Monitoring i bezpieczeństwo sieci

Autor: Chris Fry, Martin Nystrom
Tłumaczenie: Wojciech Moch
ISBN: 978-83-246-2552-9
Tytuł oryginału: Security Monitoring
Format: 168×237, stron: 224

Poznaj najskuteczniejsze metody obrony sieci korporacyjnych

- Jak stworzyć profesjonalny system kontroli zabezpieczeń?
- Jak utrzymać solidne źródła danych?
- Jak określić rodzaje zdarzeń niezbędne do wykrywania naruszeń reguł?

Wszędobylskość i niesamowite możliwości współczesnych złośliwych programów sprawiają, że nikt dziś nie może polegać wyłącznie na oprogramowaniu antywirusowym – nawet jeśli jest ono wciąż aktualizowane. Z powodu ciągle zmieniającego się zagrożenia dla systemu informatycznego organizacji niezbędne stało się aktywne monitorowanie sieci. Autorzy tej książki proponują Ci taki właśnie nowoczesny, skuteczny system zabezpieczeń. Jeśli spróbujesz wdrożyć u siebie kilka z ich zaleceń, w znacznym stopniu podniesiesz bezpieczeństwo sieci korporacyjnej. Jeśli natomiast zrealizujesz wszystkie zalecenia, masz szansę stworzyć jeden z najlepszych na świecie systemów monitorujących! Zatem do dzieła!

Książka „Monitoring i bezpieczeństwo sieci" zawiera zestaw wyjątkowych metod, służących do wykrywania incydentów w sieciach globalnych. Autorzy – eksperci do spraw bezpieczeństwa – najpierw podają elementy niezbędne do prowadzenia skutecznego monitorowania sieci, a następnie pokazują, jak stworzyć ukierunkowane strategie oraz wdrożyć pragmatyczne techniki ochrony. Z tego podręcznika dowiesz się, w jaki sposób definiować reguły dotyczące bezpieczeństwa, regulacji i kryteriów monitorowania. Nauczysz się zbierać informacje o infrastrukturze poddawanej obserwacji, wybierać cele i źródła monitorowania. Dzięki temu samodzielnie stworzysz niezawodny system kontroli zabezpieczeń!

- Implementowanie reguł monitorowania
- Rodzaje reguł
- Taksonomia sieci
- Wybieranie celów monitorowania
- Wybieranie źródeł zdarzeń
- Automatyczne monitorowanie systemów
- Telemetria sieci
- Zarządzanie adresami IP

Zabezpiecz sieć – wykorzystaj najskuteczniejsze, nowoczesne metody monitorowania systemów informatycznych!

Helion SA
ul. Kościuszki 1c
44-100 Gliwice
tel. 032 230 98 63
e-mail: helion@helion.pl

Spis treści

ROZDZIAŁ 1.

Zaczynamy

Był styczeń 2003 roku. Praca na stanowisku inżyniera sieci obsługującego sieci centrów danych w Cisco nie mogła być lepsza. 21 stycznia mój zespół świętował wyłączenie przez wiceprezesa ostatniej centrali typu Avaya PBX, dzięki czemu połączenia telefoniczne kampusu Research Triangle Park (TRP) były w 100 procentach obsługiwane w technologii VoIP. Właśnie zakończyliśmy unowocześnianie okablowania i sprzętu sieci WAN i mieliśmy nadzieję na zwiększenie dostępności naszych zdalnych centrów. Niestety 25 stycznia (to była sobota) robak SQL Slammer poczynił spustoszenie w sieciach całego świata. Robak ten, znany również pod nazwą Sapphire, atakował niezabezpieczone serwery MS-SQL, wykorzystując do tego złośliwy i samorozprzestrzeniający się kod. Specjaliści od zabezpieczeń z pewnością doskonale pamiętają ten dzień. Technika rozprzestrzeniania się robaka mogła tworzyć efekt podobny do ataku odmowy dostępu do usług (ang. *denial-of-service* — DoS), co powodowało wyłączanie kolejnych sieci.

Jedyną cechą odróżniającą tego robaka od normalnej komunikacji z serwerem SQL była duża liczba pakietów UDP o wielkości 376 bajtów kierowanych na port 1434[1].

Dostawcy usług internetowych zaczęli blokować ruch sieciowy za pomocą filtrów wejścia-wyjścia, ale było już za późno, żeby uchronić swoje systemy przed infekcją. Chodziło tu raczej o zabezpieczenie podstawowych struktur internetu.

> Robak Sapphire był najszybciej rozprzestrzeniającym się robakiem w historii. Od momentu rozpoczęcia działania w internecie podwajał swój rozmiar co 8,5 sekundy. W ciągu 10 minut zainfekował ponad 90 procent komputerów podatnych na jego atak[2].

Szybkość replikacji robaka i liczba zainfekowanych systemów oraz sieci korporacyjnych szybko spowodowała zapełnienie linii komunikacyjnych kolejnymi próbami infekcji systemów. Administratorzy sieci obsługujący łącza WAN w USA dowiedzieli się o problemie dopiero wtedy, gdy ich pagery zaczęły błyskać jak lampki bożonarodzeniowe, przekazując alarmy o zwiększonym obciążeniu sieci. Na zakończenie otrzymywali tylko informację protokołu SNMP — łącze wyłączone (ang. *link down*). Początkowo sądziliśmy, że problem związany jest z kartą sieciową D3, którą niedawno wymieniliśmy w jednym z naszych routerów. Jednak w momencie gdy ten sam problem zaczęły zgłaszać łącza innych biur regionalnych, zorientowaliśmy się, że jest to coś znacznie poważniejszego.

[1] *http://www.cert.org/advisories/CA-2003-04.html*

[2] *http://www.caida.org/publications/papers/2003/sapphire/sapphire.html*

Doświadczaliśmy już problemów z siecią powodowanych przez infekcje wirusami, takimi jak Code Red (atakował on podane serwery WWW Microsoft IIS), ale żaden z nich nie spowodował nawet części chaosu, jaki wywołał Slammer. Kilka zarażonych nim komputerów było w stanie wygenerować ruch sieciowy zdolny przeciążyć łącza sieci WAN i doprowadzić do poważnych problemów z łącznością z oddziałami na całym świecie. Ostatecznie udało się stwierdzić, że większość zarażonych systemów to nieaktualizowane serwery laboratoryjne. Ich identyfikowanie i migrowanie było naprawdę złożonym zadaniem:

- Wdrożonych zostało zbyt mało systemów wykrywania włamań do sieci (ang. *network intrusion detection systems* — NIDS), a na dodatek nikt nie był odpowiedzialny za przeglądanie i reagowanie na alarmy zgłaszane przez zainfekowane systemy.
- Systemy telemetrii sieciowej (takie jak NetFlow) i wykrywania anomalii nie były wystarczające, aby zidentyfikować zainfekowane systemy.
- Nie było możliwości ustalania priorytetów zgłoszeń. Mieliśmy do dyspozycji tylko adresy IP i nazwy DNS zainfekowanych komputerów. Niestety zabrakło informacji kontekstowych, takich jak „serwer obsługi danych", „komputer użytkownika w sieci LAN" albo „serwer laboratoryjny".

W ciągu kolejnych 48 godzin zespoły specjalistów od sieci identyfikowały zainfekowane systemy, korzystając z powolnego procesu polegającego na rozsyłaniu zalecanych list kontroli dostępu (ang. *access control list* — ACL) do wszystkich routerów WAN[3], które miały blokować pakiety. Wszystkie trafienia zasady kontroli dostępu (ang. *access control entry* — ACE) blokującej pakiety UDP na porcie 1434 oznaczały zainfekowany komputer. Nie mogliśmy jednak zidentyfikować adresów IP komputerów tworzących takie trafienia, ponieważ dodanie opcji „log" do tej reguły powodowało lawinowy wzrost wykorzystania procesorów w routerach i drastycznie zmniejszało wydajność pracy sieci. Kolejny krok polegał na analizowaniu wykorzystania portów na przełącznikach sieciowych i wyszukiwaniu w ten sposób zainfekowanych komputerów, a następnie blokowaniu im feralnego portu. Ten proces wymagał sporej liczby ludzi i oczywiście czasu.

Jeżeli zaimplementowalibyśmy choć kilka zabezpieczeń omawianych w niniejszej książce, nasze zespoły techników mogłyby znacznie szybciej ograniczyć możliwości działania robaka. Właściwe wdrożenie systemów NIDS pozwoliłoby na natychmiastowe uzyskanie adresów IP zainfekowanych systemów i odpowiednią ich segregację w zależności od przynależności do poszczególnych sieci (serwery centrów danych, serwery laboratoryjne, komputery biurkowe — będziemy o tym mówić w rozdziale 6.). Jeszcze przed wykorzystaniem sygnatur systemów NIDS moglibyśmy użyć systemu NetFlow, aby wykryć zainfekowane komputery za pomocą wykrywanych wzorców ruchu sieciowego, o których będziemy mówić w rozdziale 3. Na podstawie tych informacji można przygotować dobrze zaplanowaną, prioretyzowaną odpowiedź na zagrożenie, a na zainfekowane systemy można by nałożyć odpowiednie ograniczenia. Sama informacja o adresach IP z systemu NetFlow pozwoliłaby ma szybką, manualną inspekcję tablic ARP i powiązań adresów MAC z adresami IP w routerach. Dzięki tym informacjom administratorzy mogliby szybko wyłączyć odpowiednie porty w przełącznikach sieciowych i zablokować możliwości rozprzestrzeniania się robaka.

W tej książce opisujemy infrastrukturę oraz narzędzia, które bardzo pomogłyby nam kilka miesięcy później, gdy zaatakował robak Nachi. Niestety nie byliśmy w stanie tego przewidzieć i Nachi spowodował te same zniszczenia i był ograniczany w tym samym manualnym procesie co robak Slammer.

[3] *http://www.cisco.com/warp/public/707/cisco-sn-20030125-worm.shtml*

Szybko zmieniający się kształt zagrożeń

Chyba każdy słyszał już, że „dawno minęły dni, gdy nastolatki i script kiddies siali zamęt tylko po to, żeby się pokazać". W końcu lat 90. i na początku XXI wieku można było zauważyć ogromny wzrost liczby ataków tylu DoS. Szkodliwe oprogramowanie (ang. *malware*) będące główną siłą napędową tych ataków rozwinęło się z prostych programów atakujących pojedynczą lukę w wielkie i złożone systemy wykorzystujące wiele luk w systemie operacyjnym i różnych aplikacjach.

Przyjrzyjmy się opisowi metody infekcji stosowanej przez robaka Nachi (z 2003 roku):

> Ten robak rozprzestrzenia się, wykorzystując luki w systemie Microsoft Windows (MS03-026).
>
> Atakowane są również serwery WWW (IIS 5) podatne na atak MS03-007 na porcie 80 poprzez usługę WebDev[4].

A oto informacje na temat bardzo popularnego wirusa o nazwie SDBot z 2006 roku:

> Robak rozprzestrzenia się za pośrednictwem udostępnionych i słabo zabezpieczonych udziałów sieciowych, a niektóre wersje próbują wykorzystać podane niżej luki w różnych systemach:
>
> Wykorzystuje lukę w usłudze WebDav (MS03-007).
>
> Wykorzystuje lukę w LSAAS (MS04-011).
>
> Wykorzystuje lukę w ASN.1 (MS04-007).
>
> Wykorzystuje lukę w usługach Workstation Service (MS03-049).
>
> Wykorzystuje lukę w PNP (MS05-039).
>
> Wykorzystuje lukę w obsłudze nazwy użytkownika przy logowaniu do usługi IMAPD.
>
> Wykorzystuje lukę w systemie autoryzacji HTTP w systemie Cisco IOS.
>
> Wykorzystuje lukę w usługach serwerowych (MS06-040).
>
> Próbuje się rozprzestrzeniać za pomocą domyślnych udziałów administracyjnych, takich jak:
>
> PRINT$
>
> E$
>
> D$
>
> C$
>
> ADMIN$
>
> IPC$
>
> Niektóre warianty wirusa wyposażone są też w listy słabych kombinacji nazwy użytkownika i hasła, która pozwala na dostęp do tych udziałów.
>
> Wykorzystuje słabe hasła i konfiguracje.
>
> Niektóre wersje próbują dostać się do serwerów MS SQL za pomocą słabych haseł administracyjnych. W przypadku powodzenia wirus może wykonać zdalnie polecenia systemowe za pośrednictwem serwera SQL[5].

Ta bardziej zaawansowana forma złośliwego oprogramowania zawiera komponenty pozwalające jej na kontynuowanie działania po ponownym uruchomieniu komputera, a nawet ukrywanie się przed programami antywirusowymi. Co więcej, zastosowano w nim techniki zaciemniania kodu utrudniające analizę przechwyconego wirusa! Wiele tego typu programów zawiera też komponenty pozwalające na kradzież informacji z zainfekowanych systemów

[4] *http://vil.nai.com/vil/content/v_100559.htm*

[5] *http://vil.nai.com/vil/content/v_139565.htm*

i przekazywanie ich do swojego twórcy za pomocą składnika zdalnej kontroli (tego typu programy nazywane są *botnetem*), który umożliwia pełne sterowanie zainfekowanym systemem. Połączenie w jednym programie wszystkich tych cech, czyli zdecentralizowanej struktury sterowania (wykorzystanie struktur sieci WWW lub sieci P2P) oraz szyfrowania i polimorfizmu (dzięki czemu złośliwe oprogramowanie może się samo modyfikować przy przenoszeniu się na inny system, co umożliwia mu unikanie programów antywirusowych), daje nam odpowiedź na pytanie, dlaczego programy antywirusowe tak rzadko radzą sobie z nowymi rodzajami zagrożeń.

Słabe wyniki programów antywirusowych

Mamy nadzieję, że nikt już nie polega wyłącznie na oprogramowaniu antywirusowym jako środku do wykrywania i ochrony systemów użytkowników. Pełna strategia zabezpieczenia musi uwzględniać programy antywirusowe, zarządzanie aktualizacjami systemu operacyjnego i aplikacji, systemy wykrywania włamań do komputerów oraz odpowiednio ukształtowaną kontrolę dostępu (powiedzieliśmy przecież: „mamy nadzieję" ☺). Jeżeli ktoś nadal korzysta wyłącznie z oprogramowania antywirusowego, to czekają go wielkie rozczarowania. Na przykład latem 2008 roku wielu naszych pracowników otrzymało doskonale przygotowaną wiadomość phishingową dotyczącą niedostarczenia przesyłki przez firmę UPS:

```
-----Original Message-----
From: United Parcel Service [mailto:teeq@agbuttonworld.com]
Sent: Tuesday, August 12, 2008 10:55 AM
To: xxxxx@xxxxxxxx.com
Subject: Tracking N_ 6741030653
Unfortunately we were not able to deliver postal package you sent on July the 21st
in time because the recipient's address is not correct.
Please print out the invoice copy attached and collect the package at our office
Your UPS
```

W załączniku wiadomości znajdował się koń trojański, którego nie wykrywało 90 procent spośród 37 dostępnych nam programów antywirusowych. W tabeli 1.1 przedstawione zostały wyniki testów przeprowadzonych na kodzie binarnym konia trojańskiego.

Jak widać, wszystkie programy antywirusowe wykrywające złośliwe oprogramowanie za pomocą „złych" sygnatur nie były w stanie wykryć tego konia trojańskiego. Tego rodzaju technologia zawodzi przede wszystkim dlatego, że nawet niewielka zmiana w kodzie wirusa spowoduje, iż będzie on niewykrywalny dla istniejących sygnatur. Oczywiście dostawcy programów antywirusowych ciągle poprawiają swoje technologie — na przykład dodają wykrywanie heurystyczne lub behawioralne, ale nadal nie są w stanie udostępnić nam „pełnej" ochrony systemu. Doskonałym źródłem informacji na temat wirusów, ich możliwości i powodów tak skutecznego ukrywania się jest książka Johna Aycock'a *Computer Viruses and Malware* (wydawnictwo Springer).

Powszechność i wielkie możliwości dzisiejszego złośliwego oprogramowania powinny być wystarczającym powodem do ścisłego monitorowania swoich sieci komputerowych. Jeżeli nie jest, to być może bardziej przekonujące będzie to, że takie programy wykorzystywane są przez organizacje mafijne do szpiegowania, kradzieży tożsamości i wymuszeń.

Po co monitorować?

Przestępczość zorganizowana i zagrożenia wewnętrzne to ciągle zmieniające się zagrożenia dające nam solidne podstawy do aktywnego monitorowania zabezpieczeń sieci.

Tabela 1.1. Wyniki testów kodu binarnego konia trojańskiego

Antywirus	Wynik	Antywirus	Wynik
AhnLab-V3	–	Kaspersky	–
AntiVir	–	McAfee	–
Authentium	W32/Downldr2.DIFZ	Microsoft	–
Avast	–	NOD32v2	–
AVG	–	Norman	–
BitDefender	–	Panda	–
CAT-QuickHeal	–	PCTools	–
ClamAV	–	Prevx1	–
DrWeb	–	Rising	–
eSafe	–	Sophos	–
eTrust-Vet	–	Sunbelt	Trojan-Spy.Win32.Zbot.gen (v)
Ewido	–	Symantec	–
F-Prot	–	TheHacker	–
F-Secure	–	TrendMicro	–
Fortinet	–	VBA32	–
GData	–	ViRobot	–
Ikarus	Win32.Outbreak.UPSRechnung	VirusBuster	–
K7AntiVirus	–	Webwasher-Gateway	–

Łajdacka ekonomia i przestępczość zorganizowana

Codziennie kradzione są niewiarygodne ilości pieniędzy. Wystarczająco wiele, żeby koordynować całe grupy przestępców. Takie nielegalne związki przyspieszyły rozwój zaawansowanych wersji złośliwego oprogramowania (w tym kontekście często nazywane jest ono przestępczym oprogramowaniem — *crimeware*). Większość organizacji zajmujących się bezpieczeństwem, zarówno rządowych, jak i prywatnych, nie jest dostatecznie dobrze wyposażonych, aby zwalczać te zagrożenia za pomocą istniejących technologii i procesów.

W 2008 roku badania przeprowadzone przez firmę F-Secure przewidywały, że złośliwe oprogramowanie wykorzystywane w celach przestępczych będzie rozwijało się głównie w takich krajach jak Brazylia, Chiny, były Związek Radziecki, Indie oraz w Afryce i Ameryce Środkowej. Wynika to z faktu, że w tych krajach wielu wykształconych specjalistów nie ma możliwości użycia swoich umiejętności w sposób legalny[6].

Co prawda większość takich działań nie jest skierowana bezpośrednio przeciwko korporacjom, ale widzieliśmy już przypadki, w których wykorzystywana była znajomość nazwisk oraz relacji między członkami zespołów a ich kierownikami, co pozwalało na przygotowanie niezwykle wiarygodnych wiadomości phishingowych. Technika ta często opisywana jest terminem *phishingu wybiórczego* (ang. *spearphishing*).

Z drugiej strony działania podejmowane przez złośliwych pracowników w celu uzyskania dostępu do tajnych informacji i danych własności intelektualnej tworzą sytuację opisywaną terminem *zagrożenia wewnętrznego* (ang. *insider threat*).

[6] *http://www.f-secure.com/f-secure/pressroom/news/fsnews_20080117_1_eng.html*

Zagrożenia wewnętrzne

Badania prowadzone przez tajne służby Stanów Zjednoczonych oraz zespół CERT/CC (*Computer Emergency Response Team/Coordination Center*) potwierdzają duże znaczenie zagrożeń wewnętrznych. Co prawda nadal dyskutowana jest ich skala, jednak szacuje się, że 40 do 70 procent wszystkich naruszeń bezpieczeństwa związanych jest z zagrożeniem wewnętrznym. Tak wielka skala problemu, szczególnie w związku z bezpośrednim dostępem do danych i wiedzą na ich temat, musi skłaniać firmy do ścisłego monitorowania działań swoich pracowników. Kilka słynnych przykładów powinno skłonić każdego do poważnego potraktowania zagrożeń wewnętrznych w firmie[7]:

Horizon Blue Cross Blue Shield
: W styczniu 2008 roku ponad 300 000 nazwisk i numerów ubezpieczenia społecznego zostało skradzionych razem z laptopem, na którym były przechowywane. Pracownik na co dzień pracujący z danymi klientów zabierał ten komputer do domu.

Hannaford Bros. Co.
: W maju 2008 roku wyciekły numery 4,2 miliona kart kredytowych i debetowych. Mniej więcej 1800 przypadków defraudacji zostało powiązanych z tym właśnie wyciekiem danych. Okazało się, że numery kart były przechwytywane w trakcie przetwarzania transakcji.

Compass Bank
: W marcu 2008 roku dokonano włamania do bazy danych zawierającej nazwiska, numery kont i hasła użytkowników. Były pracownik banku skradł dysk twardy zawierający milion danych klientów i wykorzystał je do defraudacji. Używał kodera kart kredytowych oraz czystych kart, aby tworzyć nowe karty i pobierać pieniądze z kont wielu klientów banku.

Countrywide Financial Corp.
: W sierpniu 2008 roku FBI aresztowało byłego pracownika firmy za kradzież informacji osobistych, w tym numerów ubezpieczenia społecznego. Pracownik ten był starszym analitykiem finansowym w dziale pożyczek subprime. Przypuszczalny inicjator tej kradzieży co tydzień sprzedawał dane kont w grupach po 20 000 za 500$.

Nie wszystkie z wymienionych przypadków były z natury złośliwe, ale wszystkie swój początek miały od naruszenia zasad bezpieczeństwa. W rozdziałach 2. i 6. prezentować będziemy narzędzia pozwalające na wykrywanie złośliwego oprogramowania i zagrożeń wewnętrznych. W rozdziałach 4. i 5. omówimy metody prioretyzowania ograniczonych zasobów do monitorowania i wybierania danych zdarzeń pozwalających na uzyskanie najlepszych efektów przy ograniczonych kosztach.

Wyzwanie monitoringu

Specjaliści od zabezpieczeń tworzący mechanizmy monitorowania muszą zmierzyć się również z ograniczeniami stosowanych produktów, rzeczywistością monitorowania operacyjnego, ilościami generowanych zdarzeń oraz koniecznością ochrony prywatności pracowników.

Obietnice producentów

„Po prostu podłącz, a my zajmiemy się resztą”! Taka prostota konfigurowania systemu SIM (*Security Information Manager* — zarządzania informacjami o zabezpieczeniach) firmy XYZ, aby

[7] Źródło: *http://www.privacyrights.org/ar/ChronDataBreaches.htm#2008*

„automagicznie" obsługiwał naruszenia bezpieczeństwa, sprawdza się tylko w przypadku niewielkich i dobrze prowadzonych środowisk. Niestety z naszych rozmów z klientami wnioskujemy, że takie utopijne środowiska są niezwykle rzadkie. Monitorowanie bezpieczeństwa w niczym nie przypomina konfiguracji magnetowidu. Nie można go „nastawić i zapomnieć".

Technologie zabezpieczające nie są w stanie wytworzyć informacji kontekstowych, niezbędnych do przygotowania priorytetów i wyznaczenia najważniejszych punktów do monitorowania. Każde środowisko jest unikalne, ale metody omawiane w rozdziale 3. pozwalają na wbudowanie takich istotnych informacji kontekstowych do narzędzi zabezpieczających. To jednak nie wszystko!

Rzeczywistość

„Włącz kontrolę wszystkich tabel bazy danych". Działania na bazach danych w rozbudowanym środowisku korporacyjnym są kluczowym elementem stanowiącym o wydajności i stabilności, dlatego to zalecenie zmusiło nas do przemyśleń. Jaki będzie to miało wpływ na wydajność? Jakie wprowadzi ryzyko dla działalności firmy, kontroli zmian, stabilności i dostępności sieci? Zaczęliśmy rozmawiać na ten temat z administratorem baz danych za pośrednictwem poczty e-mail. Przestał odpowiadać na nasze wiadomości po tym, gdy wspomnieliśmy o zaleceniu „włączenia kontroli wszystkich tabel bazy danych"! Rzeczywiście, tak intensywna kontrola bazy danych w każdym środowisku (z wyjątkiem tych najrzadziej używanych) spowodowałaby zmniejszenie wydajności systemu do nieakceptowanego poziomu. Zalecenia, które podajemy w tej książce, zostały przetestowane i sprawdzone w trakcie naszych własnych doświadczeń, zdobytych przez nas podczas obsługi niejednej infrastruktury korporacyjnej. Nie będziemy zalecali stosowania metod, które mogą negatywnie wpłynąć na dostępność systemów, a przez to pogorszyć relacje z innymi pracownikami.

Ilości danych

W kontekście monitorowania sieci przy dużych ilościach protokołowanych danych szybko mogą się one zmienić z bardzo ważnego zbioru informacji w całkowicie nieprzejrzyste bagno. Nieprawidłowo przygotowany system NIDS lub demon syslog może generować zbyt wiele komunikatów, które zaczną zalewać systemy zbierania informacji. Nawet jeżeli systemy te będą w stanie przyjąć taki zalew komunikatów, to sama ich ilość będzie przytłaczająca dla zespołu monitorującego, który może zacząć ignorować to źródło informacji. W rozdziałach 5. i 6. przedstawimy wskazówki pozwalające na zachowanie rozsądnej liczby komunikatów nawet w najbardziej rozbudowanych środowiskach.

Prywatność

Nie można też zapomnieć o konieczności zachowania zgodności z lokalnym prawodawstwem dotyczącym ochrony danych osobowych, tym bardziej że mogą się one różnić w poszczególnych krajach. Najlepszą radą, jakiej możemy tu udzielić, jest stałe informowanie działu personalnego i prawnego o prowadzonych działaniach monitorowania sieci oraz formalne dokumentowanie zezwoleń udzielanych przez te działy. Jest to najczęściej realizowane w postaci firmowej deklaracji o monitorowaniu, która powinna stać się częścią zasad dozwolonego użycia w danej firmie.

Zlecanie monitorowania zabezpieczeń

W wielu firmach bezpieczeństwo jest tylko kolejnym punktem w dokumencie kontrolnym. „Pracownicy… jest! Obsługa IT… jest! Zabezpieczenia… jest!" itd.

Jeżeli Czytelnik już zdążył całkowicie zlecić monitorowanie bezpieczeństwa swojej sieci zewnętrznej firmie, to może przestać czytać tę książkę i sprzedać ją na internetowej aukcji. Oprawa jest zapewne jeszcze nienaruszona, więc można opisać ją „jak nowa". Z naszego doświadczenia wynika (i potwierdzają to rozmowy z naszymi klientami), że niezwykle trudno jest znaleźć firmę zabezpieczającą, która naprawdę starałaby się poznać sieć i kontekst bezpieczeństwa swoich klientów. Takie firmy najczęściej ograniczają się do obsługi najprostszych problemów z zabezpieczeniami. Proszę przyjrzeć się następującej propozycji: chcemy dowiedzieć się, kiedy ktoś zacznie kopiować dane klientów z bazy danych na lokalny komputer. Jak może nam to zapewnić zewnętrzna firma? A może lepiej: jak wysoką fakturę wystawi za taką usługę? Usługi oferowane przez większość dostawców ograniczają się do składania regularnych raportów wybranych alarmów systemów NIDS (tych samych alarmów dla każdego klienta) oraz związanych z nimi adresów IP. Naszym zdaniem jest to zdecydowanie niewystarczające.

Monitorowanie w celu minimalizacji ryzyka

Oto kilka słów, które każdego specjalistę od bezpieczeństwa przyprawiają o dreszcze: *B2B*, *partner*, *outsourcing*, *extranet*. Czasami, z powodów ściśle biznesowych, kierownictwo musi zaakceptować wyższy poziom ryzyka, takiego jak podłączenie sieci partnera jeszcze przed dokonaniem pełnej oceny bezpieczeństwa tej sieci. Niestety najczęściej takie decyzje podejmowane są przez osoby nieposiadające wystarczających uprawnień do zwiększania ryzyka bezpieczeństwa danych. Tego rodzaju decyzje wpływają na całą korporację, a często dokonywane są na podstawie niewłaściwych lub niepełnych informacji. W efekcie osoby odpowiedzialne za bezpieczeństwo danych popadają we frustrację i po prostu liczą na szczęście. Taka całkowita kapitulacja nie jest na szczęście konieczna. Jeżeli będziemy postępować zgodnie z wytycznymi podawanymi w niniejszej książce, to będziemy w stanie dopasować strategię monitorowania do takich wyjątkowych sytuacji biznesowych, minimalizując, a może nawet całkowicie usuwając dodatkowe ryzyko. Od osób decydujących o podjęciu ryzykownych działań należy domagać się specjalnych nakładów na monitorowanie, mówiąc: „Jeżeli chcecie rozpocząć ten ryzykowny projekt, to będziecie musieli łożyć na dodatkowe funkcje monitorowania sprzętu i personelu".

Monitorowanie sterowane regułami

Chcemy tutaj zróżnicować narzędzia do monitorowania sterowanego regułami (czasami nazywane są *monitoringiem ukierunkowanym* — ang. *targeted monitoring*) od monitorowania złośliwego oprogramowania, wykrywania włamań, wykrywania włamań wewnętrznych (ang. *extrusion detection*) oraz popularnych narzędzi do monitorowania. Monitorowanie sterowane regułami realizowane jest przez wyliczanie i wybieranie najważniejszych systemów, wykrywanie naruszeń poszczególnych zasad za pomocą protokołów zdarzeń. Wymaga ono analizy wygenerowanych zdarzeń i porównania ich z zasadami bezpieczeństwa obowiązującymi w danym kontekście środowiska. Opisywane tutaj metody ułatwiają przeniesienie wysiłków systemów monitorujących na systemy najistotniejsze dla firmy i zdefiniowanie alarmów związanych z regułami bezpieczeństwa obowiązującymi te systemy.

Czy to zadziała w moim przypadku?

Na podstawie doświadczeń zebranych przy pracy z jedną z najbardziej złożonych i zmienianych sieci korporacyjnych świata jesteśmy przekonani, że prezentowane tutaj narzędzia oraz metody są skuteczne i bezpieczne. Obaj zajmowaliśmy się obsługą najistotniejszych systemów, których dostępność bezpośrednio wpływała na zyski korporacji i produktywność pracowników (a przez to i na nasze kariery). Niniejszy poradnik jest wynikiem iteracyjnych usprawnień i powinien znaleźć zastosowanie przy wszystkich używanych przez Czytelnika technologiach zabezpieczających. Chodzi o to, żeby implementując zaledwie kilka zaleceń podawanych w tej książce, można było mocno podnieść swoje możliwości monitorowania sieci i reagowania na zagrożenia. Zaimplementowanie wszystkich zaleceń pozwoli utworzyć jeden z najlepszych na świecie systemów monitorujących.

Produkty komercyjne a produkty o otwartych źródłach

Obaj jesteśmy pracownikami firmy Cisco Systems i korzystamy z jej produktów zabezpieczających. Prezentujemy tutaj porady wynikające z naszego doświadczenia, dlatego w książce znajdzie się wiele odniesień do produktów firmy Cisco. Używamy jednak narzędzi o otwartych źródłach, jeżeli tylko spełniają one nasze wymagania, a jeżeli sprawdzają się w pracy, to z całego serca zalecamy ich stosowanie. Produkty o otwartych źródłach prezentowane są w książce Richarda Bejtlicha *The Tao of Network Security Monitoring* (Addison-Wesley Professional), w której opisywane są metody zastosowania takich narzędzi monitorujących jak Snort, Bro, Argus, Sguil i wielu innych. Jest to idealna pozycja dla osób, które dopiero tworzą swoją infrastrukturę monitorowania lub szukają możliwości rozbudowy już istniejącej. W tej książce staramy się pomóc Czytelnikowi jak najlepiej wykorzystać swoje narzędzia monitorujące, niezależnie od tego, jakich używa.

Firma Blanco Wireless

W celu lepszego zilustrowania naszych zaleceń będziemy prezentować ich implementację w ramach *fikcyjnej* firmy o nazwie Blanco Wireless. Jest to dostawca usług telefonii komórkowej działający na terenie USA. W ramach zarządzania kontami Blanco Wireless zbiera i przechowuje informacje osobowe swoich klientów, takie jak nazwiska, adresy, numery telefonów, numery ubezpieczenia społecznego, ocenę kredytową oraz wiele innych szczegółowych danych. Na zakończenie każdego rozdziału omówimy sposób, w jaki firma Blanco Wireless implementuje narzędzia i metody omawiane w danym rozdziale. Wśród podawanych przykładów znajdą się diagramy oraz wyjaśnienia, jak nasza fikcyjna firma wykorzystała podawane w tym rozdziale zalecenia, aby poprawić swoje monitorowanie zabezpieczeń.