OKIEM EKSPERTA

Zagrożenia cyberbezpieczeństwa i rozwój złośliwego oprogramowania

Poznaj strategie obrony przed współczesnymi niebezpieczeństwami

Wydanie II

Tim Rains

Helion

packt

Tytuł oryginału: Cybersecurity Threats, Malware Trends, and Strategies: Discover risk mitigation strategies for modern threats to your organization, 2nd Edition.

Tłumaczenie: Andrzej Watrak

ISBN: 978-83-289-0458-3

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
https://helion.pl/user/opinie/zagcy2
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *https://helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

Rozdział 1

Wprowadzenie

Jako doradca ds. bezpieczeństwa w Microsoft, a następnie w **Amazon Web Services** (AWS) współpracowałem z tysiącami organizacji z sektorów zarówno komercyjnego, jak też publicznego i zauważyłem, że większość z nich nie ma wypracowanych strategii cyberbezpieczeństwa, które ich dyrektorzy lub zespoły ds. bezpieczeństwa byliby w stanie wyartykułować. Tak naprawdę, gdy sięgam pamięcią do wszystkich briefingów na temat bezpieczeństwa, które przeprowadziłem, i do spotkań, które odbyłem z kadrą kierowniczą i ich zespołami w ciągu ostatnich kilku dekad, mogę wymienić najwyżej 10 organizacji z pisemnie sformułowanymi strategiami bezpieczeństwa cybernetycznego, które specjaliści **CISO** (ang. *Chief Information Security Officer*, główny specjalista ds. bezpieczeństwa informacji) mogliby opisać, a członkowie ich zespołów powtórzyć. Zamiast omawiać obszary cyberbezpieczeństwa, takie jak zarządzanie ryzykiem, tożsamością i dostępem, niemal wyłącznie doradzałem im w zakresie strategii cyberbezpieczeństwa. Nic w tym dziwnego, biorąc pod uwagę, że w różnych branżowych procedurach i procesach certyfikacyjnych istnieje wiele źródeł informacji o domenach cyberbezpieczeństwa, ale strategii zazwyczaj w nich nie ma.

Dlatego postanowiłem napisać książkę o strategiach cyberbezpieczeństwa dla specjalistów CISO, **CIO** (ang. *Chief Information Officer*, główny informatyk), **CTO** (ang. *Chief Technology Officer*, dyrektor techniczny), kandydatów na dyrektorów ds. cyberbezpieczeństwa, dla zespołów oraz specjalistów IT, którzy odgrywają odpowiedzialne role w tej dziedzinie. Pierwsze, oryginalne wydanie książki *Zagrożenia cyberbezpieczeństwa, trendy w rozwoju szkodliwego oprogramowania i strategie obrony* ukazało się w maju 2020 r. nakładem wydawnictwa Packt. Spotkało się z bardzo pozytywnym przyjęciem i nadal cieszy się dużym zainteresowaniem. Niniejsza publikacja jest drugim, zaktualizowanym wydaniem.

Dlaczego temat strategii cyberbezpieczeństwa jest tak popularny? Bezpieczeństwo cyfrowe nigdy nie było tak ważne dla firm komercyjnych i instytucji z sektora publicznego jak dzisiaj. W miarę jak świat coraz bardziej opanowuje technologia i internet, mnożą się cyberprzestępcy. Los światowych gospodarek jest wręcz uzależniony od stabilnej i niezawodnej technologii. Nie ma takiej branży ani regionu geograficznego, które byłyby odporne na cyberataki.

Oszacowano, że w 2021 r. globalna branża cyberbezpieczeństwa była warta ok. 140 miliardów dolarów. Uwzględniając skumulowany roczny wskaźnik wzrostu na poziomie od 12% do 15%, pod koniec dekady wielkość rynku branżowego będzie wynosiła ok. 375 miliardów dolarów. Jak grzyby po deszczu wyrastają producenci systemów cyberochrony, którzy wykorzystując widmo ciągle zmieniającego się krajobrazu zagrożeń,

sprzedają swoje produkty zaniepokojonym i często zdezorientowanym organizacjom we wszystkich branżach. To, co kiedyś było stosunkowo prostą ideą wykorzystania komputerów do podejmowania szybszych i z założenia lepszych decyzji biznesowych, doprowadziło do rozpowszechnienia się technologii, przepisów i standardów, które wymagają angażowania coraz większej liczby ludzi i procesów obronnych.

Na przykład Microsoft pod koniec lat 90., gdy zaczynałem w nim pracę, czerpał niewielkie, wręcz symboliczne dochody z tworzenia i sprzedawania produktów związanych z cyberbezpieczeństwem. Natomiast w 2021 r. przychody z tej działalności przekroczyły 10 miliardów dolarów (p. Jakkal, 2021 r.). W 2016 r. potrafiłem wytłumaczyć klientom dość rozbudowany i zaawansowany model zabezpieczeń firmy Microsoft, upchnięty na jednym slajdzie programu PowerPoint. W ciągu następnych 5 lat przekształciło się to w coś, co obecnie nazywa się „architekturami referencyjnymi bezpieczeństwa cybernetycznego Microsoft", które obejmują co najmniej dziewięć różnych modeli referencyjnych (Microsoft Corporation, 2021 r.).

Firma AWS, gdy w 2017 r. rozpocząłem w niej pracę, miała w swojej ofercie około 40 usług chmurowych. Gdy ją opuściłem prawie cztery i pół roku później, portfolio obejmowało ponad 300 pozycji z rosnącym udziałem usług bezpieczeństwa. Poza wprowadzaniem nowych usług, stale ulepszano istniejące i rozszerzano ich funkcjonalności. Wiele zespołów IT, które poświęciły czas na ocenę usług AWS przed ich wdrożeniem, musiałoby je oceniać co roku, aby mieć pewność, że nadal w pełni je rozumie.

Łącząc ekspansję tych dwóch firm z rozwojem innych dużych dostawców technologii IT i usług chmurowych (Oracle, IBM, Google itp.), z których usług często korzystają również przedsiębiorstwa, oraz tysięcy producentów systemów cyberbezpieczeństwa, z których każdy walczy o swoje miejsce w biznesie, otrzymujemy mnóstwo opcji, zawiłości, szumu i zamieszania.

Oczywiście, motorem napędowym tej ekspansji techniki, branży i złożoności jest nieustanne nagłaśnianie udanych ataków cybernetycznych. Dzięki nowym technologiom również hakerzy są szybsi i silniejsi niż wcześniej. Nowoczesne metody realizacji dużych międzynarodowych transakcji finansowych umożliwiły hakerom zbudowanie wyrafinowanych modeli biznesowych opartych na wymuszeniach i oprogramowaniu ransomware obsługiwanym przez ludzi.

Jeśli pominąłeś przedmowę do tej książki i analogię do łodzi podwodnej, przeczytaj ją, ponieważ oddaje presję otoczenia, której poddawane są dzisiaj wszystkie przedsiębiorstwa.

W konsekwencji tego, o czym przed chwilą powiedziałem, wiele organizacji, którym doradzałem, zadawało bardzo podstawowe pytania. *Jakie aspekty cyberbezpieczeństwa są najważniejsze? Co trzeba zrobić w pierwszej kolejności? Jak ustalić priorytety wymagań i możliwości? Jak to robią inne organizacje z naszej branży? Czy są dostępne informacje o zagrożeniach innych organizacji w danej branży? Czy istnieje algorytm określenia właściwych priorytetów?* Po odbyciu tysięcy takich rozmów i snuciu domysłów doszedłem do wniosku, że tak naprawdę wszyscy pytali mnie o strategię cyberbezpieczeństwa. Fundamentalne pytanie, które mi zadawali, brzmiało: *Która strategia cyberbezpieczeństwa lub kombinacja strategii będzie najskuteczniejsza w naszej organizacji, biorąc pod uwagę branżę i lokalizacje, w których działamy, nasze wymagania dotyczące zgodności z przepisami oraz ryzyko biznesowe?*

Tę książkę napisałem zainspirowany powyższym pytaniem. Mam nadzieję, że zawarte w niej wnioski pomogą Ci znaleźć odpowiedź w Twojej organizacji. Jak wspomniałem, książka jest przeznaczona dla specjalistów CISO, kandydatów na nich i dla ich współpracowników. Czy wiesz, że istnieją różne typy CISO? Niezależnie od tego, czy jesteś takim specjalistą, czy członkiem zespołu ds. bezpieczeństwa wspierającym CISO, sprzedawcą próbującym coś zaoferować CISO, członkiem zarządu, przed którym CISO odpowiada, znajomość typu specjalisty, z którym pracujesz, może sprawić, że komunikacja z nim będzie o wiele bardziej przewidywalna, owocna, a nawet przyjemna.

Różne typy (spektrum) CISO

Po spędzeniu mnóstwa czasu z CISO w ciągu ostatnich dwóch dekad mogę z całą odpowiedzialnością stwierdzić, że istnieje kilka typów specjalistów, różniących się podejściem do cyberbezpieczeństwa, dyktujących lub przynajmniej silnie propagujących własne programy bezpieczeństwa.

Taką listę nazywam „spektrum typów CISO". Nie jest ona wyczerpująca. Zawiera po prostu typy specjalistów, z którymi miałem do czynienia w ciągu ostatnich 20 lat mojej kariery.

- **Typ 1.: dyrektorzy IT**. Są to ludzie odpowiedzialni za cyberbezpieczeństwo, prawdopodobnie najbardziej techniczni ze wszystkich typów CISO, jakich spotkałem. Zazwyczaj mają większą wiedzę o informatyce niż o cyberbezpieczeństwie. Wiedzą wszystko o infrastrukturze IT, którą się zajmują, są godnymi zaufania kierownikami zespołów IT. Przydzielono im cyberbezpieczeństwo jako funkcję zawodową. Ich predyspozycje i chęć do nauki o bezpieczeństwie i zgodności wynikają nierzadko z instynktu samozachowawczego. Strefą komfortu są systemy IT. Chcą mieć wgląd w cyberbezpieczeństwo i wsparcie w tym zakresie.
- **Typ 2.: adresaci zgłoszeń**. Niektórzy kontrahenci, których spotkałem, stali się specjalistami CISO, ponieważ byli odpowiedzialni za reagowanie na incydenty w swoich organizacjach. Stali się ekspertami w tej dziedzinie i w usuwaniu skutków incydentów. Organizacje ufają im w sytuacjach kryzysowych i oczekują wsparcia w zapobieganiu takim przypadkom w przyszłości. Zazwyczaj są to fanatycy analiz zagrożeń, skupieni na wykorzystaniu swojej wiedzy technicznej w utrudnianiu hakerom osiągania ich celów. Posiadają głęboką wiedzę o systemach informatycznych, ponieważ na wcześniejszych etapach kariery byli zaangażowani w ich budowanie i administrowanie nimi.
- **Typ 3.: eksperci od zgodności i audytu**. Koncentrują się na procedurach kontrolnych, umożliwiających spełnianie standardów prawnych i branżowych. Mają doświadczenie w zarządzaniu programami zgodności i audytami. Posiadają głęboką wiedzę o rozbudowanych procedurach kontrolnych w dużych, skomplikowanych środowiskach IT, które muszą spełniać wiele standardów, m.in. PCI, CMMC, NIST SP 800-53, ISO 27000 itp. Wolą rozmawiać o procedurach i wyzwaniach związanych z wymogami zgodności niż o zagrożeniach i hakerach.

- **Typ 4.: fanatycy zasad**. Znam dwa typy CISO, którzy opierają się na głębokiej znajomości przepisów:
  - **Eksperci od zasad zarządzania, ryzyka i zgodności**. Zazwyczaj mają duże doświadczenie w pisaniu i egzekwowaniu powyższych zasad. Aby coś zrobić, stosują zasady w taki sam sposób, w jaki policja stosuje przepisy prawa.
  - **Eksperci od publicznych zasad cyberbezpieczeństwa**. Są to specjaliści CISO, z których większość nie jest ekspertami od informatyki ani cyberbezpieczeństwa w przedsiębiorstwach. To raczej prawnicy z dużym doświadczeniem w dziedzinie zasad publicznych i prywatności. Mają wiedzę o krajowych zasadach bezpieczeństwa cybernetycznego, tj. określonych przez administrację stanową lub federalną, chroniących obywateli oraz organizacje z sektorów prywatnego i publicznego funkcjonujących na ich terenach.
- **Typ 5.: stratedzy**. Zwykle skupiają się na dostosowaniu zasobów do procedur. Aby mogli to robić, potrzebują pewnej wiedzy na temat bezpieczeństwa cybernetycznego oraz świadomości biznesowej. Wielu z nich ma doświadczenie w co najmniej kilku różnych dziedzinach cyberbezpieczeństwa, na przykład w reagowaniu na incydenty i zarządzaniu ryzykiem. Zawsze szukają technologii i procesów, które pomogłyby im uzupełnić luki w kompetencjach i poprawić skuteczność strategii.
- **Typ 6.: eksperci od ryzyka**. Z mojego doświadczenia wynika, że ten typ specjalistów CISO występuje najrzadziej. Ich domeną jest ryzyko. Podchodzą do cyberbezpieczeństwa jak aktuariusze, ilościowo szacując ryzyko w celu określenia wielkości inwestycji w programy cyberbezpieczeństwa. Jeżeli dobrze pamiętam, tego typu CISO spotykałem niemal wyłącznie w firmach ubezpieczeniowych. Chyba wszyscy podlegali dyrektorom ds. ryzyka.
- **Typ 7.: doradcy ds. cyberbezpieczeństwa**. Specjaliści CISO, którzy uważają się za doradców firm, w których pracują. Zazwyczaj ich stanowiska nie mają nic wspólnego z tym, co robią ich firmy. Doradzają firmom, aby dokonywały inwestycji w cyberbezpieczeństwo, ale niekoniecznie sami projektują i wdrażają zasady. Zamiast nich robią to zespoły IT. Zwykle unikają konfliktów, które naturalnie wynikają z konfrontacji pożądanej w firmie swobody działalności z niezbędnymi regulacjami ochrony aktywów biznesowych. Wielu z nich uznaje, że ich rolą nie jest nadzór, lecz jedynie doradztwo.
- **Typ 8.: kompetentni dyrektorzy biznesowi**. Nie są ekspertami od bezpieczeństwa cybernetycznego, a czasami też IT. Są to menedżerowie, którzy dowiedli swoich umiejętności przywództwa biznesowego, zarządzając różnymi działami firmy lub szczególnie trudnymi i ważnymi projektami i przedsięwzięciami. Kierownictwo ufa im ze względu na ich sukcesy. Ponieważ udowodnili, że radzą sobie z trudnymi zadaniami, powierzono im zarządzanie cyberbezpieczeństwem. Kierownictwo im wierzy, że odniosą sukces, bo zna ich zdolności przywódcze i zarządcze oraz zakłada, że specjalistyczna wiedza o cyberbezpieczeństwie nie jest warunkiem sukcesu. Wielu z CISCO, których spotkałem, jest prawnikami.

Tak wygląda spektrum CISO. Odzwierciedla ono 90% z kilku tysięcy specjalistów, z którymi miałem do czynienia. Żadnego typu nie uważam za lepszy od innych. Każdy po prostu ma inne doświadczenia i podejście do cyberbezpieczeństwa. Jednak często zasady w organizacjach, w których pracują CISO, są podyktowane zewnętrznymi czynnikami, niezależnie od wiedzy i osobistych preferencji specjalistów. Wielu z tych, których spotkałem, było sfrustrowanych, ponieważ chcieli być określonym typem CISO, podczas gdy ich organizacje narzucały im inne typy, po raz kolejny udowadniając, że nawet na szczycie hierarchii biznesowej nie zawsze można dostać to, czego się chce.

Zawsze starałem się jak najszybciej określić typ specjalisty CISO, któremu doradzałem, aby rozmowa była bardziej konstruktywna dla nas obu. Jeżeli na przykład był przede wszystkim zainteresowany dyskusją o działaniu nowego eksploita, próba omówienia z nim kwestii zarządzania ryzykiem byłaby krótką i irytującą rozmową. Z tego powodu wiele zespołów sprzedażowych, które obsługiwałem w Microsoft i AWS, łączyły niekomfortowe relacje ze specjalistami CISO firm klienckich. Gdy poznali spektrum CISO, łatwiej im było zrozumieć specjalistów, zaoferować im zasoby i kontakty z osobami, które naprawdę mogły zająć się sprawami najbardziej dla nich interesującymi. W większości przypadków sprzedawcy zaskarbiali sobie zaufanie CISO, ponieważ w ich oczach chcieli im pomóc, a nie tylko dobić transakcji. Zidentyfikowawszy typ specjalisty CISO, którego wspierasz, możesz stać się jego zaufanym doradcą.

Teraz zastanówmy się, jak środowiska IT przedsiębiorstw są narażone na ataki. Ma to kluczowe znaczenie w zrozumieniu, opracowaniu i ocenie skuteczności strategii cyberbezpieczeństwa dla środowisk korporacyjnych.

Jak przedsiębiorstwa ulegają pierwszym atakom i podstawy cyberbezpieczeństwa

Fundamentem skutecznej strategii cyberbezpieczeństwa jest coś, co nazywam „podstawami cyberbezpieczeństwa". Skuteczna strategia wymaga solidnych podstaw. Podstawy cyberbezpieczeństwa to efekt dziesięcioleci analiz zagrożeń, które szczegółowo omawiam w dalszej części tej książki. Po 10 latach pracy w Microsoft i innych firmach, przeprowadzeniu setek badań procedur reagowania na incydenty oraz przeanalizowaniu informacji o zagrożeniach mogę z całą pewnością powiedzieć, że organizacje ulegają pierwszym atakom z zaledwie pięciu powodów. Po udanym pierwszym ataku hakerzy stosują różne taktyki, techniki i procedury, aby się przyczaić, wykraść poświadczenia, naruszyć infrastrukturę, zagnieździć się, uzyskać nielegalny dostęp do informacji, zniszczyć dane itp. Niektóre metody są wykorzystywane od dziesięcioleci, inne są nowsze i nowatorskie.

Pięć przyczyn, z których powodu organizacje ulegają pierwszym atakom, nazywam „typowymi sprawcami cyberzagrożeń":

1. niezałatane luki w zabezpieczeniach,
2. błędy w konfiguracji,
3. słabe, ujawnione i wykradzione poświadczenia,

4. socjotechnika,
5. wewnętrzne zagrożenia.

Podstawy cyberbezpieczeństwa są częścią strategii zwalczania typowych sprawców cyberzagrożeń. Przyjrzyjmy się szczegółowo wszystkim, począwszy od niezałatanych luk w zabezpieczeniach.

Niezałatane luki w zabezpieczeniach

Luka w zabezpieczeniach to wada oprogramowania, sprzętu lub kodu, która pozwala hakerowi zmusić system do zrobienia czegoś, czego nie powinien robić. Najpoważniejsze luki umożliwiają hakerowi przejęcie pełnej kontroli nad systemem i uruchamianie w nim dowolnego kodu. Mniejsze skutkują ujawnieniem danych w niezamierzony sposób lub blokadą usług świadczonych uprawnionym użytkownikom. W rozdziale 3., „Wykorzystanie trendów podatności w celu zmniejszenia ryzyka i kosztów", szczegółowo omawiam zarządzanie lukami oraz najważniejsze trendy w ujawnianiu luk przez ponad 20 minionych lat. Wnikliwą dyskusję zawarłem w powyższym rozdziale, natomiast tutaj nakreślę nieco szerszy kontekst.

Hakerzy wykorzystują luki w zabezpieczeniach do atakowania systemów na dużą skalę co najmniej od 2001 r., gdy pojawiły się robaki Code Red i Nimda. W 2003 r. robaki SQL Slammer i Blaster, wykorzystując niezałatane luki w systemach operacyjnych Microsoft Windows, skutecznie zakłóciły działanie internetu i naruszyły bezpieczeństwo setek tysięcy systemów na całym świecie. W efekcie w kolejnych latach rozwinął się rynek drobnych producentów oprogramowania wspomagającego korporacje (również te posiadające najbardziej złożone środowiska) w inwentaryzowaniu systemów IT, identyfikowaniu i łataniu luk oraz wdrażaniu środków zaradczych. Pod koniec 2022 r. w amerykańskiej bazie National Vulnerability Database były zarejestrowane ponad 192 tysiące luk w zabezpieczeniach oprogramowania i sprzętu z całej branży. Jak się dowiesz w jednym z następnych rozdziałów, w latach 2016 – 2017 liczba ta wzrosła o 128%, do niespotykanego wcześniej poziomu. Rosła dalej z roku na rok, a w samym tylko 2022 r. ujawniono ponad 25 tysięcy zagrożeń.

Gospodarkę napędza podaż i popyt na luki i eksploity, angażując szeroką gamę graczy, w tym producentów oprogramowania, hakerów, obrońców, firm komercyjnych, rządów itp. Liczba uczestników tej gry i ich wysokie wyrafinowanie wywiera presję zagrożenia na środowiska IT organizacji, co utrudnia obronę przed atakami. Szukanie niezałatanych luk w zabezpieczeniach to podstawowe metody działania hakerów.

Organizacje stosujące zaawansowane i dojrzałe metody zarządzania podatnościami skutecznie utrudniają hakerom przeprowadzanie ataków. Dobry program zarządzania jest podstawowym elementem i krytycznym warunkiem skutecznej strategii cyberbezpieczeństwa. Bez tego wysiłki organizacji w zakresie cyberbezpieczeństwa są skazane na niepowodzenie, niezależnie od czynionych inwestycji. Ta kwestia jest tak ważna, że należy ją dobitnie wyartykułować. Niezałatane luki w zabezpieczeniach systemów operacyjnych i podstawowych komponentach infrastruktury, na których opierają się zaawansowane funkcje cyberbezpieczeństwa, pozwalają hakerom całkowicie zniweczyć efekty inwestycji. Brak skutecznych procedur reagowania na ujawnienie luk w „zaufanej bazie obliczeniowej", na której opierają się systemy, czyni ją niewiarygodną.

Dokładna inwentaryzacja wszystkich zasobów IT ma kluczowe znaczenie w programie zarządzania lukami. Organizacje, które nie są w stanie dokładnie i terminowo inwentaryzować swoich zasobów, wyszukiwać, łatać i likwidować w nich luk, nie powinny dokonywać jakichkolwiek inwestycji w infrastrukturę, dopóki nie rozwiążą tego problemu. Jeśli Twoja firma jest w takiej sytuacji, przeczytaj ponownie „Przedmowę" do tej książki i zawartą w niej analogię do łodzi podwodnej. Jeżeli specjaliści CISO i menedżerowie programów zarządzania podatnościami zlecają inwentaryzowanie zasobów zespołowi IT swojej organizacji lub wewnętrznej jednostce, inwentaryzacje te muszą być kompletne, tj. nie mogą ograniczać się wyłącznie do chronionych systemów.

Zasoby, które nie są zinwentaryzowane, przeskanowane i załatane, stają się słabymi ogniwami tworzonego łańcucha bezpieczeństwa. Bardzo często stoi to w sprzeczności z kontrolowanymi przez organizacje celami dostępności systemów, ponieważ łatanie luk w zabezpieczeniach zwiększa liczbę niezbędnych restartów systemów, a więc zmniejsza ich dostępność, nawet jeśli wszystko przebiega sprawnie. Moja rada w sytuacjach, gdy zasoby inwentaryzuje strona zewnętrzna w programie zarządzania podatnościami, brzmi: ufaj, ale sprawdzaj. Zadawaj sobie dodatkowy trud i zdobywaj budżet na stałe sprawdzanie zgodności inwentaryzacji aktywów z rzeczywistością. Dotyczy to również oficjalnych i nieoficjalnych środowisk programistycznych i testowych, ponieważ od wielu lat są one ofiarami bardzo wielu przypadków naruszeń bezpieczeństwa. Do tej kategorii należą też niezatwierdzone zasoby IT (tzw. *shadow IT*) i nieoficjalne konta w chmurach obliczeniowych.

Jeżeli podmiot nie inwentaryzuje aktywów zgodnie z powyższymi wymogami lub nie robi tego dokładnie i terminowo, stanowi źródło ryzyka, o którym zarząd powinien być informowany. Szacunkowe dane o części zinwentaryzowanych zasobów, które nie są objęte programem zarządzania podatnościami, powinny być impulsem do zmiany priorytetów działalności podmiotów inwentaryzujących w celu zażegnania niebezpieczeństwa.

Wskazówka

W identyfikowaniu nieznanych i podejrzanych zasobów przydatne mogą się okazać rozwiązania typu **Cloud Access Security Brokers** (**CASB**) i Attack Surface Management. Obecnie większość takich narzędzi jest zorientowana na zasoby zewnętrzne (internetowe), ale oferta coraz częściej obejmuje również środowiska wewnętrzne.

Zarządzanie lukami omawiam dokładniej w rozdziale 3., „Wykorzystanie trendów podatności w celu zmniejszenia ryzyka i kosztów", oraz rozdziale 12., „Nowoczesne podejście do bezpieczeństwa i zgodności", w części poświęconej chmurom obliczeniowym i kontenerom. W chmurze tradycyjne metody inwentaryzacji, skanowania i łatania luk w zabezpieczeniach mogą się okazać nieadekwatne.

Oczywiście, opisane podejście jest problemem w organizacjach, które przyjęły politykę **BYOD** (ang. *Bring Your Own Device*, przynieś własne urządzenie), pozwalającą pracownikom uzyskiwać dostęp do danych przedsiębiorstwa i przetwarzać je za pomocą własnych urządzeń przenośnych. Podstawowe pytanie brzmi: Czy zespół ds. zarządzania podatnościami w firmie powinien inwentaryzować własne urządzenia pracowników i zarządzać nimi? Między innymi z tego powodu skrót *BYOD* dla wielu specjalistów ds. bezpieczeństwa oznacza przede wszystkim „przynieś własną katastrofę" (ang. *Bring*

Your Own Disaster). Różne organizacje zajmują różne stanowiska w tej kwestii. Niektóre zapewniają pracownikom firmowe i w pełni zarządzane urządzenia mobilne, a inne wymagają, aby urządzenia osobiste były rejestrowane w ramach programu zarządzania sprzętem. Widziałem również bardziej pasywny model, w którym użytkownicy byli zobowiązani do stosowania kodów dostępu PIN do swoich urządzeń i nie mogli się łączyć z sieciami swoich pracodawców, jeśli nie zainstalowali najnowszych wersji mobilnego systemu operacyjnego. Niektóre organizacje wykorzystują rozwiązania **NAC** (ang. *Network Access Control*, kontrola dostępu do sieci) i **NAP** (ang. *Network Access Protection*, ochrona dostępu do sieci) do egzekwowania zasad utrzymywania we właściwym stanie systemów łączących się z ich sieciami. Niektórzy dostawcy uczynili ten model zarządzania kamieniem węgielnym zasady „zero zaufania" (ang. *Zero Trust*), którą oferują swoim klientom. Zgodnie z nią nie można ufać żadnym endpointom, chyba że ich stan został zweryfikowany pod kątem zgodności z zasadami bezpieczeństwa urządzeń mobilnych w danej organizacji. Zazwyczaj oznacza to konieczność stosowania najnowszej wersji systemu operacyjnego, łatania znanych i najnowszych luk w zabezpieczeniach oraz aktualizowania sygnatur oprogramowania antywirusowego. Te wymogi sprawiają, że endpointy stają się bardziej wiarygodne, ponieważ spełniają minimalne standardy bezpieczeństwa ograniczające prawdopodobieństwo włamań i uzyskania przez hakerów dostępu do sieci korporacyjnej. Dopóki endpoint nie spełnia tych minimalnych standardów i nie ma czystej „karty zdrowia", wysyłane przez niego żądania nawiązania zewnętrznych połączeń są odrzucane.

Minimalizowanie liczby niezaktualizowanych systemów, które łączą się z siecią firmową, jest dobrą praktyką, ale jej stosowanie może być trudne, w zależności od kultury organizacyjnej i zasad dotyczących używania urządzeń mobilnych. Kto na przykład będzie czekać na zainstalowanie aktualizacji i ponowne uruchomienie systemu, gdy musi tuż przed odlotem uzyskać dostęp do dokumentu w sieci korporacyjnej? Z tego powodu wielu „obieżyświatów" unika łączenia się z siecią firmową, co prowadzi do pogorszenia, a nie poprawienia bezpieczeństwa endpointów. Dla zespołów ds. bezpieczeństwa bardzo cenne są dane, które pomagają w wypracowaniu racjonalnego podejścia do ryzyka.

Teraz zajmijmy się błędami w konfiguracji zabezpieczeń, które to błędy — podobnie jak niezałatane luki — potencjalnie umożliwiają hakerom wykonywanie szeregu operacji w systemie, zakłócanie jego działania, nielegalne pozyskiwanie informacji, łagodzenie i wyłączanie zabezpieczeń, przejmowanie kontroli i atakowanie innych systemów.

Błędy w konfiguracji

Błędami w konfiguracji zabezpieczeń mogą być ustawienia domyślne, na przykład predefiniowane klucze lub hasła, takie same we wszystkich systemach danego producenta. Oprócz tego błędy pojawiają się stopniowo, gdy w miarę upływu czasu zmienia się konfiguracja systemu. Gdy pracowałem w zespole Microsoft reagującym na incydenty bezpieczeństwa zgłaszane przez klientów, zbadałem setki procedur reagowania i mogę stwierdzić, że znaczna część systemów jest narażona na szwank z powodu błędów w konfiguracji zabezpieczeń. Dotyczy to w szczególności systemów dostępnych z internetu, takich jak serwery sieciowe, zapory sieciowe i inne rozwiązania znajdujące się w korporacyjnych strefach **DMZ** (ang. *Demilitarized Zone*, strefa zdemilitaryzowana). Gdy haker, wykorzystując błąd w konfiguracji, przejmie kontrolę nad systemem w strefie DMZ, może

zacząć wysyłać fałszywie uwierzytelnione zapytania w celu uzyskania dostępu do innych systemów znajdujących się zarówno w strefie, jak też poza zaporą, w wewnętrznej sieci. Jest to typowa praktyka, stosowana przez hakerów od ponad 20 lat.

Błędy w konfiguracji zabezpieczeń są również przypadłością takich endpointów jak komputery, smartfony i urządzenia **IoT** (ang. *Internet of Things*, internet rzeczy). Infrastruktury, z którymi się łączą te urządzenia, na przykład bezprzewodowe punkty dostępowe, również są sondowane przez hakerów pod kątem typowych błędów w konfiguracji. Błędy są także bolączką systemów **ICS** (ang. *Industrial Control System*, przemysłowy system sterowania). Jednym z przypadków, które kiedyś dały się we znaki zespołom ds. bezpieczeństwa, jest tzw. powrót do ostatniego stanu, czyli zastąpienie bieżących ustawień konfiguracyjnym starszymi, mniej bezpiecznymi. Zakodowane na stałe poświadczenia i podatne na ataki domyślne konfiguracje od dawna prześladują producentów wszelkiego rodzaju oprogramowania i sprzętu.

Dobry program zarządzania lukami w zabezpieczeniach zazwyczaj obejmuje identyfikację błędów w konfiguracji zabezpieczeń. Wiele skanerów podatności i narzędzi, które są używane do identyfikowania i łatania luk, jest również w stanie wykrywać błędy i dostarczać wskazówek, jak je naprawiać. Niektóre skanery potrafią określać, czy konfiguracje systemów spełniają standardy branżowe, na przykład testy porównawcze **CIS** (ang. *Center for Internet Security*, Centrum Bezpieczeństwa Internetowego) lub przyjęte wewnętrzne standardy bezpieczeństwa. Powtórzę: organizacje powinny zrezygnować z dużych inwestycji w zaawansowane funkcje cyberbezpieczeństwa, jeśli nie są w stanie identyfikować i poprawiać błędów w konfiguracji zabezpieczeń we własnych środowiskach. Nie ma sensu poświęcać sił i środków na tropienie zagrożeń **APT** (ang. *Advanced Persistent Threat*, zaawansowane trwałe zagrożenie) w środowiskach wykorzystujących dostępne w internecie, znane od dziesięcioleci zakodowane na stałe hasła, których hakerzy mogą użyć do skutecznego naruszenia bezpieczeństwa i uzyskania dostępu. Nawet jeżeli specjalista CISO znajdzie takiego intruza w swoim środowisku, to z powodu niezarządzanych, typowych błędów w konfiguracji zabezpieczeń nie będzie w stanie się go pozbyć. Przyczyną kilku największych włamań w historii były niezałatane luki połączone z błędami. Oba problemy można rozwiązać przez wdrożenie dobrego programu zarządzania podatnościami.

Jest to obowiązkowa część każdej strategii cyberbezpieczeństwa, która powinna być odpowiednio wspierana. Pamiętajmy, że łatwiej jest zarządzać rzeczami, które dają się mierzyć. Pełna, dokładna i regularnie przeprowadzana inwentaryzacja zasobów IT ma kluczowe znaczenie w programie zarządzania podatnościami. Ufaj, ale zawsze sprawdzaj inwentaryzację. Warto przy tym mieć na uwadze, że chmura ma kilka zalet w porównaniu z typowym, lokalnym środowiskiem IT. Ten temat omawiam szczegółowo w rozdziale 12., „Nowoczesne podejście do bezpieczeństwa i zgodności".

Błędy w konfiguracji zabezpieczeń mogą istnieć w nowym sprzęcie i oprogramowaniu lub pojawiać się z czasem. Innym zagrożeniem, wymagającym stałej uwagi, są złamane poświadczenia. Organizacje muszą nieustanie i proaktywnie pracować nad ograniczeniem tego rodzaju zagrożeń.

Słabe, ujawnione i wykradzione poświadczenia

Środowiska IT zaatakowane z powodu słabych, ujawnionych lub wykradzionych poświadczeń są wszędzie. Poświadczenia są ujawniane i wykradane różnymi kanałami. Są to m.in. socjotechnika (podszywanie się), szkodliwe oprogramowanie rejestrujące naciśnięcia klawiszy w systemach operacyjnych i przeglądarkach oraz zainfekowane systemy, które buforują, przechowują i przetwarzają poświadczenia. Czasami programiści umieszczają w publicznych serwisach do udostępniania kodu swoje projekty, zapominając o zawartych w nich poufnych informacjach, takich jak klucze i hasła. Źródłami poświadczeń dla hakerów są też stare, porzucone, ale nadal działające, niezabezpieczone środowiska programistyczne i testowe.

Przez lata w internecie odkryto ogromne listy wykradzionych i ujawnionych poświadczeń. Na domiar złego dostępność klastrów **HPC** (ang. *High-Performance Computing*, wysokowydajne przetwarzanie danych) i opartych na procesorach **GPU** (ang. *Graphics Processing Unit*, układ przetwarzania obrazu) narzędzi do łamania haseł sprawiła, że poświadczenia same w sobie przestały być skutecznym zabezpieczeniem zasobów i kont. Wykradzione lub ujawnione hasła haker potencjalnie może wykorzystać do uzyskania nieautoryzowanego dostępu do systemów, przeprowadzania ataku typu „ponowne użycie" i do eskalacji uprawnień. Hasło jako narzędzie do ochrony zasobów przedsiębiorstwa już dawno straciło swoją moc. Dlatego stosowanie uwierzytelnienia **MFA** (ang. *Multi-Factor Authentication*, uwierzytelnienie wieloskładnikowe) jest koniecznością zarówno dla przedsiębiorstw, jak i konsumentów. Ten typ uwierzytelnienia ogranicza ryzyko kradzieży i wycieku poświadczeń w wielu sytuacjach, choć nie we wszystkich. Nawet jeżeli haker zdobędzie poprawną nazwę użytkownika i hasło, to jeśli nie będzie dysponował drugim składnikiem niezbędnym do uwierzytelnienia, nie uzyska dostępu do konta. Inne czynniki, które można wykorzystać do uwierzytelnienia, to cyfrowe certyfikaty, jednorazowe hasła i kody PIN generowane w aplikacjach na przeznaczonym specjalnie do tego sprzęcie, połączenia telefoniczne z zarejestrowanymi wcześniej numerami stacjonarnymi lub komórkowymi itp.

Uwierzytelnienie MFA, choć bardzo skuteczne w wielu sytuacjach, nie jest złotym środkiem na obecność słabych, ujawnionych i wykradzionych poświadczeń. Zdarzyło się kilka udanych ataków na metody MFA. Jeden z nich polegał na podmianie karty SIM w celu przechwycenia wiadomości SMS z kodami PIN wysyłanymi do wcześniej zarejestrowanych telefonów komórkowych. Innym poważnym problemem jest to, że uwierzytelnienie MFA nie jest powszechnie stosowane w korporacyjnych środowiskach IT. Organizacje, które od dziesięcioleci korzystają ze starszych aplikacji, opartych na przestarzałych metodach uwierzytelniania i autoryzacji użytkowników, mają mniejsze szanse na wdrożenie MFA i ograniczenie ryzyka. Nawet jeżeli najnowocześniejsze systemy i usługi oparte na chmurze wymagają tego rodzaju uwierzytelnienia, z dużym prawdopodobieństwem można założyć, że więcej jest starszych aplikacji, w których wdrożenie uwierzytelnienia MFA nie jest łatwe.

W tym momencie przychodzi na myśl obraz góry lodowej. Kilku specjalistów CISO, z którymi rozmawiałem, przekonało się na własnej skórze o mankamentach uwierzytelnienia MFA podczas przeprowadzania testów penetracyjnych. Niemniej jednak metoda ta powinna być szeroko stosowana, ponieważ skutecznie ogranicza prawdopodobieństwo ataków z użyciem słabych, ujawnionych i wykradzionych haseł. Powinna być

obowiązkowa w nowych systemach, a ryzyko stwarzane przez stare systemy, bez MFA, powinno się starannie analizować i w miarę możliwości ograniczać. Istnieje kilku dostawców specjalizujących się w takich rozwiązaniach.

Gdy haker włamuje się po raz pierwszy do lokalnego środowiska korporacyjnego, wykorzystuje ujawnione lub wykradzione poświadczenia do przeprowadzenia rekonesansu i wyszukania kolejnych poświadczeń, umieszczonych w pamięci podręcznej lub zapisanych w różnych miejscach. Szczególnie pożądane są poświadczenia administratora, które dają nieograniczony dostęp do zasobów zaatakowanego środowiska. Zazwyczaj od razu po włamaniu haker usiłuje uzyskać dostęp do usługi katalogowej organizacji, na przykład Microsoft Active Directory (AD), aby pobrać wszystkie dostępne poświadczenia. Im więcej uda mu się ich wykorzystać do poruszania się po środowisku i zagnieżdżenia w nim, tym trudniej będzie się intruza pozbyć. Może nawet pozostać w środowisku na zawsze. Będzie próbował wykraść bazę danych kont użytkowników. Jeżeli uda mu się uzyskać wszystkie poświadczenia z usługi katalogowej, wówczas uzdrowienie takiego środowiska będzie naprawdę ambitnym zadaniem.

Jeżeli haker wykradnie zaszyfrowane poświadczenia, najsłabsze z nich złamie metodami offline w ciągu kilku godzin. Dłuższe, nietypowe i naprawdę skomplikowane hasła złamie na końcu. Od dziesięcioleci toczą się zażarte dyskusje o skuteczności haseł i tajnych fraz, liczbach i zestawach znaków, zasadach blokowania i wygaszania poświadczenia itp. Wytyczne dotyczące haseł przez lata ewoluowały, ponieważ zmieniały się zagrożenia i ryzyka oraz pojawiały nowe dane. Kilku moich współpracowników z zespołu Microsoft Identity Protection przeanalizowało dziesiątki milionów ataków, które przeprowadzano każdego dnia na korporacyjne i konsumenckie systemy zarządzania tożsamością, i opublikowało zalecenia dotyczące haseł. Polecam lekturę opracowania *Microsoft Password Guidance* (Hicock, 2016 r.).

Gdy poświadczenia wyciekną lub zostaną wykradzione, haker szybko je wykorzysta w skryptach z nadzieją, że uda mu się zalogować do instytucji finansowych, sklepów internetowych, serwisów społecznościowych i innych witryn.

Używanie tych samych haseł do różnych kont jest fatalną praktyką, a dla hakera takie poświadczenia są o wiele cenniejsze od innych. Najwartościowsze są poświadczenia dające dostęp do zasobów korporacyjnych, a także sieci społecznościowych, które mogą być bogatymi źródłami informacji o potencjalnych ofiarach.

Unikatowe hasła do poszczególnych kont i uwierzytelnienie MFA mogą ograniczyć to ryzyko. Jeśli kont jest zbyt dużo, aby przypisać im różne hasła, można ułatwić sobie zadanie wykorzystaniem magazynu haseł. Na rynku jest dostępnych wiele tego typu produktów przeznaczonych dla konsumentów i przedsiębiorstw.

Ochrona tożsamości jest od zawsze najtrudniejszą dziedziną cyberbezpieczeństwa. Zarządzanie tożsamością może być tematem osobnej książki. Poniższa, bardzo krótka lista zawiera zalecenia, które mogą być pomocne w ograniczaniu skutków stosowania słabych, ujawnionych lub wykradzionych poświadczeń:

- Uwierzytelnienie MFA jest bardzo skuteczne i należy je stosować wszędzie, gdzie jest to możliwe. Warto przeczytać poświęcony temu zagadnieniu artykuł na blogu Microsoft, *Your Pa$$word Doesn't Matter* („Twoje ha$ło nie ma znaczenia", Weinert, 2019 r.).

- Ważna jest wiedza, czy z organizacji wyciekły poświadczenia i jak dawno to się stało. Przeglądanie serwisów, w których hakerzy publikują i sprzedają online ujawnione i wykradzione poświadczenia, może dać nieco pewności, że coś ważnego nie umknęło uwadze. Wiedza o tym, jak długo takie poświadczenia są dostępne, pomaga w podejmowaniu decyzji o zresetowaniu haseł do kont, których ten problem może dotyczyć.
- Rozwiązania do zarządzania dostępem uprzywilejowanym potrafią wykrywać ataki typu „pass-the-hash", „pass-the-ticket" i „Golden Ticket", a także podejrzane aktywności i próby rekonesansu w infrastrukturze. Wiele takich rozwiązań oferuje również możliwość przechowywania haseł, pośrednictwo w uwierzytelnianiu i specjalistyczną analitykę. Niektóre z nich robią dużo hałasu w infrastrukturze i zgłaszają fałszywe alarmy, ale mimo to pomagają w wykrywaniu słabych, ujawnionych i wykradzionych poświadczeń i zarządzaniu nimi.
- W środowiskach chmurowych rozwiązania **IAM** (ang. *Identity and Access Management*, zarządzanie tożsamością i dostępem) oferują najskuteczniejsze metody zabezpieczeń. Wykorzystanie ich wszystkich możliwości ma kluczowe znaczenie dla ochrony zasobów w chmurze i wykrywania zagrożeń. Jest to jednak podejście, które może szybko zaprowadzić w niemożliwy do opanowania bałagan. Starannie przemyślana i zaplanowana strategia wdrożenia IAM w organizacji przynosi ogromne korzyści w zakresie bezpieczeństwa. Tożsamość omawiam nieco szerzej w rozdziale 9., „Strategie cyberbezpieczeństwa".

Ważnym aspektem programu ochrony poświadczeń jest edukowanie pracowników, aby byli świadomi ataków socjotechnicznych, w których hakerzy usiłują wykraść poufne informacje, na przykład podszywając się pod kogoś innego. Nie jest to jednak jedyny sposób wykorzystania socjotechniki do atakowania systemów. Ten temat jest dokładniej opisany w następnym punkcie.

Socjotechnika

Wśród „typowych sprawców cyberzagrożeń" prym wiedzie socjotechnika. W skrócie: obejmuje ona metody pozyskiwania zaufania użytkowników i prowokowania ich do podejmowania złych decyzji. Przykładem jest zmiana ustawień i obniżenie bezpieczeństwa systemu bez znajomości konsekwencji takiego działania lub nieświadoma instalacja szkodliwego oprogramowania w systemie. Hakerzy wykorzystują łatwowierność swoich ofiar.

Liczba ataków socjotechnicznych jest o rząd wielkości większa od liczby ataków innych typów. Na przykład wg danych Microsoft z ponad 470 miliardów wiadomości e-mail obsłużonych przez Office 365 w lipcu 2019 r. ok. 4 miliardów (0,85%) było atakami socjotechnicznymi polegającymi na podszywaniu się. Podobnie trojany, szkodliwe oprogramowanie wykorzystujące socjotechnikę, od wielu lat nieprzerwanie jest najbardziej rozpowszechnioną kategorią wirusów. Opisuję je dokładniej w rozdziale 4., „Ewolucja malware".

Biorąc pod uwagę ogromną liczbę ataków socjotechnicznych i historię ich skuteczności, przeciwdziałanie im nie może być kwestią dobrej woli organizacji. Podstawowym elementem strategii cyberbezpieczeństwa w przedsiębiorstwie jest łagodzenie skutków ataków socjotechnicznych. Innymi słowy, nieuwzględnienie socjotechniki w strategii cyberbezpieczeństwa oznacza ignorowanie największego ilościowo zagrożenia atakami.

Ataki socjotechniczne są zazwyczaj przeprowadzane przez hakerów spoza organizacji, na co użytkowników trzeba przygotować przez ich odpowiednie edukowanie i szkolenia. Innym poważnym niebezpieczeństwem, przed którym trudno jest się bronić, są ataki wewnętrzne. Jest to ostatnia kategoria zagrożeń, której poświęciłem następny punkt.

Zagrożenia wewnętrzne

Zagrożenia wewnętrzne, które omawiam ze specjalistami CISO i zespołami ds. bezpieczeństwa, dzielę na trzy kategorie, od najbardziej do najmniej prawdopodobnych:

1. Użytkownicy i administratorzy, którzy popełniają błędy lub podejmują niewłaściwe decyzje dotyczące zaufania, co skutkuje naruszeniem bezpieczeństwa.
2. „Samotne wilki" lub bardzo małe grupy osób, które wykorzystują uprzywilejowany dostęp, aby wykradać informacje lub w inny sposób naruszać ich poufność i integralność, jak również aby ograniczać dostępność technologii informatycznych i danych.
3. Spisek wtajemniczonych osób, które współpracują ze sobą, aby rozmyć podział obowiązków w zakresie kontroli bezpieczeństwa. Zauważyłem, że ta kategoria zagrożenia jest zazwyczaj podnoszona w dyskusjach na temat bezpieczeństwa środowisk operatorów i chmury.

Ograniczanie zagrożeń wewnętrznych jest ważnym aspektem cyberbezpieczeństwa i powinno być podstawą każdej strategii obejmującej całe przedsiębiorstwo. Pomocne jest jasne rozdzielenie obowiązków, przyjęcie zasady minimalnych przywilejów, automatyzacja, monitorowanie i audyt. Stałem się wielkim zwolennikiem techniki prowokacji po tym, jak zobaczyłem, jak można ją wykorzystywać do identyfikowania wewnętrznych zagrożeń. Istnieje kilka odmian tej techniki, ale główna idea polega na podstawieniu hakerowi systemu z ogólnie znanymi lukami w zabezpieczeniach i błędami w ich konfiguracji. Taki system w przypadku wykrycia szkodliwej interakcji ostrzega o obecności hakera i istnieniu wewnętrznych zagrożeń. Specjaliści ds. bezpieczeństwa nazywają czasami takie podejście „kanarkiem w kopalni węgla" przeniesionym do środowiska IT. Wdrożenie techniki prowokacji przy wtajemniczeniu jak najmniejszej liczby osób i zachowaniu poufności może pomóc w identyfikacji zagrożeń z co najmniej dwóch z trzech opisanych wyżej kategorii. Ważne jest jednak, aby zachować przejrzystość wobec odpowiednich osób w organizacji oraz zapewnić odpowiedni nadzór i widoczność.

Tak wygląda pięć przyczyn, z których powodu organizacje ulegają pierwszym atakom. Obrona przed nimi ma fundamentalne znaczenie dla trwałego zapewnienia cyberbezpieczeństwa.

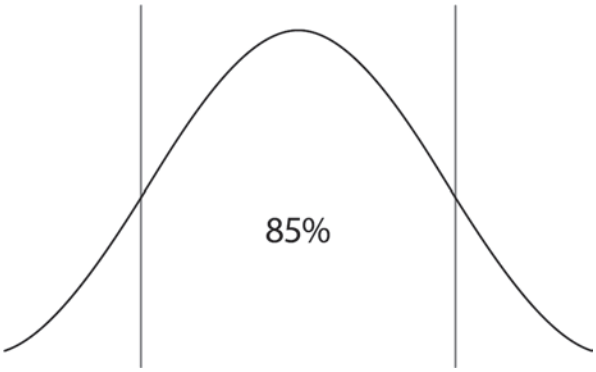
Ostrzeżenie

Ujawnienie tajnego programu identyfikacji zagrożeń wewnętrznych, nawet jeżeli jest to konieczne w celu uzyskania pomocy innych osób, jest prostą drogą do trwałego wprowadzenia atmosfery nieufności w organizacji. Powołanie komitetu sterującego programem przeciwdziałania zagrożeniom wewnętrznym, składającego się z przedstawicieli wyższego szczebla z biura CISO (OCISO), działu prawnego, działu personalnego, działu ds. oszustw i działu IT, pozwoli uniknąć późniejszych problemów lub je zminimalizować, o ile uda się zidentyfikować wewnętrznych hakerów i podjąć adekwatne działania. Komitet sterujący, który ustala statut i zakres programu oraz zatwierdza jego wytyczne, może zapobiec uprzedzeniom partnerów i umożliwić bardziej efektywne zarządzanie programem.

Koncentracja na podstawach cyberbezpieczeństwa

Aby zbudować udany program zapewnienia cyberbezpieczeństwa, trzeba skutecznie i nieprzerwanie zapobiegać wszystkim pięciu rodzajom zagrożeń. Ta umiejętność stanowi podstawę solidnej strategii cyberbezpieczeństwa. W przeciwnym razie inwestycje w nią będą przynosić coraz mniejsze korzyści.

Gdy haker wykorzysta jeden lub kilka opisanych wyżej sposobów, aby włamać się do infrastruktury organizacji, może zastosować mnóstwo nowatorskich i zaawansowanych taktyk, technik i procedur. Organizacje, które koncentrują się na podstawach cyberbezpieczeństwa, skutecznie uniemożliwiają hakerom osiąganie ich celów. Jak pokazuje rysunek 1.1, zespoły bezpieczeństwa, które koncentrują się na 85% wnętrza krzywej dzwonowej opisującej podstawy cyberbezpieczeństwa, a nie na odległych 7,5% na obu końcach, są znacznie bardziej efektywne. Niestety, urok wizji polowania na zaawansowane, trwałe zagrożenia może odciągnąć zasoby od mniej atrakcyjnej, ale krytycznej pracy wewnątrz krzywej.



Rysunek 1.1. Krzywa dzwonowa pokazująca, że zespoły ds. bezpieczeństwa powinny poświęcać większość czasu na pracę u podstaw

Jeżeli rzeczywiście jest tylko pięć przyczyn, z których powodu organizacje ulegają pierwszym atakom, dlaczego w branży panuje tak duże zamieszanie w kwestii priorytetów w programach cyberbezpieczeństwa? Moim zdaniem składa się na to kilka czynników. Jednym z nich jest sposób, w jaki czołowe media opisują ataki oraz incydenty bezpieczeństwa i naruszenia danych, czasami myląc taktykę hakerów z ich motywacjami. To z kolei prowadzi do podejmowania przez organizacje niewłaściwych decyzji dotyczących priorytetów bezpieczeństwa.

Różnice między motywacją a taktyką hakera

Jednym z powodów, dla których moim zdaniem tak wiele organizacji nie koncentruje się na podstawach cyberbezpieczeństwa, jest sposób, w jaki duże włamania były nagłaśniane w mediach w ciągu ostatniej dekady. Powszechnie mówiono, że był to „jak dotąd najbardziej zaawansowany atak" lub „akcja państwa totalitarnego". Gdyby jednak przyjrzeć się bliżej takiemu przypadkowi, okazałoby się, że poszkodowana organizacja była narażona na ataki z co najmniej jednego z typowych powodów, które opisałem wcześniej w tym rozdziale.

Są hakerzy, którzy działają otwarcie, ponieważ wiedzą, że za sprawą ich lokalizacji, przepisów prawa lub sponsora nie grożą im konsekwencje za nielegalną działalność. Kiedyś był to wyjątek od reguły, że trzeba było ukrywać swoje prawdziwe powiązania i tożsamość. Jednak w państwach totalitarnych rozmnożyły się grupy hakerskie. Agencje wywiadowcze śledzą obecnie ponad 30 takich grup, które identyfikują się z państwami totalitarnymi i twierdzą, że działają w dobrej wierze.

Powiązanie ataku z konkretną osobą lub grupą jest niezwykle trudne, ponieważ internet opiera się na protokołach opracowanych ponad 40 lat temu. Inżynierowie, którzy wymyślili te niezwykle skalowalne i wyrafinowane protokoły, nie mieli pojęcia, że w przyszłości branża warta 100 miliardów dolarów rocznie będzie zajęta wykrywaniem nowych luk w zabezpieczeniach, badaniami nad wirusami, zabezpieczeniami przed socjotechniką oraz zwalczaniem rozprzestrzeniających się wyrafinowanych organizacji przestępczych z państw totalitarnych. Pakietu protokołów TCP/IP (wersja 4), będącego fundamentem internetu, nie projektowano z myślą o wspomaganiu śledczych w identyfikowaniu sprawców cyberataków, którzy wykorzystują rozległe sieci zainfekowanych systemów rozproszonych po całym świecie. Porównywanie fragmentów kodu z dwóch próbek szkodliwego oprogramowania w celu ustalenia, czy są one dziełami tych samych osób, nie jest wiarygodnym sposobem identyfikowania hakerów, zwłaszcza gdy wiadomo, że jest to powszechnie stosowana technika. W dużych środowiskach, zhakowanych od wielu miesięcy lub lat, jednoznaczna identyfikacja „pacjenta zero", od którego rozpoczął się atak, oparta na danych pochodzących z zagrożonych systemów nie jest możliwa.

Znacznie łatwiej jest identyfikować hakerów, którzy wykorzystują nowoczesny model biznesowy ransomware. Zazwyczaj ujawniają swoją tożsamość lub przynajmniej przynależność do grup przestępczych, gdy żądają okupu od swoich ofiar. Przynależność do znanego gangu, zwłaszcza takiego z udanymi atakami na koncie, może wzbudzać strach

w ofiarach, które traktują groźby poważnie, szczególnie gdy gang jest znany z dotrzymywania obietnic zarówno tych dobrych, jak i złych.

Identyfikacja jest dość łatwa, gdy znany gang publikuje wpis na blogu w dark webie w taki sam sposób, jak to robił w przeszłości, wraz z danymi swoich ostatnich ofiar, potwierdzając w ten sposób, że ma w posiadaniu skradzione dane, i żąda okupu od ofiary. W rozdziale 4., „Ewolucja malware", analizuję niektóre przypadki ewolucji oprogramowania ransomware.

Gdy zespoły ds. bezpieczeństwa znajdują symptomy naruszenia bezpieczeństwa dokładnie odpowiadające śladom znanej grupy cyberprzestępczej, nietrudno dojść do wniosku, że jest ona zaangażowana w atak. Symptomy naruszenia bezpieczeństwa opisuję szczegółowo w rozdziale 2., „Co trzeba wiedzieć o analizie zagrożeń". Uważam jednak, że nawet jeżeli uda się zidentyfikować i ująć hakera, raczej nie uzyska się od niego informacji o prawdziwych motywacjach, ponieważ przestępcy rzadko je ujawniają. Dotyczy to szczególnie grup zorganizowanych i państw totalitarnych. W takich sytuacjach można się gubić w domysłach o jego motywacjach. Działalność instytucji rządowych i ich niezliczone pobudki omawiam w rozdziale 6., „Role instytucji rządowych w cyberbezpieczeństwie".

W przypadku ransomware można by sądzić, że motywacja jest oczywista — zysk. Jednak wyniki badań zagrożeń przeprowadzonych przez Microsoft sugerują coś innego. Podczas rosyjskiej inwazji w 2022 r. hakerzy używali „fałszywego" oprogramowania ransomware przeciwko ukraińskim instytucjom rządowym. Motywacją w tym przypadku nie była chęć osiągnięcia korzyści finansowych, tylko zniszczenie ukraińskich zasobów. Zdaniem **MSTIC** (ang. *Microsoft Threat Intelligence Community* — Społeczność Microsoft ds. Analizy Zagrożeń) szkodliwe oprogramowanie, które ma wyglądać jak ransomware, ale nie jest ukierunkowane na wymuszenie okupu, ma być destrukcyjne i zaprojektowane tak, by uszkodzić atakowane urządzenia (Microsoft Corporation, 15 stycznia 2022 r.). Najwyraźniej wirus typu wiper był zamaskowanym ransomware. Różnica polegała na tym, że nie miał za zadanie szyfrowania danych w odwracalny sposób z użyciem klucza, tylko ich zniszczenie. Nie był to pierwszy ani ostatni raz, kiedy hakerzy próbowali ukryć swoje motywacje.

Mimo wszystko wielu specjalistów ds. cyberbezpieczeństwa korzysta z tego typu danych, aby ustalić motywacje, powiązania i tożsamość hakerów. Motywacje mogą być następujące:

- **Rozgłos**: hakerzy chcą udowodnić, że są sprytniejsi od swoich ofiar i dużych, zaawansowanych technicznie firm.
- **Zysk**: jak omawiam w rozdziale 4., „Ewolucja malware", po udanych globalnych atakach w 2003 r. szkodliwe oprogramowanie zaczęło ewoluować w kierunku osiągnięcia zysku i ten trend trwa do dzisiaj.
- **Szpiegostwo gospodarcze**: na przykład grupy w Chinach kradną cenną własność intelektualną krajów zachodnich, aby zapewnić rodzimym branżom przewagę konkurencyjną i gospodarczą.
- **Szpiegostwo militarne**: motywacja tak stara jak same rządy, które chcą poznać zdolności bojowe swoich przeciwników i sojuszników.
- **Haktywizm**: różnice w poglądach politycznych lub filozoficznych różnych organizacji i instytucji.

- **Polityka zagraniczna**: rządy prowadzą wyrafinowane operacje cybernetyczne, manipulacje kulturowe, wojny informacyjne oraz rozpowszechniają fałszywe informacje, aby wywierać presję na inne państwa i manipulować nimi. Przykładem jest wpływanie na wyniki wyborów i obniżanie morale ludności cywilnej przeciwnika podczas wojny.
- **Inne**: obejrzyj dowolny film o Jamesie Bondzie, w którym główną rolę odgrywa **SPECTRE** (ang. *Special Executive for Counterintelligence, Terrorism, Revenge, and Extortion* — Specjalny Zarząd ds. Kontrwywiadu, Terroryzmu, Zemsty i Wymuszeń), a poznasz kilka kreatywnych motywacji.

Zdecydowanie uważam, że większość organizacji tak naprawdę nie zna motywacji hakerów. Jeżeli tak jest w istocie, skąd specjaliści CISO mają wiedzieć, jaka jest adekwatna reakcja? Kto powinien wspierać poszkodowaną organizację w reagowaniu na ataki: władze lokalne, wojsko, międzynarodowa koalicja?

Rozmawiałem z organizacjami, których strategie cyberbezpieczeństwa w dużej mierze opierają się na identyfikowaniu sprawców. Mając za sobą setki dochodzeń w zakresie reagowania na incydenty u klientów Microsoft i publikowanie przez prawie dekadę informacji o zagrożeniach, uważam, że sprawna identyfikacja hakera z jakąkolwiek wiarygodnością jest nazbyt ambitnym celem. Z pewnością postępy, jakie poczynili w ciągu ostatnich kilku lat analitycy zagrożeń i twórcy narzędzi cyberbezpieczeństwa, nieco zwiększyły szanse powodzenia. Zespoły ds. bezpieczeństwa, bogatsze o wiedzę o taktykach, technikach i procedurach hakerów, o katalogi śladów włamań oraz ulepszone, zautomatyzowane narzędzia do wykrywania ataków i reagowania na nie, mogą bronić się przed znanymi cyberprzestępcami znacznie skuteczniej niż kiedykolwiek wcześniej. Mimo że nowe możliwości wyglądają obiecująco i wydają się skuteczne, a hakerzy ujawniają się przez żądanie okupu i umieszczanie wpisów na blogach, ataki trwają nieprzerwanie i obecnie są chyba jeszcze bardziej dotkliwe niż wcześniej.

Na szczęście wiedza, kim są hakerzy, nie jest warunkiem koniecznym w skutecznej strategii cyberbezpieczeństwa. Wszyscy cyberprzestępcy, bez względu na to, jak są wyrafinowani i kto sponsoruje ich działalność, wykorzystują pięć opisanych wcześniej dróg włamań. Zdaniem Microsoft „cyberprzestępcy z państw totalitarnych najczęściej stosują do włamywania się do sieci ofiar te same narzędzia, co inni hakerzy" (Microsoft Corporation, październik 2011 r.). Moim zdaniem z prawdopodobieństwem 99,9% można przewidzieć taktykę hakerów, którzy będą próbowali włamać się do środowiska IT przedsiębiorstwa. Właśnie dlatego organizacje powinny inwestować w podstawy cyberbezpieczeństwa i usuwać „typowych sprawców cyberzagrożeń".

Siła napędową rozwoju dużej i dobrze prosperującej branży analizy zagrożeń jest niezaspokojona potrzeba identyfikacji sprawców, ich taktyk, technik, procedur i śladów włamań. W następnym rozdziale zagłębimy się w analizę zagrożeń. Dowiesz się, czym ona jest, jak odróżniać dobre informacje od złych oraz jak wykorzystują je zespoły ds. cyberbezpieczeństwa w przedsiębiorstwach. Przygotujesz się w ten sposób do oceny strategii cyberbezpieczeństwa zaprojektowanych w celu ograniczenia prób włamań opisanych w kolejnych rozdziałach.

Podsumowanie

Znajomość zagadnień omówionych w tym rozdziale będzie Ci potrzebna w dalszej części tej książki. W tym rozdziale przedstawiłem podstawy cyberbezpieczeństwa i typowych sprawców cyberzagrożeń. W dalszej części książki nieustannie odwołuję się do tych pojęć.

Organizacje, które biegle opanowały podstawy cyberbezpieczeństwa, skutecznie utrudniają hakerom osiąganie ich celów. Solidne fundamenty i koncentracja na podstawach są niezbędne do wypracowania skutecznej strategii.

Nie należy mylić motywacji hakera z jego taktyką. Ponieważ precyzyjna identyfikacja cyberprzestępcy jest trudna lub wręcz niemożliwa, większość organizacji nie jest w stanie określić, kto przeprowadza ataki i jakie są jego prawdziwe motywy. Niezależnie od tego, czy hakerem jest twórca szkodliwego oprogramowania, czy stoi za nim państwo totalitarne, główne przyczyny pierwszych ataków na środowiska IT są ograniczone do typowych sprawców cyberzagrożeń. Dogłębna znajomość podstaw cyberbezpieczeństwa skutecznie utrudnia ataki, niezależnie od tego, czy stoi za nimi rząd państwa totalitarnego próbujący wykraść własność intelektualną, czy szantażysta używający oprogramowania ransomware.

Przypisy

- Center for Internet Security, źródło: *https://www.cisecurity.org/cis-benchmarks*.
- R. Hicock, *Microsoft Password Guidance* („Zalecenia Microsoft dotyczące haseł"), Microsoft Corporation, 2016 r., źródło: *https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf*.
- V. Jakkal, *Microsoft surpasses $10 billion in security business revenue, more than 40 percent year-over-year growth* („Microsoft osiągnął przychód 10 miliardów dolarów z działalności związanej z bezpieczeństwem, odnotowując ponad 40-procentowy wzrost w skali roku"), Microsoft Corporation, 2021 r., źródło: *https://www.microsoft.com/security/blog/2021/01/27/microsoft-surpasses-10-billion-in-security-business-revenue-more-than-40-percent-year-over-year-growth*.
- K. Kark, T. Aguas, *The new CISO: Leading the strategic security organization* („Nowy CISO: kierowanie strategiczną organizacją bezpieczeństwa"), „Deloitte Review", nr 19, 26 lipca 2016 r., źródło: *https://www2.deloitte.com/content/dam/insights/us/articles/ciso-next-generation-strategic-security-organization/DR19_TheNewCISO.pdf*.
- Microsoft, *Destructive malware targeting Ukrainian organizations* („Destrukcyjne szkodliwe oprogramowanie wymierzone w ukraińskie organizacje"), Microsoft Corporation, 15 stycznia 2022 r., źródło: *https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations*.
- Microsoft, *Microsoft Cybersecurity Reference Architectures* („Referencyjne architektury cyberbezpieczeństwa Microsoft"), Microsoft Corporation, 2021 r., źródło: *https://docs.microsoft.com/en-us/security/cybersecurity-reference-architecture/mcra*.

- Microsoft, *Microsoft Digital Defense Report*, Microsoft Corporation, październik 2021 r., źródło: *https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi*.
- Microsoft, *Microsoft Digital Defense Report* („Raport Microsoft o obronie cyfrowej"), Microsoft Corporation, źródło: *https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022*.
- National Vulnerability Database, źródło: *https://nvd.nist.gov/vuln*.
- T. Rains, *Cybersecurity Threats, Malware Trends, and Strategies* („Zagrożenia cyberbezpieczeństwa, trendy w rozwoju szkodliwego oprogramowania i strategie obrony"), Packt Publishing, 2020 r., źródło: *https://www.packtpub.com/product/cybersecurity-threats-malwaretrends-and-strategies/9781800206014*.
- A. Weinert, *Your Pa$$word doesn't matter* („Twoje ha$ło nie ma znaczenia"), Microsoft Corporation, 9 lipca 2019 r., źródło: *https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/your-pa-word-doesn-t-matter/ba-p/731984*.

Bądź świadomy, bądź bezpieczny i nie daj się złapać w sieć cyberprzestępców!

Dowiedz się, jak się zmienia krajobraz zagrożeń cyberbezpieczeństwa. Dynamiczny cyfrowy postęp to nie tylko liczne korzyści, ale również rozwój oprogramowania służącego przestępcom. A to oznacza jedno: Twoja organizacja jest bezustannie narażona na coraz bardziej wyrafinowane ataki. Jeden błąd w strategii obrony lub w konstrukcji zabezpieczeń, jedna ludzka omyłka lub źle podjęta decyzja może oznaczać katastrofę o dalekosiężnych konsekwencjach.

Trzymasz w rękach drugie wydanie książki, którą docenili specjaliści bezpieczeństwa IT na całym świecie. Dzięki niej zrozumiesz zasady tworzenia skutecznych strategii cyberbezpieczeństwa dla swojej organizacji. Poznasz długoterminowe trendy w ujawnianiu i wykorzystywaniu luk w zabezpieczeniach, regionalne różnice w rozpowszechnieniu szkodliwego oprogramowania, leżące u ich podstaw czynniki społeczno-ekonomiczne, a także ewolucję ransomware. Zdobędziesz także cenne informacje na temat zagrożeń, których źródłami są rządy państw, i zapoznasz się z dogłębną analizą nowoczesnych strategii cyberbezpieczeństwa w chmurze. Dzięki tej wciągającej lekturze dowiesz się, jak wygląda dobra analiza cyberzagrożeń i jak oceniać skuteczność strategii cyberbezpieczeństwa w organizacji.

W książce:

- krytyczne aspekty skuteczności strategii cyberbezpieczeństwa w organizacji
- zarządzanie lukami w zabezpieczeniach
- ochrona przed zagrożeniami internetowymi
- ograniczanie dostępu do danych instytucjom rządowym
- zalety i wady popularnych strategii cyberbezpieczeństwa
- wdrażanie i ocena skuteczności strategii cyberbezpieczeństwa

Tim Rains specjalizuje się w programowaniu w języku C#. Pracuje w Microsofcie, tworzy rozwiązania dla Microsoft Azure. Zdał ponad 80 egzaminów Microsoftu. Zajmuje się też dydaktyką: prowadzi szkolenia wprowadzające do usług Digital Experience Platform, wiodącego systemu CMS. Warto wspomnieć, że jego zespół przygotowywał pierwsze kursy języka C#, i to jeszcze w momencie, gdy ten był we wczesnej fazie alfa.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-289-0458-3
9 788328 904583
Cena: 109,00 zł
<packt>