Wydanie III

Cyberbezpieczeństwo
Strategie ataku i obrony

Jak osiągnąć najwyższy możliwy stan zabezpieczeń systemu informatycznego

Yuri Diogenes
Erdal Ozkaya

Helion
Packt

Tytuł oryginału: Cybersecurity - Attack and Defense Strategies: Improve your security posture to mitigate risks and prevent attackers from infiltrating your system, 3rd Edition

Tłumaczenie: Lech Lachowski

ISBN: 978-83-8322-421-3

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

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

Printed in Poland.

Spis treści

ROZDZIAŁ 9

Czym jest cyberstrategia?

Rozdział 3

Cyberstrategia to udokumentowane podejście do różnych aspektów cyberprzestrzeni. Jest opracowywana głównie w celu zaspokojenia potrzeb cyberbezpieczeństwa określonego podmiotu przez zdefiniowanie sposobu ochrony danych, sieci, systemów technicznych i ludzi. Skuteczna cyberstrategia jest zwykle powiązana ze stopniem ryzyka naruszenia cyberbezpieczeństwa podmiotu. Obejmuje wszystkie możliwe wektory ataków, które mogą być wykorzystywane przez złośliwe strony zewnętrzne.

W większości cyberstrategii centralne miejsce zajmuje cyberbezpieczeństwo, gdyż zagrożenia cybernetyczne stają się coraz bardziej zaawansowane, w miarę jak dla aktorów zagrożenia stają się dostępne coraz lepsze narzędzia i techniki eksploitacji. W związku z tymi zagrożeniami zaleca się organizacjom opracowanie cyberstrategii, które zapewnią ochronę ich infrastruktury cybernetycznej i zmniejszą ryzyko.

W tym rozdziale zostaną omówione następujące tematy:

- budowanie strategii marketingowej;
- cele budowania cyberstrategii;
- najlepsze strategie cyberataków;
- najlepsze strategie cyberobrony;
- korzyści z posiadania proaktywnej strategii cyberbezpieczeństwa;
- najlepsze strategie cyberbezpieczeństwa dla firm.

Zacznijmy od omówienia podstawowych elementów potrzebnych do zbudowania cyberstrategii.

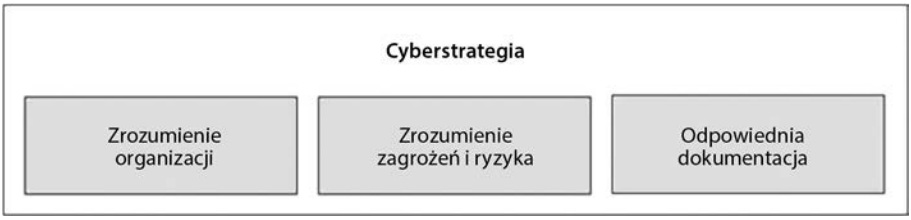
Jak zbudować cyberstrategię?

W VI w. p.n.e. Sun Tzu powiedział: „Jeśli znasz siebie i swego wroga, przetrwasz pomyślnie sto bitew.

Jeśli nie poznasz swego wroga, lecz poznasz siebie, jedną bitwę wygrasz, a drugą przegrasz. Jeśli nie poznasz ni siebie, ni wroga, każda potyczka będzie dla ciebie zagrożeniem".

Ten cytat wciąż ma zastosowanie do cyberstrategii i wyjaśnia, dlaczego tak ważne jest zrozumienie zarówno swojej firmy, jak i zagrożeń, jakie stwarzają dla niej cyberprzestępcy — będzie to stanowić podstawę silnej cyberstrategii, która pomoże chronić Twoją firmę przed atakiem.

Do zbudowania cyberstrategii będziesz potrzebować trzech głównych filarów, dzięki którym utworzysz solidne fundamenty. Pokazaliśmy to na rysunku 3.1.



Rysunek 3.1. Podstawy cyberstrategii

Te trzy komponenty mają kluczowe znaczenie dla zrozumienia, co zapewnia skuteczność cyberstrategii.

1. Zrozumienie organizacji

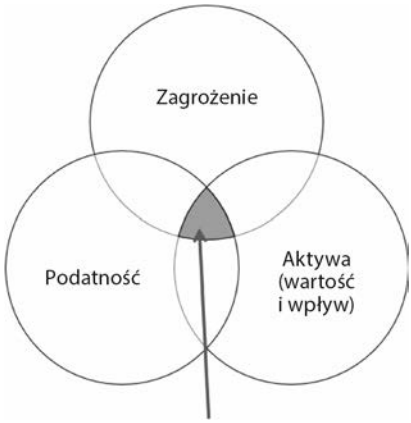
Im więcej wiesz o swojej firmie, tym lepiej możesz ją zabezpieczyć. Bardzo ważne jest, aby poznać cele i zadania swojej organizacji, ludzi, z którymi się pracuje, branżę i jej aktualne trendy, a także ryzyko, jakie grozi firmie, oraz jej apetyt na ryzyko i najcenniejsze aktywa. Posiadanie kompletnego spisu aktywów jest niezbędne do ustalenia priorytetów planów strategicznych na podstawie ryzyka i wpływu ataku na te aktywa. Wszystko, co robimy, musi odzwierciedlać wymagania biznesowe zatwierdzone przez kierownictwo wyższego szczebla.

2. Zrozumienie zagrożeń i ryzyka

Nie jest łatwo zdefiniować ryzyko, ponieważ słowo „ryzyko" jest używane na wiele różnych sposobów. Chociaż istnieje wiele definicji tego terminu, norma ISO 31000 definiuje ryzyko jako „wpływ niepewności na cele", gdzie wpływ określa pozytywne lub negatywne odchylenie od stanu oczekiwanego. W tym przypadku posłużymy się definicją ryzyka z normy ISO.

Słowo „ryzyko" łączy w sobie trzy elementy: zaczyna od potencjalnego zdarzenia, a następnie łączy jego prawdopodobieństwo z jego potencjalną dotkliwością. W wielu szkoleniach na temat zarządzania ryzykiem ryzyko jest definiowane następująco (zobacz rysunek 3.2):

Ryzyko (potencjalna strata) = zagrożenie · podatność · aktywa



Rysunek 3.2. Ilustracja definicji ryzyka

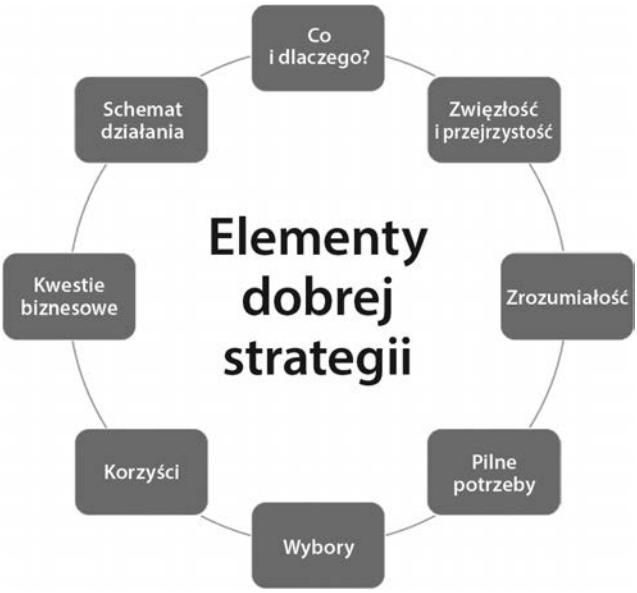
Trzeba zrozumieć, że nie do wszystkich zagrożeń warto stosować środki zaradcze. Jeśli środki zaradcze będą kosztowniejsze niż wdrożenie albo ryzyko nie będzie poważne, może ono zostać zaakceptowane.

3. Odpowiednia dokumentacja

Dokumentacja działa jako rodzaj normalizacji różnych procesów, która zapewnia, że wszyscy w organizacji pracują w ten sam sposób i dążą do tego samego wyniku. Jest to kluczowy aspekt każdej strategii i odgrywa szczególnie ważną rolę, jeśli chodzi o zapewnienie ciągłości działania firmy. Dokumentowanie planu cyberstrategii zapewni wydajność, spójność i spokój ducha wszystkim zaangażowanym stronom. Dokumentacja nie powinna być jednak traktowana jako działanie jednorazowe, ponieważ nawet po spisaniu planu cyberstrategii nadal będzie wymagała aktualizowania w celu odzwierciedlania zmian w krajobrazie cyberbezpieczeństwa.

Na rysunku 3.3 pokazaliśmy przykład tego, co powinna uwzględniać dobra dokumentacja cyberstrategii.

Możemy podsumować, że cyberstrategia to plan zarządzania ryzykiem bezpieczeństwa organizacyjnego zgodnie z firmową definicją tolerancji ryzyka z zamiarem realizacji celów biznesowych i organizacyjnych. Cyberstrategia powinna być w pełni zgodna ze strategią biznesową, a także z czynnikami i celami biznesowymi. Po zapewnieniu tej zgodności można budować aspekty techniczne i zwiększać poziom bezpieczeństwa cyberstrategii w cyberprzestrzeni. Omówimy te aspekty dalej w rozdziale, ale teraz, gdy znasz już podstawy opracowywania cyberstrategii, poświęćmy chwilę na omówienie korzyści, jakie przynosi jej wdrożenie.



Rysunek 3.3. Elementy, które powinien uwzględniać plan cyberstrategii

Dlaczego trzeba budować cyberstrategię?

Organizacje stale zmagają się z zagrożeniami, jakimi są ataki przeprowadzane przez zatwardziałych profesjonalnych cyberprzestępców. Smutna rzeczywistość jest taka, że wiele włamań przeprowadzają państwa narodowe, cyberterroryści i potężne grupy cyberprzestępcze. Istnieje czarny rynek dla hakerów, który ułatwia zakup lub wynajem narzędzi, technik i personelu do dokonywania włamań, a ponadto umożliwia pranie pieniędzy pozyskanych z udanych ataków. Nierzadko atakujący mają znacznie większą wiedzę techniczną w zakresie cyberbezpieczeństwa niż przeciętny pracownik działu IT. Dlatego atakujący mogą wykorzystać swoją zaawansowaną wiedzę, aby łatwo ominąć wiele narzędzi cyberobrony skonfigurowanych przez działy IT w wielu organizacjach.

Wymaga to zatem przedefiniowania sposobu, w jaki organizacje powinny radzić sobie z zagrożeniami cybernetycznymi i aktorami zagrożeń, gdyż pozostawienie tych zadań działowi IT nie jest wystarczające. Chociaż jeszcze kilka lat temu zwiększanie poziomu zabezpieczenia systemów i instalowanie większej liczby narzędzi bezpieczeństwa mogło się sprawdzać, dziś organizacje potrzebują dobrze przemyślanej cyberstrategii, która będzie kierować działaniami z zakresu cyberobrony. Oto niektóre z powodów, dla których cyberstrategie są niezbędne:

- Cyberstrategie dostarczają szczegółowych informacji na temat taktyki bezpieczeństwa — określają ogólne taktyki zapewnienia bezpieczeństwa organizacji. Taktyki te dotyczą procesów reagowania na incydenty, planów przywracania sprawności po katastrofie i ciągłości biznesowej oraz reakcji behawioralnych na ataki, aby pomóc dodatkowo uspokoić interesariuszy. Mogą być pomocne w informowaniu interesariuszy o gotowości organizacji do radzenia sobie z cyberatakami.
- Cyberstrategie odchodzą od założeń — niektóre defensywne mechanizmy cyberbezpieczeństwa stosowane obecnie w organizacjach opierają się na założeniach przyjmowanych przez dział IT lub konsultantów ds. cyberbezpieczeństwa. Zawsze istnieje jednak ryzyko, że te założenia mogą być mylące i być może dostosowane tylko do określonego celu, takiego jak zapewnianie zgodności z normami. Natomiast cyberstrategie to świadome plany działania obejmujące różne zagrożenia cybernetyczne i związane z nimi ryzyko. Ponadto ich opracowywaniu przyświeca wspólny cel końcowy: dostosowanie celów bezpieczeństwa do celów biznesowych.
- Cyberstrategie poprawiają działanie organizacji — zapewniają scentralizowaną kontrolę i podejmowanie decyzji w sprawach dotyczących cyberbezpieczeństwa, ponieważ są budowane we współpracy z różnymi interesariuszami. Gwarantuje to, że różne działy w organizacji mogą pracować w koordynacji, aby osiągnąć wspólny zestaw celów bezpieczeństwa. Menedżerowie liniowi mogą na przykład instruować młodszych pracowników, aby nie udostępniali danych logowania, co może zapobiec phishingowi. Zgodnie z cyberstrategią taki niewielki wkład różnych działów firmy pomaga poprawić ogólny stan zabezpieczeń organizacji.
- Cyberstrategia dowodzi długoterminowego zaangażowania w bezpieczeństwo — zapewnia, że organizacja będzie podejmować znaczące wysiłki i angażować istotne zasoby w celu zagwarantowania bezpieczeństwa. Takie zaangażowanie jest dobrym sygnałem dla interesariuszy, że organizacja pozostanie bezpieczna podczas ataków.
- Cyberstrategia upraszcza kwestie cyberbezpieczeństwa dla interesariuszy — pomaga zrozumieć złożone zagadnienia z zakresu cyberbezpieczeństwa. Informuje wszystkich interesariuszy o ryzyku i zagrożeniach w cyberprzestrzeni, a następnie wyjaśnia, w jaki sposób są one łagodzone za pośrednictwem zestawu niewielkich osiągalnych celów.

Możemy podsumować, że bez cyberstrategii nie zoptymalizujesz swojej inwestycji, nie nadasz priorytetu potrzebom firmy, a ogólny stan zabezpieczenia stanie się znacznie bardziej złożony.

Cyberstrategie mogą przyjmować dwa podejścia do kwestii bezpieczeństwa: perspektywę defensywną lub perspektywę ataku. W perspektywie defensywnej cyberstrategia koncentruje się na informowaniu interesariuszy o strategiach defensywy, które organizacja wdrożyła w celu ochrony przed zidentyfikowanymi zagrożeniami. Natomiast cyberstrategie przyjmujące perspektywę ataku mogą koncentrować się na udowodnieniu skuteczności istniejących zabezpieczeń, aby znaleźć wady i je naprawić. Dlatego strategie ataku mogą w szerokim zakresie obejmować różne metody, które będą wykorzystywane do testowania gotowości organizacji na atak. Niektóre strategie mogą być połączeniem tych dwóch perspektyw, uwzględniając testowanie i wzmacnianie istniejących mechanizmów defensywnych. Wybrane podejście będzie zależało od dostępnych zasobów i celów biznesowych. W następnych podrozdziałach omówimy niektóre powszechnie stosowane cyberstrategie ataku i defensywy.

Najlepsze cyberstrategie ataku

Jednym z najlepszych sposobów zabezpieczania organizacji jest myślenie z perspektywy hakera i podejmowanie prób naruszenia bezpieczeństwa organizacji przy użyciu tych samych narzędzi i technik, których użyłby przeciwnik.

Strategie defensywne można testować przez wykonywanie zewnętrznych testów spoza sieci lub testów wewnętrznych. Te procesy testowe mają na celu zapewnienie, że zaimplementowana strategia bezpieczeństwa będzie skuteczna i zgodna z celami procesów biznesowych.

W kolejnych punktach przedstawimy niektóre z najlepszych cyberstrategii ataku, jakie organizacje powinny wziąć pod uwagę podczas testowania swoich systemów.

Strategie testowania zewnętrznego

Te strategie testowania obejmują próby naruszenia bezpieczeństwa organizacji z zewnątrz, czyli spoza jej sieci. W takim przypadku w celach testowych cyberataki będą kierowane na publicznie dostępne zasoby. Można zaatakować firewall na przykład za pomocą ataku DDoS, aby uniemożliwić przepływ do sieci organizacji dozwolonego ruchu. Ataki kieruje się także na serwery pocztowe w celu zablokowania komunikacji e-mailowej w organizacji. Celem ataków mogą być również serwery WWW, na których można potencjalnie znaleźć niewłaściwie umieszczone pliki, takie jak poufne informacje przechowywane w publicznie dostępnych folderach. Do innych popularnych celów należą m.in. serwery nazw domenowych (ang. *Domain Name Server* — DNS) i systemy wykrywania włamań (ang. *Intrusion Detection System* — IDS), które zwykle są udostępniane publicznie. Poza systemami technicznymi zewnętrzne strategie testowania obejmują także ataki skierowane na personel lub użytkowników. Takie

ataki mogą być przeprowadzane za pośrednictwem platform mediów społecznościowych, e-maili i połączeń telefonicznych. Najczęściej stosowaną metodą ataku jest inżynieria społeczna, w której cele są przekonywane do dzielenia się poufnymi informacjami lub wysyłania pieniędzy, aby opłacić nieistniejące usługi, zapłacić okup itd., dlatego zewnętrzne strategie testowania powinny naśladować te ataki.

Strategie testowania wewnętrznego

Obejmują one ataki przeprowadzane w obrębie organizacji w celu naśladowania zagrożeń wewnętrznych, które mogą próbować złamać zabezpieczenia organizacji. Tego rodzaju zagrożenia mogą stanowić niezadowoleni pracownicy i goście ze złośliwymi intencjami. Wewnętrzne testy naruszenia bezpieczeństwa zawsze zakładają, że przeciwnik ma standardowe uprawnienia dostępu, zna miejsce przechowywania poufnych informacji i może uniknąć wykrycia, a nawet wyłączyć niektóre narzędzia bezpieczeństwa.

Celem testów wewnętrznych jest wzmocnienie zabezpieczeń systemów udostępnianych regularnym użytkownikom, aby utrudnić włamanie się do nich. Niektóre z technik stosowanych w testach zewnętrznych mogą być stosowane także w testach wewnętrznych, ale wewnątrz sieci ich wydajność często wzrasta, gdyż mają one do dyspozycji więcej celów.

Strategia testowania ślepego

Jest to strategia testowa, która ma na celu zaskoczenie organizacji. Testowanie odbywa się to przy ograniczonym informowaniu działu IT, aby jego pracownicy mogli potraktować je jako prawdziwy atak. Testowanie ślepe polega na atakowaniu narzędzi bezpieczeństwa, wykonywaniu prób złamania zabezpieczeń sieci i obieraniu za cel użytkowników, aby uzyskać od nich poświadczenia lub poufne informacje. Takie testowanie jest często kosztowne, ponieważ zespół testerów nie otrzymuje żadnej formy wsparcia ze strony działu IT, aby uniknąć ostrzegania go o planowanych atakach. Jednak często prowadzi do odkrycia wielu nieznanych luk w zabezpieczeniach.

Strategia testowania ukierunkowanego

Ten typ testów izoluje tylko jeden cel i przeprowadza na nim wiele ataków, aby odkryć te, które mogą się powieść. Jest to bardzo skuteczne podczas testowania nowych systemów lub określonych aspektów cyberbezpieczeństwa, takich jak reagowanie na incydenty związane z atakami wymierzonymi w kluczowe systemy. Jednak ze względu na wąski zakres testy ukierunkowane nie dają pełnych informacji na temat podatności na ataki całej organizacji.

Najlepsze cyberstrategie defensywne

Cyberbezpieczeństwo często sprowadza się głównie do systemów defensywnych wdrożonych przez organizację. Istnieją dwie strategie defensywne powszechnie stosowane przez organizacje: obrona w głąb i obrona wszerz.

Obrona w głąb

Obrona w głąb (ang. *defense in depth*) jest również określana jako zabezpieczanie warstwowe i obejmuje zastosowanie warstwowych mechanizmów defensywnych, aby utrudnić atakującym włamanie się do organizacji. Ponieważ stosuje się wiele warstw zabezpieczeń, po złamaniu jednego poziomu zabezpieczeń atakujący napotyka jedynie kolejny poziom. Ze względu na tę redundancję próba włamania się do systemów staje się złożona i kosztowna dla hakerów.

Strategia obrony w głąb wydaje się atrakcyjna dla organizacji, które uważają, że żadna pojedyncza warstwa zabezpieczeń nie jest odporna na ataki. Dlatego zawsze stosuje się wiele systemów defensywnych w celu ochrony systemów, sieci i danych. Organizacja, która chce chronić na przykład swój serwer plików, może wdrożyć w swojej sieci system wykrywania włamań i firewall. Może również zainstalować na serwerze program antywirusowy dla punktów końcowych i jeszcze lepiej szyfrować jego zawartość. Ponadto może wyłączyć zdalny dostęp i zastosować uwierzytelnianie dwuskładnikowe dla każdej próby logowania. Każdy haker próbujący uzyskać dostęp do poufnych plików na serwerze będzie musiał skutecznie złamać wszystkie te warstwy zabezpieczeń. Szanse na powodzenia są bardzo małe, ponieważ każda warstwa bezpieczeństwa ma własną złożoność. Oto typowe komponenty podejścia obrony w głąb:

- **Bezpieczeństwo sieci** — ponieważ sieci są najbardziej narażonymi powierzchniami ataku, pierwsza linia obrony ma zwykle na celu ich ochronę. Dział IT może zainstalować firewall, aby zablokować złośliwy ruch, a także uniemożliwić użytkownikom wewnętrznym wysyłanie złośliwego ruchu lub odwiedzanie złośliwych sieci.

  Ponadto w sieci wdrażane są systemy wykrywania włamań, które pomagają wykrywać podejrzane działania. Ze względu na powszechne stosowanie przeciwko firewallom ataków DDoS zaleca się organizacjom kupowanie firewalli, które mogą wytrzymać takie ataki w sposób ciągły.
- **Ochrona hostów** (bezpieczeństwo komputerów i serwerów) — w ochronie urządzeń komputerowych przed zainfekowaniem złośliwym oprogramowaniem są niezbędne systemy antywirusowe. Nowoczesne systemy antywirusowe są wyposażone w dodatkowe funkcjonalności, takie jak wbudowane firewalle, które można wykorzystać do dalszego zabezpieczenia hosta w sieci.

- **Szyfrowanie** — jest często najbardziej zaufaną linią obrony, gdyż opiera się na złożoności matematycznej. Organizacje decydują się na szyfrowanie poufnych danych, aby zapewnić dostęp do nich wyłącznie upoważnionemu personelowi. Kiedy takie dane zostaną ukradzione, nie będzie to duży cios dla organizacji, ponieważ większość algorytmów szyfrowania nie jest łatwa do złamania.
- **Kontrola dostępu** — kontrola dostępu jest stosowana jako metoda ograniczania za pomocą uwierzytelniania zakresu osób, które mogą uzyskiwać dostęp do określonych zasobów w sieci. Organizacje często łączą fizyczne i logiczne mechanizmy kontroli dostępu, aby utrudnić potencjalnym hakerom ich złamanie. Fizyczne mechanizmy kontroli obejmują stosowanie zamków i ochroniarzy, aby uniemożliwić fizyczny dostęp do wrażliwych obszarów, takich jak serwerownie. Natomiast logiczne mechanizmy kontroli wiążą się z użyciem uwierzytelniania, które chroni systemy przed nieautoryzowanym dostępem. Tradycyjnie używano tylko kombinacji nazwy użytkownika i hasła, ale ze względu na zwiększoną liczbę naruszeń bezpieczeństwa zaleca się uwierzytelnianie dwuskładnikowe.

Zabezpieczenia warstwowe są najczęściej stosowaną cyberstrategią defensywną. Staje się to jednak coraz bardziej kosztowne i nieefektywne. Hakerzy nadal są w stanie ominąć kilka warstw zabezpieczeń przy użyciu technik ataków takich jak phishing, w których atakowany jest bezpośrednio użytkownik końcowy. Ponadto wiele warstw zabezpieczeń to większe koszty instalacji i utrzymywania, co stanowi spore wyzwanie dla małych i średnich przedsiębiorstw (MŚP). Z tego powodu rośnie liczba organizacji rozważających podejście typu obrona wszerz.

Obrona wszerz

Obrona wszerz (ang. *defense in breadth*) to nowa strategia defensywna, która łączy tradycyjne podejście do bezpieczeństwa z nowymi mechanizmami zabezpieczeń. Jej celem jest zapewnienie bezpieczeństwa w każdej warstwie modelu OSI. Do warstw modelu OSI należą następujące warstwy: fizyczna, łącza danych, sieciowa, aplikacji, prezentacji, sesji i transportowa. Dlatego gdy hakerom udaje się obejść konwencjonalne narzędzia bezpieczeństwa, są powstrzymywani przez inne strategie defensywne stosowane na kolejnych warstwach modelu OSI. Ostatnią warstwą zabezpieczeń jest zazwyczaj warstwa aplikacji. Rośnie popularność tzw. **firewalli aplikacji internetowych** (ang. *Web Application Firewall* — WAF), które są bardzo skuteczne w atakach ukierunkowanych na określone aplikacje. WAF może udaremnić przeprowadzony atak i można utworzyć regułę, aby zapobiec podobnym atakom w przyszłości, dopóki nie zostanie zastosowana poprawka. Oprócz tego programiści świadomi kwestii bezpieczeństwa używają podczas tworzenia aplikacji metod projektu **OWASP** (ang. *Open Web Application Security Project*). Metody te kładą nacisk na tworzenie aplikacji, które zapewniają

standardowy poziom bezpieczeństwa i rozwiązują problemy związane z typowymi lukami w zabezpieczeniach. W przyszłości dostarczane będą prawie w pełni zabezpieczone aplikacje. Będą one zatem w stanie udaremniać lub wytrzymywać ataki samodzielnie, bez polegania na innych systemach defensywnych.

Kolejną koncepcją stosowaną w defensywie wszerz jest automatyzacja zabezpieczeń. Polega ona na tym, że systemy są opracowywane z funkcjonalnościami wykrywania ataków i automatycznego stosowania środków defensywnych. Funkcjonalności te opierają się na uczeniu maszynowym, w którym systemy uczą się swoich stanów pożądanych i normalnych ustawień środowiska. Gdy występują anomalie w ich stanie lub środowisku, aplikacje mogą przeprowadzać skanowanie w poszukiwaniu zagrożeń i stosować środki zaradcze. Technologia ta jest już stosowana w aplikacjach bezpieczeństwa w celu poprawy ich efektywności. Istnieją firewalle oparte na sztucznej inteligencji i programy antywirusowe oparte na hostach, potrafiące obsługiwać incydenty naruszenia bezpieczeństwa bez potrzeby udziału czynnika ludzkiego. Obrona wszerz jest jednak wciąż nową strategią i wiele organizacji obawia się jej stosowania.

Bez względu na to, czy organizacja wykorzystuje obronę wszerz (w celu zapewnienia bezpieczeństwa wszystkich sektorów organizacji), obronę w głąb (aby zapewnić określonemu sektorowi wiele warstw zabezpieczeń) czy nawet kombinację obu rodzajów obrony, warto, aby ogólna strategia cyberbezpieczeństwa organizacji była proaktywna.

Korzyści z posiadania proaktywnej strategii cyberbezpieczeństwa

Samo wdrożenie strategii cyberbezpieczeństwa przestaje już być wystarczające. Biorąc pod uwagę potencjalne negatywne skutki incydentu naruszenia bezpieczeństwa, aby strategia cyberbezpieczeństwa przynosiła największe korzyści, musi funkcjonować proaktywnie. Proaktywna strategia bezpieczeństwa zasadniczo koncentruje się na przewidywaniu zagrożeń i stosowaniu środków zaradczych, zanim dojdzie do jakiegoś incydentu. Oto niektóre z korzyści płynących z proaktywnego podejścia do cyberbezpieczeństwa:

- Podejście proaktywne jest mniej kosztowne w porównaniu do podejścia reaktywnego. Reaktywne podejście do cyberbezpieczeństwa oznacza opracowywanie systemów i reguł, które koncentrują się na reagowaniu na incydenty naruszenia bezpieczeństwa po ich wystąpieniu. Ryzykowność takiego podejścia polega na tym, że jeśli organizacja stanie w obliczu nowego rodzaju zagrożenia, może nie być w pełni przygotowana do radzenia sobie z jego konsekwencjami. Będzie to prawdopodobnie bardziej kosztowne niż podejście proaktywne.

- Proaktywne podejście do zarządzania ryzykiem pozwala być o krok przed aktorami zagrożeń. Wyprzedzanie potencjalnych napastników to wymarzona sytuacja dla każdego zespołu ds. bezpieczeństwa. Oznacza to, że zespół ds. bezpieczeństwa opracowuje środki ochrony organizacji, które powstrzymają atakujących. Przy zastosowaniu takiego podejścia aktorzy zagrożeń będą mieli trudności z opracowaniem jakiegokolwiek znaczącego ataku na systemy, a w przypadku incydentu naruszenia bezpieczeństwa można się spodziewać tylko niewielkiego negatywnego efektu.
- Proaktywne podejście zwiększa przejrzystość. Zapewnia zespołowi ds. bezpieczeństwa i całej organizacji środki reagowania na incydenty naruszenia bezpieczeństwa i na wszelkie potencjalne zagrożenia związane z takimi incydentami. Dostarcza jasnego planu, który określa, w jaki sposób organizacja będzie wykonywała działania w razie wystąpienia ewentualnych zagrożeń. W przypadku stosowania reaktywnego podejścia do kwestii bezpieczeństwa zamieszanie będące następstwem incydentu związanego z naruszeniem bezpieczeństwem może doprowadzić do dalszych strat i dalszych opóźnień w przywracaniu sprawności systemów organizacyjnych.
- Proaktywne podejście utrudnia atakującym przeprowadzanie ataków. Atakujący nieustannie poszukują w organizacjach słabych punktów do eksploitacji. W proaktywnym podejściu organizacja sama stosuje podobne taktyki, stale oceniając swoje systemy w celu zidentyfikowania możliwych do eksploitacji luk w zabezpieczeniach systemu. Po znalezieniu takich luk w zabezpieczeniach organizacja podejmuje działania w celu ich wyeliminowania, zanim zostaną wykorzystane przez aktorów zagrożenia atakujących organizację. Dlatego proaktywne podejście pomaga zapobiegać znajdowaniu luk w zabezpieczeniach przez cyberprzestępców i eksploitacji tych luk ze szkodą dla organizacji.
- Proaktywne podejście pozwala dostosować strategie cyberbezpieczeństwa do wizji organizacji. Dobrze zaplanowane i proaktywne podejście do zarządzania ryzykiem i cyberbezpieczeństwa jest niezbędne, aby pomóc organizacji w dopasowaniu jej planów cyberstrategii do własnej wizji. Niezaplanowana cyberstrategia może mieć niekorzystny wpływ na działalność biznesową i plany organizacji zarówno w perspektywie krótko-, jak i długoterminowej. Jednak dzięki proaktywnemu podejściu organizacja może mieć pewność, że strategia będzie dostosowana do jej długoterminowej wizji, a planowanie budżetu i implementowanie strategii będzie dopasowane do wizji prowadzonej działalności.
- Proaktywne podejście rozwija kulturę świadomości kwestii związanych z bezpieczeństwem. Każdy członek organizacji ma kluczowe znaczenie dla wdrożenia strategii cyberbezpieczeństwa. Pracownicy, podobnie jak zasoby informacyjne w organizacji, mogą być atakowani jako słabe ogniwa

w systemie bezpieczeństwa, a następnie wykorzystywani do uzyskania dostępu do systemu organizacji. Dlatego rozwój kultury świadomości bezpieczeństwa przynosi ogromne korzyści w zakresie bezpieczeństwa organizacji i zwiększa jej zdolność do powstrzymywania atakujących.

- Proaktywne podejście pomaga organizacji wyjść poza zapewnianie wyłącznie zgodności z regulacjami. Często organizacje opracowują strategię cyberbezpieczeństwa, która odpowiada wymogom zgodności, aby uniknąć problemów z prawem. W większości przypadków te wymagania dotyczące zgodności wystarczą do ochrony organizacji przed wieloma zagrożeniami, zwłaszcza tymi powszechnymi. Strategia cyberbezpieczeństwa mająca na celu spełnienie minimalnych wymogów prawnych nie pozwala jednak zapobiegać najniebezpieczniejszym atakom, które często są przeprowadzane, aby bardziej zaszkodzić organizacji.
- Proaktywne podejście do opracowywania cyberstrategii sprawia, że organizacja w równym stopniu inwestuje w trzy fazy cyberbezpieczeństwa: zapobieganie, wykrywanie i reagowanie. Wszystkie te trzy fazy są istotne dla zaimplementowania skutecznej strategii bezpieczeństwa. Skupienie się na jednym obszarze przy jednoczesnym zaniedbaniu innego prowadzi do powstawania nieefektywnych strategii, które nie przynoszą organizacji pełnych korzyści lub nie obsługują odpowiednio incydentów naruszenia bezpieczeństwa, jeśli takie wystąpią.

Jak widać, korzystanie z proaktywnej cyberstrategii ma wiele zalet i jest wiele powodów, dla których Twoja firma powinna z niej skorzystać. Ponadto istnieje wiele konkretnych strategii cyberbezpieczeństwa, które możesz zastosować w celu zapewnienia bezpieczeństwa swojej organizacji.

Najlepsze strategie cyberbezpieczeństwa dla firm

Ostatnimi czasy odnotowano wzrost liczby incydentów naruszenia bezpieczeństwa i wiele firm padło ofiarą cyberprzestępców atakujących ich dane lub inne zasoby informacyjne.

Jednak dzięki starannemu rozwojowi strategii cyberbezpieczeństwa nadal możliwe jest zapewnienie firmie wystarczającego bezpieczeństwa w tych trudnych czasach. Oto jedne z najlepszych strategii cyberbezpieczeństwa, które możesz wdrożyć w celu poprawy bezpieczeństwa swojej organizacji:

- szkolenie pracowników w zakresie zasad bezpieczeństwa;
- ochrona sieci, informacji i komputerów przed wirusami, złośliwym kodem i oprogramowaniem szpiegującym;
- stosowanie firewalla dla wszystkich połączeń internetowych;
- aktualizowanie oprogramowania;
- korzystanie z kopii zapasowych;
- zaimplementowanie ograniczeń fizycznych;
- zabezpieczanie sieci wi-fi;
- rotacja haseł;
- ograniczenie dostępu dla pracowników;
- stosowanie unikatowych kont użytkowników.

Poszczególne strategie omówimy szerzej w kolejnych punktach tego podrozdziału.

Szkolenie pracowników w zakresie zasad bezpieczeństwa

Pracownicy są niewątpliwie istotnym aspektem strategii cyberbezpieczeństwa. W wielu przypadkach aktorzy zagrożeń atakują pracowników lub słabości spowodowane zachowaniem pracowników, aby uzyskać dostęp do systemów firmy. Zespół ds. bezpieczeństwa musi opracować podstawowe praktyki bezpieczeństwa, które muszą być przestrzegane przez wszystkich pracowników w miejscu pracy i podczas przetwarzania danych związanych z pracą. Ponadto informacje na temat tych praktyk i reguły bezpieczeństwa muszą być odpowiednio przekazywane pracownikom za każdym razem, gdy są one ustanawiane lub wprowadzane są w nich jakiekolwiek zmiany. Pracownicy powinni znać kary za nieprzestrzeganie tych zasad bezpieczeństwa. Kary powinny być jasno określone, pomaga to bowiem w kultywowaniu kultury bezpieczeństwa wśród pracowników.

Ochrona sieci, informacji i komputerów przed wirusami, złośliwym kodem i oprogramowaniem szpiegującym

Aktorzy zagrożeń najprawdopodobniej będą atakować wymienione w tytule zasoby organizacji. Do infiltracji systemów będą używać złośliwego kodu, wirusów i oprogramowania szpiegującego, gdyż są to najczęściej używane metody nielegalnego uzyskania dostępu do dowolnego systemu. Dlatego organizacja musi zapewnić ochronę swoich komputerów, informacji i sieci przed takimi taktykami infiltracji. Można to osiągnąć m.in.

przez zainstalowanie skutecznych systemów antywirusowych i regularne ich aktualizowanie w celu zwalczania wirusów i innego złośliwego kodu. Zaleca się automatyczne sprawdzanie aktualizacji zainstalowanych systemów antywirusowych, aby mieć pewność, że system jest aktualny i może zwalczać wszelkie nowe ataki.

Stosowanie firewalla dla wszystkich połączeń internetowych

Połączenia internetowe są obecnie najbardziej prawdopodobną opcją, którą atakujący mogą wykorzystywać do atakowania systemów. Dlatego zapewnienie bezpieczeństwa połączeń internetowych jest ważnym i skutecznym sposobem zapewnienia bezpieczeństwa systemów. Firewall to zestaw programów, które pomogą uniemożliwić osobom postronnym dostęp do danych przesyłanych w sieci prywatnej. Firewalle powinny być zainstalowane na wszystkich komputerach, również na tych, których pracownicy mogą używać w celu uzyskiwania dostępu do sieci organizacji z domu.

Aktualizowanie oprogramowania

Wszystkie aplikacje i systemy operacyjne wykorzystywane w organizacji powinny być aktualizowane. Aby mieć pewność, że system działa na bieżącej i zaktualizowanej wersji oprogramowania, co zmniejsza ryzyko wykrycia i eksploitacji przez cyberprzestępców luk w zabezpieczeniach starych systemów, zweryfikuj, czy w organizacji obowiązuje reguła pobierania i instalowania aktualizacji dla wszystkich używanych w niej aplikacji i programów. Aktualizacje powinny być skonfigurowane tak, aby były wykonywane automatycznie. W celu zapewnienia efektywności tego procesu aktualizacji należy go stale monitorować.

Korzystanie z kopii zapasowych

Organizacja powinna zawsze przechowywać kopie zapasowe wszystkich ważnych informacji i danych biznesowych. Procesy tworzenia kopii zapasowych należy uruchamiać regularnie, codziennie lub co tydzień, dla każdego komputera używanego w organizacji. Przykładami poufnych danych, które mogą wymagać tworzenia kopii zapasowych, są dokumenty programu Word i bazy danych.

Zaimplementowanie ograniczeń fizycznych

Ograniczenie fizycznego dostępu jest skuteczną strategią utrzymywania intruzów z dala od systemu. W wielu przypadkach intruzi próbują uzyskać fizyczny dostęp do jednych systemów, aby uzyskać dostęp do innych. Niektóre zasoby informacyjne, takie

jak laptopy, są szczególnie podatne i gdy nie są używane, powinny być przechowywane pod kluczem. Kradzieży mogą dokonać nawet pracownicy, dlatego konieczne są fizyczne ograniczenia, aby zapewnić bezpieczeństwo wszystkich aktywów organizacji.

Zabezpieczanie sieci wi-fi

Pamiętaj o zabezpieczaniu i ukrywaniu sieci wi-fi przed złośliwymi osobami. Punkty dostępu bezprzewodowego można skonfigurować w taki sposób, aby nazwa sieci nie była rozgłaszana. Ponadto można użyć szyfrowania i haseł, dzięki którym tylko uwierzytelnione osoby będą upoważnione do uzyskania dostępu do systemów.

Rotacja haseł

Hakowanie haseł jest jednym z najprostszych sposobów na uzyskanie dostępu do dowolnego systemu. Pracownicy powinni zostać poinstruowani, aby zmieniać swoje hasła i nie używać wspólnych haseł. Zapobiega to wykorzystywaniu przez atakujących długotrwale stosowanego hasła, które może być współdzielone przez współpracowników.

Ograniczenie dostępu dla pracowników

Wprowadzanie ograniczeń i przyznawanie uprawnień w korzystaniu z systemu organizacji powinno opierać się na rozpoznaniu potrzeb pracowników. Pracownicy powinni mieć dostęp tylko do tych zasobów w systemie, których potrzebują do swojej pracy, a dostęp ten może być ponadto ograniczony do określonych przedziałów czasu zgodnych z godzinami pracy. Ograniczenie możliwości instalowania oprogramowania podczas korzystania z systemów firmowych gwarantuje, że personel nie będzie mógł zainstalować złośliwego oprogramowania przypadkowo lub w inny sposób.

Stosowanie unikatowych kont użytkowników

Organizacje powinny dopilnować, aby pracownicy korzystali z unikatowych kont użytkowników, przy czym poszczególni użytkownicy powinni mieć indywidualne konta. Gwarantuje to, że każdy użytkownik będzie odpowiedzialny za swoje konto użytkownika i będzie mógł zostać pociągnięty do odpowiedzialności za zaniedbania lub złośliwe działania na tym koncie. Wszystkich użytkowników należy także poinstruować, aby pamiętali o używaniu silnych haseł do swoich kont użytkowników w celu zapewnienia bezpieczeństwa i uniknięcia zhakowania. Ponadto uprawnienia dla tych kont użytkowników należy ustalać na podstawie stażu pracy pracownika i jego potrzeb dotyczących korzystania z systemu. Uprawnienia administracyjne powinny być przyznawane wyłącznie dla zaufanego personelu IT, który będzie pociągany do odpowiedzialności za wszelkie nadużycia i nieprawidłowości związane z korzystaniem z takich uprawnień.

Użytkownicy stanowią takie samo, a być może nawet większe zagrożenie dla systemu jak luki w zabezpieczeniu oprogramowania, ponieważ wiadomo, że atakujący wykorzystują słabości użytkowników, aby uzyskać dostęp do systemów docelowych. Z tego względu w poprzednich punktach uwzględniliśmy zarówno aspekty behawioralne, jak i kwestie techniczne związane z działaniami użytkowników, które możesz zaimplementować w różnych strategiach cyberbezpieczeństwa, jakie zdecydujesz się wybrać dla swojej organizacji.

Podsumowanie

W tym rozdziale omówiliśmy cyberstrategie, powody wskazujące na konieczność ich stosowania oraz podejścia, które można zastosować podczas ich opracowywania. Jak wyjaśniliśmy, cyberstrategia to udokumentowane podejście organizacji do różnych aspektów cyberprzestrzeni. Jednak głównym problemem w większości cyberstrategii jest bezpieczeństwo. Cyberstrategie są niezbędne, gdyż zapobiegają przyjmowaniu przez organizacje określonych założeń, pomagają scentralizować podejmowanie decyzji dotyczących cyberbezpieczeństwa, dostarczają szczegółów na temat taktyk stosowanych w celu radzenia sobie z kwestiami związanymi z cyberbezpieczeństwem, zapewniają długoterminowe zaangażowanie w bezpieczeństwo i upraszczają złożoność zagadnień cyberbezpieczeństwa. W tym rozdziale przedstawiliśmy dwa główne podejścia stosowane w opracowywaniu cyberstrategii — ofensywne i defensywne.

Cyberstrategie pisane z perspektywy ataku koncentrują się na technikach testowania bezpieczeństwa, które będą wykorzystywane do znajdowania i usuwania luk w zabezpieczeniach. Natomiast cyberstrategie pisane z perspektywy defensywnej szukają sposobów zapewnienia jak najlepszej obrony organizacji. W tym rozdziale opisaliśmy również dwie główne strategie defensywne: obronę w głąb i obronę wszerz. Obrona w głąb koncentruje się na stosowaniu wielu redundantnych narzędzi bezpieczeństwa, podczas gdy obrona wszerz ma na celu ograniczanie ataków na różnych warstwach modelu OSI. W dążeniu do poprawy stanu cyberzabezpieczeń organizacja może zdecydować się na wykorzystanie defensywnej strategii bezpieczeństwa, ofensywnej strategii bezpieczeństwa albo obu tych strategii.

Rozdział ten zawiera również przykłady najlepszych strategii cyberbezpieczeństwa, które mogą być skutecznie wykorzystywane przez organizacje do zabezpieczania prowadzonej działalności.

W następnym rozdziale postaramy się przybliżyć zagadnienie łańcucha niszczenia cyberzabezpieczeń oraz jego znaczenie w kontekście stanu zabezpieczeń organizacji.

Dalsza lektura

Oto lista materiałów źródłowych, które możesz wykorzystać do poszerzenia swojej wiedzy w zakresie tematów omówionych w tym rozdziale:

- Strategia cyberbezpieczeństwa Stanów Zjednoczonych: *https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf*.
- Strategia cyberbezpieczeństwa Australii: *https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf*.
- Strategia cyberbezpieczeństwa Banku Kanady: *https://www.bankofcanada.ca/wp-content/uploads/2019/06/cyber-security-strategy-2019-2021.pdf*.
- *Developing a National Strategy for Cybersecurity* (Microsoft): *https://www.microsoft.com/en-us/cybersecurity/content-hub/developing-national-strategy-for-cybersecurity*.
- Narodowa Strategia Cyberbezpieczeństwa Rządu Wielkiej Brytanii: *https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021*.
- Narodowe Strategie Cyberbezpieczeństwa agencji ENISA: *https://www.enisa.europa.eu/topics/national-cyber-security-strategies*.
- *Achieving Productivity without Exposing the Endpoint*: *https://www.comodo.com/endpoint-protection-strategy.php*.
- *Top 10 Cybersecurity Trends*: *https://www.simplilearn.com/top-cybersecurity-trends-article*.
- Wybór artykułów na temat cyberbezpieczeństwa: *https://www.erdalozkaya.com/category/cybersecurity/*.
- Hacker Combat — materiały, które pomogą Ci przyjąć nastawienie hakera: *https://hackercombat.com/*.
- Global CISO Forum — witryna, w której możesz rozwijać swoje umiejętności związane z pracą na stanowisku dyrektora ds. bezpieczeństwa informacji (ang. *Chief Information Security Officer* — CISO): *https://www.globalcisoforum.com*.
- Erdal Ozkaya, *Cybersecurity Leadership Demstified*: *https://www.packtpub.com/product/cybersecurity-leadership-demystified/9781801819282*.

Skorowidz

A

B

C

D

E

F

G

H

I

J

K

L

Ł

M

N

O

P

Q

R

S

Ś

T

U

V

W

Z

Nie daj się zinfiltrować! Poznaj tajniki cyberbezpieczeństwa!

Przyśpieszenie transformacji cyfrowej oznacza również uelastycznienie zasad pracy zdalnej. W takim środowisku zapewnienie cyberbezpieczeństwa jest trudniejsze, a złośliwe operacje stają się częstsze. Standardowy zestaw zabezpieczeń już nie wystarcza. Organizacje muszą przemyśleć swoje polityki bezpieczeństwa i dostosować je do nowych warunków. Na tym polu przewagę zyskuje się dzięki łączeniu taktyk defensywnych z ofensywnymi.

Ta książka jest skierowana do specjalistów z zakresu bezpieczeństwa IT, pentesterów, konsultantów do spraw bezpieczeństwa lub tych, którzy chcą działać jako etyczni hakerzy. Do pracy z nią przyda się znajomość sieci komputerowych, chmury obliczeniowej i systemów operacyjnych. Dzięki lekturze zdobędziesz aktualne informacje o kluczowych aspektach oceny zagrożeń i stanu systemu bezpieczeństwa, a także o zasadach utrzymywania właściwego stanu zabezpieczeń. Dowiesz się też, jak powinien wyglądać proces reagowania na incydenty. Zapoznasz się z taktykami zespołu czerwonego oraz zespołu niebieskiego, jak również z zasadami ich współdziałania. Znajdziesz tu dogłębne omówienie wzorców rozpoznawania nieregularnych zachowań w organizacji, technik analizy sieci i radzenia sobie ze złośliwym oprogramowaniem. Ten wyczerpujący przewodnik pozwoli Ci na ustalenie, jakich mechanizmów kontroli bezpieczeństwa potrzebujesz, jak je wdrożyć, wreszcie jak przeprowadzać poszczególne etapy procesu reagowania na incydenty.

W książce:

- łagodzenie skutków incydentów i odzyskiwanie sprawności systemu
- ochrona obciążeń roboczych i kwestie zerowego zaufania
- najlepsze narzędzia, takie jak Nmap i Metasploit i framework MITRE ATT&CK
- bezpieczeństwo tożsamości i egzekwowanie reguł
- integracja systemów wykrywania zagrożeń z rozwiązaniami SIEM

Yuri Diogenes

Menedżer w zespole Microsoft Cloud Security. Napisał ponad 20 książek dotyczących bezpieczeństwa informacji i technologii Microsoftu. Zdobył wiele certyfikatów branżowych IT/security.

Erdal Ozkaya

Profesor cyberbezpieczeństwa Charles Sturt University w Australii. Jest też przedsiębiorcą, a także autorem lub współautorem ponad 10 książek na temat bezpieczeństwa informacji i technologii Microsoftu. Posiada liczne certyfikaty branżowe IT/security.

Helion

helion.pl

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

KOD KORZYŚCI
Sięgnij po więcej!

ISBN 978-83-8322-421-3

9 788383 224213

Cena: 119,00 zł

Packt›