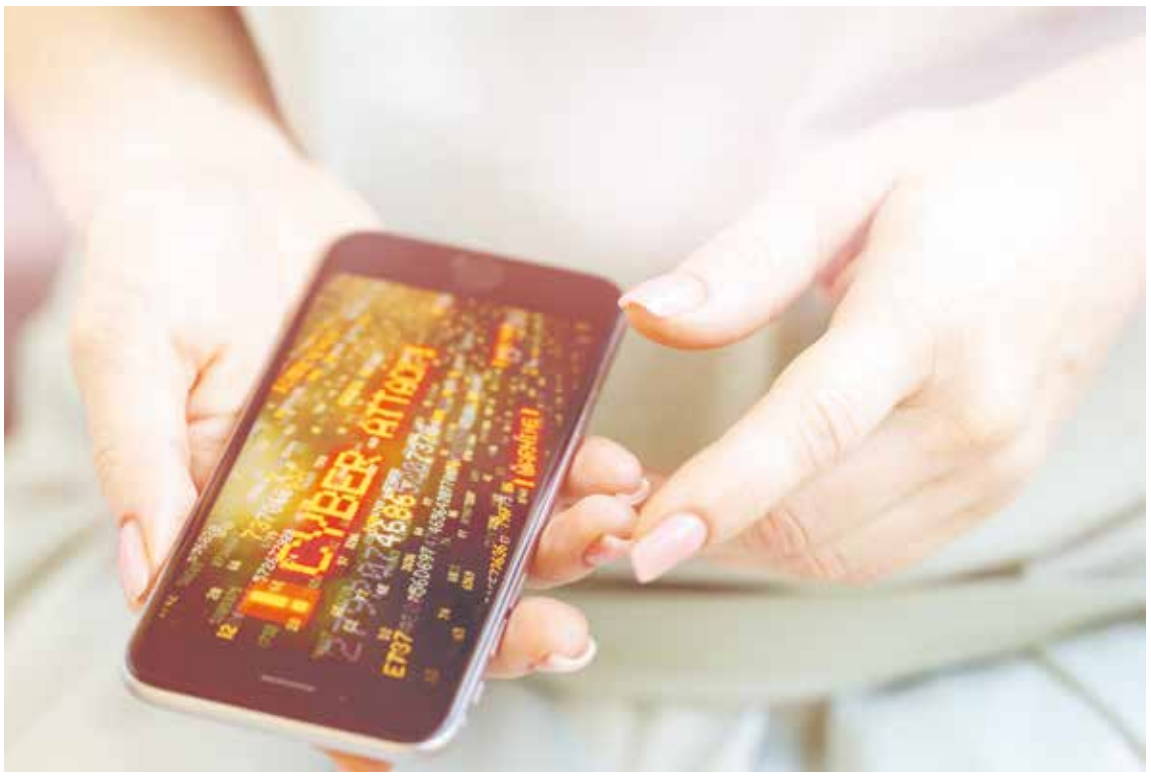
Ludzkie błędy otwierają drzwi przestępcom

Oszuści coraz częściej stosują metody socjotechniczne do prowadzenia ataków. Należą do nich m.in. phishing i smishing. Oba polegają na rozsyłaniu wiadomości (odpowiednio drogą mailową i SMS-ową) oddziałujących na emocje i mających skłonić ofiarę do kliknięcia w link lub otwarcia załącznika. To następnie może przyczynić się do zainfekowania urządzenia złośliwym oprogramowaniem i umożliwia cyberprzestępcom uzyskanie dostępu do danych. Jeśli takie oprogramowanie zostanie zainstalowane na prywatnym sprzęcie służącym do pracy, ofiara może stracić nie tylko swoje osobiste dane, ale także te służbowe. Dlatego nigdy nie należy klikać w linki zawarte w podejrzanie wyglądających wiadomościach. Błędy ludzkie mogą również przybierać formę przeoczeń i zaniedbań, wynikających m.in. z niedoboru pracowników odpowiedzialnych za zabezpieczanie infrastruktury IT. Z luką kompetencyjną w obszarze cyberbezpieczeństwa zmaga się obecnie wiele firm na całym świecie. W badaniu Fortinet „2022 Cybersecurity Skills Gap" 60 proc. respondentów przyznało, że ma problem z zatrudnieniem specjalistów od bezpieczeństwa IT. Ich zbyt niska liczba, w połączeniu z brakiem odpowiedniej ochrony, może doprowadzić do tego, że incydenty dotyczące bezpieczeństwa pozostaną niewykryte, a cyberprzestępcy zyskają cenny czas na przeszukanie zasobów wewnątrz firmowej sieci. Raport „Cost of a Data Breach 2022", opracowany przez firmę IBM, wskazuje, że średni czas upływający od momentu naruszenia bezpieczeństwa do chwili jego wykrycia wynosi aż 277 dni.

Jak zapobiegać cyberatakom?

Podstawową formą zapobiegania atakom jest prawidłowe zarządzanie ryzykiem. Firmy muszą określić, jakie są ich najważniejsze zasoby w infrastrukturze IT, jakimi drogami przestępcy mogą dostać się do systemu i jakie działania należy podjąć w celu minimalizowania negatywnych skutków ataku. Obejmuje to również zabezpieczanie urządzeń pracowników, które stanowią dodatkową ścieżkę potencjalnego włamania.

Bardzo ważnym elementem zapobiegania cyberatakom jest edukacja. Pracodawcy powinni zapewnić swoim pracownikom możliwość poszerzania wiedzy z zakresu cyberzagrożeń i sposobów reagowania na nie. Szkolenia, webinary i programy treningowe, pokazujące jak należy dbać o cyberhigienę, mogą uchronić przedsiębiorstwo przed poważnymi stratami, zarówno dotyczącymi danych, jak i finansowymi.



NIE UFAJ WŁASNYM OCZOM, BO MOGĄ CIĘ MYLIĆ

Wołodymyr Zelenskij nakazuje poddać się Ukrainie. Tom Cruise instruuje, jak używać detergentów, a Salvador Dali ożywa – co łączy te historie? To wierutna bzdura, a do jej stworzenia wykorzystano technologię deepfake.

Krzysztof **Szukała**

Inspektor Ochrony Danych Osobowych (ISC)2 CISSP, Grupa 3 S

Jeżeli ransomware nie dał wystarczająco popalić zespołom ds. bezpieczeństwa, to na horyzoncie pojawiło się nowe wyzwanie — fala cyfrowych oszustów używających tej technologii.

W marcu w mediach społecznościowych pojawiło się nagranie, na którym prezydent Ukrainy, Wołodymyr Żeleński wydaje polecenie swoim żołnierzom, aby poddali się siłom rosyjskim. Kapitulacja? W żadnym wypadku, to po prostu… deepfake. A to tylko jeden z wielu przykładów potencjalnych zagrożeń, jakie stworzyć może wykorzystanie tej technologii.

Ofiarami są nie tylko głowy państw, „żartownisie" upodobali sobie także gwiazdy kina i sportu, a nawet postaci historyczne. Na platformie TikTok opublikowano film z udziałem Toma Cruise'a, który doradzał, jak radzić sobie z detergentami podczas sprzątania. Film obejrzano ponad pół miliona razy, problem w tym, że jego główny bohater nigdy w nim nie uczestniczył.

Co więcej, obecnie rosnącą popularnością cieszy się socialmediowy trend Deep Nostalgia, polegający na tym, że przy użyciu technologii deepfake, opracowanej przez My Hertige i zdjęcia, internauci „ożywiają" zmarłe osoby i nagrywają swoje reakcje. Postać mruga oczami, prezentuje zadziwiająco realną mimikę twarzy, ciepło się uśmiecha, a w przede wszystkim wywołuje wzruszenie i łzy stęsknionej osoby.

Ślepa wiara

To znak, że zjawisko to staje się coraz bardziej zaawansowane i przybiera na sile. Poprzednie przypadki, które stawały się viralami, miały często charakterystyczne oznaki, że z materiałem jest coś nie tak, jak choćby nieporadne montaże czy nietypowa mimika lub gesty postaci.

Deepfake świetnie radzi sobie z naśladowaniem prawdziwych ludzi. Jest wielce prawdopodobne, że szybko stanie się to problemem dla wszystkich. Ta metoda wykorzystuje sztuczną inteligencję i techniki głębokiego uczenia do generowania sfałszowanych obrazów osób lub całych wydarzeń. Ataki tego typu wzrosły o 13 proc. – w VMware Global Incident Response Threat Report, 66 proc. respondentów stwierdziło, że miało z nimi do czynienia w ciągu ostatnich 12 miesięcy.

Rozwój technologii deepfake sprawia, że nietrudno wyobrazić sobie jej eksploatację przez cyberprzestępców, zwłaszcza w celu wyłudzenia pieniędzy. Zdaniem większości respondentów badania VMware ataki deepfake częściej przybierały formę wideo (58 proc.) niż audio (42 proc.), a do najpopularniejszych metod ich dostarczania należały: wiadomości e-mail (78 proc.), mobilne przesyłanie wiadomości (57 proc.), głos (34 proc.), kanały social (34 proc.).

Komplementarność cyberprzestępczości

Może i ransomware generuje więcej nagłówków, ale to włamania do firmowej poczty elektronicznej są obecnie najdroższym formatem cyberoszutsw — według szacunków FBI, każdego roku kosztuje to firmy miliardy dolarów. Cyberprzestępcy, wykorzystując wiadomości e-mail, włamują się na konta należące do przełożonych — ewentualnie sprytnie podszywają się pod ich adresy e-mail – i proszą pracowników o autoryzację dużych transakcji finansowych, które niejednokrotnie mogą opiewać na kwoty rzędu setek tysięcy.

Przykładowo: przełożony w prowadzonej korespondencji informuje, że pieniądze muszą zostać niezwłocznie wysłane, być może w ramach poufnej transakcji biznesowej, której nie wolno nikomu wyjawić. Jest to klasyczna sztuczka socjotechniczna nastawiona na zmuszenie ofiary do szybkiego przelania pieniędzy bez żądania potwierdzenia od kogokolwiek, kto mógłby zorientować się, że jest to fikcyjna dyspozycja. Nim ktokolwiek zdąży się zorientować, cyberprzestępcy i pieniądze rozpływają się w powietrzu.

Takie ataki są bardzo często skuteczne, niemniej wiele osób pozostaje podejrzliwymi wobec nietypowych, nagłych wiadomości od szefa. Gdyby jednak cyberprzestępcy mogli użyć deepfake'a do wystosowania swojej fikcyjnej prośby, wówczas ofiarom może być znacznie trudniej odmówić, ponieważ byliby przekonani, że rzeczywiście rozmawiają ze swoim szefem na kamerze. Niejedna organizacja umieszcza na swojej stronie internetowej listę kierownictwa wyższego szczebla. Członkowie zarządu często przemawiają na imprezach lub w mediach, więc z łatwością można znaleźć nagrania ich wystąpień.

Przestępcy mogliby, przy użyciu zaawansowanych technik uczenia głębokiego, wykorzystać publicznie dostępne informacje i materiały, aby stworzyć fałszywą postać np. członka zarządu. Następnie wykorzystując luki w poczcie elektronicznej, umówić rozmowę wideo z pracownikiem i poprosić go o dokonanie (fałszywej) transakcji. Jeśli ofiara uwierzy, że rozmawia ze swoim przełożonym, jest mało prawdopodobne, że odmówi wykonania polecenia. Oszuści wykorzystywali już sztuczną inteligencję, aby przekonać współpracowników, że rozmawiają przez telefon ze swoim szefem. Dodanie elementu wideo sprawi, że jeszcze trudniej będzie wykryć, że w rzeczywistości kontaktują się z oszustami.

Fałszywy obraz obnaża wady pracy zdalnej

Cyberprzestępcy używają deepfake'ów, aby ubiegać się o zdalne stanowiska pomocy technicznej IT, czyli role, które umożliwiałyby dostęp do wrażliwych danych osobowych pracowników i klientów, a te można by wykraść i wykorzystać. Co więcej, hakerzy będą wykorzystywać „fałszywe obrazy" i inne treści generowane przez AI do przeprowadzania obcych operacji wywierania wpływu.

Wprawdzie postęp technologiczny sprawia, że coraz trudniej jest odróżnić deepfake od autentycznego materiału wideo, ale FBI radzi by szukać w wideo wypaczeń obrazu, nienaturalnych ruchów głowy i tułowia, a także problemów z synchronizacją ruchów twarzy i ust czy towarzyszącym dźwiękiem. Sfałszowane wideo może bez trudu zostać nowym wektorem cyberprzestępczości, stąd powstrzymanie tego trendu będzie nie lada sztuką. Niewykluczone, że organizacje zostaną zmuszone do opracowania nowych zasad uwierzytelniania decyzji podczas spotkań online – zespoły Security Operations Center powinny baczniej monitorować i analizować stan bezpieczeństwa organizacji w tym aspekcie. Zresztą to także wyzwanie dla wiarygodności pracy zdalnej – co to znaczy, że nie możemy wierzyć w to, co widzimy na ekranie? Im bardziej firmy i ich pracownicy będą świadomi potencjalnych zagrożeń, jakie stwarza dziś deepfake, tym łatwiej będzie chronić się przed atakami – w przeciwnym razie mamy kłopoty.

Ataki w Polsce wciąż rosną. Firmy doświadczają ich ponad 1200 w tygodniu!

Od sierpnia rośnie liczba ataków cybernetycznych w Polsce – wynika z danych Check Point Research. Na początku ostatniego z letnich miesięcy przeciętna polska organizacja doświadczała ich w tygodniu około 620. Wraz z końcem lata ich ilość zwiększyła się o ponad 400 do 1025. Skąd wziął się tak potężny przyrost.

Wojciech **Głażewski**

dyrektor generalny, Check Point Software Technologies

Ponad połowa (53 proc.) ataków dokonywanych jest za pośrednictwem złośliwych plików dostarczanych w wiadomościach e-mail. To trend przeciwny do dominującego. W skali globalnej zaledwie 18 proc. ataków przeprowadzanych jest w ten sposób, a głównym wektorem jest sieć.

Z danych Check Pointa można odczytać, że krajem, z którego dokonywanych jest najwięcej ataków na polskie firmy, są Stany Zjednoczone (47 proc.). W czołówce znajdują się również Niemcy (9 proc.) oraz Polska (9 proc.). Mogą one jednak mylić, lokalizacje wskazywane są bowiem na podstawie adresów IP. Oznacza to, że za atakami stać mogą w głównej mierze np. rosyjscy hakerzy, podszywający się pod użytkowników z USA lub Niemiec.

Najczęściej wykrywanym zagrożeniem jest z kolei malware Formbook, mający wpływ nawet na 8,2 proc. polskich sieci. Jest to „złodziej danych", przeznaczony dla systemu operacyjnego Windows, który może zbierać dane uwierzytelniające, zrzuty ekranu, monitorować i rejestrować naciśnięcia klawiszy, a także pobierać i uruchamiać pliki zgodnie z oczewianiami atakujących. Narzędzie to dostępne jest obecnie jako Malware as a Service na podziemnych forach hakerskich.