O'REILLY®

Zarządzanie powierzchnią ataku w cyberbezpieczeństwie

Strategie i techniki ochrony zasobów cyfrowych

Ron Eddings
MJ Kaufmann

Helion

Tytuł oryginału: Attack Surface Management:
Strategies and Techniques for Safeguarding Your Digital Assets

Tłumaczenie: Piotr Pilch

ISBN: 978-83-289-3269-2

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
helion.pl/user/opinie/zapoat
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: *helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

ROZDZIAŁ 1.

Podstawy: przegląd zarządzania powierzchnią ataku

Zarządzanie powierzchnią ataku to nie tylko modne hasło z dziedziny cyberbezpieczeństwa, które pozwoli Ci zabłysnąć na spotkaniu. Uznane firmy branżowe zajmujące się analizą, takie jak Gartner, od 2022 roku uznają ASM za cenne narzędzie służące do zarządzania pojawiającymi się zagrożeniami i powierzchnią ataku w organizacji. Rząd Stanów Zjednoczonych (*https://www.whitehouse.gov/wp-content/uploads/2024/02/M-24-09-Guidance-on-Compliance-with-the-Congressional-Review-Act.pdf*), agencja National Institute of Standards and Technology (NIST; *https://www.nist.gov/*) oraz inne organy regulacyjne (*https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act*) coraz częściej podkreślają znaczenie ograniczania ryzyka i minimalizacji powierzchni ataku. ASM ma na celu dostarczenie praktycznych informacji, które pozwalają łatwiej identyfikować słabe punkty i zagrożenia związane z cyfrowym profilem Twojej firmy. Celem zarządzania ASM jest proaktywne identyfikowanie zagrożeń i łagodzenie podatności, zanim staną się one punktami wejścia dla atakujących. Realizacja tego zadania w wielu środowiskach jest złożona, kluczowa i wymagająca. Z tego powodu zarządzanie ASM stało się strategicznym zadaniem dla zespołów ds. bezpieczeństwa w firmach niezależnie od ich wielkości.

Zarządzanie powierzchnią ataku: co to jest i dlaczego jest ważne?

ASM odgrywa kluczową rolę w efektywnym zarządzaniu działaniami z zakresu cyberbezpieczeństwa, zmniejszaniu ryzyka, poprawie poziomu zgodności oraz proaktywnym wzmacnianiu stanu zabezpieczeń organizacji w celu zapewnienia ciągłości działań biznesowych i budowania odporności cybernetycznej. Podejście to obejmuje kilka aspektów mających na celu ułatwienie określenia, gdzie mogą wystąpić ataki i jaki mogą mieć wpływ. Odbywa się to drogą identyfikacji, klasyfikacji, ustalania priorytetów i zabezpieczania wszystkich potencjalnych podatności w ekosystemie organizacji. Wszystko to określa się mianem *powierzchni ataku organizacji*.

Choć wiele firm stosuje już standardowe metodologie oceny ryzyka, firmy mogą uzupełnić je o ASM. ASM uzupełnia i rozszerza te metodologie, zapewniając ukierunkowane i ciągłe podejście do procesu identyfikacji i łagodzenia potencjalnych luk w zabezpieczeniach w cyfrowych i fizycznych obszarach firmy. W przeciwieństwie do przeprowadzanych okresowo tradycyjnych ocen ryzyka ASM oferuje dynamiczną ocenę zagrożeń w czasie rzeczywistym w miarę ich ewolucji, ściśle dopasowując się do faz procesu Risk Management Framework zdefiniowanego przez agencję NIST.

Na przykład podczas fazy kategoryzacji ASM pomaga w klasyfikacji zasobów na podstawie poziomu ich ekspozycji, co przekłada się na dokładniejsze określenie ryzyka. W przypadku faz wdrażania i oceny możliwości ciągłego monitorowania w ramach ASM sprawiają, że wybrane środki kontroli zabezpieczeń są wdrażane i skuteczne względem bieżących zagrożeń.

Dzięki integracji ASM z procesem obsługi ryzyka, takim jak zdefiniowany przez agencję NIST, organizacje mogą wyjść poza sztywne oceny i bardziej elastycznie dostosowywać stan swoich zabezpieczeń, aby móc proaktywnie reagować na znane zagrożenia i takie, które dopiero co się pojawiły.

Później omówimy każdy element tego procesu i przypadki użycia, ale najpierw wyjaśnijmy dokładnie, co rozumiemy przez powierzchnię ataku.

Co rozumiemy przez powierzchnię ataku?

Powierzchnia ataku (ang. *attack surface*) to kompleksowe pojęcie opisujące wszystkie bez wyjątku punkty w organizacji, za pośrednictwem których nieuprawniony użytkownik lub atakujący może uzyskać dostęp, wyodrębnić dane ze środowiska lub przejąć zasoby do niecnych celów. Celowo rozróżniamy *użytkownika* i *atakującego*, ponieważ istnieje między nimi istotna różnica. Ataki często są kojarzone z zewnętrznymi podmiotami (przeważnie są to osoby ze złymi zamiarami lub przestępcy), ale niezamierzone ataki mogą być również przeprowadzane przez użytkowników wewnątrz Twojej firmy. Powierzchnia ataku obejmuje fizyczny sprzęt i systemy oprogramowania, takie jak serwery, sieci, aplikacje i zautomatyzowane procesy. Uwzględnia ona także elementy ludzkie, czyli osoby wchodzące w interakcję z tymi systemami, procesy biznesowe, poprzez które systemy są obsługiwane, a także środowisko i elementy zabezpieczeń fizycznych. Odwołując się do wszystkich potencjalnych punktów wejścia do technologii stosowanej w ekosystemie organizacji, standardowo używa się terminu *powierzchnia ataku organizacji* (ang. *organizational attack surface*).

Gdy mowa jest o powierzchniach ataku, łatwo skupić się tylko na głównych elementach infrastruktury informatycznej, takich jak serwery i punkty końcowe. Ważne jest jednak zrozumienie, że ogólna powierzchnia ataku ekosystemu informatycznego jest znacznie szersza. Publiczne i prywatne interfejsy sieciowe służą jako bramy wymiany danych i mogą być potencjalnymi punktami wejścia dla nieautoryzowanego dostępu. Luki w oprogramowaniu, których nie usunięto, zapewniają cyberprzestępcom możliwość wykorzystania przestarzałych systemów. Narażone na atak bazy danych zawierające poufne informacje mogą być celem włamań do danych. Usługi chmurowe i aplikacje internetowe zdecydowanie zbyt często nie są właściwie zarządzane i zabezpieczane i dodatkowo zwiększają powierzchnię ataku organizacji.

Złożoność powierzchni ataku zwiększa się, gdy pod uwagę weźmie się takie czynniki jak praca zdalna, zasady związane z podejściem „przynieś własne urządzenie", IoT (*Internet of Things*) oraz łańcuch dostaw. Obecnie nasze modele informatyczne przesunęły się w kierunku efemerycznej infrastruktury wirtualnej i zasobów, w przypadku których pracownicy mogą uzyskiwać dostęp do zasobów firmy z dowolnego miejsca, zamiast z serwerowni lub fizycznych komputerów w biurze zarządzanych bezpośrednio przez zespół informatyków. Oznacza to, że prawie każde urządzenie używane przez pracowników, zarówno prywatne, jak i służbowe, może być połączone z siecią firmową z dowolnego miejsca na świecie. Każda z tych zmiennych zwiększa liczbę potencjalnych punktów wejścia do ekosystemu organizacji (jak wcześniej wspomniano, całościowo postrzeganego jako powierzchnia ataku organizacji). Im większa lub bardziej złożona jest całkowita powierzchnia ataku w organizacji, tym więcej możliwości mają przestępcy do wykorzystania luk i naruszenia zabezpieczeń firmy.

Zarządzanie zawiłościami powierzchni ataku organizacji jest wyzwaniem nawet wtedy, gdy infrastruktura firmy jest niezmienna. Jednakże celem większości firm, nawet tych małych i średnich, jest rozwój, a nowoczesne firmy nieustannie się zmieniają. Istnieje wiele czynników wewnętrznych powodujących zmiany w ekosystemie informatycznym. Czynniki, które mogą wydawać się niezwiązane z powierzchnią ataku, takie jak wdrażanie nowego oprogramowania, dług techniczny lub zatrudnianie nowego pracownika, w rzeczywistości mają na nią wpływ. Inne, mniej powszechne czynniki wewnętrzne, mogą obejmować dodawanie nowego sprzętu, zmianę zasad bezpieczeństwa lub dostosowywanie uprawnień dostępu pracowników.

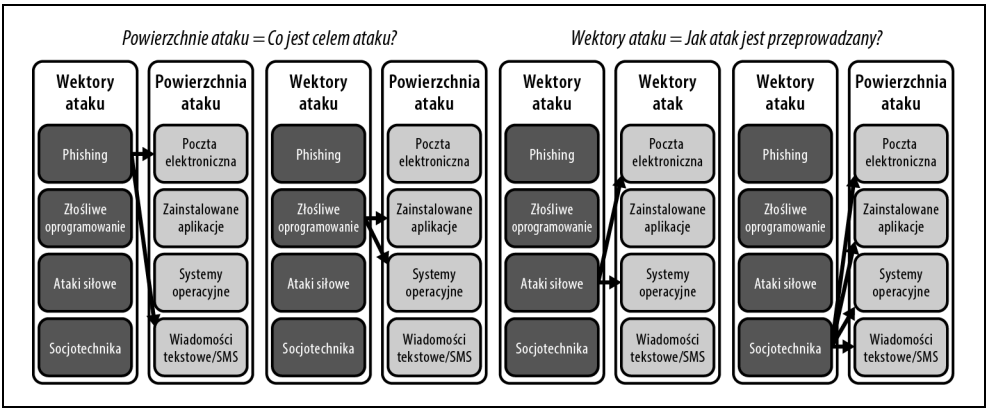
Na powierzchnię ataku organizacji mają wpływ zewnętrzne czynniki (np. obszerniejsze środowisko technologiczne), począwszy od sposobu, w jaki epidemia COVID przyspieszyła migrację do technologii chmury, a skończywszy na ewoluujących cyberzagrożeniach, takich jak pojawienie się modelu RaaS (*Ransomware-as-a-Service*). W przeciwieństwie do czynników wewnętrznych te zewnętrzne są poza kontrolą firmy. Najbardziej znanym czynnikiem zewnętrznym są cyberprzestępcy stale odkrywający luki w istniejących aplikacjach lub opracowujący nowe techniki i narzędzia do omijania środków kontroli zabezpieczeń.

Prowadzi to nas do koncepcji *wektorów ataku* (ang. *attack vectors*). Wektory ataku umożliwiają hakerom wykorzystywanie luk w systemie, a podobnie jak w przypadku powierzchni ataku, obejmuje to także czynnik ludzki.

Porównanie wektorów ataku z powierzchniami ataku

Planując i przeprowadzając atak na system, atakujący musi zidentyfikować słabości, które może wykorzystać, oraz metody umożliwiające to. Zestaw słabych punktów nazywamy powierzchniami ataku, a metody to wektory ataku. Wektory te odnoszą się do wszystkich narzędzi, taktyk i technik używanych do wykorzystania powierzchni ataku. Powierzchnie ataku to cele lub miejsca, w których osoby ze złymi zamiarami mogą zastosować wektory ataku. Być może słyszałeś, jak ludzie używają tych terminów zamiennie, ale nie są one synonimami. Są ze sobą powiązane, ale różne.

Wyobraź sobie wektor ataku jako łuk i strzałę, natomiast powierzchnia ataku jest środkiem tarczy. Koncepcja ta została zilustrowana na rysunku 1.1. Widoczny jest na nim zestaw różnych wektorów ataku i powiązanych z nimi powierzchni ataku. Ważne jest jednak, aby zauważyć, że nie uwzględniają one wszystkiego. Firmy mogą je podzielić inaczej (na przykład dzieląc złośliwe oprogramowanie na mniejsze wektory, takie jak oprogramowanie *ransomware*, oprogramowanie szpiegujące itp.). Bardzo rzadko jeden wektor ataku obejmuje każdą powierzchnię ataku. Jednakże te powierzchnie, które są bardziej narażone, częściej mogą być celem ataku.



Rysunek 1.1. Przykłady powierzchni ataku i odpowiadające im wektory ataku

Wektory ataku obejmują szerokie spektrum typów ataków, począwszy od zmyślnych ataków socjotechnicznych, a skończywszy na zaawansowanych *exploitach* technicznych. Popularność i zastosowanie poszczególnych wektorów zależą od powierzchni ataku i preferencji atakującego. Wektory ataku mogą się zmieniać wraz z odkrywaniem nowych luk w zabezpieczeniach, pozwalając cyberprzestępcom wykorzystywać je i zmuszając zespoły ds. bezpieczeństwa do szybkiego eliminowania luk. Wraz z rozszerzaniem się powierzchni ataku organizacji liczba potencjalnych wektorów ataku rośnie wykładniczo. Z kolei ograniczenie powierzchni ataku przez minimalizację punktów podatności redukuje liczbę możliwych wektorów ataku.

Może to wydać się wyjątkowo abstrakcyjne, ale konsekwencje są bardzo realne. Aby lepiej zobrazować relację między powierzchniami ataku a wektorami ataku, przedstawiamy poniżej kilka przykładów wektorów. W każdym z nich opisujemy rzeczywiste naruszenia zabezpieczeń, które wynikły z udanego użycia poszczególnych typów wektora, a także powierzchni ataku.

Atak socjotechniczny

Ataki te polegają na takim manipulowaniu ludźmi, by skłonić ich do ujawnienia poufnych informacji lub uzyskania nieautoryzowanego dostępu do systemów. Często wykorzystują one zwodnicze metody komunikacji, takie jak phishing lub podszywanie się:

- Przykład: w trzecim kwartale 2023 roku zaobserwowano wzrost ataków socjotechnicznych, w przypadku których grupa K2A243 (Scattered Spider) wykorzystywała zaawansowane oszustwa phishingowe bazujące na wiadomościach e-mail, w tym ataki za pośrednictwem usługi Microsoft Teams z użyciem złośliwego oprogramowania DarkGate.

Główną wykorzystywaną powierzchnią ataku byli pracownicy z dostępem do systemów. Dodatkową powierzchnią była poczta elektroniczna. Za pomocą socjotechniki pracownicy byli nakłaniani, by ujawnili swoje dane uwierzytelniające w wiadomości SMS.

Komponent poczty elektronicznej służył do dostarczania wiadomości przekonujących do instalacji narzędzi i złośliwego oprogramowania. Bez skutecznej obrony nic nie powstrzymywało atakujących przed przeniknięciem. Powodzenie tego złożonego ataku zależało od każdego z elementów.

Tego typu ataki przyczyniły się do wzrostu wykazanej liczby ataków socjotechnicznych i zwiększenia liczby ataków BEC (*Business Email Compromise*) związanych z firmowymi wiadomościami e-mail. W ich przypadku cyberprzestępcy nakłaniali pracowników do przelewu pieniędzy lub udostępnienia poufnych informacji.

- Wektor ataku: wiadomości e-mail i wiadomości tekstowe.
- Główna powierzchnia ataku: pracownicy.
- Dodatkowa powierzchnia ataku: systemy poczty elektronicznej, usługa Teams, telefony (za pośrednictwem wiadomości SMS).

Ataki z użyciem exploitów oprogramowania

Są to ataki wykorzystujące słabości lub luki w oprogramowaniu albo sprzęcie w celu uzyskania nieautoryzowanego dostępu lub spowodowania zakłóceń. Często wiążą się one z zastosowaniem zaawansowanych technik hakerskich:

- Przykład: przeprowadzony w grudniu 2021 roku atak z użyciem oprogramowania *ransomware* wykorzystał lukę w produkcie firmy Kaseya, co miało wpływ na ponad 1000 firm na całym świecie. Cyberprzestępcy zorganizowani w ramach grupy REvil zażądali 70 milionów dolarów za odszyfrowanie danych.

  W tym przypadku główną powierzchnią ataku były luki w oprogramowaniu firmy Kaseya, które zostały wykorzystane przez tę grupę. Stały się one punktem wejścia do wprowadzenia do systemu oprogramowania *ransomware*. Bez tej luki wiele systemów, które padły ofiarą atakujących, byłoby dla nich niedostępnych.

  Serwery, które samoczynnie uruchamiały aktualizacje oprogramowania firmy Kaseya, skonfigurowane tak, by automatycznie ufać dostawcy, stanowiły dodatkowy element powierzchni ataku. Zainfekowane oprogramowanie nie mogłoby zostać na nich zainstalowane bez zaufania, które umożliwiło przeprowadzenie ataku.

- Wektor ataku: zmodyfikowane oprogramowanie.
- Główna powierzchnia ataku: oprogramowanie firmy Kaseya.
- Dodatkowa powierzchnia ataku: serwery z oprogramowaniem firmy Kaseya.

Ataki z użyciem złośliwego oprogramowania

Ataki z wykorzystaniem złośliwego oprogramowania polegają na instalowaniu w systemie ofiary bez jej wiedzy szkodliwego oprogramowania, takiego jak wirusy, „robaki" (ang. *worms*), konie trojańskie i oprogramowanie *ransomware*. Może to prowadzić do kradzieży danych, uszkodzenia systemu lub nieautoryzowanego dostępu do sieci:

- Przykład: Uniwersytet Kalifornijski w San Francisco w listopadzie 2021 roku padł ofiarą ataku z użyciem złośliwego oprogramowania. Grupa Conti dysponująca oprogramowaniem *ransomware* wykorzystała phishingową wiadomość e-mail do zainstalowania złośliwego oprogramowania, co doprowadziło do kradzieży danych i zaszyfrowania plików, a następnie żądania okupu w wysokości 1,14 miliona dolarów.

  Grupa ta posłużyła się systemem poczty elektronicznej jako główną powierzchnią ataku, wysyłając za jego pośrednictwem zainfekowane wiadomości e-mail. Umożliwiło to dostarczenie złośliwego oprogramowania do urządzeń pracowników. Otworzyli oni te wiadomości, ponieważ nie wdrożono żadnego oprogramowania filtrującego, które mogłoby wykryć szkodliwe pliki. W rezultacie grupa Conti była w stanie uruchomić ładunek danych i zainfekować urządzenia w firmie. Ponieważ nie miały one wystarczających środków do powstrzymania złośliwego oprogramowania, ich podatność została wykorzystana, co uczyniło je dodatkową częścią powierzchni ataku.

- Wektor ataku: wiadomości e-mail.
- Główna powierzchnia ataku: pracownicy.
- Dodatkowa powierzchnia ataku: systemy poczty elektronicznej i urządzenia użytkowników.

Ataki typu „man in the middle"

W przypadku ataków typu *man in the middle* (MitM) osoba ze złymi zamiarami potajemnie przechwytuje i ewentualnie ingeruje w komunikację między dwiema stronami, które sądzą, że komunikują się bezpośrednio ze sobą. Może to prowadzić do kradzieży danych lub ich manipulacji:

- Przykład: w kwietniu 2018 roku holenderskie władze złapały czterech rosyjskich oficerów wywiadu GRU z zespołu zajmującego się hakerstwem cybernetycznym, którzy próbowali przeprowadzić operację z atakiem MitM, którego celem była sieć WiFi Organizacji ds. Zakazu Broni Chemicznej.

  Powierzchnią ataku była infrastruktura sieciowa tej organizacji, która umożliwiała atakującym przejęcie sieci i przechwycenie jej ruchu. Infrastruktura nie posiadała odpowiednich środków kontroli do wykrywania fałszywego punktu dostępu, który mógłby przechwytywać ruch sieciowy użytkowników.

- Wektor ataku: sieć WiFi.
- Główna płaszczyzna ataku: infrastruktura sieciowa.

Zagrożenia wewnętrzne

Zagrożenia te występują, gdy ktoś wewnątrz firmy (na przykład pracownik lub kontrahent) nadużywa przyznanego mu dostępu, aby celowo lub nieumyślnie naruszyć jej zabezpieczenia:

- Przykład: w kwietniu 2023 roku agencja FBI aresztowała członka Gwardii Narodowej Sił Powietrznych w stanie Massachusetts odpowiedzialnego za ściśle tajne i poufne dokumenty, które wyciekły do internetu.

  Osoba ta wykorzystała zbyt liberalne prawa dostępu do kradzieży danych. Nieprzestrzeganie zasady najmniejszych uprawnień w połączeniu z niezdolnością do odpowiedniego wykrywania podejrzanych wzorców dostępu do danych umożliwiło ujawnienie danych poufnych.

- Wektor ataku: nadużycie praw dostępu.
- Główna płaszczyzna ataku: uprawnienia dostępu.
- Dodatkowa płaszczyzna ataku: systemy magazynowania danych.

Choć nie jest to pełna lista wektorów ataku, te przykłady głośnych naruszeń nakreślają szeroki zakres unikatowych zagrożeń dla bezpieczeństwa organizacji i pokazują potrzebę stosowania różnorodnych strategii zapobiegania im i łagodzenia ich skutków. Kluczowym aspektem godnym uwagi jest tutaj to, że pojedynczy wektor ataku może mieć zastosowanie do wielu płaszczyzn ataku. Płaszczyzny i wektory ataku rzadko tworzą relację jeden do jednego. Często jest to relacja wiele do wielu.

Warto zwrócić uwagę na zmienną naturę wektorów ataku. Nieustannie ewoluują one w miarę jak przestępcy znajdują nowe sposoby na obejście metod obrony wdrożonych w organizacji. Mając to na uwadze, niezbędna jest nieustanna czujność. Nie ma cudownego rozwiązania, nie ma metody obrony, która byłaby w stu procentach niezawodna. Bez względu na to, jak innowacyjne są nasze środki bezpieczeństwa, cyberprzestępcy znajdą sposoby na ich obejście. Z tego właśnie powodu trzeba być przygotowanym na pojawiające się zagrożenia i ataki typu *zero-day*.

Nie oznacza to, że złoczyńcy nie będą korzystać ze sprawdzonych metod wykorzystywania znanych od dawna luk w zabezpieczeniach. Tak naprawdę od tego zwykle zaczynają. Na tym jednak nie poprzestają. Gdy zawodzą ogólnie znane *exploity* i ataki niewymagające dużego nakładu działań, cyberprzestępcy podwajają swoje wysiłki, szukając nowych i pomysłowych sposobów na uporanie się z metodami obrony. W pewnym stopniu właśnie ten fakt sprawia, że zarządzanie powierzchnią ataku jest trudne i kluczowe w przypadku każdej rozwijającej się organizacji.

Czym jest zarządzanie powierzchnią ataku?

Gdy już lepiej rozumiemy powierzchnie ataku i wektory ataku, przyjrzyjmy się dokładniej, czym jest zarządzanie powierzchnią ataku (ASM) i dlaczego jest to ważne. ASM to zrozumienie i analizowanie powierzchni ataku oraz nadzorowanie nimi. Obejmuje ono identyfikację, ocenę i łagodzenie luk w zabezpieczeniach w całym cyfrowym profilu organizacji.

Dlaczego zatem jest to istotne dla Twojej firmy? ASM pomaga zrozumieć całą organizacyjną powierzchnię ataku i prawidłowo ustalić priorytety ochrony, co pozwala uzyskać opłacalne rezultaty inwestycji w cyberbezpieczeństwo. Powszechnie wiadomo, że nie można zapobiec każdemu atakowi. Ponadto zespoły ds. cyberbezpieczeństwa działają przy ograniczonych zasobach, co oznacza, że w przypadku cyberataków można albo ustawiczne „gasić coraz to nowe pożary", albo zastosować strategiczne i uporządkowane podejście do kwestii radzenia sobie z zagrożeniami i lukami oraz zmniejszania ryzyka. I tu właśnie wkracza ASM.

Strategiczny charakter ASM uwzględnia stale zmieniający się „krajobraz" zagrożeń oraz mniej dynamiczną powierzchnię ataku organizacji, która, choć przeważnie okresowo jest statyczna, zmienia się, aby nadążyć za nowymi technologiami i zmieniającymi się procesami biznesowymi. Obejmując te aspekty obecności firmy w obszarze cyfrowym, ASM oferuje całościowe

podejście do obrony przed szerokim spektrum cyberzagrożeń. Dzięki monitorowaniu i adaptacji ciągłe zarządzanie powierzchnią ataku powoduje, że w miarę identyfikacji luk w zabezpieczeniach zostaną one oceniane pod kątem ich potencjalnego wpływu. Po dokonaniu oceny luk możliwe staje się albo ich wyeliminowanie, albo skuteczne złagodzenie ich wpływu w celu całościowego poprawienia jakości obrony przed cyberzagrożeniami.

Powierzchnia ataku współczesnych firm przeszła znaczące zmiany w ostatnich latach. Wiele globalnych czynników zapoczątkowało przejście od ściśle tradycyjnych ról biurowych do kombinacji tradycyjnych, zdalnych i hybrydowych modeli pracy, a także przyspieszyło adaptowanie technologii chmury. To z kolei wyeliminowało zależność od niegdyś zaufanych granic korporacji, w przypadku których większość zabezpieczeń była zapewniana przez sieci wewnętrzne. Pracownicy mają obecnie dostęp z różnych lokalizacji geograficznych do zasobów korporacyjnych, zarówno lokalnie, jak i w chmurze, korzystając z sieci publicznych i prywatnych, a czasami nawet używając osobistych urządzeń. Wszystko to sprawia, że tradycyjne metody obrony, takie jak zapory sieciowe i listy kontroli dostępu, są mniej skuteczne.

W przypadku pracy zdalnej firmy mogą gwarantować bezpieczeństwo niektórych urządzeń przez wymuszanie aktualizacji i zasad bezpieczeństwa. Nie mogą jednak rozszerzyć poziomu kontroli na ogromną liczbę sieci, z których korzystają pracownicy, takich jak sieci domowe, a także zlokalizowane w kawiarniach, bibliotekach lub hotelach. To rozszerzenie potencjalnej powierzchni ataku wymusiło połączenie starych i nowych strategii bezpieczeństwa, skupiających się na zmniejszaniu ryzyka związanego z połączeniami zewnętrznymi. Wirtualne sieci prywatne (VPN) od dawna są standardem zapewniającym bezpieczne połączenia między klientem a biurem. Firmy musiały rozszerzyć to rozwiązanie o monitorowanie dostępu, wykrywanie zagrożeń i bardziej rygorystyczne środki kontroli dostępu, aby uwzględnić zagrożenia, w przypadku których urządzenie lub dane uwierzytelniające użytkownika padły ofiarą włamania.

Nastąpił również znaczący wzrost wykorzystania platform do współpracy i komunikacji, takich jak Slack, Microsoft Teams i Zoom, które ułatwiają pracę w skali globalnej. Platformy te stały się niezbędnymi narzędziami do usprawnienia efektywnej komunikacji i współpracy w różnych obszarach geograficznych i strefach czasowych.

Wraz z zależnością od tych platform pojawiają się jednak nieodłączne zagrożenia i rozszerzona powierzchnia ataku, szczególnie w odniesieniu do udostępniania i przechowywania informacji. Choć platformy zwiększają produktywność i poziom łączności, mogą być również potencjalnymi celami włamań do danych, nieautoryzowanego dostępu i wycieków informacji, zwłaszcza gdy udostępniane są poufne lub zastrzeżone informacje. Możliwość szybkiej współpracy i udostępniania danych pozwala także na natychmiastowe rozprzestrzenianie się niebezpiecznych treści, w tym plików zainfekowanych ukrytymi zagrożeniami, takimi jak oprogramowanie *ransomware*, narzędzie *rootkit* lub złośliwe oprogramowanie.

Wraz z wyzwaniami związanymi ze zdalnymi dostępem i współpracą firmy dokonały przejścia z tradycyjnych, lokalnych środowisk informatycznych na usługi i narzędzia oparte na technologii chmury, co stanowi znaczącą zmianę w sposobie zarządzania danymi i operacjami. Zostało to spowodowane potrzebą lepszego dostępu dla pracowników z różnych krajów, koniecznością przyspieszenia cykli projektowych oraz zaletami skalowalnych i opłacalnych operacji.

Usługi oparte na chmurze oferują niezrównaną elastyczność i efektywność, pozwalając firmom na szybkie skalowanie w górę lub w dół w zależności od potrzeb. Adaptowanie technologii chmurowych niesie jednak ze sobą unikatowe wyzwania, zwłaszcza w zakresie bezpieczeństwa.

Jedną z głównych związanych z bezpieczeństwem konsekwencji powszechnego adaptowania technologii chmury jest przejście do modeli wspólnej odpowiedzialności. W tych modelach dostawca usług chmurowych i firma klienta są odpowiedzialni za różne aspekty bezpieczeństwa. Wiele firm nie było jednak w pełni przygotowanych na tę zmianę i odkryło, że ich istniejące narzędzia i technologie nie zawsze były zgodne ze środowiskami chmurowymi lub tak skuteczne w zabezpieczaniu tych środowisk. Dodatkowo sytuację tę pogłębiało przechodzenie na nowsze technologie, takie jak konteneryzacja, w ramach których tradycyjne zespoły informatyków ds. bezpieczeństwa borykają się z trudnościami z powodu braku szkoleń lub przygotowania. Powoduje to zwiększanie powierzchni ataku i powstawanie poważnych luk w zabezpieczeniach. Ten brak przygotowania może prowadzić do podatności w zakresie ochrony danych poufnych.

Ponadto sytuację komplikują środowiska chmurowe obsługujące wielu użytkowników, w których korzystają oni ze wspólnych zasobów, tak jak ma to miejsce w wielu środowiskach SaaS (*Software-as-a-Service*). Ryzyko jest tutaj dwojakie. Po pierwsze, dane poufne mogą potencjalnie zostać ujawnione innym użytkownikom lub samemu dostawcy usług chmurowych, a po drugie, w przypadku włamania po stronie dostawcy może dojść do ujawnienia danych firmy. Zrozumienie, jakie dane są przechowywane w tych miejscach, stanowi kluczowy element zarządzania powierzchnią ataku w chmurze.

Szczególną uwagę należy zwrócić na grupę różnorodnych urządzeń występujących we współczesnym środowisku sieciowym. Czujniki IoT, systemy technologii operacyjnej i smartfony reprezentują zróżnicowane, często słabiej zabezpieczone węzły, które znacznie poszerzają powierzchnię ataku firmy. Urządzenia te różnią się znacznie pod względem systemów operacyjnych, protokołów bezpieczeństwa i podatności na zagrożenia, co sprawia, że ich zabezpieczenie jest wyjątkowo trudne.

Warto pamiętać, że nawet pomimo tego, że większość omawianych dotąd technologii dotyczy wewnętrznych działań firmy, powierzchnia ataku rozciąga się też na infrastrukturę obsługującą klientów. Zmiana ta jest szczególnie widoczna w przypadku interfejsów API i usług sieciowych, które bezpośrednio komunikują się z klientami. Interfejsy te często pełnią funkcję kluczowych bram do danych i usług firmy, co czyni je atrakcyjnymi celami cyberataków.

Potrzeba ASM po części wynika ze stopniowej ewolucji cyberzagrożeń. Stały się one bardziej wyrafinowane i zróżnicowane, fundamentalnie zmieniając „krajobraz" cyberbezpieczeństwa. Początkowo cyberzagrożenia były stosunkowo proste i ograniczone pod względem zasięgu, często celując w konkretne, dobrze zdefiniowane luki w systemach. Jednakże wraz z postępem technologicznym i rosnącą złożonością środowisk informatycznych zagrożenia te stały się bardziej zawiłe i zmienne, obejmując wszystko, począwszy od zaawansowanego złośliwego oprogramowania i *ransomware*, a skończywszy na złożonych atakach socjotechnicznych i cyberatakach sponsorowanych przez państwa. Obserwując te zmiany rozwojowe, można zauważyć podobną ewolucję wyzwań we własnej firmie. Ten zmieniający się model podkreśla znaczenie przemyślenia na nowo stosowanych strategii z zakresu cyberbezpieczeństwa. Tradycyjne podejścia

do kwestii bezpieczeństwa często okazują się niewystarczające w przypadku tych zaawansowanych zagrożeń. Z tego powodu wiele firm wdraża strategiczne i dynamiczne metodologie, takie jak ASM.

Jedną ze zmian, która przyspieszyła potrzebę proaktywnej obrony, jest znacząca ewolucja cyberprzestępczości w wyniku pojawienia się zaawansowanych, trwałych zagrożeń (*APT — Advanced Persistent Threat*) i ataków ukierunkowanych. Zagrożenia APT reprezentują nowy poziom zagrożeń, które zazwyczaj, choć nie wyłącznie, sponsorowane są przez państwa lub inicjowane przez bardzo dobrze zorganizowane grupy przestępcze koncentrujące się na długotrwałych i ukrytych operacjach przeciwko konkretnym celom. Ataki te przeważnie mają na celu szpiegostwo, kradzież danych lub wyrządzenie długotrwałych szkód w infrastrukturze krytycznej. W porównaniu z bardziej oportunistyczną cyberprzestępczością tego rodzaju ataki wyróżniają się trwałością, poziomem zaawansowania i znacznym zaangażowaniem zasobów. Zagrożenia APT wykorzystują zwykle jednocześnie kombinację wielu taktyk, tworząc liczne punkty wejścia, co pozwala im na wielokrotny dostęp do celów nawet wtedy, gdy niektóre kanały zostaną zablokowane.

Podobny trend widoczny jest w dziedzinie złośliwego oprogramowania. W przypadku ataków opartych na modelu RaaS grupy nie koncentrują się wyłącznie na dostarczaniu takiego oprogramowania, ale często dogłębnie infiltrują środowisko, zanim zaczną wdrażać ładunki oprogramowania *ransomware*. Ustanawiają one przyszłe punkty wejścia oraz umieszczają ukryte i nieaktywne, złośliwe oprogramowanie, umożliwiające łatwe wznowienie przyszłych ataków nawet po tym, jak pracownicy ds. zabezpieczeń uznali, że ich firma przetrwała atak.

Ta ewolucja złośliwego oprogramowania odzwierciedla równoległą eskalację metod stosowanych przez cyberprzestępców, wykraczając poza tradycyjne wektory ataku w kierunku bardziej podstępnych i trudnych do wykrycia technik. Ataki te mają już nie tylko postać prostych załączników wiadomości e-mail. Obecnie stosowane są często złożone schematy phishingowe, wykorzystując ludzkie słabości do uzyskania dostępu do sieci lub przesyłając zainfekowane pliki za pośrednictwem zaufanych ścieżek, takich jak portale internetowe używane przez kontrahentów lub firmy zewnętrzne, co sprawia, że wykrywanie i zapobieganie tym atakom staje się trudniejsze.

Atak XZ (*https://www.wired.com/story/xz-backdoor-everything-you-need-to-know/*) na tym właśnie polegał, naruszając zabezpieczenia biblioteki oprogramowania *open source*, które były uważane za godne zaufania. Posłużyły one do osadzenia złośliwego ładunku w oprogramowaniu korzystającym z bibliotek kompresji. Repozytorium bibliotek było postrzegane jako bezpieczne i zarządzane w ramach procesu crowdsourcingu, na którym opiera się kod *open source*. Osoby ze złymi zamiarami zmanipulowały jednak ten proces, będąc „pomocnymi", co pozwoliło na wprowadzenie i zatwierdzenie ładunku ze szkodliwym kodem w bazie kodu.

Sytuacja jeszcze bardziej się skomplikowała, gdy cyberprzestępcy opracowali nowe odmiany złośliwego oprogramowania i wektory ataku, w tym zaawansowane oprogramowanie *ransomware* i narzędzia *rootkit*, a także ukryte zagrożenia osadzone w pozornie bezpiecznych typach plików, takich jak dokumenty. Ewolucja ta sprawiła, że tradycyjne rozwiązania stały się mniej skuteczne, ponieważ szybkie zmiany w metodach oznaczają, że wykrywanie oparte

na sygnaturach często nie nadąża za zmianami. Nawet techniki identyfikacji behawioralnej, które służą do wykrywania wzorców złośliwej aktywności, są obchodzone przez nowsze i bardziej wyrafinowane zagrożenia.

Odzwierciedlając ewolucję złośliwego oprogramowania, ataki phishingowe przeszły znaczącą transformację, stając się wysoce zaawansowane i ukierunkowane. Minęły czasy podstawowych i łatwych do wykrycia phishingowych wiadomości e-mail. Obecnie cyberprzestępcy pieczołowicie tworzą zwodnicze wiadomości dostosowane do poszczególnych odbiorców lub konkretnych organizacji. Taka personalizacja utrudnia odróżnianie bezpiecznych informacji od tych szkodliwych.

Przestępcy często przeprowadzają dokładne rozeznanie, aby spersonalizować swoje podejście. Aby tworzyć przekonujące scenariusze, wykorzystują media społecznościowe i publicznie dostępne informacje. Umiejętnie naśladują ton, język i wygląd komunikacji prowadzonej przez zaufane podmioty, takie jak instytucje finansowe, agencje rządowe lub znane korporacje. Biorąc na swój cel taktyki z zakresu inżynierii społecznej, te zaawansowane ataki phishingowe skutecznie manipulują odbiorcami, skłaniając ich do ujawnienia poufnych informacji, takich jak dane logowania lub szczegóły finansowe, albo nieświadomego wykonywania działań zagrażających bezpieczeństwu firmy, takich jak przelewy środków czy udzielanie dostępu do zastrzeżonych systemów.

Jak widać na przykładzie zaawansowanych technik stosowanych w przypadku zagrożeń APT, złośliwego oprogramowania i phishingu, „krajobraz" cyberzagrożeń stale ewoluuje, stając się coraz bardziej złożony i trudny do opanowania. Trend ten toruje drogę dla nowych zagrożeń, które wykorzystują najnowsze osiągnięcia technologiczne, takie jak sztuczna inteligencja i uczenie maszynowe. Te rozwijające się zagrożenia stanowią kolejną granicę w obszarze cyberprzestępczości.

Choć technologie z zakresu sztucznej inteligencji i uczenia maszynowego znacznie usprawniły wykrywanie zagrożeń i reagowanie na nie, otworzyły również drzwi do nowych luk w zabezpieczeniach. Na przykład cyberprzestępcy mogą wykorzystać te technologie do tworzenia adaptacyjnego, złośliwego oprogramowania. Takie oprogramowanie może używać algorytmów uczenia maszynowego do analizy i zrozumienia napotkanych mechanizmów obronnych, co pozwala mu dynamicznie modyfikować swój kod, aby uniknąć wykrycia przez oprogramowanie antywirusowe. Przykładem tego jest polimorficzne, złośliwe oprogramowanie, które może zmieniać swój podstawowy kod i sygnaturę, co sprawia, że jest niezwykle trudne do zidentyfikowania i zneutralizowania przez tradycyjne rozwiązania antywirusowe oparte na sygnaturach.

Co więcej, sztuczna inteligencja i uczenie maszynowe mogą być wykorzystywane do przeprowadzania zautomatyzowanych cyberataków na dużą skalę. Przestępcy mogą wdrażać boty bazujące na sztucznej inteligencji do prowadzenia szeroko zakrojonych kampanii phishingowych, w ramach których każda wiadomość jest w unikatowy sposób dostosowana do konkretnych osób, co zwiększa prawdopodobieństwo sukcesu. Takie boty mogą się uczyć i doskonalić, dostosowując swoje komunikaty na podstawie interakcji z użytkownikami, aby stać się bardziej przekonującymi. Sztuczna inteligencja może też zostać użyta w bardziej złożonych cyberatakach, takich jak ataki DDoS (*Distributed Denial of Service*), w ramach których optymalizuje ona strategie w czasie rzeczywistym, czyniąc je bardziej destrukcyjnymi i trudniejszymi do zwalczenia.

Zastosowanie sztucznej inteligencji w takich scenariuszach stanowi znaczącą eskalację w „wyścigu zbrojeń" w cyberprzestrzeni, ponieważ wyposaża przestępców w narzędzia, które mogą analizować ogromne ilości danych, szybciej identyfikować luki w zabezpieczeniach i przeprowadzać ataki z bezprecedensową efektywnością i skalą.

Ta ewolucja obejmująca wiele wektorów, z punktu widzenia organizacji znacznie rozszerzyła potencjalne powierzchnie ataku. Ponieważ nowoczesne zagrożenia nie biorą już za cel tylko tradycyjnej, wewnętrznej infrastruktury informatycznej, firmy muszą uwzględniać luki w zabezpieczeniach usług chmurowych, urządzeń przenośnych i urządzeń IoT, a także czynniki ludzkie, co sprawia, że zarządzanie powierzchnią ataku staje się koniecznością. Może to prowadzić do wniosku, że ASM to po prostu inna forma zarządzania podatnościami. Jednakże bardziej poprawne byłoby stwierdzenie, że zarządzanie nimi jest w rzeczywistości niewielką częścią struktury ASM.

Zarządzanie podatnościami, choć istotne, funkcjonuje w ograniczonym zakresie, skupiając się głównie na identyfikacji i łagodzeniu konkretnych luk w systemie. Jeśli będzie stosowane niezależnie, podejście to może przytłoczyć firmy obszernymi listami podatności, utrudniając skuteczne ustalanie priorytetów bez szerszego kontekstu strategicznego. W przeciwieństwie do tego podejście ASM wzbogaca informacje dostarczane przez rozwiązania do zarządzania podatnościami, integrując je w szerszych ramach organizacyjnych, umożliwiając zespołom ds. bezpieczeństwa skupienie wysiłków tam, gdzie mogą najbardziej znacząco poprawić stan zabezpieczeń bez negatywnego wpływu na cele biznesowe.

Zarządzanie podatnościami

Zarządzanie podatnościami to podstawowy element ASM, ale cechuje się wąskim zakresem skupiającym się na wykrywaniu i łagodzeniu luk w konkretnym systemie, aplikacji lub sieci. Proces ten obejmuje skanowanie pod kątem słabych punktów, identyfikowanie ich, a następnie podejmowanie kroków w celu rozwiązania tych problemów. Gdy jednak zarządzanie podatnościami jest stosowane samodzielnie, firmy są często przytłoczone obszerną listą rezultatów poszukiwań. Bez szerszego kontekstu może to prowadzić do trudnej sytuacji, w której ustalenie tego, w jakiej kolejności należy zająć się lukami, staje się zniechęcającym zadaniem.

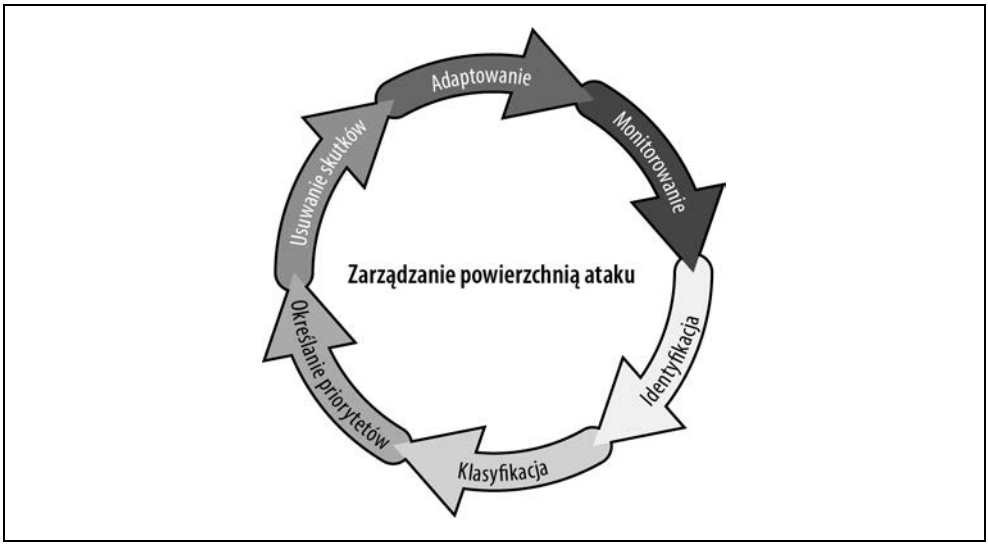
Bez integracji dodatkowych warstw analizy i wyciągania wniosków samo zarządzanie podatnościami może prowadzić do reaktywnego podejścia, w przypadku którego firmy stale próbują eliminować problemy bez strategicznego planu lub zrozumienia ich szerszego wpływu. Takie nigdy niekończące się zapętlenie powoduje, że firmy spędzają większość czasu na rozwiązywaniu pilnych i ważnych problemów, nie mając czasu na proaktywne zajęcie się ważnymi kwestiami, zanim staną się one krytyczne. Zarządzanie podatnościami skupia się na konkretnych problemach, zwiększając świadomość pracowników i zapewniając praktyczne porady dotyczące łagodzenia skutków, natomiast zarządzanie powierzchnią ataku pozwala ocenić ogólny stan ryzyka i wszystkie potencjalne słabe punkty.

W ramach ASM korzysta się z ustaleń rozwiązań służących do zarządzania podatnościami i umieszcza się je w kontekście szerszych ram działalności i celów biznesowych firmy. Oznacza to identyfikację problemów, zrozumienie, jak pasują one do powierzchni ataku, a także ocenę ich potencjalnego wpływu na działalność biznesową. Dzięki temu zarządzanie ASM umożliwia firmom ustalanie priorytetów podatności na podstawie ich znaczenia i potencjalnej

szkodliwości, dzięki czemu zasoby i wysiłki są skoncentrowane na obszarach, które mają najbardziej znaczący wpływ na inwestycje. Podejście to przekształca zarządzanie podatnościami z prostej listy kontrolnej luk w zabezpieczeniach w strategiczne narzędzie, dostosowując działania z zakresu cyberbezpieczeństwa do celów biznesowych i ułatwiając bardziej proaktywną i skuteczną obronę przed cyberzagrożeniami.

Składniki ASM

ASM składa się z sześciu podstawowych kroków, które pomagają ustalić punkt odniesienia w postaci istniejących zasobów i ich ogólnej wartości dla firmy. Kroki te opierają się na sobie nawzajem, tworząc fundament danych zasilających kolejne etapy (rysunek 1.2). Kroki obejmują wszystko, począwszy od wstępnego rozpoznania powierzchni ataku, a skończywszy na monitorowaniu i zarządzaniu. Dzięki ciągłemu monitorowaniu w miarę potrzeb można identyfikować i adaptować środki kontroli, zasady lub procedury bezpieczeństwa, aby nieustannie poprawiać stan zagrożeń. Podobnie jak wiele procesów w obszarze cyberbezpieczeństwa, ASM nie jest jednorazowym projektem, lecz cyklicznym powtarzającym się procesem, zwłaszcza gdy ekosystem informatyczny ulega zmianom lub ewoluuje „krajobraz" zagrożeń. Pora omówić bardziej szczegółowo poszczególne składniki ASM.



Rysunek 1.2. Podobnie jak wiele procesów związanych z bezpieczeństwem, ASM jest złożone z wielu składników. Skuteczne zarządzanie powierzchnią ataku to ciągły proces identyfikacji, klasyfikacji, określania priorytetów i eliminacji różnych punktów, za pomocą których atakujący może próbować uzyskać dostęp do środowiska organizacyjnego lub uzyskać z niego dane

Identyfikacja

Pierwszy krok ASM koncentruje się głównie na zrozumieniu tego, co istnieje w ekosystemie firmy. Proces ten obejmuje dokładną analizę, w ramach której każda technologia jest systematycznie identyfikowana i katalogowana. Dotyczy to zarówno rozpoznanych systemów, jak i tych nieznanych lub ewentualnie przeoczonych (często określanych mianem *nieautoryzowanych rozwiązań informatycznych*). Identyfikacja tych zasobów tworzy solidną podstawę do opracowania bazowej strategii bezpieczeństwa.

Choć ASM przypomina tradycyjne zarządzanie zasobami informatycznymi, cechuje się ono kluczowymi różnicami w sposobie realizacji procesu oceny istniejących zasobów. Przyjrzyjmy się dokładnie tym różnicom:

Zakres i charakter zasobów

Tradycyjne zarządzanie zasobami koncentruje się głównie na namacalnych zasobach informatycznych w firmie, takich jak sprzęt, aplikacje i urządzenia sieciowe. Podejście to polega na utrzymywaniu szczegółowego rejestru tych zasobów, śledzeniu ich wykorzystania oraz zarządzaniu ich cyklem eksploatacyjnym. Z kolei ASM rozszerza zakres o zasoby niematerialne, takie jak dane, konta użytkowników i usługi chmurowe, a także takie elementy zewnętrzne jak usługi firm zewnętrznych i składniki łańcucha dostaw. ASM ma na celu identyfikację wszystkich potencjalnych punktów ataku, w tym zasobów często pomijanych w tradycyjnym zarządzaniu aktywami, zapewniając tym samym bardziej kompleksowy obraz powierzchni ataku organizacji.

Identyfikacja nieznanych i dynamicznych zasobów

Inwentaryzacja w ramach tradycyjnego zarządzania zasobów jest prosta i opiera się na statycznym odwzorowywaniu znanych i regularnie monitorowanych zasobów. Jednakże ASM wykracza poza standardowy stos technologii informatycznych. W jego ramach poszukuje się zarówno znanych, jak i nieznanych zasobów, w tym tych krótkotrwałych i dynamicznych, takich jak tymczasowe instancje lub kontenery technologii chmury. Aby nadążyć za szybko zmieniającym się charakterem nowoczesnych środowisk informatycznych (zwłaszcza opartych na technologii chmury), ASM wykorzystuje dynamiczne wykrywanie i ciągłe monitorowanie, zapewniając, że żadne potencjalne luki nie zostaną przeoczone.

Osiąganie widoczności i zasięgu

Widoczność w standardowym zarządzaniu zasobami często ogranicza się do zasobów w kontrolowanym środowisku informatycznym. W ASM dąży się jednak do większej widoczności, rozszerzając ją o prywatne urządzenia pracowników lub nieautoryzowane rozwiązania informatyczne. Kładzie się nacisk na zrozumienie zewnętrznej ekspozycji zasobu. Narzędzia ASM korzystają z takich zaawansowanych technik jak skanowanie zewnętrzne i analiza zagrożeń, aby identyfikować zasoby narażone na potencjalne ataki. Tym samym zapewnia się bardziej całościowy obraz luk w zabezpieczeniach organizacji.

Zrozumienie kontekstu zasobów

W tradycyjnym zarządzaniu zasobami kontekst dotyczy ich aspektów operacyjnych, takich jak wydajność, utrzymywanie i zgodność. W przypadku ASM większą uwagę zwraca się na kontekst bezpieczeństwa zasobów, skupiając się na tym, jak mogą one zostać wykorzystane,

i oceniając ich stan zabezpieczeń oraz znaczenie w ramach ogólnej powierzchni ataku. Informacje zebrane dzięki temu podejściu są kluczowe dla zrozumienia konsekwencji naruszenia bezpieczeństwa każdego zasobu i tego, w jakim stopniu przyczynia się ono do zwiększenia podatności firmy na cyberzagrożenia.

Przyjęcie proaktywnego podejścia ukierunkowanego na kwestię bezpieczeństwa

Cele standardowych procesów zarządzania zasobami są nakierowane na informacje o ich wykorzystaniu, kosztach oraz zarządzaniu cyklem eksploatacyjnym. W przypadku podejścia ukierunkowanego na kwestię bezpieczeństwa w ramach ASM priorytetem jest identyfikacja luk w zabezpieczeniach, błędnych konfiguracji i potencjalnych wektorów ataku, aby można było proaktywnie ustalać priorytety i zarządzać działaniami naprawczymi.

Klasyfikacja

Choć identyfikacja zasobów pozwala ustalić, co istnieje w środowisku, nie dostarcza kontekstu opisującego znaczenie poszczególnych zasobów. W ramach tego kroku rozwiązuje się problem identyfikacji przez kategoryzowanie zasobów. Polega to na klasyfikowaniu ich na podstawie różnych kryteriów, takich jak typ danych, wymagania dotyczące zgodności, funkcje i znaczenie z punktu widzenia bezpieczeństwa.

Aby skutecznie zarządzać powierzchnią ataku firmy, trzeba rozróżnić klasyfikację zasobów od klasyfikacji danych. Choć oba procesy polegają na kategoryzacji elementów na podstawie wrażliwości i ryzyka, klasyfikacja zasobów koncentruje się na urządzeniach, oprogramowaniu i systemach jako całości, biorąc pod uwagę takie czynniki jak ich rola w działalności biznesowej, podatność na zagrożenia i potencjalny wpływ naruszenia zabezpieczeń. Z kolei klasyfikacja danych dotyczy wprost typu danych obsługiwanych przez dany zasób, takich jak informacje poufne, prywatne lub publiczne, a także środków bezpieczeństwa niezbędnych do ich ochrony.

Klasyfikacja zasobu może być faktycznie uzależniona od typu przetwarzanych lub przechowywanych przez niego danych, jednak kryteria i konsekwencje klasyfikacji zasobów i danych są odmienne. Zrozumienie tej różnicy jest kluczowe do tego, aby zespoły mogły wdrożyć odpowiednie środki kontroli zabezpieczeń i zapewniania zgodności, zapewniając odpowiednią ochronę swoich zasobów i danych.

Zastanówmy się, co to oznacza:

Dostosowanie środków kontroli zabezpieczeń

Różne zasoby mają różne wymagania odnośnie zakresu bezpieczeństwa, a klasyfikacja zasobów pozwala organizacjom odpowiednio dostosować środki kontroli zabezpieczeń. Rozważmy na przykład dwie bazy danych firmy, jedną zawierającą dane poufne, a drugą zarządzającą publicznie dostępnymi danymi. Choć obie mogą wymagać ścisłej kontroli dostępu i regularnych kopii zapasowych, baza z danymi poufnymi wymaga szyfrowania zawierających je pól. Klasyfikacja zasobów podkreśla te odmienne wymogi, umożliwiając organizacjom wdrożenie odpowiednich środków kontroli zabezpieczeń tam, gdzie są one najbardziej potrzebne. Pomaga to firmom uniknąć tworzenia reguł bezpieczeństwa o zbyt szerokim zasięgu nadmiernie chroniących niewymagające tego zasoby lub niedostatecznie chroniących te, które tego wymagają.

Określanie potrzeb w zakresie zgodności

Wymogi bezpieczeństwa nie koncentrują się wyłącznie na zewnętrznych atakujących. Często muszą one uwzględniać zgodność z wymaganiami nadzorczymi, prawnymi i regulacyjnymi. Klasyfikacja zasobów odgrywa kluczową rolę w zapewnieniu spełnienia bieżących wymagań. Kategoryzacja zasobu musi uwzględniać znajdujący się w nim typ danych pod kątem tego, czy nie podlega któremuś ze specyficznych przepisów. Na przykład zasób zawierający dane osobowe dotyczące zdrowia zostałby sklasyfikowany pod kątem zgodności z ustawą HIPAA, a ponadto wymagałby konkretnych środków kontroli bezpieczeństwa i prywatności. Bez uwzględnienia tych potrzeb łatwo byłoby przeoczyć niezbędne środki kontroli, co mogłoby prowadzić do kar, grzywien i szkód dla reputacji firmy.

Planowanie reagowania na incydenty i odzyskiwania danych

Klasyfikacja zasobów pozwala również rozróżnić, co jest najważniejsze dla działalności biznesowej. Ułatwia to utrzymanie ciągłości biznesowej dzięki opracowaniu takich planów reagowania na incydenty, które priorytetowo traktują najważniejsze zasoby, co pozwala na szybsze odzyskiwanie przy krótszych przestojach. Przykładem może być przywracanie usług internetowych i wspierającej je infrastruktury, które są niezbędne z punktu widzenia operacji wykonywanych przez klientów. Takie ustalenie priorytetów w planowaniu pomaga firmom utrzymać ciągłość operacyjną nawet w obliczu incydentów dotyczących bezpieczeństwa, minimalizując wpływ na funkcje biznesowe i reputację.

Ustalanie priorytetów

W ramach ASM uznaje się, że nie wszystkie luki lub ryzyka niosą ze sobą taki sam stopień ryzyka, zwłaszcza gdy pod uwagę weźmie się powiązane z nimi zasoby. Konieczne jest określanie priorytetu luk w zabezpieczeniach w oparciu o ich potencjalny wpływ w stosunku do wartości, jaką dany zasób przedstawia dla firmy. Takie podejście zapewnia efektywną alokację ograniczonych zasobów na potrzeby zarządzania powierzchnią ataku. Istnieje wiele sposobów ustalania tych priorytetów, które dokładniej omówimy w rozdziale 5., w tym ilościowej i jakościowej metody oceny ryzyka. Będzie też mowa o ich roli w procesie ustalania priorytetów.

Serwery zawierające dane poufne lub systemy dostępne z zewnątrz, a także inne systemy wysokiego ryzyka, mają pierwszeństwo w stosowaniu środków kontroli zabezpieczeń. W przypadku tych systemów priorytet ustala się drogą częstych aktualizacji, solidnego monitorowania i rygorystycznej kontroli dostępu. Nie oznacza to, że inne systemy są ignorowane. Po prostu uwaga skupia się na tych, które najbardziej tego potrzebują. Dzięki zapewnieniu, że najważniejsze zasoby są priorytetowo chronione, organizacje zyskują najbardziej znaczące ograniczenie poziomu ryzyka w stosunku do zainwestowanych zasobów.

Działania zaradcze

Po ustaleniu priorytetów kolejnym krokiem jest podjęcie działań zaradczych polegających na zabezpieczeniu powierzchni ataku mających najwyższy priorytet. Obejmuje to uporanie się z lukami i błędnymi konfiguracjami, które narażają zasoby na atak, w tym wdrożenie ukierunkowanych środków kontroli w celu ochrony przed zagrożeniami w obrębie powierzchni ataku. Ze

względu na ograniczone zasoby większości firm w ASM podkreśla się znaczenie strategicznych środków bezpieczeństwa. Idealne zabezpieczenie wszystkiego nie jest możliwe, stąd pojawia się potrzeba podejścia ukierunkowanego.

Jednym z głównych powodów stosowania ASM jest konieczność zrównoważenia przez firmy ich ograniczonych zasobów z potrzebą zabezpieczenia powierzchni ataku. Informacje z faz identyfikacji i klasyfikacji pomagają w ustalaniu priorytetów przez określenie luk i błędnych konfiguracji stanowiących największe zagrożenie. Różnica między tym podejściem a standardowym zarządzaniem lukami polega na tym, że ASM wykorzystuje dogłębne zrozumienie stanu zabezpieczeń firmy i potencjalnego wpływu różnych zagrożeń. Z kolei tradycyjne zarządzanie lukami skupia się jedynie na z góry ustalonych ocenach.

Organizacje borykają się z zalewem danych z narzędzi do zarządzania podatnościami, co prowadzi do wykrycia więcej podatności niż można skutecznie wyeliminować. Jeśli nawet firma skupi się wyłącznie na słabych punktach o wysokim priorytecie, wyeliminowanie ich może nie zmniejszyć efektywnie ryzyka. Na przykład usunięcie 20 krytycznych luk w zabezpieczeniach przestarzałego serwera, który ma zostać wkrótce wycofany i znajduje się tylko w sieci wewnętrznej, jest prawdopodobnie mniej skuteczne niż usunięcie jednej luki w publicznie dostępnym interfejsie API sklepu internetowego firmy. W ramach ASM wykorzystuje się kontekstowe informacje biznesowe. Dzięki temu organizacje mogą skupić się na środkach kontroli zabezpieczeń w obszarach, które przyniosą największe ograniczenie rzeczywistego ryzyka, zamiast po prostu sprawdzać punkty na liście kontrolnej bezpieczeństwa.

Dostosowywanie

Wraz z monitorowaniem zarządzanie powierzchnią ataku wiąże się z regularnym dostosowywaniem go do zmieniającego się środowiska. W miarę rozwoju firm i ich zwiększającego się profilu cyfrowego zmienia się również ich powierzchnia ataku. Okresowa ponowna ocena i dostosowanie strategii bezpieczeństwa są niezbędne, aby nadążyć za tymi zmianami i zapewnić, że stan bezpieczeństwa firmy pozostaje solidny i elastyczny.

Jak wcześniej wspomniano, tradycyjnie firmy miały dość często przez dłuższe okresy statyczną powierzchnię ataku. Jednakże z czasem, zwłaszcza w rozwijających się firmach, zachodzą zdarzenia lub sytuacje wymagające zmian w ekosystemie informatycznym. Nowoczesne organizacje opierają się jednak na szybko rozwijających się i ewoluujących infrastrukturach informatycznych z nieustannymi zmianami w kodzie wprowadzanymi przez procesy integracji i ciągłego wdrażania, dodawaniu przez zespoły nowych dostawców w łańcuchu dostaw, a nawet umieszczaniu bez sprawdzenia zabezpieczeń przypadkowych skryptów na głównej stronie przez pracowników działu marketingu. Wszystko to sprawia, że powierzchnia ataku podlega ciągłym zmianom.

Nawet w przypadku bardziej statycznych organizacji uruchamianie nowych fizycznych lub wirtualnych systemów, dodawanie nowego oprogramowania, adaptowanie usług nowego dostawcy czy otwieranie nowego biura zamiejscowego to przykłady typowych zmian, które mogą rozszerzyć powierzchnię ataku. Warto zauważyć, że zmiany nie zawsze prowadzą do jej powiększenia. Czasami ją zmniejszają (na przykład w wyniku wycofania starych systemów, usuwania nieużywanego oprogramowania lub eliminowania nieużywanych portów).

Gdy wiadomo wcześniej o nadchodzących zmianach, można się do nich przygotować. Planowanie ułatwia pracę w ramach ASM a dostosowywanie obecnych środków kontroli zabezpieczeń, zasad lub procedur do potrzeb zmodyfikowanej powierzchni ataku, umożliwia utrzymanie solidnego stanu zabezpieczeń.

Monitorowanie

Ciągłe monitorowanie jest kluczowym elementem praktyki ASM. Polega ono na nieustannym nadzorze wszystkich zasobów sieciowych, wykrywaniu zmian w powierzchni ataku oraz identyfikowaniu nowych podatności w miarę ich pojawiania się. Dzięki wdrożeniu narzędzi i protokołów zapewniających monitorowanie w czasie rzeczywistym (lub zbliżonym do niego) firmy mogą szybko reagować na nowe zagrożenia, eliminować luki w zabezpieczeniach i dopasowywać swoje strategie bezpieczeństwa. Takie proaktywne podejście nie tylko pomaga w natychmiastowym wykrywaniu zagrożeń, ale także znacząco przyczynia się do możliwości adaptowania ASM do potrzeb firmy.

Potrzeba ciągłego monitorowania wynika też z nieustannej ewolucji cyberprzestępców. Firma nigdy nie osiąga trwale „bezpiecznego" stanu, gdyż „krajobraz" zagrożeń stale się zmienia. Ciągłe monitorowanie wspiera możliwości adaptowania, dostarczając informacji o pojawiających się trendach i potencjalnych przyszłych zagrożeniach. Umożliwia to firmom trzymanie na bezpieczny dystans osób ze złymi zamiarami oraz ciągłe doskonalenie i aktualizowanie mechanizmów obrony w celu nadążenia za najnowszymi rozwiązaniami w dziedzinie bezpieczeństwa.

Strategiczna rola ASM w cyberbezpieczeństwie

Ważne jest, aby rozpatrywać powierzchnię ataku jako strategiczny plan działania zespołów ds. cyberbezpieczeństwa. Staje się to coraz bardziej istotne w kontekście ograniczonych zasobów i przytłaczającej ilości danych generowanych przez istniejące narzędzia zabezpieczeń, ponieważ pozwala zespołom skoncentrować swoje wysiłki związane z bezpieczeństwem. ASM pełni funkcję mapy drogowej, wskazując podatne miejsca wymagające ochrony. W obecnym „krajobrazie" cyberbezpieczeństwa firmy stają w obliczu lawiny luk i potencjalnych problemów, które znacznie przekraczają ich możliwości radzenia sobie z nimi.

Sytuację tę dodatkowo komplikuje powszechny niedobór wykwalifikowanych specjalistów ds. cyberbezpieczeństwa, co prowadzi do powstawania zespołów, które są przeciążone i często zawierają niedostateczną liczbę osób. W takim środowisku zrozumienie i mapowanie powierzchni ataku jest nie tylko korzystne, lecz niezbędne. Dzięki ustalaniu priorytetów kluczowych luk zespoły ds. cyberbezpieczeństwa mogą strategicznie alokować swoje ograniczone zasoby, skupiając wysiłki na wdrażaniu ukierunkowanych środków bezpieczeństwa tam, gdzie są one najbardziej potrzebne.

I wreszcie, zarządzanie powierzchnią ataku jest niezbędne do zapewnienia zgodności z przepisami i standardami, takimi jak PCI DSS, HIPAA, RODO i SOX. Standardy te wymagają ścisłego przestrzegania procedur bezpieczeństwa, które zapobiegają nieuprawnionemu ujawnieniu danych klientów. Włamania do danych lub inne incydenty związane z bezpieczeństwem spowodowane nie-

odpowiednimi środkami kontroli będą miały znaczące konsekwencje prawne, które mogą bezpośrednio wpłynąć na wyniki finansowe firmy z powodu kar, procesów sądowych lub kosztownych i obowiązkowych planów naprawczych.

Nieprzestrzeganie przepisów wiąże się również z mniej bezpośrednimi kosztami, takimi jak brak zgodności z wytycznymi Komisji Papierów Wartościowych i Giełd dotyczącymi raportowania istotnych informacji, pozwy zbiorowe, wpływ na cenę akcji i utrata zaufania klientów. Klienci są bardziej świadomi i, decydując o współpracy z firmą, biorą pod uwagę to, jak dobrze chronione są ich dane. Firmy, które padły ofiarą naruszenia bezpieczeństwa danych, zwłaszcza gdy wynikało to z ich własnego zaniedbania, tracą klientów, a odzyskanie ich wymaga więcej niż tylko biernego oczekiwania. W takiej sytuacji niezbędne jest wykazanie fundamentalnej zmiany w podejściu firmy do priorytetowego traktowania kwestii bezpieczeństwa, takiej jak zapewniana w ramach ASM.

Uwzględnienie perspektywy atakującego

Zarządzanie powierzchnią ataku stanowi istotną zmianę w podejściu do cyberbezpieczeństwa polegającą na przejściu od postawy czysto defensywnej do takiej, która zawiera elementy strategii ofensywnej. Uwzględniając perspektywę atakującego, ASM oferuje bardziej kompleksowe i proaktywne podejście do zabezpieczania środowisk informatycznych poprzez włączenie elementów strategii ofensywnej do tradycyjnych postaw defensywnych. Co więcej, pomaga również zweryfikować, czy istniejące środki kontroli zabezpieczeń działają skutecznie i zapewniają niezbędną ochronę.

Zmiana punktu widzenia

ASM stanowi koncepcję o przełomowym charakterze. Większość firm koncentruje swoje działania w zakresie bezpieczeństwa na podejściu opartym na obronie, realizowanym przez tzw. zespół „niebieskich".. Zespół ten ma na celu ochronę systemów informatycznych przed cyberatakami poprzez identyfikację luk w zabezpieczeniach, wdrażanie środków bezpieczeństwa i ciągłe monitorowanie. Niektóre firmy wykorzystują też podejście ofensywne powiązane z określeniem zespołu „czerwonego", którego członkowie starają się obejść zabezpieczenia i przeniknąć przez nie, wskazując miejsca, w których kontrole są niewystarczające lub całkowicie ich brakuje.

ASM wymaga znaczącej zmiany myślenia, polegającej na spojrzeniu na własne zasoby oczami atakującego. Jednakże dokonanie tej transformacji może być wyzwaniem. Jako specjaliści ds. bezpieczeństwa jesteśmy tradycyjnie przyzwyczajeni do skupiania się na obronie. Uczy się nas priorytetowego traktowania ochrony zasobów, monitorowania działań i reagowania na zagrożenia.

Cyberprzestępcy, którzy zazwyczaj kierują się takimi celami jak zysk finansowy, przynależność do haktywistów lub motywacje polityczne, często dążą do minimalnego wysiłku i maksymalnej anonimowości. Pobudza to kreatywność i myślenie strategiczne. Szukają oni słabego punktu, który daje największą przewagę w trakcie ataku. Przyjęcie punktu widzenia atakującego wymaga fundamentalnej zmiany podejścia i innowacyjnego myślenia. Przejście do tej bardziej ofensywnej perspektywy obejmuje kilka kluczowych kroków. Pierwszym jest identyfikacja

podatności w systemie. Kolejnym krokiem jest dogłębna analiza tego, dlaczego te podatności mogą być atrakcyjne.

Następny kluczowy krok to przyjęcie sposobu myślenia przeciwnika i rozważenie takich pytań jak: „Gdybym był atakującym, jakie cele wydawałyby się najbardziej atrakcyjne? Jakie taktyki zastosowałbym, aby wykorzystać te podatności?". Zaangażowanie się w tego rodzaju myślenie strategiczne jest niezbędne do przejścia w obszarze cyberbezpieczeństwa z postawy reaktywnej na proaktywną. Umożliwia to przewidywanie potencjalnych ataków, a nie tylko reagowanie na nie po ich wystąpieniu.

Spojrzenie na całokształt

Przyjęcie sposobu myślenia przeciwnika wymaga od nas spojrzenia na całokształt sytuacji i zrozumienia kontekstu wykrytych w firmie podatności. Specjaliści ds. bezpieczeństwa często mierzą się z fragmentarycznym obrazem środowiska zabezpieczeń swojej firmy. Ta niepełna perspektywa może wynikać z ograniczeń czasowych i złożoności infrastruktur informatycznych o dużej skali. Istniejące narzędzia często zapewniają wgląd jedynie w wybrane obszary, takie jak technologia chmury. Choć wyniki analizy w danym obszarze mogą być szczegółowe, często brakuje im kontekstu przepływu procesów biznesowych albo integracji lub interakcji z innymi zasobami informatycznymi, co ogranicza ich rzeczywistą wartość.

Z kolei atakujący skrupulatnie analizują kontekst biznesowy i przepływ operacji, aby zidentyfikować obszary najbardziej podatne na skuteczne ataki lub głębszą penetrację systemu. Podejście to wykracza poza podatności czysto technologiczne. Obejmuje ono kompleksową ocenę procesów biznesowych, przepływu danych i czynników ludzkich, które mogą stanowić potencjalne cele.

Do uzyskania całościowego obrazu wykorzystuje się informacje zebrane podczas oceny ryzyka, która wykracza poza konwencjonalny stos technologiczny. Początkowo może wydawać się to przytłaczające, ale nie musi być realizowane od razu w całości. Dzieląc proces oceny na etapy i określając ich priorytety, zadanie można rozbić na łatwiejsze do przyswojenia części, które ostatecznie zapewnią pokrycie wszystkich zasobów organizacji.

Inwentaryzacja zasobów stanowi nasz punkt wyjścia w tym etapowym procesie. Znając stan posiadania, można opracować plan wdrożenia ocen ryzyka. Inwentaryzacja zapewnia, że podczas określania zakresu oceny ryzyka uwzględnimy wszystkie zasoby z naszych najbardziej krytycznych lub wrażliwych obszarów, takich jak kluczowe zasoby danych i istotne procesy operacyjne.

Można zacząć od posiadanej infrastruktury chmurowej, a jeśli jest to zbyt szeroki zakres, można zawęzić go wyłącznie do konkretnego zestawu używanych systemów e-commerce. Dzięki takiemu podziałowi można lepiej zaplanować i przydzielić zasoby. A zatem zarządzanie ASM jest procesem systematycznym, a nie sprintem w kierunku jednego, monolitycznego celu, który prawie na pewno zakończyłby się niepowodzeniem.

Ocena ryzyka ostatecznie obejmie wszystkie aspekty działalności firmy, w tym procesy operacyjne, praktyki zarządzania danymi oraz role pracowników w systemie. Oczywiście jest to element końcowego etapu, ponieważ tak kompleksowe podejście oferuje pełny wgląd pozwalający na zrozumienie, w jaki sposób różne komponenty współdziałają i potencjalnie generują ryzyko.

Taka interakcja jest widoczna podczas mapowania potencjalnych ścieżek ataku. Analizowanie tego, jak różne systemy informatyczne współdziałają ze sobą, ujawnia mniej oczywiste podatności, w przypadku których informacje poufne mogą być narażone lub mogą istnieć podatne na atak punkty wejścia. Dokładne mapowanie tych ścieżek pozwala firmom uzyskać cenne informacje o stanie ich bezpieczeństwa, co pozwala im wyprzedzająco identyfikować i wzmacniać obszary, które potencjalnie mógłby wykorzystać atakujący. Takie proaktywne podejście jest kluczowe dla przejścia z reaktywnej do ofensywnej postawy w obszarze obrony cyberbezpieczeństwa.

Na pierwszy rzut oka może się wydawać, że widoczność niezbędna zespołom ds. bezpieczeństwa prowadzi też do nadmiernego rozszerzenia uprawnień i naruszenia podziału obowiązków. Problem ten można rozwiązać, wdrażając rygorystyczne mechanizmy nadzoru. Powinny one obejmować kompleksową infrastrukturę logowania, regularne audyty, kontrolę dostępu opartą na rolach, system zarządzania incydentami oraz ścisły nadzór w celu utrzymania mechanizmów kontroli i równowagi.

Adaptując proces iteracyjny, który respektuje zasady minimalnych uprawnień i ochrony prywatności, firmy mogą stopniowo poszerzać swoją wiedzę o powierzchni ataku w kontrolowany i bezpieczny sposób, unikając tym samym zagrożeń wynikających ze zbyt szerokiego lub nadmiernie inwazyjnego podejścia.

Identyfikacja łatwych celów

Cyberprzestępcy często stosują strategie podobne do tych używanych przez drapieżniki w naturze, szukając najpierw najsłabszych i najbardziej bezbronnych celów. To efektywne podejście pozwala im wykorzystywać najbardziej dostępne podatności przy minimalnym wysiłku. Te „łatwe cele" nierzadko obejmują ludzi, przestarzałe systemy, przewidywalne hasła, wprowadzone na stałe dane uwierzytelniające oraz inne przeoczone luki w zabezpieczeniach środowiska informatycznego. Cyberprzestępcy postrzegają te słabości jako łatwy łup, czyniąc je w swojej strategii pierwszym punktem ataku.

Skupienie się na łatwych do wykorzystania podatnościach nie wyklucza jednak prób przeprowadzenia bardziej złożonych i wyrafinowanych ataków. Zrozumienie tego zachowania w stylu drapieżnika jest niezbędne do skutecznego zarządzania powierzchnią ataku, które podkreśla wagę identyfikacji i zabezpieczania oczywistych, lecz często zaniedbywanych podatności. Firmy mogą ustalać priorytety dla tych słabych punktów, aby zapobiec uzyskaniu przez przestępców łatwych punktów zaczepienia pozwalających na dostęp do ich systemów.

Rozpoznawanie i usuwanie typowych podatności stanowi fundament proaktywnego podejścia do obrony. Czujność jest niezbędna w trakcie identyfikowania słabych punktów, które cyberprzestępcy regularnie wykorzystują, w tym niezaktualizowanego oprogramowania, systemów z domyślnymi konfiguracjami oraz słabych mechanizmów uwierzytelniania.

Regularne skanowanie pod kątem podatności oraz oceny bezpieczeństwa stają się podstawowymi narzędziami w arsenale ASM. Skanowania i oceny pozwalają firmom wyprzedzać działania atakujących, identyfikując i łagodząc te „łatwe cele", zanim atakujący zdążą się nimi posłużyć.

„Krajobraz" zagrożeń nieustannie ewoluuje. Stała czujność i uwzględnianie wykrytych luk w procesie oceny powierzchni ataku są niezbędne do zapewnienia trwałego bezpieczeństwa i odporności infrastruktury informatycznej firmy na nowe i pojawiające się zagrożenia.

Nie trać celu z oczu

Proces *analizy krytyczności zasobów* odgrywa kluczową rolę w tym strategicznym podejściu. Polega on na dokładnej ocenie tego, jakie zasoby są niezbędne dla podstawowych funkcji i działania firmy. Analiza ta uwzględnia takie czynniki jak znaczenie danego zasobu z punktu widzenia operacji biznesowych, wrażliwość przechowywanych w nim danych oraz potencjalne skutki dla firmy w przypadku naruszenia bezpieczeństwa tego zasobu. Pod uwagę bierze się też to, jakie urządzenia stanowią największe ryzyko lub mogą wyrządzić największe szkody w przypadku niewłaściwego użycia, uwzględniając różne rodzaje zagrożeń wewnętrznych.

Po zidentyfikowaniu zasobów o najwyższym priorytecie kluczowe jest wdrożenie strategii wielowarstwowej ochrony, czyli ochrony w głąb (ang. *defence in depth*). Przykładem jest zastosowanie kombinacji zapór sieciowych wraz z systemem wykrywania włamań generującym alerty w przypadku ominięcia przez kogoś zapory. Celem jest użycie wielu środków do zabezpieczania do ochrony tych zasobów, tak aby nawet w przypadku naruszenia jednej warstwy pozostałe nadal zapewniały ochronę.

Warto zaznaczyć, że nie chodzi tu wyłącznie o kluczowe systemy lub krytyczne z punktu widzenia misji firmy. Takie podejście przypominałoby ustawienie wszystkich strażników przy głównej bramie zamku, pozostawiając wejście do piwnicy bez nadzoru. Chodzi raczej o to, że systemy te są traktowane priorytetowo i otrzymują większą część ograniczonych dostępnych zasobów.

W całej organizacji nadal muszą być przestrzegane podstawowe standardy, które w ujęciu całościowym przyczyniają się do ograniczania powierzchni ataku. Każde wyjście na zewnątrz może mieć zamki i nadzór, ale główna brama będzie dodatkowo wzmocniona. Dzięki takiemu podejściu podstawowy poziom bezpieczeństwa jest nadal obecny, ale uwaga skupia się na najbardziej prawdopodobnych celach ataku.

Dostosuj się i pokonaj przeszkody

„Krajobraz" cyberzagrożeń nieustannie ewoluuje, a osoby ze złymi zamiarami ciągle opracowują nowe taktyki i strategie, by pokonywać zabezpieczenia. Obrońcy muszą robić to samo. W takim środowisku czujność staje się czymś więcej niż tylko praktyką — jest koniecznością. ASM zasadniczo polega na utrzymywaniu ciągłego stanu czujności, ścisłym monitorowaniu pojawiających się podatności i przygotowywaniu do szybkiego dostosowywania mechanizmów obronnych w celu ograniczania skutków nowych ataków. Ten ciągły proces adaptacji jest nie tylko korzystny, ale i niezbędny do unikania potencjalnych zagrożeń. Wymaga on zrozumienia, że to, co działa dziś, już jutro może nie być skuteczne.

Dostosowywanie się do rozwijających się zagrożeń wymaga dwutorowego podejścia, czyli śledzenia na bieżąco „krajobrazu" zagrożeń oraz budowania postawy w zakresie bezpieczeństwa cechującej się elastycznością i „zwinnością". Bycie na bieżąco oznacza regularne pozyskiwanie

i analizowanie informacji dotyczących zagrożeń (ang. *threat intelligence*), które mogą rzucić światło na pojawiające się wektory ataków oraz taktyki, techniki i procedury stosowane przez atakujących. Wiedza ta jest nieoceniona przy przewidywaniu potencjalnych scenariuszy ataków i odpowiednim przygotowywaniu obrony.

Z kolei budowanie dobrej kondycji bezpieczeństwa, wyróżniającej się elastycznością i „zwinnością" polega na opracowaniu strategii bezpieczeństwa, która pozwala szybko i skutecznie reagować na nowe informacje o potencjalnych zagrożeniach i podatnościach. Obejmuje to możliwość szybkiej rekonfiguracji systemów, implementacji nowych środków kontroli zabezpieczeń i dopasowywania zasad w miarę zmieniającego się środowiska zagrożeń. Chodzi o stworzenie ram bezpieczeństwa, która nie jest sztywna, ale wystarczająco solidna, aby oprzeć się obecnym zagrożeniom, a jednocześnie na tyle elastyczna, by ewoluować wraz z przyszłymi wyzwaniami.

Strategia proaktywna: wcielanie się w rolę atakującego

Przyjęcie sposobu myślenia atakującego polega na zadaniu sobie pytania: „Co bym zrobił, gdybym był atakującym?". Takie podejście pozwala specjalistom ds. bezpieczeństwa przewidywać potencjalne metody ataku, myśleć kreatywnie o podatnościach i opracowywać skuteczniejsze strategie obrony. Umożliwiając zrozumienie logiki przeciwnika i potencjalnych celów, ASM przekształca podejście do cyberbezpieczeństwa z reaktywnego na proaktywne, gwarantując, że obrona jest solidna i strategicznie ukierunkowana na najbardziej prawdopodobne zagrożenia.

Zarządzanie powierzchnią ataku zmienia strategię cyberbezpieczeństwa, łącząc taktyki obronne z ofensywnym sposobem myślenia. Taka perspektywa umożliwia firmom analizę systemów z punktu widzenia atakującego, przewidywanie ich ruchów, a także budowanie bardziej odpornych i proaktywnych systemów obrony, co ostatecznie prowadzi do bezpieczniejszego i solidniejszego środowiska informatycznego.

Strategie „polowania" na zagrożenia (ang. *threat hunting*), takie jak Atomic Red Team oraz projekt M.O.R.D.O.R., opierają się na wykorzystaniu sposobu myślenia atakującego. Te cenne narzędzia umożliwiają organizacjom proaktywne identyfikowanie i łagodzenie potencjalnych luk w zabezpieczeniach. Biblioteka Atomic Red Team pozwala zespołom ds. bezpieczeństwa przeprowadzać konkretne, ukierunkowane ataki (atomowe) na własne systemy, aby w czasie rzeczywistym testować i poprawiać skuteczność istniejących mechanizmów obrony. Pomaga to sprawić, że środki bezpieczeństwa są wystarczająco solidne, aby poradzić sobie z różnymi scenariuszami ataków.

Podobnie projekt M.O.R.D.O.R. dostarcza wstępnie zarejestrowanych, realistycznych scenariuszy ataków opartych na zaobserwowanych zagrożeniach, umożliwiając firmom symulowanie pełnych cykli ataków. Pozwala to nie tylko sprawdzić odporność obecnych zabezpieczeń, ale także skutecznie szkolić zespoły ds. bezpieczeństwa w zakresie rozpoznawania złożonych i wieloetapowych zagrożeń oraz reagowania na nie.

Przypadki użycia ASM i wyzwania dla bezpieczeństwa

Zarządzanie powierzchnią ataku to wieloaspektowe rozwiązanie w przypadku różnorodnych wyzwań organizacyjnych, które za pomocą jednego solidnego programu pozwala uporać się z wieloma przypadkami użycia. Wdrażając ASM, firmy mogą jednocześnie rozwiązywać różne problemy związane z ich kondycją cyberbezpieczeństwa. Obejmuje to zwiększenie widoczności zasobów sieciowych, identyfikację i łagodzenie podatności, zapewnienie zgodności ze standardami regulacyjnymi oraz poprawę ogólnej odporności zabezpieczeń. Kompleksowe podejście w ramach ASM nie tylko usprawnia proces zarządzania bezpieczeństwem sieci firmy, ale także zapewnia, że wiele problemów, takich jak słabe punkty w sieci, ryzyko braku zgodności i potencjalne wektory ataku, jest rozwiązywanych równocześnie. Współczesna infrastruktura jest zbyt rozległa i skaluje się zbyt szybko, aby tradycyjne praktyki bezpieczeństwa były skuteczne. Zarządzanie powierzchnią ataku zostało zaprojektowane tak, aby pomóc firmom uzyskać kontrolę nad tymi środowiskami i efektywnie zarządzać ryzykiem przy wykorzystaniu obecnych zasobów kadrowych zespołów, a nie takich, jakie chciałyby mieć lub na które chciałyby móc sobie pozwolić .

Problemy z widocznością

Jednym z najistotniejszych wyzwań, na które odpowiada zarządzanie powierzchnią ataku, są problemy z widocznością wynikające ze złożoności nowoczesnych infrastruktur. Czasy, gdy infrastruktura firmy ograniczała się do jednego centrum danych już minęły. Powszechne adaptowanie infrastruktury chmurowej, konteneryzacji, wirtualizacji i produktów opartych na modelu SaaS spowodowało rozproszenie danych na różnych platformach, które często są poza bezpośrednią kontrolą organizacji. Takie rozproszenie zmniejsza kontrolę nad danymi i często wiąże się z niewystarczającymi wbudowanymi narzędziami do zapewnienia widoczności.

Tradycyjne narzędzia zaprojektowane dla środowisk lokalnych mają trudności z dostosowaniem się do tych nowych, rozproszonych środowisk. Co więcej, nawet wtedy, gdy narzędzie dobrze sprawdza się poza tradycyjnym centrum danych w konkretnym środowisku, przeważnie nie może współpracować z innymi narzędziami, aby stworzyć jednolity obraz wszystkich zasobów i danych firmy. W rezultacie uzyskuje się rozproszony i niepełny obraz powierzchni ataku organizacji, pozostawiający groźne luki w obszarze widoczności i zwiększający ryzyko naruszenia bezpieczeństwa.

Stosowanie ASM pomaga organizacjom przezwyciężyć ograniczenia tradycyjnych narzędzi, oferując możliwości dostosowane do zarządzania złożonością nowoczesnych infrastruktur rozproszonych. Dzięki integracji różnych źródeł danych i zapewnieniu wglądu w różne środowiska, zarówno lokalne, jak i chmurowe albo hybrydowe, ASM ułatwia wypełnienie luki dotyczącej widoczności. Umożliwia to firmom odwzorowanie i zrozumienie całej powierzchni ataku, niezależnie od tego, gdzie znajdują się ich dane i zasoby. Takie całościowe rozpoznanie jest niezbędne do identyfikacji ukrytych podatności, monitorowania pojawiających się zagrożeń i zapewnienia spójnych praktyk bezpieczeństwa we wszystkich segmentach infrastruktury informatycznej.

Zarządzanie zasobami

Zarządzanie zasobami to jedna z praktyk, z którą nierozerwalnie związane jest ASM. Zarządzanie zasobami wykorzystuje procesy *ciągłego wykrywania zasobów* i *świadomości zmian*, aby regularnie identyfikować oraz śledzić nowe i istniejące zasoby w sieci firmy. Zapewnia to, że inwentarz zasobów jest stale aktualna, co pozwala na bardziej responsywne zarządzanie bezpieczeństwem w ciągle zmieniającym się środowisku informatycznym.

Kategoryzacja i monitorowanie zasobów w ramach ASM to istotny krok obejmujący klasyfikację zasobów na podstawie ich typu, znaczenia i potencjalnego ryzyka. Kategoryzacja jest niezbędna do skutecznego ustalania priorytetów działań związanych z bezpieczeństwem i alokowania zasobów tam, gdzie są najbardziej potrzebne. ASM obejmuje również dynamiczną ocenę ryzyka i określanie priorytetów. Jest to proces, w ramach którego stale ocenia się i klasyfikuje zasoby pod kątem ich podatności na zagrożenia i znaczenia dla działalności biznesowej. I wreszcie, identyfikacja podatności stanowi fundament ASM, koncentrując się na systematycznym wykrywaniu słabych punktów lub błędów w zasobach, które mogłyby stać się celem cyberataków.

Informowanie o zasobach

W zakresie *wiedzy o zasobach* (ang. *asset intelligence*) ASM rozszerza tradycyjne metody zarządzania zasobami. W tym ujęciu wiedza o zasobach wykracza poza zwykłe wykrywanie i monitorowanie. Obejmuje ono integrację informacji kontekstowych o każdym zasobie w sieci firmy. Oznacza to zrozumienie roli danego zasobu, jego ustawień konfiguracyjnych, sposobu, w jaki łączy się i współdziała z innymi zasobami, a także jego zależności w szerszej architekturze sieciowej. W wyniku uwzględnienia tych warstw kontekstu ASM zapewnia możliwość głębszego i subtelniejszego zrozumienia każdego zasobu, umożliwiając precyzyjniejsze i skuteczniejsze zarządzanie powierzchnią ataku. Takie podejście jest kluczowe z punktu widzenia identyfikacji potencjalnych luk i wzajemnych zależności, które mogą być niewidoczne w standardowej strukturze zarządzania zasobami.

Nieautoryzowane zasoby informatyczne

Jednym z głównych wyzwań, przed jakimi stają firmy w przypadku infrastruktury informatycznej, jest wyśledzenie licznych zasobów, które funkcjonują poza standardowymi procesami informatycznymi. W niektórych sytuacjach zasoby te są tymczasowymi systemami stworzonymi w celu ułatwienia realizacji danego projektu, lecz niewłaściwie usuniętymi, co skutkuje pozostawieniem długu technologicznego do wyeliminowania w późniejszym terminie. Jeśli takie zasoby informatyczne „zombie" pozostają przez długi czas bez zarządzania, tworzą łatwe do wykorzystania powierzchnie ataku. Alternatywnie zasoby mogą pojawić się jako nieautoryzowane technologie informatyczne (ang. *rogue IT*), takie jak rozwiązania SaaS zakupione przez dział firmy we własnym zakresie i przez niego używane.

Niezależnie od rodzaju nieautoryzowane technologie informatyczne tworzą powierzchnie ataku, które nie są śledzone ani zarządzane, narażając firmę na długotrwałe ryzyko. W wielu przypadkach tego rodzaju narażenie może utrzymywać się nawet w trakcie incydentu, a firma dowiaduje się o włamaniu dopiero po powiadomieniu o nim przez kogoś z zewnątrz.

W procesie wykrywania podatności szczególnie cenne jest zarządzanie powierzchnią ataku, które pozwala identyfikować ryzyka oraz zarządzać nimi. Są one związane z nieautoryzowanymi rozwiązaniami informatycznymi (zostanie to omówione bardziej szczegółowo w rozdziale 4.), systemami starszej generacji i dynamicznymi środowiskami chmurowymi. W przypadku ASM wykrywanie zagrożeń uwzględnia lokalizowanie niezarządzanych, przestarzałych lub zapomnianych systemów w sieci, które mogą stanowić znaczące zagrożenie dla bezpieczeństwa ze względu na brak ich regularnej konserwacji i monitorowania.

Środowiska chmurowe są częstym miejscem występowania nieautoryzowanych zasobów informatycznych, co sprawia, że ASM jest nieodzowne do utrzymania widoczności w tych dynamicznych środowiskach. Zapewniając pełne pokrycie i ciągłe monitorowanie, ASM gwarantuje, że wszystkie zasoby, niezależnie od ich lokalizacji czy złożoności, są uwzględnione i zabezpieczone.

Tak wszechstronne podejście do identyfikowania oraz zarządzania ekspozycją na zagrożenia jest kluczowe dla firm, aby mogły utrzymywać silną kondycję cyberbezpieczeństwa cechującą się odpornością, zwłaszcza w obliczu coraz bardziej zróżnicowanych i rozproszonych infrastruktur informatycznych.

Zarządzanie ryzykiem

ASM pomaga firmom skutecznie ograniczać i rozumieć zagrożenia w obszarze cyberbezpieczeństwa. Zapewnia ono kontekstowe analizowanie elementów ryzyka, umożliwiając organizacjom ocenę zagrożeń pod kątem ich znaczenia i potencjalnego wpływu na operacje biznesowe. Ocena ta ma kluczowe znaczenie w rozpoznawaniu tego, jakie zagrożenia stanowią największe niebezpieczeństwo dla zasobów i celów firmy. Skupienie ASM na znaczących elementach ryzyka sprowadza się do ustalania priorytetów różnych alertów bezpieczeństwa i informacji, aby ułatwić skoncentrowanie wysiłków na łagodzeniu najbardziej wpływowych zagrożeń, optymalizując tym samym alokację zasobów i skuteczność odpowiedzi.

Dalsze rozszerzanie możliwości zarządzania ryzykiem polega na zastosowaniu ASM do proaktywnego wykrywania zagrożeń. Wykorzystuje ono strategie i narzędzia do identyfikacji potencjalnych zagrożeń, zanim przerodzą się one w pełnowymiarowe ataki. Takie wyprzedzające podejście w przypadku ASM gwarantuje, że firmy nie tylko reagują na zagrożenia, ale są o krok do przodu w przewidywaniu i neutralizowaniu potencjalnych elementów ryzyka w obszarze cyberbezpieczeństwa.

Nadążanie za dynamicznym „krajobrazem" zagrożeń

Szybkie tempo zmian we współczesnych środowiskach informatycznych zostało znacznie przyspieszone przez powszechne adaptowanie technologii chmury. W ciągu kilku ostatnich lat drastycznie wzrosła szybkość, z jaką programiści mogą tworzyć i implementować nowe funkcjonalności oprogramowania. Zmiany, które kiedyś zajmowały tygodnie lub miesiące, obecnie można wprowadzić w ciągu kilku dni. Przyspieszone tempo rozwoju i wdrażania, choć korzystne pod względem efektywności i innowacyjności, często przewyższa możliwości tradycyjnych mechanizmów bezpieczeństwa aplikacji. Istniejące procesy zabezpieczeń opracowane z myślą

o bardziej rozłożonych w czasie cyklach projektowych z trudem nadążają za tym dużym tempem, pozostawiając potencjalne luki w zabezpieczeniach podczas wdrażania lub aktualizowania nowego oprogramowania.

ASM odgrywa kluczową rolę w umożliwieniu firmom dostosowania się do tego przyspieszonego tempa zmian. Zapewniając pełny i aktualny widok powierzchni ataku, zarządzanie to pomaga organizacjom zidentyfikować i skupić się na obszarach najbardziej dotkniętych nagłymi zmianami. To skupienie jest konieczne, ponieważ są to obszary, w których z największym prawdopodobieństwem pojawią się podatności o największym wpływie. ASM umożliwia firmom sprawne identyfikowanie i eliminowanie pojawiających się podatności, zapewniając, że środki bezpieczeństwa ewoluują wraz ze środowiskiem informatycznym.

Nadawanie priorytetu ryzykom

ASM stanowi istotną korzyść w ramach złożonego zadania ustalania priorytetów elementów ryzyka, zwłaszcza w kontekście nowoczesnego środowiska zaawansowanych narzędzi zabezpieczeń. Umożliwiają one firmom wykrywanie różnorodnych podatności w ich sieciach, systemach i aplikacjach, oferując niezrównany i obszerny wgląd w zakres cyberbezpieczeństwa. Choć zwiększona zdolność wykrywania prowadzi do znacznego napływu danych i potencjalnych zagrożeń dotyczących bezpieczeństwa, zarządzanie ASM przekształca to wyzwanie w korzyść. Wyposaża ono zespoły ds. bezpieczeństwa w możliwość efektywnego przetwarzania ogromnej liczby alertów, pozwalając im skutecznie identyfikować i nadawać priorytety najgroźniejszym lukom. Ustalanie priorytetów ma zasadnicze znaczenie, gdyż zapewnia, że najbardziej znaczące zagrożenia są usuwane w pierwszej kolejności przy użyciu odpowiednich zasobów. Oznacza to optymalizowanie odpowiedzi organizacji na potencjalne incydenty związane z bezpieczeństwem.

Określanie priorytetów elementów ryzyka stało się coraz bardziej złożonym, ale niezbędnym zadaniem, szczególnie w świetle postępu w dziedzinie narzędzi zabezpieczeń. Te zaawansowane narzędzia umożliwiają firmom wykrywanie szerokiego i zróżnicowanego spektrum luk w ich sieciach, systemach i aplikacjach. Choć ta zwiększona zdolność wykrywania jest niewątpliwie korzystna, powoduje ona też zalew danych dotyczących potencjalnych zagrożeń w zakresie bezpieczeństwa. Ten napływ może być często przytłaczający, prowadząc do powstania środowiska, w którym zespoły ds. bezpieczeństwa są zasypywane alertami. Scenariusz ten stwarza znaczące wyzwania polegające na rozróżnieniu, które luki stanowią największe zagrożenie, a ponadto ustalenie kolejności, w jakiej należy się nimi zająć.

Sama ilość wykrytych luk może prowadzić do sytuacji, w której poważniejsze zagrożenia giną w szumie mniej istotnych problemów. W rezultacie kluczowa jest zdolność do skutecznego ustalania priorytetów elementów ryzyka. Wymaga ona zrozumienia technicznych aspektów każdej luki oraz dużej świadomości ich potencjalnego wpływu na szersze działania i cele firmy. Określanie priorytetów zapewnia, że najistotniejsze luki są szybko eliminowane, co minimalizuje ryzyko poważnych włamań lub zakłóceń w kluczowych funkcjach firmy. W konsekwencji rola zespołów ds. bezpieczeństwa ewoluuje od zwykłego reagowania na alerty do strategicznego zarządzania ryzykiem opartego na pełnym zrozumieniu „krajobrazu" cyberzagrożeń i unikatowych podatności firmy.

W obliczu wszystkich wykrywanych luk firmy stają przed większym wyzwaniem w postaci zarządzania ustalaniem priorytetów na podstawie ryzyka, co bardziej szczegółowo zostanie omówione w rozdziale 5. Skuteczne określanie priorytetów elementów ryzyka nie polega wyłącznie na identyfikacji najbardziej znaczących zagrożeń, ale także na dostosowaniu reakcji na te zagrożenia do dostępnych zasobów firmy. Obejmuje to uwzględnienie dostępności personelu technicznego, zrozumienie ograniczeń budżetowych oraz ocenę możliwości wdrożenia konkretnych środków bezpieczeństwa. Ustalając priorytety elementów ryzyka w kontekście tych ograniczeń, firmy mogą zapewnić bardziej efektywną alokację swoich ograniczonych zasobów. Takie strategiczne podejście gwarantuje, że najpoważniejsze luki są szybko usuwane przy odpowiednim poziomie pilności. Maksymalizuje to zatem wpływ działań firmy dotyczących cyberbezpieczeństwa w ramach jej ograniczonych możliwości operacyjnych.

Podstawową kwestią jest określenie kontekstu podatności w strukturze operacji biznesowych w celu umożliwienia ustalenia priorytetów. Niezbędne jest dogłębne zrozumienie kontekstu biznesowego każdej luki. Proces ten pozwala ocenić, w jaki sposób konkretna luka może wpłynąć na infrastrukturę informatyczną oraz szersze operacje i cele biznesowe. Na ogólnym poziomie podstawowe czynniki w ramach tej oceny obejmują:

- Poziom istotności zagrożonego systemu dla kluczowych funkcji biznesowych.
- Typ zagrożonych danych (osobowe, finansowe lub poufne informacje korporacyjne).
- Potencjalne konsekwencje naruszenia zabezpieczeń dla reputacji i sytuacji prawnej firmy.

Umieszczając te elementy w kontekście, firmy mogą dokładniej kategoryzować luki w zabezpieczeniach na podstawie ich potencjalnego wpływu na operacje biznesowe. Umożliwia to bardziej strategiczną i ukierunkowaną odpowiedź, zapewniając, że zasoby i wysiłki służą zmniejszaniu skali elementów ryzyka stanowiących największe zagrożenie dla podstawowych celów i funkcji firmy.

Ryzyko związane z fuzjami i przejęciami

ASM przynosi znaczące korzyści, eliminując zawiłości związane z szybkim rozszerzaniem się powierzchni ataku. Gdy firma przejmuje inną firmę, zyskuje nowe zasoby, a także dziedziczy związane z nimi zagrożenia dla bezpieczeństwa. ASM odgrywa kluczową rolę w systematycznej ocenie kondycji bezpieczeństwa i potencjalnych podatności nowo przyłączonego podmiotu. Umożliwia ono całkowity wgląd we wszystkie zasoby, w tym sprzęt, oprogramowanie, zasoby cyfrowe, konta użytkowników i repozytoria danych, co jest niezbędne do zrozumienia pełnego zakresu rozszerzonej powierzchni ataku.

ASM nie opiera się na założeniu istnienia bezpośredniego zaufania między przedsiębiorstwami. Zamiast tego kluczowym, wstępnym krokiem procesu zarządzania jest rygorystyczna weryfikacja powierzchni ataku w celu upewnienia się, że wszystkie zasoby, podatności i zagrożenia zostały dokładnie zidentyfikowane i ocenione. Weryfikacja ta jest niezbędna do ustanowienia solidnych podstaw na potrzeby ASM. Po przeprowadzeniu weryfikacji może być ono systematycznie stosowane do zarządzania ryzykiem związanym z powierzchnią ataku i jego ograniczania. Ustanowienie rygorystycznych standardów weryfikacji powierzchni ataku zapewnia, że strategie ASM opierają się na dokładnych danych i mogą skutecznie chronić firmę przed potencjalnymi naruszeniami zabezpieczeń.

Efektywne wykorzystanie ASM pozwala pokonać wyzwania wynikające z różnic w infrastrukturze bezpieczeństwa oraz obecności wcześniej nieznanych lub niezarządzanych zasobów. Zapewniając jasną i dokładną ocenę nowej, połączonej powierzchni ataku, ASM umożliwia podejmowanie świadomych decyzji i strategiczne planowanie zabezpieczeń, gwarantując, że rozszerzone środowisko cyfrowe firmy jest bezpieczne i odporne.

Reagowanie na incydenty i ustalanie priorytetów

ASM doskonale sprawdza się w usprawnianiu reakcji na incydenty i ustalaniu związanych z nimi priorytetów. Dzięki temu zarządzaniu uzyskuje się lepszą widoczność wykorzystania zasobów, co pozwala na dokładniejsze i pełniejsze zrozumienie sposobu użytkowania zasobów sieciowych. Widoczność ta jest niezbędna do szybkiego wykrywania anomalii, które mogą wskazywać na potencjalne zagrożenia lub naruszenia.

Ponadto ASM pomaga w szybkim wykrywaniu anomalii, umożliwiając organizacjom błyskawiczną identyfikację i reakcję na nietypowe działania, które mogą sygnalizować naruszenie zabezpieczeń. Szybkie wykrycie jest niezbędne do zminimalizowania skutków takich incydentów. ASM wykorzystuje zautomatyzowane generowanie alertów i efektywne mechanizmy rozwiązywania problemów. Systemy te są tak zaprojektowane, aby automatycznie ostrzegać zespoły ds. bezpieczeństwa o potencjalnych zagrożeniach i usprawnić proces reagowania i usuwania problemów. Automatyzacja skraca czas reakcji i zapewnia lepiej zorganizowane i praktyczne podejście do zarządzania incydentami dotyczącymi bezpieczeństwa.

Usprawnienie reagowania na incydenty

Zarządzanie powierzchnią ataku znacząco usprawnia reagowanie na incydenty przez dostarczanie dokładnego odwzorowania wszystkich potencjalnych punktów wejścia do sieci firmy. Takie kompletne odwzorowanie obejmuje zarówno oczywiste, jak i mniej widoczne punkty dostępu, które mogą zostać wykorzystane przez cyberprzestępców. ASM umożliwia firmom wdrożenie proaktywnych środków obrony drogą identyfikacji tych potencjalnych luk. Środki te mogą obejmować wzmocnienie zapór sieciowych, wprowadzenie bardziej rygorystycznych mechanizmów kontroli dostępu oraz ciągłe monitorowanie punktów wejścia pod kątem nietypowych działań.

W razie naruszenia zabezpieczeń szczegółowa znajomość punktów wejścia w przypadku ASM ułatwia szybkie zidentyfikowanie źródła włamania. Szybkie zlokalizowanie początkowego punktu ataku jest kluczowe do zapewnienia skutecznej i szybkiej odpowiedzi, co ma zasadnicze znaczenie z punktu widzenia ograniczenia rozprzestrzeniania się efektów włamania i zmniejszenia jego ogólnego wpływu.

Narzędzia do ASM oferują wgląd w działania podejmowane przez atakujących po przeniknięciu do systemu. Umożliwiają one firmom śledzenie ruchów atakujących w ich sieciach oraz identyfikowanie danych lub zasobów, do których uzyskano dostęp lub włamano się. Śledzenie jest niezbędne do oceny pełnego zakresu incydentu. Dzięki ASM organizacje mogą dokładniej określić skalę włamania i podjąć kroki konieczne do powstrzymania go i złagodzenia jego skutków.

Wnioski wyciągnięte z obserwacji zachowania atakujących i zrozumienie wpływu ich działań są bezcenne dla przyszłego planowania zabezpieczeń. Pozwalają one firmom udoskonalić swoje strategie ASM, dostosowując je pod kątem lepszego przewidywania i przeciwdziałania przyszłym zagrożeniom dzięki zrozumieniu motywacji i metod stojących za atakami dotyczącymi konkretnych obszarów ich sieci.

Przydział zasobów

ASM oferuje znaczące korzyści w zakresie alokacji zasobów pomimo nieodłącznych wyzwań stawianych przez ograniczone zasoby. Przewaga ASM polega na możliwości ułatwienia planowania strategicznego i optymalizacji tych zasobów. Dzięki skutecznemu identyfikowaniu i ustalaniu priorytetów potencjalnych zagrożeń i luk w środowisku informatycznym firmy ASM umożliwia bardziej ukierunkowane i efektywne przydzielanie zasobów. Takie podejście gwarantuje, że najbardziej kluczowym obszarom powierzchni ataku zapewnia się niezbędną uwagę i wymagane zasoby, poprawiając ogólny stan bezpieczeństwa przy optymalnym wykorzystaniu zasobów.

Inwestycje w bezpieczeństwo informacji muszą być starannie zaplanowane, ponieważ wszystkie budżety są z natury ograniczone. Kluczowy jest wybór narzędzi i technologii, które oferują wymierne korzyści i wszechstronność. Przykładem są narzędzia zdolne do skanowania podatności w różnych środowiskach, takich jak środowiska lokalne i chmurowe, zamiast ograniczania się do tylko jednego obszaru. Takie podejście nie tylko zapewnia efektywność, ale także maksymalizuje zwrot z inwestycji. Ponadto zespoły ds. bezpieczeństwa informacji często znajdują się w sytuacji wymagającej konkurowania, gdy rywalizują o fundusze z innymi działami. Aby zapewnić sobie niezbędne zasoby, wymaga to jasnego przedstawienia kierownictwu wyższego szczebla wymiernych korzyści i znaczenia inwestycji związanych z bezpieczeństwem.

Ciągłe szkolenia i rozwijanie umiejętności zespołu ds. bezpieczeństwa także odgrywają kluczową rolę w alokacji zasobów. Nadążanie za najnowszymi technologiami i zagrożeniami wymaga ciągłych szkoleń, co wiąże się z inwestowaniem i tak już ograniczonych zasobów. Pojawienie się technologii chmury obliczeniowej to doskonały przykład tego, jak brak umiejętności w zakresie nowych technologii może prowadzić do poważnych naruszeń zabezpieczeń, takich jak te wynikające z błędnie skonfigurowanych usług chmurowych. Liczne przypadki włamań spowodowanych niewłaściwą konfiguracją zasobników usługi S3 (S3 buckets), które ujawniły dane poufne, dobitnie przypominają o tym problemie.

Zespoły ds. bezpieczeństwa nieustannie zmagają się z równoważeniem działań operacyjnych związanych z bezpieczeństwem i wdrażaniem nowych, bardziej odpornych środków kontroli zabezpieczeń. Skierowanie zasobów do jednego obszaru nieuchronnie ogranicza ich dostępność w innych. Sytuację komplikuje fakt, że członkowie zespołu mają ograniczoną liczbę godzin pracy w tygodniu, które muszą być rozważnie przeznaczone na realizowanie codziennych operacji i wprowadzanie proaktywnych środków bezpieczeństwa. Osiągnięcie tej równowagi jest kluczowe, ponieważ oba aspekty są niezbędne do utrzymania bezpiecznej i odpornej firmy.

Wymuszanie zasad

ASM odgrywa kluczową rolę w przypadku wymuszania zasad, a zwłaszcza zapewniania w firmach zgodności i przestrzegania przepisów. W obliczu złożoności współczesnego świata cyberbezpieczeństwa przestrzeganie różnych norm prawnych i regulacyjnych jest nie tylko obowiązkowe, ale niezbędne do utrzymania integralności i zaufania organizacji. ASM ułatwia to zadanie, zapewniając ramy, dzięki którym firmy mogą zagwarantować, że ich działania, zwłaszcza w obszarze rozwiązań informatycznych i cyberbezpieczeństwa, są zgodne z wymogami prawnymi i regulacyjnymi.

Wymogi zgodności i przestrzegania przepisów

Skutecznie skorzystanie z ASM pomaga firmie dostosować się do wymogów prawnych i regulacyjnych oraz wewnętrznych zasad dotyczących przetwarzania i ochrony danych. Wymogi zgodności i przestrzegania przepisów mają na celu respektowanie prawa i ochronę firmy przed potencjalnymi naruszeniami zabezpieczeń i ich konsekwencjami. ASM zapewnia organizacjom wgląd i możliwość zrozumienia, w jaki sposób ich dane są narażone, umożliwiając im dostosowanie środków kontroli do obszernego zestawu następujących wymagań branżowych i rządowych:

Nadzór wewnętrzny

W kontekście cyberbezpieczeństwa odnosi się to do zestawu zasad, procedur i środków kontroli ustanowionych przez firmę w celu efektywnego zarządzania jej działaniem i związanymi z nimi zagrożeniami. Ten aspekt nadzoru jest niezbędny do określenia, w jaki sposób identyfikowane, oceniane i ograniczane są elementy ryzyka związane z cyberbezpieczeństwem. Skuteczny nadzór wewnętrzny wymaga pełnego zrozumienia apetytu na ryzyko firmy, co ma wpływ na proces opracowywania solidnych zasad z zakresu cyberbezpieczeństwa.

Regulacje zewnętrzne

Zgodność z przepisami zewnętrznymi jest kluczowa z punktu widzenia strategii firmy dotyczącej cyberbezpieczeństwa. Przepisy takie jak amerykańska ustawa HIPAA (*Health Insurance Portability and Accountability Act*), ustawa Sarbanesa-Oxleya lub ogólne rozporządzenie o ochronie danych (RODO) określają dla firm konkretne wymagania dotyczące cyberbezpieczeństwa. Na przykład ustawa HIPAA koncentruje się na ochronie informacji o zdrowiu pacjentów, ustawa Sarbanesa-Oxleya dotyczy integralności danych finansowych, a rozporządzenie RODO kładzie nacisk na ochronę praw do danych osobowych w Unii Europejskiej. Przestrzeganie tych przepisów jest obowiązkowe, a brak zgodności z nimi może skutkować znacznymi karami finansowymi, konsekwencjami prawnymi i utratą reputacji. Zrozumienie niuansów każdego prawa mającego zastosowanie w przypadku Twojej firmy pomaga w dostosowaniu strategii odnoszącej się do cyberbezpieczeństwa, aby zapewnić zgodność i uniknąć potencjalnych konsekwencji jej braku.

Wymogi branżowe

Oprócz ogólnych wymagań wynikających z przepisów niektóre branże podlegają konkretnym wymogom określającym standardy cyberbezpieczeństwa. Na przykład standard PCI DSS (*Payment Card Industry Data Security Standard*) jest kluczowy dla firm obsługujących transakcje kartami kredytowymi. Standard SOC 2 (*Service Organization Control 2*)

jest istotny w przypadku dostawców usług, a standard ISO 27001 jest nieodzowny przy zarządzaniu bezpieczeństwem informacji. Te wymogi branżowe oferują uporządkowaną strukturę dla najlepszych praktyk w zakresie cyberbezpieczeństwa i zazwyczaj wymagają od organizacji regularnego raportowania i audytów zgodności. Przestrzeganie tych wymogów to nie tylko spełnianie wymagań zawartych w przepisach. Odgrywa to również znaczącą rolę w procesie budowania i utrzymywania zaufania klientów i partnerów. Demonstrowanie zaangażowania w rygorystyczne standardy cyberbezpieczeństwa przez zapewnienie zgodności z wymogami branżowymi odzwierciedla zaangażowanie firmy w ochronę własnych danych oraz danych jej klientów i interesariuszy.

Poziom zgodności jest dodatkowo zwiększany przez rolę ASM w procesie usprawniania raportowania i tworzenia dokumentacji. Dzięki utrzymywaniu szczegółowych rejestrów i generowaniu kompleksowych raportów ASM wspiera przejrzystość i odpowiedzialność w zakresie praktyk dotyczących cyberbezpieczeństwa. Te rejestry i raporty są niezbędne do wykazania zgodności podczas audytów i przeglądów, a ponadto pełnią funkcję nieocenionych zasobów w procesie ciągłego doskonalenia praktyk bezpieczeństwa.

Podsumowanie

Po przeczytaniu tego rozdziału powinieneś lepiej rozumieć zagadnienie zarządzania powierzchnią ataku i jego fundamentalną rolę w obszarze cyberbezpieczeństwa. Zaczynając od przejrzystej definicji ASM, przeanalizowaliśmy kompleksowy charakter powierzchni ataku organizacji, obejmującej sprzęt, systemy oprogramowania oraz czynniki ludzkie obecne przy interakcji z tymi technologiami.

W miarę jak firmy coraz częściej włączają do swojej infrastruktury zaawansowane technologie, takie jak chmura obliczeniowa, IoT oraz sztuczna inteligencja, złożoność i zakres ich powierzchni ataku zwiększają się, powodując unikatowe wyzwania w zakresie bezpieczeństwa. ASM jest ciągłym i proaktywnym środkiem obrony przed pojawiającymi się zagrożeniami, dostosowującym się do zmian technologicznych i elementów ryzyka, aby zapobiegawczo reagować na zagrożenia, zanim atakujący zdążą je wykorzystać.

Przyjrzymy się bliżej w dalszej kolejności konkretnym typom powierzchni ataku. Omówimy, jak ewoluowały one od tradycyjnych środowisk do obecnego nowoczesnego i rozwijającego się ekosystemu informatycznego. Zagłębimy się w to, jak każdy składnik, począwszy od starszych systemów, a skończywszy na zaawansowanych rozwiązaniach chmurowych, przyczynia się do tworzenia organizacyjnej powierzchni ataku i jak doprowadziło to do potrzeby opracowania dostosowanych strategii bezpieczeństwa, które odpowiadają na unikatowe wyzwania stawiane przez te różnorodne elementy. Zrozumienie specyfiki każdego typu powierzchni ataku pozwoli lepiej przygotować się na poradzenie sobie ze złożonością zabezpieczeń w środowisku Twojej firmy.

Pozycja obowiązkowa dla osób, które na poważnie chcą zminimalizować i chronić narażone obszary.

Steve Winterfeld, ekspert do spraw cyberbezpieczeństwa

Pojęcie *powierzchni ataku* oznacza całość punktów dostępu, przez które możliwe jest dokonanie cyberataku. Bardzo często powierzchnia ataku jest rozległa, rozproszona i nieustannie się zmienia, co stanowi idealne pole działania dla cyberprzestępców. Okazuje się, że zarządzanie powierzchnią ataku to podstawa rozsądnego zabezpieczenia zasobów cyfrowych.

W tym kompleksowym przewodniku znajdziesz przejrzysty plan działania, który pozwoli Ci krok po kroku przeanalizować stan ekspozycji organizacji na zagrożenia, a następnie opracować i wdrożyć skuteczną strategię zarządzania powierzchnią ataku. Dowiesz się, jak uczynić ją częścią kluczowych procesów bezpieczeństwa — od reagowania na incydenty, przez metodyki DevOps, po zapewnianie zgodności z regulacjami. Dzięki tej książce w pełni zrozumiesz zasady zarządzania powierzchnią ataku i nauczysz się przejmować kontrolę nad swoimi zasobami, zanim zrobią to atakujący.

W książce:

- zarządzanie powierzchnią ataku w cyberbezpieczeństwie
- metody oceny i odwzorowywania powierzchni ataku organizacji
- strategie identyfikacji, klasyfikacji i ustalania priorytetów kluczowych zasobów
- powiązanie technicznych podatności z ryzykiem biznesowym
- zasady ciągłego monitorowania
- eliminacja luk w zabezpieczeniach

Ron Eddings jest współzałożycielem firmy Hacker Valley Media. Wcześniej doradzał największym organizacjom, a także pełnił funkcję architekta do spraw bezpieczeństwa w Intel Corporation i Palo Alto Networks.

MJ Kaufmann jest założycielką Write Alchemist. Jako profesor akademicki realizowała pionierskie projekty z zakresu cyberbezpieczeństwa na Uniwersytecie Stanu Floryda, współpracowała też z takimi firmami jak Bitdefender, Cisco i Snyk.

Helion

helion.pl

HELION S.A.
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!

ISBN 978-83-289-3269-2

9 788328 932692

Cena: 99,00 zł