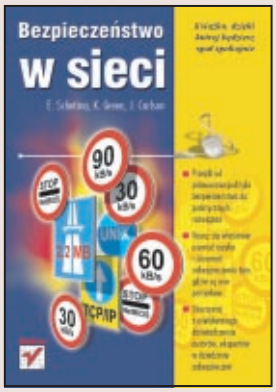
Bezpieczeństwo w sieci



Autorzy: E. Schetina, K. Green, J. Carlson
Tłumaczenie: Arkadiusz Romanek
ISBN: 83-7197-801-4
Tytuł oryginału: Internet Site Security
Format: B5, stron: 416

Internet, oferuje takie same możliwości tym, którzy chcą wykorzystać go dla wspólnego dobra, jak i tym, którzy widzą w nim instrument wykorzystywany do niesienia zła. Zamierzeniem tej książki jest wyposażenie specjalistów zajmujących się kwestiami bezpieczeństwa w przewodnik, który przeprowadzi ich przez cały proces tworzenia bezpiecznej infrastruktury internetowej: od stworzenia polityki bezpieczeństwa do bezpieczeństwa realnego. Autorzy skupiają się na rzeczywistych, znanych im z wieloletniego doświadczenia zagrożeniach (są pracownikami firmy TrustWave Corporation, zajmującej się zabezpieczeniami sieci komputerowych).

Rzeczywiste przypadki, możliwe do zastosowania rozwiązania i daleko posunięty realizm to jest to, co odróżnia tą książkę od innych publikacji. Poznasz wszystkie najważniejsze technologie, które pozwolą Ci bezpiecznie komunikować się z ogólnoświatową siecią. Książka nie tylko przedstawi je teoretycznie, lecz dostarczy Ci sprawdzone, skutecznie działające rozwiązania.

Po przeczytaniu będziesz bogatszy o wiedzę na temat:

- Tworzenia całościowej strategii tworzenia bezpiecznej infrastruktury internetowej
- Konstruowania i uzasadniania budżetu na cele bezpieczeństwa
- Zabezpieczania systemów Windows i Unix
- Pisania bezpiecznych aplikacji internetowych
- Tworzenia procedur bezpieczeństwa, integrowania firewalli i systemów wykrywania włamań
- Reagowania na niebezpieczne incydenty i wykrywania ich sprawców

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Rozdział 2.

Tworzenie bezpiecznej infrastruktury sieciowej

W poprzednim rozdziale omawialiśmy różnego rodzaju zagrożenia, które wywołują potrzebę zapewnienia bezpieczeństwa naszym zasobom. Doszliśmy do wniosku, że prawdziwym celem dobrego systemu bezpieczeństwa jest ochrona naprawdę istotnych zasobów firmy, których utrata bądź uszkodzenie może wpłynąć na zaprzestanie lub zakłócenie działalności przedsiębiorstwa. Takimi ważnymi zasobami mogą być: obraz i wizerunek firmy, jej wytwory, mechanizmy dystrybucji produktów, własność intelektualna lub zdolność do prowadzenia działań handlowych. Na poziomie technicznym zwykle skupiamy się na ochranianiu systemów a nie samych zasobów. Administratorzy koncentrują się najczęściej na zapewnianiu najnowszych uaktualnień i łatek systemowych, na wprowadzaniu programowych poprawek, których celem jest utrudnienie zadania włamywaczowi, bądź na monitorowaniu plików z raportami w poszukiwaniu podejrzanych zachowań użytkowników systemu. Na ogół nie myślą oni o tym, czy ich działania pasują do ogólnego obrazu i jak współgrają z polityką i procedurami bezpieczeństwa obowiązującymi w ich miejscu pracy.

Potrzeba bezpieczeństwa

Zamierzeniem autorów jest przedstawienie w tym rozdziale tego, w jaki sposób odosobnione czynniki, jak zarządzanie, systemy, architektura, polityka bezpieczeństwa i audyt, składają się na pewną całość — plan bezpieczeństwa. Celem nadrzędnym planu jest zapewnienie ochrony zasobów i funkcji biznesowych przedsiębiorstwa, a jego wdrożenie przekłada się na praktyczne rozwiązania służące na przykład ochronie serwerów sieciowych i pocztowych. Umiejętność spojrzenia na całość zagadnienia z szerszej perspektywy jest tym, co odróżnia prawdziwego specjalistę od zwykłego, choć dobrego, technika. Książka ta w głównej mierze opisuje różne zagadnienia techniczne takie, jak sposób zabezpieczenia serwera czy wzmocnienia bezpieczeństwa systemu Linux. Jednak ten rozdział, w odróżnieniu od kolejnych, umożliwia spojrzenie na zagadnienie z pewnej odległości pozwalającej na właściwą ocenę prawdziwej wagi bezpieczeństwa.

Chcielibyśmy, aby czytelnik przestał krótkowzrocznie skupiać się na rozwiązaniach punktowych takich, jak zapory sieciowe czy listy dostępowe i przeniósł wzrok trochę wyżej, na poziom, z którego wyraźnie widać, jak ważne są pojedyncze składniki planu bezpieczeństwa.

Zajmijmy się teraz prostym przypadkiem (który w gruncie rzeczy nie ma nic wspólnego z aspektami technicznymi zapewnienia bezpieczeństwa), tj. zakończeniem współpracy z jednym z pracowników firmy. Z punktu widzenia działu zasobów ludzkich (HR), najważniejszymi czynnościami, które trzeba wykonać w takim przypadku, są: zwrot identyfikatora, poinformowanie odchodzącego pracownika o usługach zdrowotnych, z których wciąż może skorzystać, upewnienie się co do poprawności adresu, na który trafi ostatnie wynagrodzenie czy też wyrównanie pieniężne za niewykorzystane dni urlopu. Jedną z ważnych czynności, o której często się zapomina, jest zawiadomienie o fakcie rozwiązania umowy pracowników działu IT i podjęcie decyzji co do przyszłości konta dostępowego tego pracownika i informacji, które na nim przechowuje. Czy konto powinno być usunięte natychmiast, czy raczej zarchiwizowane i przechowywane przez pewien określony czas? Co z jego komputerem przenośnym? Czy jego dysk twardy powinien być sformatowany, a sprzęt przekazany innemu pracownikowi? Czy pliki umieszczone na koncie w sieci powinny być zachowane czy usunięte? I wreszcie najważniejsze — co zrobić z dostępem do sieci korporacyjnej? W wielu przypadkach pracownik zostaje zwolniony, a po pewnym czasie okazuje się, iż konto, dzięki któremu mógł zdalnie logować się do sieci, nie zostało zablokowane i wciąż jest wykorzystywane choćby do wysyłania i odbierania poczty elektronicznej. To, w jaki sposób wygląda likwidowanie konta i blokowanie dostępu zwalnianego pracownika, często zależy od prywatnych decyzji administratora systemu, mimo że powinno zostać wyraźnie określone w procedurach bezpieczeństwa obowiązujących wszystkie piony firmy.

W przypadku gdy pracownik jest zwalniany z powodu skłonności do wysyłania niewybrednych (być może ordynarnych czy nielegalnych) wiadomości elektronicznych, ważne jest, aby jego konto pocztowe zostało zablokowane i zarchiwizowane na przykład na potrzeby przyszłego procesu sądowego. O takim postępowaniu nie myśli zwykle administrator, któremu powiedziano, że pewna osoba przestała być pracownikiem firmy i istnienie jej konta jest zbyteczne.

Przy tworzeniu możliwie najbezpieczniejszej infrastruktury sieciowej konieczne jest postrzeganie bezpieczeństwa jako całości. Każdy ci to powie: łańcuch jest tak mocny jak jego najsłabsze ogniwo. W tym rozdziale zajmiemy się poszczególnymi ogniwami. Sprawdzimy, w jaki sposób ze sobą współpracują i wzajemnie od siebie zależą. W trakcie tego sprawdzianu chcielibyśmy pokazać, jak wszyscy w jakiś sposób odpowiedzialni za zapewnienie bezpieczeństwa mogą ze sobą współdziałać, dążąc do tego samego celu, którym jest bezpieczeństwo zasobów firmy.

Co oznacza termin „bezpieczeństwo”?

Każdy inaczej rozumie bezpieczeństwo systemu. Dla administratorów termin ten może oznaczać pewność, że system, nad którym sprawują pieczę, nie zostanie zhakowany; dla twórców stron internetowych bezpieczeństwo gwarantowane jest przez SSL podczas

przetwarzania informacji o numerach kart kredytowych klientów dokonujących zakupów poprzez witrynę internetową; dla członków zarządu bezpieczeństwo oznacza stan, w którym firma jest odpowiednio chroniona przed stratami, a oni sami się do tego w jakiś sposób przyczynili. Specjalista IT znajduje się gdzieś pomiędzy tymi różnymi stanowiskami i przejmuje się nie tylko technicznymi aspektami zapewnienia bezpieczeństwa, ale i takimi zagadnieniami, jak zachowanie prywatności klientów, poprawny audyt i kontrola nad konfiguracjami sprzętowymi i programowymi.

Często różnym funkcjom i poziomom odpowiedzialności towarzyszy obojętny stosunek do poczynań współpracowników — administrator nie przejmuje się procedurami i procesem, a menedżera nie interesuje proces implementacji rozwiązań bezpieczeństwa. Z racji tego, że książka ta skierowana jest w głównej mierze do czytelników, do których należy zajmowanie się kwestiami technicznymi tj. specjalistów IT, projektantów stron i administratorów, uznaliśmy, iż ważne jest, aby zaznajomić ich z całością zagadnienia ochrony zasobów informacyjnych. Powód jest prosty — naprawdę *powinni* oni być zainteresowani obowiązującą polityką bezpieczeństwa i całościowym procesem. W kolejnych podrozdziałach znajdą się przemyślenia dotyczące aspektu bezpieczeństwa informacji, na który spojrzymy z perspektywy realizatorów, administratorów i dyrektorów technicznych. Chcielibyśmy pokazać im obszary, na które szczególnie powinni zwrócić uwagę i, być może, uczulić ich na niektóre komponenty całościowego zagadnienia zapewnienia bezpieczeństwa czasami umykające uwadze.

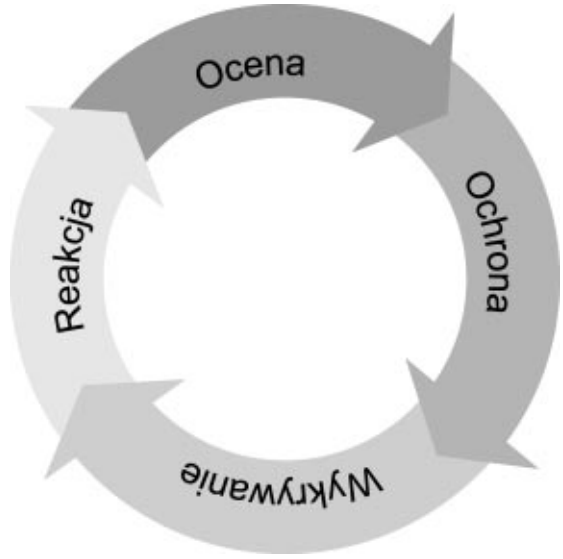
Proces zapewnienia bezpieczeństwa

Każda książka dotycząca bezpieczeństwa, czy jest to praca czysto techniczna opisująca luki w protokole TCP/IP czy poradnik audytorski przedstawiający metody tworzenia strategii, powinna mówić o procesie zapewnienia bezpieczeństwa jako całości i nie koncentrować się na szczegółach pojedynczego przypadku. Przez cały czas będziemy się starali podkreślać, że bezpieczeństwo to ciągły proces a nie ostateczny cel, o którym, kiedy zostanie osiągnięty, można zapomnieć. W tym podrozdziale zajmiemy się nie tylko pojedynczymi składnikami i celami stawianymi przed procesem, ale i nim samym. Na kolejnych stronach chcielibyśmy zaprezentować przegląd czynności składających się na proces zapewnienia bezpieczeństwa. Nie jest ważna twoja funkcja w firmie i zakres odpowiedzialności — chcielibyśmy, abyś zrozumiał, jaka jest twoja rola w całym procesie i dowiedział się, jakie elementy powinny szczególnie przykuwać twoją uwagę i jakie czynniki mogą mieć wpływ na końcowy wynik twoich poczynań.

Jak powiedziano wcześniej — bezpieczeństwo to proces a nie moment w czasie. Proces ten może być podzielony na cztery główne fazy:

- ocena i polityka,
- ochrona zasobów,
- monitorowanie i wykrywanie,
- reakcja i odzyskiwanie.

Te cztery komponenty wchodzą w skład procesu, który graficznie może być przedstawiany jako „koło bezpieczeństwa".



Rysunek 2.1. *Proces zapewnienia bezpieczeństwa*

W stadium nazwanym *ocena i polityka* organizacje określają swoje wymagania dotyczące bezpieczeństwa, a także zakres odpowiedzialności i przydzielają funkcje organizacyjne. Na tym etapie może także nastąpić przegląd aktualnych mechanizmów bezpieczeństwa i podjęcie decyzji o tym, czy są one wystarczające. Wyniki analizy przekładają się na zasady polityki bezpieczeństwa, w której definiuje się sposoby i metody ochrony zasobów firmy.

Kiedy polityka i procedury bezpieczeństwa są już zdefiniowane, przechodzimy do kolejnego stadium nazwanego *ochroną zasobów*. W tej fazie wprowadza się właściwe środki ochronne odpowiadające poszczególnym elementom polityki bezpieczeństwa. Środki te mogą mieć charakter proceduralny (na przykład regularne przeglądanie plików raportów systemowych) lub implementacyjny (na przykład instalacja zapór sieciowych).

Po zastosowaniu pewnych środków zapewnienia bezpieczeństwa należy sprawdzić ich efektywność. Ten sprawdzian odbywa się podczas fazy nazwanej *monitorowanie i wykrywanie*. Jeżeli na przykład nigdy nie przyglądasz się ruchowi, jaki odbywa się poprzez zainstalowany firewall, możesz być pewny, że nie wiesz, czy poprawnie spełnia on swoje zadanie.

I wreszcie, jako że żadne środki nie zapewniają 100% bezpieczeństwa, w procesie musi być miejsce na fazę zwaną *reakcją i odzyskiwaniem*. Musisz wiedzieć na przykład, jak powinieneś zareagować w przypadku ataku typu *denial-of-service* (w dowolnym tłumaczeniu „blokada usług" — w dalszej części książki używany będzie skrót *DoS* — *dop. tłum.*). Czy wiesz, kogo powinieneś wtedy powiadomić, do kogo zadzwonić? A jeżeli nastąpi awaria serwera sieciowego i strona korporacyjna przestanie być dostępna dla internautów? Czy wiesz, jakie działania należy podjąć, aby znów działała?

Kiedy przejdziesz już przez wszystkie cztery fazy, nadchodzi czas na rozpoczęcie procesu od nowa i ponowną ocenę i korekty polityki bezpieczeństwa. Jeżeli strategia, zastosowane środki, monitoring i mechanizmy reakcji nie są regularnie analizowane, istnieje duża szansa, że szybko staną się przestarzałe i zostaniesz zaskoczony przez jakieś nowe technologie, nowe zagrożenia lub niekorzystne zmiany, jakie dokonały się w organizacji czy w sieci. Jeśli program zapewnienia bezpieczeństwa ma być efektywny, musi być wspierany przez wszystkie środowiska i grupy wewnątrz firmy — od dyrektora wykonawczego, przez menedżerów, aż po użytkownika końcowego, dział zasobów ludzkich, pracowników administracyjnych i pracowników działu IT. Każdy z przedstawicieli tych grup ma w procesie do odegrania swoją rolę, gdy chodzi o tworzenie, wdrażanie czy też monitorowanie zastosowanych rozwiązań i ich zgodności z procedurami obowiązującymi w firmie. Bez wkładu, jaki wnoszą do procesu pojedyncze jednostki (a szczególnie osoby z kręgu menedżerów wyższego stopnia i dyrektorów), program bezpieczeństwa nigdy nie odniesie sukcesu.

Zajmijmy się teraz bardziej szczegółowo każdą z opisanych faz procesu zapewnienia bezpieczeństwa.

Ocena i polityka

Faza ta wydaje się być dla specjalistów IT najmniej interesująca. Dzieje się tak prawdopodobnie dlatego, że wiąże się ona z potrzebą wielu rozmów, wywiadów i mnóstwem pracy papierkowej i niewiele ma wspólnego z tworzeniem i zarządzaniem serwerami, pisaniem kodów i projektowaniem nowej architektury sieciowej. Ogólne odczucie, które towarzyszy przechodzącym przez to stadium, wiąże się z przekonaniem o niskiej wartości tych działań — być może dlatego, iż w tej fazie nie dostajemy odpowiedzi na pytanie „jak?". Wynikiem zakończonej fazy oceny jest tylko kilka „co (należy zrobić)?"

Przyjęta polityka bezpieczeństwa nie powie ci na przykład, że potrzebujesz zastosowania wirtualnej sieci prywatnej. Będziesz wiedział tylko o istnieniu potrzeby zabezpieczenia przesyłu informacji pomiędzy siedzibą firmy a filiami, w których korzysta się z dostępu zdalnego. Taka informacja nie jest zbyt ekscytująca. Z drugiej jednak strony pewna grupa specjalistów IT wydaje się być zadowolona z posiadania jasno określonej polityki bezpieczeństwa wskazującej, które elementy są ważniejsze od innych. Ogólnie mówiąc, polityka pomaga im zdefiniować własne cele i, patrząc na to z perspektywy walki o fundusze, stanowi silną kartę przetargową podczas określania budżetu. Jeżeli na przykład powiesz swemu szefowi: „Proszę posłuchać, potrzebujemy dyspozycyjnej zapory sieciowej i będzie to kosztowało 200 tys. złotych", pierwszą reakcją zapewne nie będzie natychmiastowe wystawienie zlecenia zakupu. Jeżeli jednak inaczej ubierzesz to w słowa, mówiąc: „Proszę posłuchać, nasza polityka bezpieczeństwa zakłada, że przez 99,9% czasu będziemy potrzebowali dostępu do sieci ogólnoświatowej — potrzebujemy nowej zapory sieciowej", wtedy prawdopodobnie reakcja będzie bardziej pozytywna. Jeśli szef okaże się mało podatny na tego rodzaju propozycje, możesz wspomnieć, że zarząd powołał grupę specjalistów, których zadaniem będzie przeprowadzenie sprawdzianu zgodności sytuacji w firmie z założeniami

przyjętej polityki bezpieczeństwa, a kolejne spotkanie podsumowujące wyniki testu odbędzie się już za miesiąc. Zdziwisz się, jak szybko tego rodzaju oświadczenia uwalniają potrzebne fundusze i zasoby.

Wielu spośród administratorów ma tendencję do lekceważenia testów penetracyjnych sieci, które przeprowadzane są przez firmy zewnętrzne. Są zdania, że jeżeli takie testy cokolwiek wykażą, to będzie to ukazanie administratorów w złym świetle. Jeśli jednak testy uzmysłowią wszystkim, że twoja sieć przypomina szwajcarski ser, wtedy być może ktoś zacznie wreszcie brać na poważnie uwagi o potrzebie systemu wykrywania włamań, wzmocnienia metody uwierzytelniania i dodatkowego etatu dla administratora, który pomoże nadążyć za nowymi programami korygującymi i naprawiającymi odkryte luki w systemach zainstalowanych na twoich serwerach. Wiesz już, dlaczego tak ważne jest twoje zaangażowanie w proces oceny i tworzenia polityki bezpieczeństwa? Ostatecznie przecież wyniki tego procesu mogą zaważyć na wysokości otrzymywanych przez ciebie funduszy.

Programy IA

Punktem wyjścia dla procesu zapewnienia bezpieczeństwa są czynności na poziomie organizacyjnym a nie fizycznym, na którym zaczynasz od konfiguracji serwera czy systemu operacyjnego. Przywołując dobrze znaną i trochę oklepaną analogię, nie zbudujesz domu, który ma ci służyć przez lata, stawiając go na słabych fundamentach. W przypadku procesu bezpieczeństwa fundamentem jest program ochrony informacji *IA* (skrót *IA* pochodzi od angielskiego *information assurance*). Mówiąc o IA, mamy na myśli program łączący wszystkie aspekty bezpieczeństwa, poczynając od odpowiedzialności organizacyjnej do ról pojedynczych osób, od całości łańcucha odpowiedzialności do mechanizmów audytu. Pierwszą decyzją, jaka jest podejmowana podczas programu IA, jest wskazanie pewnej osoby wewnątrz firmy, która będzie posiadała właściwe upoważnienia i będzie odpowiedzialna za przeprowadzenie programu IA w przedsiębiorstwie. Pełnomocnictwo i obowiązki tego rodzaju mogą być udzielone pojedynczej osobie albo też całemu pionowi lub działowi w firmie. Odpowiedzialność obejmuje podjęcie kompleksowych działań zmierzających do zapewnienia bezpieczeństwa zasobom informacyjnym i systemom służącym do przetwarzania chronionych informacji.

Zwykle programem IA kieruje dyrektor IA, który odpowiada bezpośrednio przed prezesem lub radą nadzorczą przedsiębiorstwa. Wewnątrz każdej organizacji, czy będzie to dział zasobów ludzkich (HR), IT, pion produkcji, sprzedaży czy też pion operacyjny, ktoś sprawuje funkcję specjalisty IA. Jest to osoba kontaktowa, jeśli chodzi o wszystkie sprawy związane z zagadnieniami bezpieczeństwa w firmie, i składa raporty bezpośrednio dyrektorowi IA. W zależności od wielkości firmy i jej potrzeb człowiek ten może być zatrudniony na pół etatu bądź też może to być jego jedyne zajęcie. Każda z wyznaczonych osób ma wpływ na rozwój i monitorowanie zgodności programu z przyjętą w firmie polityką bezpieczeństwa.

Podstawowym celem poprawnie wdrożonego programu IA ma być uruchomienie „koła bezpieczeństwa", które zacznie działać we wszystkich działach i pionach przedsiębiorstwa. Do zadań jednostkowych zalicza się:

1. Ocenę infrastruktury informacyjnej, określenie zasobów krytycznych i stworzenie dokumentu, w którym jasno opisane zostaną istotne zasoby i ich wrażliwość.
2. Stworzenie polityki bezpieczeństwa odpowiadającej elementom, które zostały zawarte w powstałym dokumencie.
3. Określenie zakresu odpowiedzialności organizacyjnej i planu wdrażania polityki bezpieczeństwa.
4. Implementację środków technicznych służących do wdrażania polityki bezpieczeństwa.
5. Wprowadzenie w życie procedur administracyjnych służących do wdrażania polityki bezpieczeństwa.
6. Monitorowanie i ulepszanie programu IA.

Rozumienie wagi programu IA

Pewna firma telekomunikacyjna zleciła nam niedawno przeprowadzenie oceny stanu bezpieczeństwa. Na początku procesu stwierdziliśmy, że nikt spoza pionu IT nie tylko nie został powiadomiony o fakcie przeprowadzania takiej oceny, ale że w trakcie operacji nawet nie planowano żadnej współpracy pomiędzy przedstawicielami innych działów. Odpowiedzialność za politykę bezpieczeństwa w firmie spoczywała na pracowniku z działu HR, ale osoba ta nie miała żadnych uprawnień do wydawania decyzji związanych z pozostałymi działami — czy to pionem produkcji czy też centrum operacyjnym.

Kiedy wytłumaczyliśmy, na czym właściwie polega proces oceny, nasze wyjaśnienia spowodowały konieczność zastanowienia się nad rzeczywistymi potrzebami firmy. Ostatecznie nasz projekt został zaprezentowany CEO, który wyznaczył zastępców kierowników każdego działu jako współodpowiedzialnych za proces oceny bezpieczeństwa. Pierwszym naszym zadaniem, jeszcze przez rozpoczęciem całości procesu, była więc pomoc w stworzeniu struktur organizacyjnych i uświadomieniu celów programu IA. Efektem końcowym było przesunięcie odpowiedzialności za proces oceny na wyższy poziom, ponieważ osoba odpowiedzialna za program IA składała raporty bezpośrednio członkom rady nadzorczej.

Gdyby program przeprowadzony został w sytuacji organizacyjnej, którą zastaliśmy pierwszego dnia, raporty o stanie bezpieczeństwa mogłyby ugrzęznąć na poziomie pracownika HR pełniącego obowiązki specjalisty IA. Stałoby się tak niechybnie, gdyby ocena bezpieczeństwa stawiała kogoś w złym świetle (szczególnie gdyby chodziło o pracowników z działu HR). Po zmianach organizacyjnych wszystkie uwagi mogłyby docierać (gdyby okazało się to konieczne) bezpośrednio do rady nadzorczej firmy. Były także inne zalety tych zmian. Dzięki możliwości konsultacji z menedżerami, zastępcami kierowników itp. grupa ludzi zajmująca się przeprowadzaniem oceny mogła teraz zebrać dużo więcej istotnych informacji dotyczących struktury przedsiębiorstwa, zasobów krytycznych. Informacji byłoby mniej, gdyby ocena ograniczyła się tylko do pracowników pionu IT.

Najważniejsze pytanie, które zadawaliśmy, brzmiało: „Jaka strata lub jakiego rodzaju przerwa w działalności może spowodować bankructwo firmy?" Nie jest to pytanie, na które potrafi odpowiedzieć zwykły administrator systemu. Potrafi za to ktoś z grona kierowniczego. Nasze działania doprowadziły do przeprowadzenia oceny stanu bezpieczeństwa w firmie, ale także do określenia programu IA i zdefiniowania pierwszej w historii firmy polityki bezpieczeństwa. Przytoczony tutaj przykład wskazuje wyraźnie, jak ważne jest rozpoczęcie procesu od odpowiedniego miejsca i stworzenie podwalin procedur i polityki bezpieczeństwa. Elementy te są ważniejsze niż zbyt pochopne koncentrowanie się na aspektach technicznych.

Ocena funkcjonalna

Jeśli w firmie zdefiniowano już program IA lub przynajmniej określono rolę i zakres odpowiedzialności osoby, której zadaniem będzie przeprowadzenie procesu oceny, następnym krokiem jest ocena funkcjonalna. Cel tej fazy jest jasno określony: identyfikacja zasobów informacyjnych będących w posiadaniu organizacji i klasyfikacja ich w zależności od „poziomu krytyczności", wagi, wartości i wpływu, jaki miałaby ich utrata na działalność firmy.

Na tym etapie w dużej mierze będziemy mieli do czynienia z tzw. „robotą papierkową", której rezultatem niekoniecznie musi być rekomendacja zakupu nowej zapory sieciowej czy zalecenie wskazujące na konieczną zmianę długości hasła i jego formy (składu hasła). Jednym z najważniejszych elementów przydatnych nam w dalszej pracy, a jednocześnie pozornie nie mającym żadnego związku z zagadnieniami bezpieczeństwa jest tzw. matryca krytyczności (tj. matryca, w której sklasyfikowane będą zasoby informacyjne, przy czym głównym kryterium będzie waga danych zasobów — ich krytyczność z punktu widzenia działalności firmy).

Zanim zdecydujesz się na opuszczenie pozostałej części rozdziału, dobrze by było gdybyś poświęcił trochę czasu, żeby dowiedzieć się, czym tak naprawdę jest matryca krytyczności. Podstawowym powodem wymuszającym na nas utworzenie matrycy krytyczności jest stwierdzenie, iż dopóki nie wiesz, które zasoby są rzeczywiście istotne z punktu widzenia działalności organizacji, nie znasz ich wpływu na procesy biznesowe zachodzące w firmie i nie wiesz, co stałoby się z przedsiębiorstwem, jeśli dane zasoby uległyby zniszczeniu, dopóty nie określisz poprawnie niezbędnych środków bezpieczeństwa. Jako administrator możesz na przykład spędzać mnóstwo czasu, zabezpieczając serwer sieciowy i nie przejmować się ochroną istotnej bazy danych, która w tym czasie mogłaby być bez trudu splądrowana czy wykradziona. Jeżeli w takim przypadku włamanie na serwer przynosi nieporównywalnie niższe straty niż utrata danych z bazy, twoje wysiłki idą na marne. Będąc pracownikiem działu IT, możesz niestety nie wiedzieć, gdzie ukryte są prawdziwe skarby. Ta wiedza często dana jest menedżerom, członkom zarządu i innym pracownikom firmy, którzy nie należą do kadry pracowniczej pionu IT.

Jeśli wszyscy ci ludzie dobrze wykonują swoją pracę, członkowie zespołu dokonującego oceny zajmą się wszystkimi elementami, które mają jakikolwiek wpływ na bezpieczeństwo zasobów. Elementy te będą się zmieniać w zależności od rodzaju dokonywanej oceny i nazewnictwa stosowanego przez dokonujących analizy. Można jednak uznać, że w mniejszym lub większym stopniu pokrywać się będą z elementami wyszczególnionymi poniżej:

- polityka;
- zarządzanie ryzykiem;
- zarządzanie i kontrola nad kontami użytkowników;
- sterowanie konfiguracją sprzętową i programową;
- kontrola sesji;

- bezpieczeństwo sieci;
- dostęp zdalny;
- administrowanie systemem;
- reakcja na incydent;
- audyt;
- ochrona antywirusowa;
- planowanie reakcji na przypadkowe zdarzenia;
- kopie bezpieczeństwa i odzyskiwanie;
- konserwacja, utrzymanie sprzętu itd.;
- bezpieczeństwo fizyczne;
- aspekty bezpieczeństwa w odniesieniu do personelu;
- szkolenia i zwiększanie świadomości dotyczącej bezpieczeństwa;
- odzyskiwanie danych po naruszeniu bezpieczeństwa.

Zadaniem oceny funkcjonalnej jest zdobycie wszystkich istotnych informacji, dzięki którym będziesz mógł stworzyć podstawy polityki bezpieczeństwa odnoszącej się do elementów ważnych z punktu widzenia działalności firmy. Proces oceny rozpoczyna najczęściej spotkanie informacyjne, na którym wszyscy zainteresowani poznają sposób, w jaki proces będzie przebiegał. Ważne jest, aby na spotkaniu pojawili się reprezentanci wszystkich grup, które będą w jakiś sposób zaangażowane w proces: osoby reprezentujące pion IT, dział zasobów ludzkich (HR), działy sprzedaży i marketingu, dyrektorzy i kierownicy przedsiębiorstwa, przedstawiciele działu prawnego, pracownicy eksploatacji i technicy oraz wszystkie inne osoby reprezentujące istotne z punktu widzenia działalności firmy działy i departamenty. Powinni oni znać swoją rolę i jej znaczenie dla całości procesu. Dzięki uczestnictwu w pierwszym spotkaniu informacyjno-organizacyjnym i poznaniu wagi procesu ci wszyscy ludzie stają się naszymi sprzymierzeńcami.

Kolejnym krokiem zespołu oceny będzie gromadzenie jak najbogatszej wiedzy o firmie: o jej działalności, zachodzących w niej procesach i sposobie współpracy poszczególnych działów. Informacje są zbierane za pośrednictwem serii wywiadów i rozmów, których celem będzie określenie krytycznych zasobów informacyjnych firmy. Pierwsze wywiady często wywołują kolejne spotkania, bo w miarę jak odkrywana jest struktura przedsiębiorstwa, pojawiają się wątki i zagadnienia, których wcześniej nie poruszano. Jako wynik całej serii zabiegów powstaje lista krytycznych zasobów informacyjnych i wspomniana już (będzie o niej mowa także w dalszej części rozdziału) matryca krytyczności.

Matryca krytyczności jest tematem, który warto trochę lepiej poznać, gdyż to ona stanie się podstawą budowania polityki bezpieczeństwa. Matryca określa każdy zasób informacyjny: ważne bazy danych, źródła informacji lub procesy i dokonuje ich klasyfikacji przy pomocy trzech czynników zwanych *atrybutami wpływu*. Oto one:

- *Poufność* — co stanie się, gdy dany zasób zostanie ujawniony nieodpowiednim osobom?
- *Integralność* — co stanie się, gdy informacja zostanie w jakiś sposób uszkodzona lub zmodyfikowana?
- *Dostępność* — co stanie się, gdy zasób będzie przez pewien czas niedostępny?

Każdemu z tych atrybutów przydziela się pewną *wartość wpływu*, która wskazuje na jego wagę. Często wartość określana jest trójstopniowo: niska, średnia i wysoka. Definicja poszczególnych wartości wpływu zależy głównie od rodzaju przedsiębiorstwa i prowadzonej działalności. Może na przykład wyglądać jak ta poniżej:

- *Niska* (N) — niedogodność i kłopot dla klientów firmy. Straty finansowe z powodu zaburzenia działalności firmy są minimalne. Ryzyko ogólnego pogorszenia relacji z klientami jest niskie.
- *Średnia* (Ś) — firma X może nie wywiązać się z przyjętych zobowiązań. Możliwe jest wszczęcie przeciwko niej postępowań sądowych, które na tak ograniczonym rynku mogą spowodować czasową utratę konkurencyjności.
- *Wysoka* (W) — sprawy sądowe w toku. Duże straty finansowe firmy. Umowy zerwane. Wynikiem ostatecznym jest całkowita utrata konkurencyjności i zastopowanie działalności firmy.

Matryca krytyczności to tabela, w której wyszczególniono istotne zasoby i przyporządkowano im pewne wartości zgodnie z kryteriami zaprezentowanymi powyżej. Taka przykładowa matryca została zaprezentowana w tabeli 2.1.

Tabela 2.1. *Prosta przykładowa matryca krytyczności*

Zasoby krytyczne	Poufność	Integralność	Dostępność
Baza zawierająca dane dotyczące klientów firmy	W	W	N
Lista płac	N	Ś	N

W matrycy z powyższej tabeli uwzględniono dwa zasoby: bazę danych o klientach i listę płac. Przyporządkowane zasobom wartości wpływu pokazują, że jeżeli baza zawierająca dane o klientach zostanie ujawniona (na przykład trafi do konkurencji lub do szerszego grona osób nieuprawnionych), to będzie to miało bardzo duży wpływ na działalność firmy (z punktu widzenia poufności). Jeśli baza zostanie w jakiś sposób uszkodzona, także będzie to związane z wysokim wpływem na codzienną działalność firmy (z perspektywy integralności), bo być może jest ona wykorzystywana podczas sprzedaży produktów przedsiębiorstwa. Jeżeli baza danych stanie się przez pewien czas niedostępna, wpływ na działalność firmy będzie stosunkowo niski (patrząc z punktu widzenia atrybutu dostępności), dlatego że wgląd w dane klientów nie jest niezbędny przez cały czas. Matryca krytyczności może wspomóc twórców polityki bezpieczeństwa w procesie decyzyjnym podczas przydzielania właściwego poziomu zabezpieczenia poszczególnym zasobom firmy i przekłada się bezpośrednio na środki wdrażane przez pracowników działu IT.

Przeczytaj jeszcze raz ostatnie zdanie wcześniejszego akapitu, bo mówi ono o tym, że niewielka tabela w dokumencie, którym może wcale się nie interesujesz, może bezpośrednio wpłynąć na twoje poczynania. Konieczność dostępu do bazy danych o klientach może na przykład wymagać zastosowania metod silnego uwierzytelniania takich, jak tokeny czy karty mikroprocesorowe (tzw. *smart cards*), szyfrowania transmisji w sieci VPN, częstej konieczności sporządzania kopii bezpieczeństwa czy nawet drogich macierzy RAID (które zapewnią zachowanie integralności), ale nie usprawiedliwi nadmiarowych klastrów bazy, bo tak naprawdę to nie dyspozycyjność jest tu najważniejsza. Zwróć uwagę — to wszystko, o czym była mowa w tym podrozdziale, naprawdę jest ważne!

Tworzenie polityki

Przeszedłeś już przez fazę oceny, w trakcie której udzieliłeś odpowiedniego wsparcia grupie konsultantów. Zespół dokonujący oceny stworzył matrycę krytyczności, która właściwie definiuje stosunek do istotnych zasobów firmy. Następnym zadaniem będzie stworzenie polityki bezpieczeństwa określającej, w jaki sposób wybrane zasoby powinny być ochraniane. Trzeba pamiętać, że dokument, w którym nakreślono zasady polityki bezpieczeństwa, ma sporą wagę. Podobnie jak dokumenty z fazy oceny w dużym stopniu wpływa on na poziom i standard zastosowanych później środków bezpieczeństwa.

Polityka bezpieczeństwa określa zasoby, które powinny być zabezpieczone — nie wskazuje na zastosowanie konkretnych metod. Polityka może mówić o konieczności zastosowania szyfrowania informacji krytycznych, ale nie dowiesz się z niej, czy do szyfrowania masz wykorzystać algorytm TripleDES czy IDEA. Nie dowiesz się także, z którego oprogramowania masz skorzystać i nie uzyskasz informacji o sposobie implementacji szyfrowania. Takich informacji nie uwzględnia się w polityce bezpieczeństwa, gdyż w przypadku zmiany stosowanej w firmie technologii całą politykę także należałoby zmienić. Jeżeli na przykład ktoś znajdzie w kodzie algorytmu TripleDES jakieś wady, które sprawią, że stanie się on bezużyteczny, polityka bezpieczeństwa, w której mowa o tym algorytmie, stanie się natychmiast anachronizmem. Patrząc na to z pewnej perspektywy, taka „ogólność" polityki bezpieczeństwa jest korzystna dla specjalistów z działu IT, ponieważ pozostawia szczegóły dotyczące wdrażania konkretnych rozwiązań w rękach tych, którzy będą bezpośrednio odpowiedzialni za działanie całego systemu zabezpieczeń. Nieodpowiednie rozwiązania nie będą narzucane z góry przez osoby, które nie mają żadnego doświadczenia w kwestiach technicznych i technologicznych, a zagadnienie bezpieczeństwa znają tylko teoretycznie.

Tworzenie polityki bezpieczeństwa nie polega na wycinaniu i wklejaniu do nowego dokumentu przygotowanych zawczasu pięknie brzmiących instrukcji i zaleceń. Jeżeli twój dokument nie zawiera rozwiązań odnoszących się bezpośrednio do sytuacji w twojej firmie, jest bezużyteczny, nie ma nic wspólnego z rzeczywistością. Nikt nie będzie postępował zgodnie z zawartymi w nim procedurami i, co gorsza, dokument ten nie pozwoli na właściwą ochronę zasobów firmy. Ta książka nie zrobi z ciebie guru polityki bezpieczeństwa. Na rynku znajdziesz wiele pozycji książkowych, propozycji standardów i szkoleń, które mają taki cel. Jednak, podobnie jak w przypadku innych innymi tematów, o których mowa w tym rozdziale, dobrze by było, gdybyś wiedział,

w jaki sposób powstaje polityka bezpieczeństwa. Dzięki tej wiedzy będziesz potrafił odpowiednio wspomóc proces jej powstawania, będziesz mógł wziąć w nim czynny udział i będziesz miał wpływ na końcowe rozwiązania, które powinny zostać zastosowane.

Proces tworzenia polityki bezpieczeństwa rozpoczyna się zaraz po zakończeniu fazy oceny. Stosuje się różne metody wykorzystywane podczas jej powstawania. Czasami polityka jest tworzona na podstawie zakresu odpowiedzialności organizacyjnej lub funkcjonalnej (obszarowej). Wydaje nam się, że jeżeli patrzy się na zagadnienie polityki z punktu widzenia podziału organizacyjnego w firmie (na przykład: co ma robić dział IT, co HR, a co użytkownicy końcowi itd.), bardzo trudno jest zlokalizować przypadki zachodzenia na siebie — lub przeciwnie — braku odpowiedzialności za pewne procesy. Z drugiej strony, gdy polityka jest rozpatrywana w oparciu o podział funkcjonalny dokonany w poprzednim podrozdziale (zarządzanie ryzykiem, kontrola nad kontami, sterowanie konfiguracją itd.), uzyskujemy pewność, że żaden z aspektów nie pozostanie pominięty. Odpowiedzialność za każdy obszar może być później przydzielona wybranej grupie lub pojedynczym osobom.

Biorąc pod uwagę, że większość użytkowników końcowych nie będzie miało ochoty na czytanie całej polityki bezpieczeństwa, wiele organizacji tworzy coś na kształt wzorca dokumentu polityki, w którym znajdują się wyszczególnione obszary odpowiedzialności. Na podstawie takich wzorców tworzy się potem bardziej zwięzłe wersje dokumentu zawierające politykę bezpieczeństwa, specjalnie przystosowane i przeznaczone dla wybranych grup: kierowników, użytkowników końcowych, działu IT. Z naszego doświadczenia wynika, że takie rozwiązania sprawdzają się najlepiej. Model polityki bezpieczeństwa będzie w dużej mierze zależał od potrzeb organizacji.

Warto wspomnieć, że w proces powstawania polityki bezpieczeństwa warto zaangażować wszystkie osoby, których „błogosławieństwa" będziesz wcześniej czy później potrzebował. Ważne jest, aby np. dział prawny był zaangażowany już we wczesne stadium procesu. Zdziwiłbyś się, jak bardzo nieprzyjemny może być dyrektor działu prawnego, kiedy położysz mu na biurku dokument, który w twoim mniemaniu jest końcową wersją polityki bezpieczeństwa. Bardzo często zdarza się, iż pewne kwestie prawne (które przeciętnemu pracownikowi nie przyjdą do głowy) mogą drastycznie wpłynąć na treść i jej końcowy kształt. Jaka stąd płynie nauka? Odpowiednie osoby muszą być zaangażowane w proces możliwie wcześnie. Informuj ich o postępie procesu, uczyń z nich swoich przyjaciół i sojuszników po to, aby ewentualne problemy zostawały odpowiednio wcześnie zauważane i rozwiązywane. Zrozumiesz, że jeżeli polityka będzie właściwie przygotowana i realna, a nie na pokaz, jej przestrzeganie i wprowadzanie stanie się łatwiejsze.

Tworzenie procedur i dokumentów operacyjnych

Zdefiniowanie polityki wyższego poziomu to jeszcze nie koniec procesu tworzenia odpowiedniej dokumentacji. Kolejnym istotnym elementem będą procedury i strategia operacyjna. To w tej fazie zagadnienia „co" pochodzące z polityki wyższego poziomu zostają przekształcone w „jak" wskazujące na określone procesy, systemy i implementacje. Z dokumentu dotyczącego ogólnej polityki bezpieczeństwa dowiesz

Prawdziwy koszt bezpieczeństwa

Nasza firma została zaangażowana, by pomóc pewnej organizacji, która straciła wysokiego rangą specjalistę z działu IT. Zarządzający przedsiębiorstwem, którego roczny dochód szacowany był na miliony dolarów, wpadli w panikę, bo człowiek ten został zatrudniony przez konkurencję. Jednym z kluczowych zasobów firmy była pewna baza danych. To właśnie ona w dużej mierze generowała zysk przedsiębiorstwa. Obawy kierownictwa wzbudzała możliwość, że wraz z ich pracownikiem konkurencja przejęła także bazę danych.

Nasz zespół przeprowadził analizę, której wynikiem było potwierdzenie uzasadnionych obaw. Co więcej, były pracownik nie tylko ukradł bazę, ale — korzystając ze sprzętu firmy, prawdopodobnie w godzinach pracy — stworzył oprogramowanie, które razem z bazą zostało przekazane konkurencji. Mógłbyś pomyśleć, że jego działania powinny spotkać się z ostrą reakcją, być może nawet procesem sądowym. No cóż... Pojawił się pewien poważny problem — w przedsiębiorstwie nie obowiązywała żadna polityka bezpieczeństwa. Nigdzie jasno nie zdefiniowano, że takie postępowanie jest niedozwolone! Tak więc, pomimo że w tym przypadku mieliśmy do czynienia z oczywistym i poważnym nadużyciem, były pracodawca nie mógł podjąć poważniejszych kroków zmierzających do wszczęcia postępowania sądowego. Dlaczego? Ponieważ w żadnym dokumencie nie było mowy, że takie działania są zabronione. Gdy przedsiębiorstwo wyszło już z kryzysu, a odniesione rany trochę się zagoiły, zdecydowano się na przeprowadzenie oceny stanu zabezpieczeń w firmie i w konsekwencji na stworzenie polityki bezpieczeństwa z prawdziwego zdarzenia. Ale stało się to trochę za późno — już po zdarzeniu, które mogło spowodować się naprawdę bardzo wysokie straty finansowe.

się, że należy regularnie sporządzać kopie awaryjne wszystkich informacji krytycznych, ale to w dokumencie operacyjnym znajdą się zalecenia co do stosowanych w tym celu środków i metod administrowania nimi.

Dokument operacyjny może na przykład wskazywać, że metodą archiwizacji dobrze odpowiadającą wymaganiom integralności ujętym w polityce będzie sporządzanie zapisów kopii zapasowych na taśmach i przechowywanie ich w specjalnie utworzonej bibliotece. W dokumencie operacyjnym mogą także znaleźć się informacje określające, kiedy takie zapisy archiwizacyjne powinny być tworzone, gdzie i jak długo taśmy powinny być przechowywane, kto może mieć do nich dostęp i jak mają wyglądać procedury ich wykorzystywania. Nie trudno się domyślić, iż dokumenty operacyjne powstają jako bezpośredni rezultat analiz przeprowadzonych w fazie oceny. Jest to jeszcze jeden powód, który przemawia za uczestnictwem specjalistów IT i administratorów w poczynaniach zespołu oceny: od tego zespołu zależy twój los — to on właściwie decyduje o wyposażeniu cię w odpowiednie narzędzia i środki, z którymi będziesz sobie później musiał radzić. Dokumenty i procedury operacyjne powinny być tak zaprojektowane, aby łatwo było dokonać ich późniejszej ponownej oceny i abyś mógł wykazać zgodność swoich poczynań z przyjętymi w firmie zasadami. W zależności od stanu architektury sieciowej i infrastruktury procedury mogą być definiowane w fazie ochrony zasobów lub wcześniej, w fazie tworzenia oceny i polityki.

Ocena techniczna

Polityka i ocena — czy ta faza nigdy się nie skończy? W trakcie całego procesu możemy mieć do czynienia z różnymi rodzajami ocen. Niektóre z nich (takie jak ocena organizacyjna) są wyraźnie ćwiczeniami wyższego poziomu. Inne (jak te wyszczególnione

w kolejnych podrozdziałach) wykonywane są na poziomie niższym, a ich celem jest dokopanie się do fundamentów infrastruktury IT. Podczas oceny technicznej dokonuje się dobrze znane testy penetracyjne, które pokazują, jak system poradzi sobie z atakami dokonywanymi od wewnątrz lub z zewnątrz sieci. Kilka testów technicznych dotyczy innych, wybranych obszarów infrastruktury sieci. W tej sekcji przyjrzymy się tym testom. Sprawdzimy, w jaki sposób są przeprowadzane, jakie korzyści przyniesie ich wykonanie i czy warte są wydanych na nie pieniędzy.

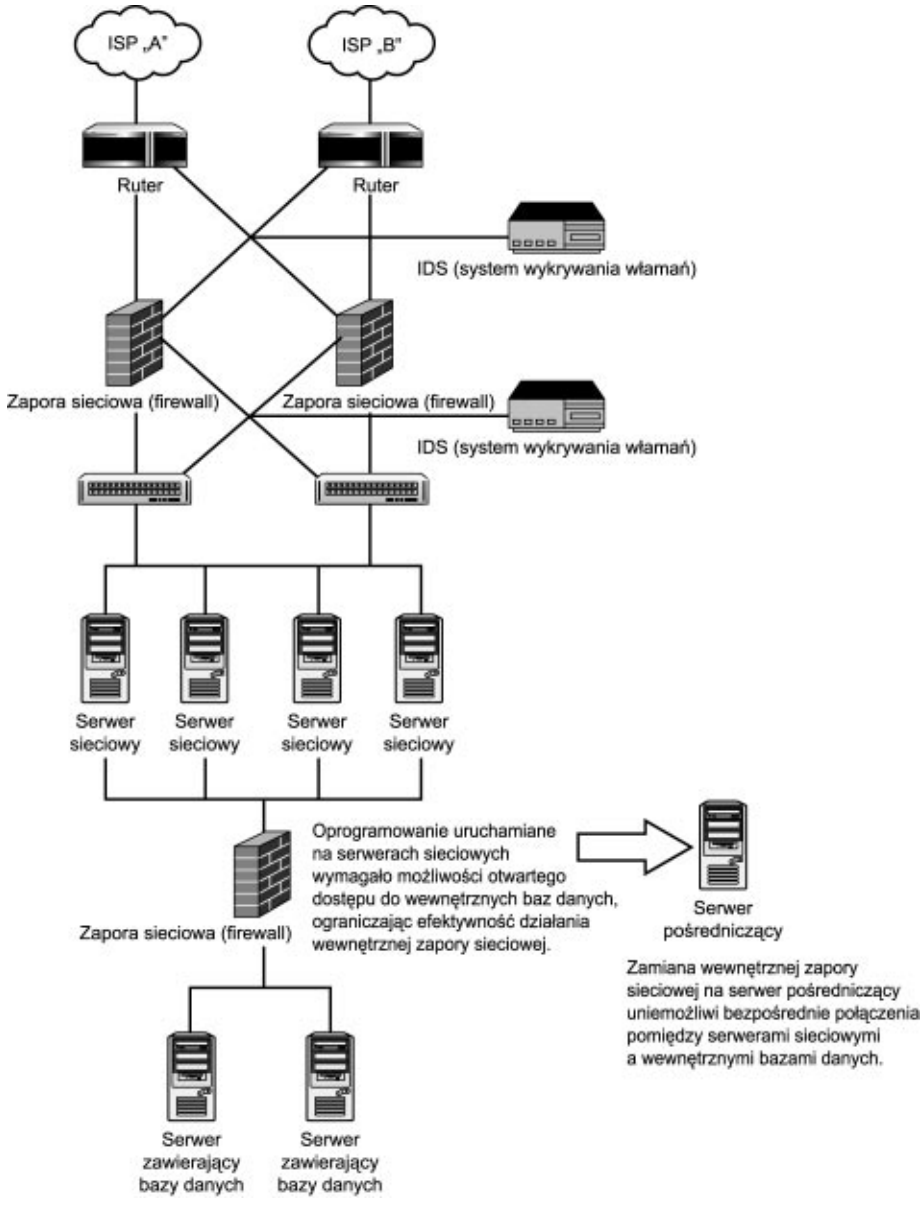
Ocena architektury

W wielu przedsiębiorstwach stosuje się środki wydające się odpowiednim zabezpieczeniem informacji, na której nam zależy. Mogą to być systemy zapór sieciowych, wykrywania włamań itp. Czasami jednak okazuje się, że istniejąca architektura sieciowa sprawia, że stają się one nieefektywne. W dalszych rozdziałach tej książki zaprezentujemy kilka typowych modeli architektury sieciowej i wskażemy, w jaki sposób powinny być one stosowane. Na razie jednak chcielibyśmy zwrócić uwagę na znaczenie możliwości oceny efektywności nie tylko pojedynczych elementów kontroli bezpieczeństwa, ale i oceny całości architektury sieci.

Nasza firma została zaangażowana do przeprowadzenia oceny stanu bezpieczeństwa wielkiej instytucji finansowej, która rozbudowywała infrastrukturę wspierającą rozwiązania bankowości internetowej. Niemal cała struktura sieci była stworzona przez sprzedawcę sprzętu komputerowego, który, jak tego się można było domyślać, określił wyraźnie markę ruterów, przełączników, a także zapór sieciowych i urządzeń służących do wykrywania włamań.

Chociaż trudno było jej cokolwiek zarzucić z punktu widzenia dostępności, jednak struktura sieci powodowała pewne problemy, które nie były związane z komponentami (tj. z urządzeniami). Serwery sieciowe, do których klienci mieli bezpośredni dostęp, miały także bezpośrednie połączenie z wewnętrznymi serwerami baz danych i komputerem centralnym (mainframe), gdzie przechowywane i przetwarzane były wszystkie żądania przychodzące od użytkowników kont. Mimo że pomiędzy serwerami sieciowymi a serwerami wewnętrznych baz danych stał firewall, używane oprogramowanie wymuszało otwarty dostęp do baz danych. Efekt był taki, że pomimo fizycznej obecności w rzeczywistości zapora sieciowa była bezużyteczna. Lepszym rozwiązaniem byłoby ustawienie w tym miejscu serwera pośredniczącego (proxy), dzięki któremu zapora sieciowa mogłaby skutecznie ograniczać ruch pomiędzy serwerami sieciowymi a bazami danych i niemożliwe byłoby bezpośrednie połączenie (patrz rysunek 2.2). W przypadku ewentualnego ataku na serwery sieciowe, napastnik nie mógłby dostać się dalej, tj. do serwerów z bazami danych zawierającymi krytyczne informacje ani do komputera centralnego lub do wewnętrznej sieci korporacyjnej.

Z przytoczonego przykładu można wyciągnąć dwa wnioski. Po pierwsze, nigdy nie pozwalaj sprzedawcy sprzętu na projektowanie struktury twojej sieci bez nadzoru i oceny ze strony niezależnych konsultantów. Po drugie, nigdy nie zakładaj, że architektura jest bezpieczna, nawet gdy z punktu widzenia topologii sieci nic jej nie można zarzucić. Przed uznaniem struktury za bezpieczną oprogramowanie, dostępność danych i usług należy poddać testom.



Rysunek 2.2. *Wymagania funkcjonalne mogą ograniczyć efektywność wewnętrznej zapory sieciowej*

Testy penetracyjne

Testy penetracji sieci równie dobrze mogłyby zostać umieszczone w sekcji monitorowanie i wykrywanie włamań, ale z uwagi na fakt, że zwykle są one wymagane przez zespoły dokonujące audytu (a nie administratorów), zostały umieszczone w tej sekcji. W dużym skrócie testy te polegają na przeprowadzeniu prób włamania do systemu. Zespół specjalistów na różne sposoby sprawdza skuteczność działania mechanizmów

zabezpieczających sieć: próbują oni ataków z zewnątrz (z Internetu) lub od wewnątrz (ze stanowisk fizycznie znajdujących się w siedzibie firmy), wykorzystują łączność komutowaną i łącza partnerskie, a czasami nawet korzystają z metod inżynierii społecznej (tzw. *social engineering*). W tym momencie testy stają się naprawdę ciekawe. Każdy z nich ma odrobinę inny charakter. Wartość i znaczenie każdego z nich także jest inne.

Poszukiwanie słabych punktów — skanowanie sieci

Pierwszy typ testu zwany jest czasami skanowaniem systemu. Tego rodzaju testy wykonywane są najczęściej przy użyciu zautomatyzowanego narzędzia, które skanuje komputery macierzyste w sieci, sprawdza występowanie znanych luk programowych lub systemowych i przygotowuje specjalne raporty. Dzięki takiemu skanowaniu dowiesz się, czy przypadkiem ktoś bez twojej wiedzy nie uruchomił nowego serwera lub usługi (na przykład łączności telnetowej), która nie powinna być uruchamiana. Ponadto uzyskasz informacje o wszystkich nietypowych konfiguracjach (np. oprogramowania serwerowego Windows NT), w których nie zastosowano niezbędnych pakietów Service Pack lub uaktualnień. Jeżeli testy tego rodzaju wykonywane są regularnie (np. co miesiąc lub co kwartał), dają ci coś w rodzaju niepewnego odczucia, że drzwi do twojej sieci nie są szeroko otwarte dla każdego, kto ma ochotę wejść.

Odnajdywanie słabości sieci — testy

Kolejny rodzaj testów penetracyjnych pochodzi jakby „z wyższej półki". Zaawansowane testy wyszukujące słabości systemów oferowane są przez większość firm profesjonalnie zajmujących się zapewnianiem i oceną stanu bezpieczeństwa. Do testów wykorzystywane są komercyjne skanery takie, jak ISS Scanner czy Network Associates' Cybercop Scanner — trochę bardziej dokładne niż ich odpowiedniki, o których była mowa w poprzednim podrozdziale. Niestety wiele przedsiębiorstw polega wyłącznie na tego rodzaju testach i nie wykonuje dodatkowych szczegółowych badań wykrytych słabości systemowych.

Ponieważ obsługa takiego zaawansowanego skanera polega niemal wyłącznie na podawaniu mu kolejnych adresów IP do sprawdzenia, można by rzec, iż wartość tego rodzaju testów jest w niepewna. Przecież równie dobrze takie testy mógłby przeprowadzić specjalista z działu IT. Wystarczy tylko kupić odpowiednie narzędzia. Tego rodzaju testy są najczęściej wykonywane na żądanie zespołów dokonujących audytu, a jeżeli przeprowadzi je ogólnie znana, poważna i szanowana firma, uważa się je za wystarczające. Okazuje się jednak, że testy te nie są bez wad. Przede wszystkim trzeba przypomnieć, że skanery są uaktualniane co pewien czas, więc z pewnością nie nadążają za odkrywanymi coraz to nowymi lukami i słabościami systemów. Już w chwili dokonywania testu próbujesz nadążyć za dniem wczorajszym. Po drugie, skanery potrafią odszukać większość słabości twojego systemu, ale z pewnością nie wszystkie. Testy skanowania są prawdopodobnie wystarczające, jeśli głównym twoim zadaniem jest ochrona przed „skryptowcami" czy napastnikami, którzy używają raczej gotowych rozwiązań pobranych z Internetu i przygotowanych przez innych hakerów i nie poświęcają tygodni czy miesięcy na „próbkowanie" systemu i wyszukiwanie jego możliwych słabości. Jeżeli jednak sądzisz, że zasoby, które ochraniasz, mają wielką wartość, powinieneś wykonać testy penetracyjne jeszcze wyższego poziomu.

Zespoły testerów (Red Team)

Najbardziej zaawansowaną (i być może najbardziej dokładną) formą testów penetracyjnych jest skorzystanie z usług tzw. Red Team. Grupa praktyków-specjalistów ds. bezpieczeństwa wykorzystuje wszystkie dostępne im metody i znane słabości, próbując włamać się do danego systemu tak, jakby to właśnie oni byli prawdziwymi napastnikami. Red Team zbiera wszystkie informacje dotyczące sieci pochodzące z ogólnie dostępnych źródeł i z Internetu, a potem wykonuje zautomatyzowane skany pozwalające na uzyskanie obrazu struktury sieci i dostępnych w niej zasobów informacyjnych. Prowadzi to do wyszczególnienia i identyfikacji poszczególnych serwerów i umożliwia rozpoznanie najdogodniejszej drogi prowadzącej do nadużycia i zdobycia wartościowych zasobów. Po zakończeniu tej fazy rozpoczyna się zwykle etap prób wykorzystania poznanych słabości.

Na prostym przykładzie pokażemy teraz, dlaczego Red Team jest efektywniejszy niż zautomatyzowane skanery. Wbudowane w skanery oprogramowanie sprawia, że urządzenia „myślą", iż wszystko dzieje się zgodnie z pewnymi standardami (IETF RFC). Jeżeli więc skaner odnajduje na serwerze usługę korzystającą z portu 1433, przyjmuje, że serwer działa pod kontrolą systemu operacyjnego z rodziny Windows i że chodzi tu z pewnością o bazę danych SQL (właściwie MSQL). Przyjmując takie założenia, natychmiast uruchamia wszystkie znane mu metody wykorzystania słabości MSQL. Członkowie zespołu Red Team potrafią jednak lepiej zinterpretować płynące z serwera odpowiedzi i zauważają, że charakterystyka odpowiedzi nasuwa raczej przypuszczenie, że na serwerze uruchomiony jest Window Terminal Server (lub Citrix WinFrame) a nie MSQL. Skaner został wprowadzony w błąd, dlatego że przemyślny administrator, chcąc uchronić system przed hakerami, zamienił porty. Kiedy członkowie zespołu Red Team określą już rzeczywistą usługę, która wykorzystuje dany port, nie będą marnować czasu na nieefektywne próby wykorzystania znanych luk MSQL, tylko zajmą się potencjalnymi słabościami odkrytej usługi.

Wadą metody polegającej na wykorzystywaniu zespołu „najemnych napastników" jest niemożność określenia rzeczywistych umiejętności wchodzących w jej skład osób. Red Team, który składa się z ludzi niedoświadczonych, nie będzie zbyt efektywny. Ponieważ umiejętności wymagane w przypadku tego zespołu należą raczej do „ciemnej strony" sztuki bezpieczeństwa, trudno jest być pewnym, że dostaje się to, za co się płaci. Na etapie podejmowania decyzji o wyborze firmy, która będzie odpowiedzialna za stworzenie zespołu Red Team, dobrym rozwiązaniem jest pytanie o opinie i referencje, jakie mogą udzielić dotychczasowi zleceniodawcy. Jeżeli w twojej firmie masz dobrych specjalistów, którzy świetnie znają się na zagadnieniach sieci, systemów operacyjnych itd., poproś ich o zweryfikowanie i ocenę profesjonalizmu (choćby tylko na podstawie rozmowy telefonicznej) członków zespołu Red Team.

Skaner vs. testerzy

Zespoły Red Team są podobne do komandosów — potrafią się przystosować, improwizować i skutecznie uderzyć, gdy przyjdzie na to pora. Skaner umie tylko wysyłać pakiety zaadresowane na wskazane adresy IP, w nadziei na wykorzystanie znanej słabości i luk systemowych. Członkowie Red Team zdolni są do skomplikowanej analizy wszystkich posiadanych informacji o celu, która często pozwala wykorzystać mniej widoczne słabości.

Poniżej znajduje się przykład opisujący przypadek, gdy skaner nie odnalazł luki, która została wykorzystana przez nasz zespół.

Niektóre słabości mogą być wykorzystane tylko wtedy, gdy istnieje kilka dodatkowych czynników. Napastnik może wykorzystać do nadużycia bibliotekę *msadc.dll* tylko wtedy, gdy spełnione są wszystkie poniższe warunki:

1. Serwer będący celem ataku pracuje pod kontrolą systemu z rodziny Windows.
2. Biblioteka *msadc.dll* jest obecna i dostępna na serwerze będącym celem.
3. Na serwerze uruchomiony jest IIS w wersji 4.0.
4. Na serwerze dokonanych zostało kilka specjalnych skojarzeń plików.
5. Na serwerze są obecne pewne specjalne zasoby.

Automatyczny skaner stwierdzi istnienie luki, gdy spełniony zostanie warunek 2. i biblioteka *msadc.dll* znajduje się w standardowej (spodziewanej) lokalizacji. Wynikiem testu dokonanego przez skaner wykorzystywany przez Red Team mogą być na przykład takie komunikaty:

A. Biblioteka *msadc.dll* odnaleziona, serwer jest podatny na atak.

B. Biblioteka *msadc.dll* nie znaleziona, serwer jest bezpieczny.

Okazuje się jednak, że wynik podany przez skaner nie jest do końca zgodny z prawdą. W przypadku A skaner wskazuje, że jeżeli biblioteka *msadc.dll* jest obecna, to serwer jest podatny na atak. W rzeczywistości serwer nie byłby narażony na atak napastnika wykorzystującego *msadc.dll*, *gdyby*:

1. Na serwerze nie został zainstalowany system Windows. W przypadku innych systemów operacyjnych obecność biblioteki nic napastnikowi nie daje.
2. Na serwerze uruchomiona jest wersja IIS 5.0 a nie 4.0. Serwer nie jest narażony na wykorzystanie biblioteki.
3. Na serwerze nie ma odpowiednich zasobów programowych, które są wymagane do wykorzystania biblioteki. Serwer nie jest podatny na atak.
4. Nie dokonano pewnych niezbędnych skojarzeń rozszerzeń plików. Nie można skorzystać z omawianej słabości.

Jeżeli więc biblioteka *msadc.dll* została odnaleziona w swej typowej lokalizacji, a skaner zakomunikuje istnienie niebezpieczeństwa dla badanego serwera, niebezpieczeństwo to może okazać się tylko teoretyczne. W opisywanej przez nas rzeczywistej sytuacji skaner doniósł o nieodnalezieniu biblioteki (komunikat B) *msadc.dll* i uznał, że serwer nie jest podatny na zagrożenie płynące z możliwości jej wykorzystania.

Komunikat skanera nie rozwiał jednak wątpliwości członków Red Team. Zdawali sobie oni sprawę z tego, że biblioteka równie dobrze może mieć inną lokalizację. Niektórzy administratorzy, postępując zgodnie z zasadą „minimum uprawnień (informacji) = maksimum bezpieczeństwa", ukrywają położenie bibliotek systemowych. Potrafią oni w ten sposób oszukać mniej doświadczonych hakerów. Jednak członkowie Red Team (i bardziej zdeterminowani hakerzy) nie nabierają się na takie sztuczki. Udało im się odszukać *msadc.dll*, ale okazało się, że na serwerze nie ma odpowiedniego oprogramowania, które umożliwiłyby wykorzystanie tej słabości. To jednak nie koniec. Obecność *newdsn.exe* na serwerze będącym celem ataku umożliwiła im stworzenie niezbędnych do wykorzystania *msadc.dll* zasobów programowych. Ostatecznie, pomimo że skaner nie odnalazł w ogóle biblioteki *msadc.dll* (która pozwoliłaby na dokonanie nadużycia), zespół „najemnych napastników" odkrył możliwość wykorzystania luki w systemie.

Testy penetracyjne — aplikacje

Załóżmy, że udało ci się znaleźć grupę kompetentnych osób, które dokonały oceny bezpieczeństwa serwerów i struktury sieci. Słabości i luki systemowe zostały wykryte i system jest tak szczelny jak tylko możliwe. Czy to wszystko, co można było zrobić? No cóż, to zależy. Działalność wielu firm w Internecie opiera się na szeroko pojętym przetwarzaniu transakcji (często na bieżąco — w trybie online). Na przykład wiele instytucji finansowych umożliwia zarządzanie twoim rachunkiem bankowym, dokonywanie transakcji giełdowych, składanie wniosków o karty kredytowe itp. właśnie za pośrednictwem sieci. Problem, z którym mamy do czynienia, jest następujący: pomimo że większość słabości i luk w systemach operacyjnych czy wad sprzętu sieciowego jest dość dobrze znana, oprogramowanie, które jest (przykładowo) wykorzystywane do dokonywania transakcji giełdowych, zostało prawdopodobnie stworzone zupełnie niedawno — przez grupę programistów zamkniętych na sześć miesięcy w ciemnym pokoju. Chodzi o to, że słabości takich aplikacji wykonywanych na specjalne zlecenie nie są jeszcze znane. Co gorsze, żaden automatyczny skaner ich nie wykryje z prostego powodu — potencjalne wady są typowe tylko i wyłącznie dla tej jednej aplikacji. Tak więc nawet w sytuacji gdy system operacyjny zostanie poprawnie zabezpieczony, piętą achillesową całej struktury może okazać się wyspecjalizowane oprogramowanie. Wady oprogramowania mogą na przykład pozwalać jednemu klientowi banku na bezprawne korzystanie z zasobów pieniężnych innego.

W dalszych rozdziałach tej książki zajmiemy się specyfiką luk w aplikacjach i powiemy, w jaki sposób sprawdzać oprogramowanie na obecność takich wad grożących nadużyciem. Teraz jednak ograniczmy się do stwierdzenia, że testy penetracyjne aplikacji są tak samo ważne jak testy struktury sieci. Niektóre aplikacje pozwalają na przykład na sprawdzenie informacji o koncie bankowym (w tym o wysokości salda) za pomocą numeru konta umieszczonego w adresie URL. W tak prostym przypadku wystarczy, że przebiegły użytkownik stworzy URL i zamieni własny numer konta w adresie na numer konta osoby, o której chce zasięgnąć informacji. Za pomocą zwykłej przeglądarki może w ten sposób poznać stan konta innej osoby, nie dokonując prób włamania się do systemu operacyjnego, ani nie korzystając z żadnych innych nielegalnych metod. Wady aplikacji tego rodzaju są jak dotąd w pełni wykrywalne tylko dzięki zespołom specjalnych testerów. Wiele instytucji zaczyna coraz bardziej doceniać wagę testów penetracyjnych, które stają się niezbędną częścią procesu audytu.

Przeglądanie kodu źródłowego i audyt sprzętowy

Testy penetracyjne są dobrą metodą umożliwiającą sprawdzenie systemu w warunkach bojowych, ale ich efektywność jest ograniczana przez czas, jaki może zostać poświęcony na ich wykonanie. Potencjalny haker ma do dyspozycji tygodnie, miesiące, a nawet lata, w trakcie których próbuje znaleźć furtkę umożliwiającą mu wejście do systemu. Czas, którym dysponuje zespół testerów, czy czas działania skanera jest bardzo ograniczony. Są to tylko dni lub tygodnie. Z tego właśnie powodu ważna jest możliwość przeprowadzenia testów jeszcze innego rodzaju. Mamy tu na myśli kontrolowany audyt, który charakteryzuje się tym, że audytor uzyskuje bezpośredni dostęp do systemu. Ponieważ infrastruktura sieci składa się generalnie z kilku komponentów, ważne jest, aby podczas kontrolowanego (czasami mówi się „wspomaganego”) audytu sprawdzono każdą grupę — to znaczy:

- serwery, na których zainstalowane są różne systemy operacyjne i różne aplikacje komercyjne,
- urządzenia sieciowe,
- nietypowe aplikacje wykonywane na specjalne zlecenie,
- inne wyposażenie takie, jak centralki PBX i systemy sterowane głosem.

Przypomnijmy jeszcze raz, iż tymi zagadnieniami zajmiemy się szczegółowo w kolejnych rozdziałach. Argumentacja, której używa się, mówiąc o potrzebie przeprowadzania testów kontrolowanego audytu, jest prosta i przekonująca. Po pierwsze, całkiem prawdopodobna jest sytuacja, w której, mimo że np. na platformie uniksowej uruchamia się usługę zdalnego logowania (telnet) bez potrzeby podawania haseł, usługa ta jest blokowana przez firewall i nie zostanie odkryta podczas testów penetracyjnych. Jutro jednak administrator może zmienić konfigurację zapory sieciowej i umożliwić połączenia telnetowe, bo jest to na przykład konieczne z punktu widzenia interesu firmy (załóżmy, że partner biznesowy musi uzyskać możliwość dostępu do AS/400). W ten sposób administrator nieumyślnie powoduje powstanie luki w systemie bezpieczeństwa. W wyniku przeprowadzenia kontrolowanego audytu wykrywane są wszystkie tego rodzaju słabości systemu, gdyż audytor ma pełny dostęp i może skontrolować konfigurację systemu, włącznie z rodzajem dostępnych usług, poziomów łatek programowych, uprawnień użytkowników itp.

Kolejnym powodem, dla którego warto przeprowadzać tego rodzaju kierowane testy, jest fakt, że audytorzy mogą pomóc ci określić najbardziej optymalną konfigurację systemu (a także wspomogą cię listami kontrolnymi audytu). Dzięki nim będziesz w posiadaniu dokładnych informacji dotyczących takich szczegółów konfiguracji, jak: rodzaj możliwych do uruchomienia usług, uprawnienia do plików, ustawienia kont użytkowników itd. Jeżeli sprawujesz opiekę nad zespołem serwerów sieciowych i często zdarza się, że włączasz do struktury nowe systemy — wystarczy, że skonfigurujesz nowy system zgodnie z zaleceniami, sprawdzisz go według elementów listy kontrolnej i możesz być pewien, że system spełnia wymagania bezpieczeństwa. Podobnie jak w przypadku zespołów Red Team dobrze jest sprawdzić możliwości, umiejętności i referencje osób dokonujących audytów kierowanych.

Kolejnym rodzajem kierowanego audytu jest testowanie kodu źródłowego nietypowego (wykonywanego na zamówienie) oprogramowania. Autorzy tej książki mają sporo doświadczeń zebranych podczas prac dla amerykańskiego Ministerstwa Obrony Narodowej i mogą zapewnić, że każda linia kodu aplikacji, które tworzyliśmy, była skrupulatnie sprawdzana przez specjalistów dobrze znających swoją pracę i zagadnienia bezpieczeństwa oprogramowania. Szukali oni np. możliwości potencjalnego przepełnienia bufora, zastanawiali się, jakie byłyby konsekwencje pojawienia się usterek lub awarii aplikacji albo programów rezydentnych. Ci ludzie potrafią obejrzeć każdą linijkę kodu, zwracając uwagę na wszystkie miejsca potencjalnych problemów z bezpieczeństwem.

W dzisiejszych czasach realia rynku zwykle nie pozwalają na taką dokładność i skrupulatność, ale przeglądanie kodu źródłowego powinno być ważnym elementem w procesie tworzenia i rozwoju oprogramowania. Dobrą metodą usprawniającą test kodu

źródłowego jest wybranie tych fragmentów kodu, których działanie ma jakiś związek ze stroną zewnętrzną (klientem) lub wewnętrzną (komponentami wewnętrznymi systemu). W przypadku aplikacji stworzonej do obsługi bankowości elektronicznej należy dobrze sprawdzić wszystkie komponenty sieci, w których zachodzi interakcja z użytkownikiem końcowym, kierowane są zapytania do bazy danych i następuje dostęp do informacji na kontach, a nie na przykład część kodu odpowiedzialną za sporządzanie raportów, gdyż nie daje ona praktycznie żadnych możliwości nadużyć. Testy kodu źródłowego przynoszą pewną korzyść twórcom oprogramowania, bo mają oni okazję usłyszeć ocenę swojej pracy z punktu widzenia bezpieczeństwa aplikacji, a nie, jak to zwykle bywa, jej funkcjonalności. Większość programistów zwykle chętnie poddaje się krytyce, mogą się dzięki niej jeszcze wiele nauczyć, a testy kodu prowadzą czasami do powstania standardów wspomagających tworzenie bezpieczniejszych aplikacji.

Ochrona zasobów

Podsumujmy: podstawowe zasady polityki bezpieczeństwa w firmie zostały zdefiniowane, odpowiednie testy struktury systemu zostały przeprowadzone i znasz już słabe strony swojej sieci lub jesteś gotów do rozmieszczenia urządzeń, co pozwoli ci wreszcie rozpocząć fazę wdrażania teorii w życie. Jeżeli twój poziom wiedzy technicznej uważasz za wystarczający do zrozumienia większości zawartych w tej książce informacji, jest duża szansa, że wiesz, jakie są funkcje zapory sieciowej, jak działa ruter i jaka jest różnica pomiędzy przełącznikiem a koncentratorem. W dalszej części książki zajmiemy się bardziej szczegółowo zagadnieniami bezpieczeństwa związanymi ze wspomnianymi urządzeniami. W tym rozdziale jednak (jak to wciąż przypominamy) ograniczymy się do rozważań na nieco bardziej poziomie teoretycznych i z popatrzmy z pewnej perspektywy na lokalizację i funkcjonowanie komponentów sieci. Jeszcze raz chcielibyśmy powtórzyć, że celem tego rozdziału nie jest przemiana czytelnika w guru polityki bezpieczeństwa czy eksperta od ruterów, ale sprowokowanie do spoglądania nieco „z góry" na całość zagadnienia bezpieczeństwa, które umożliwi lepsze zrozumienie wysiłków wszystkich działów i pionów organizacyjnych i własnej roli w tym procesie.

Wdrożenie polityki bezpieczeństwa

Trzeba pamiętać o tym, że każdy zastosowany środek ochronny (od zasad definiujących długość i skład haseł, po instalację zapory sieciowej) powinien mieć swoje uzasadnienie wynikające z polityki bezpieczeństwa. Oczywiście same metody wdrażania odpowiednich środków nie są szczegółowo opisane w dokumencie dotyczącym polityki. Powinny one być określone przez osoby, które dobrze rozumieją i znają potencjalne zagrożenia. Ignorowanie zaleceń zawartych w polityce bezpieczeństwa podczas fazy decydowania o wdrażanych środkach jest zawsze poważnym błędem. W ostatecznym rozrachunku będziesz przecież oceniany na podstawie tego, w jaki sposób wypełniasz zalecenia przyjętej polityki.

Jeśli potrafisz mądrze wykorzystać zawarte w polityce zalecenia, z pewnością będziesz umiał usprawiedliwić zastosowane przez siebie rozwiązania i zakup sprzętu.

Jeżeli na przykład dostępność witryny firmowej jest jednym z pryncypiów (była oceniana wysoko w matrycy krytyczności), łatwo będzie wytłumaczyć konieczność tworzenia infrastruktury o możliwie wysokiej dyspozycyjności — a więc spełnią się twoje marzenia o wielu jednoczesnych łączach do Internetu, złożonej sieci kratowej ruterów (wzajemnie się uzupełniających), zapór sieciowych, urządzeń do wyrównywania obciążenia serwerów i samych serwerów. Gdyby aspekt dostępności witryny oceniono nisko a strona firmowa miała charakter statyczny i niemal wyłącznie informacyjny, trudno byłoby ci uzasadnić wydatki poniesione na większą ilość sprzętu sieciowego.

Nauka dla pracowników działu IT jest następująca: wybieraj projekty najlepiej dostosowane do zdefiniowanej polityki. A jeśli wydaje ci się, że polityka jest zła, to niewystarczająco zaangażowałeś się w proces jej tworzenia albo powinna zostać zmieniona, aby środki bezpieczeństwa uznane przez ciebie za niezbędne zostały zastosowane w przedsiębiorstwie, które jest twoim pracodawcą. O wiele łatwiej jest wpływać na politykę, kiedy jeszcze jest ona w fazie powstawania, niż wtedy, gdy dokument został zaaprobowany przez dziesięciu wiceprezesów, prawników itd. Rada jest prosta — nie stój z boku, udzielaj się w procesie powstawania polityki tak wcześnie i tak często, jak to tylko uznasz za konieczne.

Środki ochronne

Każdy element zaprezentowanego tu modelu bezpieczeństwa może być rozumiany jak kolejna warstwa chroniąca zasoby informacyjne przedsiębiorstwa. Definiowanie założeń polityki bezpieczeństwa oraz faza oceny i testów prowadzą do podejmowania decyzji określających zasoby, które powinny zostać chronione między innymi za pomocą wybranych środków. Z uwagi na fakt, że książka ta została poświęcona technicznej stronie zapewnienia bezpieczeństwa, nie będziemy tu zajmować się bezpieczeństwem fizycznym czy zagadnieniem świadomości wagi bezpieczeństwa wśród pracowników — skupimy się wyłącznie na komponentach bezpieczeństwa związanych z siecią. Najważniejsza porada, jakiej możemy udzielić czytelnikowi zaraz na początku, jest następująca: środki bezpieczeństwa powinny być wdrażane w całości jako jeden współpracujący system, a nie po kawałku, fragmentarycznie. Nie znaczy to, że na ten system muszą składać się koniecznie urządzenia pochodzące od jednego producenta. Jeżeli rutery i przełączniki to sprzęt Cisco, nie musisz od razu kupować zapory sieciowej Cisco. Chodzi o to, że każdy pojedynczy element powinien wykonywać zadania, które dopełniają oraz uzupełniają funkcje i role pozostałych komponentów sieci. Taki system powinien właściwie zabezpieczać zasoby, które zostały uznane za warte ochrony na podstawie matrycy krytyczności w polityce bezpieczeństwa obowiązującej w przedsiębiorstwie.

Dobrym przykładem wzajemnie uzupełniających się elementów jest para: system wykrywania włamań (IDS) plus zapora sieciowa. Sam firewall nie zabezpieczy sieci przed wszystkimi atakami. Zadaniem systemu wykrywania włamań jest raportowanie o wszystkich użytkownikach, którym udało się przedostać przez zaporę sieciową. Nie będziesz chciał wyrzucić zapory sieciowej tylko dlatego, że uruchomiłeś IDS i odwrotnie, nie możesz nie doceniać możliwości systemu wykrywania włamań tylko dlatego, że całkowicie ufasz możliwościom swojej zapory. Idea stojąca za tymi przykładami wydaje się oczywista, ale mówiąc obrazowo, wielu specjalistów, montując

stalowe drzwi na pudełkach kartonowych, nazywa je bezpiecznymi. Gdy kupisz nawet najdroższą, najszybszą i najlepszą zaporę sieciową i umieścisz ją przed serwerem z IIS w wersji 4.0 pracującym pod kontrolą niezabezpieczonego systemu operacyjnego Windows NT, możesz być pewien, że włamanie na ten serwer nastąpi tak szybko, jak szybko pierwszy lepszy „skryptowiec" spróbuje wykorzystać dobrze znane luki i słabości systemu. Jeżeli wszystkie komponenty nie będą z sobą odpowiednio współpracować, to uznając, że sieć jest bezpieczna, oszukujesz samego siebie.

Środki bezpieczeństwa to nie to samo co bezpieczny system

Oto prawdziwa historia. Pewne przedsiębiorstwo, którego roczny przychód wynosi blisko pół miliarda dolarów, wynajęło zewnętrznych konsultantów mających zabezpieczyć infrastrukturę sieciową za pomocą zapory sieciowej (nie powiemy jakiego producenta). W okresie następującym po incydencie lądowania w Chinach amerykańskiego samolotu z aparaturą szpiegowską należący do nich serwer sieciowy został skutecznie zaatakowany. Przedsiębiorstwo wynajęło naszą firmę do oceny stanu zabezpieczeń i przyczyn udanego włamania.

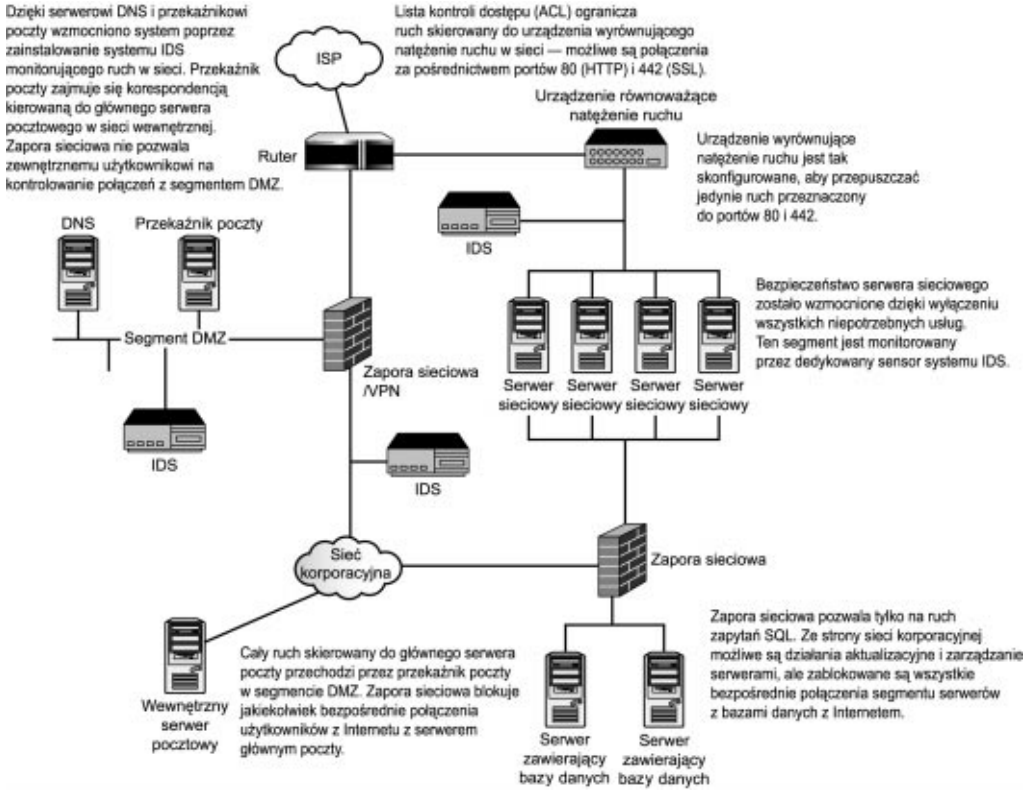
W wyniku przeprowadzonych analiz okazało się, że na serwerze zainstalowana była całkowicie niezabezpieczona wersja (4.0) programu Microsoft Internet Information Server, a firewall nie zrobił nic, aby uniemożliwić czy przerwać atak. Dalsze badania wykazały, że był on tak skonfigurowany, że nie zachowały się żadne dzienniki zdarzeń systemowych (zresztą podobnie było z oprogramowaniem serwera). Nie było więc żadnego śladu, za którym można by było podążyć w poszukiwaniu sprawcy nadużycia. Zabezpieczyliśmy serwer, wznowiliśmy działanie witryny internetowej i przeprowadziliśmy pobieżny audyt konfiguracji zapory sieciowej. W trakcie jego trwania okazało się, że baza danych przedsiębiorstwa zawierająca najbardziej krytyczne informacje jest przechowywana na komputerze mainframe, a firewall pozwala na wolny do niego dostęp niemal z każdego miejsca w sieci!

Przedstawiciele firmy stwierdzili, że komputer mainframe ma tak doskonałe zabezpieczenie, że nie można się do niego włamać, więc nie szkodzi, że firewall umożliwia do niego dostęp. Oczywiście nikt w przedsiębiorstwie nie wiedział, jakiego rodzaju zabezpieczenia zostały zastosowane i w jaki sposób skonfigurowane, a także dlaczego właściwie uważa się te zabezpieczenia za nie do przejścia. Ważne było to, że zostały zainstalowane przez „eksperta" i to wszystkim wystarczało.

Sytuacja pogarszała się z każdym krokiem. Im dokładniej przyglądaliśmy się strukturze sieci, tym bardziej okazywała się dziurawa. Wystarczy powiedzieć, że zamiast zapory sieciowej równie dobrze można było wstawić bezpośrednie przyłącze do Internetu. Wyszłoby na to samo. Przypadek opisywany był klasycznym przykładem pokładania zbyt wielkiego zaufania w pojedynczy komponent sieci bez zastanawiania się, jak współgra on z innymi elementami infrastruktury i profilem bezpieczeństwa całej organizacji. Dlaczego przedsiębiorstwo było tak źle przygotowane? Między innymi dlatego, że w organizacji nie obowiązywała żadna polityka bezpieczeństwa.

Pomimo że w kolejnych rozdziałach zajmiemy się głębszą analizą architektury sieci wewnętrznej, warto z pewnością już teraz rozważyć wybrany przykład, aby dobrze przygotować grunt do późniejszych analiz każdego komponentu infrastruktury z osobna. Przykład typowej architektury pokazano na rysunku 2.3. Składa się ona z przyłącza do Internetu zapewnianego przez jednego dostawcę usług internetowych, po którym umieszczono ruter. Za ruterem znajduje się zapora sieciowa i urządzenie służące do wyrównywania obciążenia ruchu w sieci i równomiernego rozkładania go na pojedyncze jednostki z grupy serwerów sieciowych. Serwery mają połączenie z wewnętrznymi

serwerami baz danych, a zawartość witryny jest aktualizowana dzięki wewnętrznym łączom z siecią korporacyjną. Ośrodek posiada swój własny serwer pocztowy i serwer DNS, a także możliwość tworzenia wirtualnych sieci prywatnych, umożliwiając zdalny dostęp dla pojedynczych użytkowników znajdujących się poza główną siedzibą firmy.



Rysunek 2.3. *Architektura zapewniająca pewien (dość wysoki) poziom bezpieczeństwa zasobów*

Mimo iż nie warto zbytnio rozwodzić się nad strukturą ośrodka zaprezentowanego na rysunku 2.3 (zostanie to zrobione w rozdziale 8.), należy zauważyć, że w tym przypadku architektura poprawnie realizuje wszystkie założenia bezpieczeństwa, a wszystkie składniki sieci umieszczone są we właściwych miejscach i dobrze spełniają swoją rolę. Ponieważ w tym przypadku mamy do czynienia z dość złożonym ośrodkiem i ruchem sieciowym o wyjątkowo dużym natężeniu, twórca struktury sieci optował za rezygnacją z dodatkowej zapory sieciowej pomiędzy grupą serwerów sieciowych a Internetem. Zamiast zapory zaproponowano wzmocnienie systemów operacyjnych zainstalowanych na serwerach i tak skonfigurowano ruter i listy kontroli dostępu urządzenia wyrównującego obciążenie sieci, że dozwolone zostały tylko dwa rodzaje usług: HTTP i SSL.

Z uwagi na fakt, że ośrodek posiadał własny serwer nazw domen (DNS) obok głównej zapory sieciowej, zadanie ograniczenia dostępu z Internetu spełnia także segment

DMZ[1]. Ma on nie dopuścić do wewnętrznej sieci korporacyjnej ruchu, który nie jest związany z usługami poczty i DNS. Twórca architektury proponował umieszczenie głównego serwera poczty w sieci korporacyjnej, ale, aby zminimalizować ryzyko potencjalnych nadużyć, zdecydował o zainstalowaniu w sektorze DMZ przekaźnika pocztowego, który uniemożliwiałby bezpośrednie połączenia pomiędzy wewnętrznym serwerem pocztowym a Internetem. Ponadto serwery baz danych odgrodzone są od serwerów sieciowych za pomocą osobnej zapory sieciowej. Pozwala to na korzystanie z zasobów umieszczonych na serwerach baz danych bez zbytniego narażania ich na ewentualne nadużycia, w przypadku gdyby jeden z serwerów sieciowych padł ofiarą ataku. Zapora sieciowa pomiędzy tymi serwerami pozwala także administratorom lub programistom w sieci korporacyjnej zarządzać i uaktualniać dane na obu grupach serwerów bez tworzenia możliwości ataku bezpośredniego na wewnętrzną sieć przedsiębiorstwa. We wszystkich newralgicznych miejscach ośrodka zainstalowane zostały systemy wykrywania włamań, które monitorują ruch pomiędzy segmentami i ograniczają do minimum możliwość niezauważonego ataku.

Oczywiście zaprezentowana architektura to tylko jedno z możliwych rozwiązań, ale warto zauważyć, że w tym przypadku każdy komponent ma swoją własną funkcję w procesie zabezpieczenia ośrodka. Niektóre wymagania funkcjonalne (na przykład konieczność zapewnienia wysokiej przepustowości i dostępu do grupy serwerów sieciowych) powodują, że kwestie bezpieczeństwa (umieszczenie przed serwerami dodatkowej zapory sieciowej) schodzą na dalszy plan. Niektóre komponenty składowe ośrodka będą miały więcej pracy (np. monitorowanie przez IDS względnie słabo zabezpieczonych serwerów sieciowych), ale wszystkie one (włącznie z listami ACL na ruterze i urządzeniu rozkładającym obciążenie) umieszczone zostały w odpowiednich miejscach sieci. Ta architektura powinna spełnić wszystkie założenia sprecyzowane w dokumencie zawierającym zasady polityki bezpieczeństwa obowiązujące w przedsiębiorstwie. Jest to też odpowiedni przykład dobrej współpracy wszystkich komponentów, która przekłada się na wysoki poziom zabezpieczenia ogólnego.

Monitorowanie i wykrywanie

Na tym etapie mamy już gotowy program IA, ustalono też zakres odpowiedzialności wybranych działów organizacji. Zespół, którego zadaniem było nadzorowanie pracy nad całością programu IT, dokonał wypunktowania i kategoryzacji krytycznych zasobów przedsiębiorstwa. W oparciu o nie powstała polityka bezpieczeństwa, która została zaakceptowana przez kierownictwo wyższego szczebla. Poszczególne komponenty składające się na ogólny program bezpieczeństwa zostały rozmieszczone i uruchomione — od komponentów fizycznych (zapór sieciowych), przez oprogramowanie (systemy operacyjne), po programy uświadamiania wagi procedur bezpieczeństwa.

[1] DMZ jest skrótem od „DeMilitarized Zone” — co może być tłumaczone jako „obszar wpływów sieci niekomercyjnych”. Jest to potoczna nazwa części sieci, co do której nie ma się pełnego zaufania. DMZ stwarza miejsce w sieci, w którym izoluje się systemy dostępne dla użytkowników Internetu od tych, do których dostęp mają tylko pracownicy. Z DMZ można korzystać również w przypadku partnerów handlowych czy innych jednostek zewnętrznych — *przyp. tłum*.

Metody zarządzania i kierowania komponentami zostały określone w dokumentacji procedur operacyjnych. Wydaje się, że wszystkie elementy zostały uwzględnione i prawidłowo ze sobą współdziałają. Nadszedł czas, aby pracownicy bezpieczeństwa pokazali, na co ich stać, i uruchomili wszystkie nowe aplikacje, serwery i usługi.

Powstrzymaj się przez chwilę, bo nie nadszedł jeszcze czas. Może się wydawać, że wszystkie te komponenty programu bezpieczeństwa zapewniają odpowiednią ochronę krytycznych zasobów przedsiębiorstwa. Skąd jednak możemy być tego pewni? Co się stanie, gdy odkryta zostanie nowa luka w systemie operacyjnym zainstalowanym na serwerze? A jeżeli ktoś obszedł standardową drogę i, nie powiadamiając nikogo, wprowadził jakąś zmianę do konfiguracji zapory sieciowej? Może już teraz jakiś haker lub nieuczciwy pracownik ostrożnie wypróbowuje działanie twojej zapory i stara się znaleźć jakąś słabość, lukę w systemie zabezpieczeń?

Bezpieczeństwo nie kończy się na etapie wdrożenia wybranych rozwiązań. Jeżeli zastosowane środki mają dobrze spełniać swoje role, niezbędne jest ciągłe monitorowanie, powtarzające się testy i oceny, które, jeżeli wskażą jakieś wady, pozwolą na szybką reakcję i natychmiastowe ulepszenie systemu bezpieczeństwa. Mówimy właśnie o fazie nazywanej monitorowanie i wykrywanie — jednym z czterech elementów składowych koła bezpieczeństwa. Jej celem jest sprawdzenie, czy wszystkie zastosowane elementy pracują tak, jak powinny. Można tego dokonać na kilka sposobów.

Przeglądanie dzienników zdarzeń systemowych

Najłatwiejszym sposobem monitorowania działania urządzeń jest przejrzenie ich dzienników zdarzeń systemowych. Zapory sieciowe, rutery, serwery sieciowe i baz danych, kontrolery domen itd. potrafią tworzyć raporty, w których zawarty może być opis niemal każdego zdarzenia: nawiązane lub nieudane połączenia, zapisy logowania i wylogowania się z systemu, błędy, korzystanie z plików itp. Zdefiniowane w procedurach operacyjnych działania administratorów obejmują także obowiązek przeglądania tych zdarzeń w poszukiwaniu działań, które w jakiś sposób naruszają zasady bezpieczeństwa.

Kiedy już ta konieczność została określona, wróćmy na chwilę do rzeczywistości. Niemal niemożliwe jest ręczne przeglądanie tak wielkiej ilości danych. Po pierwsze dlatego, że zapisy zdarzeń są strasznie nudne i monotonne, a po drugie dlatego, że wszystkie urządzenia sieciowe mogą dostarczyć ogromną ilość informacji — tak wielką, że niemożliwą do ogarnięcia i przeczytania przez zwykłego człowieka (szczególnie jeśli mamy do czynienia z ośrodkiem o dużym natężeniu ruchu). Czy jest na to rada? Istnieje oczywiście specjalne oprogramowanie, którego głównym zadaniem jest poszukiwanie przypadków, które mogą oznaczać naruszenie zasad bezpieczeństwa. Aplikacje zwracają uwagę na przykład na kilkukrotne nieudane próby logowania się do systemu (może to oznaczać próby odgadywania hasła) lub połączenia sekwencyjne, tj. dokonywane z pewną stałą częstotliwością, co może oznaczać, że ktoś dokonuje tzw. omiatania systemu (ang. *sweeping*), próbując ustalić jego topologię.

Z pewnością zauważyłeś, że ważne jest zachowanie równowagi pomiędzy pożądaną ilością informacji o użytkownikach zalogowanych, wielkością danych, które chcesz

przechowywać, i niezbędną wydajnością pracy systemu. Zbieranie informacji o użytkownikach zabiera cykle pracy procesora (czy jednostki centralnej w systemach wieloprocesorowych) i wpływa na czas dostępu do dysku. Z tego też powodu aplikacje bazujące na serwerach zwykle zbierają minimalną ilość tego typu informacji. Inny sprzęt sieciowy taki jak rutery i przełączniki wymagają specjalnego urządzenia zbierającego dane pochodzące z ich dzienników (np. serwer syslog), gdzie wysyłane są dane o użytkownikach logujących się do sieci.

Ponieważ obecność takiego serwera nie jest niezbędna do pracy pozostałych urządzeń sieciowych, wiele firm nigdy ich nie instaluje. Dla tych, którzy się zdecydowali na umieszczenie go w sieci, połączone informacje dotyczące logowania mogą być zbyt obszerne i trochę tajemnicze. Zapora sieciowa, którą skonfigurowano tak, by zapisywała za dużo informacji dotyczących zalogowanych użytkowników, może stracić na wydajności do tego stopnia, że nie poradzi sobie z ruchem o średnim natężeniu. Wymagania dotyczące konieczności zapisu informacji o użytkownikach zależą od ustaleń, które znalazły się w zdefiniowanej polityce bezpieczeństwa ustalonej w danej firmie. Jeżeli w polityce znajdą się stwierdzenia mówiące o konieczności zapisu informacji o wszystkich zewnętrznych i wewnętrznych połączeniach i przechowywaniu tych danych przez 6 miesięcy, to takich założeń będziesz musiał się trzymać i starać się je wypełnić. Takie założenia będą oczywiście niosły ze sobą specjalne wymagania co do wyboru sprzętu i jego oprogramowania podczas fazy planowania struktury sieci i mogą być usprawiedliwieniem dla zakupu jakiegoś niezwykle wydajnego analizatora składniowego, który zajmował się będzie tylko dziennikami zdarzeń systemowych. Jeżeli będą tego wymagały założenia polityki, być może trzeba będzie dokonać specjalnych analiz możliwości i wydajności systemów raportowania.

Za podstawową zasadę uznaje się konieczność tworzenia raportów dotyczących zdarzeń takich, jak odmowa połączenia, nieudane logowania i próby nieautoryzowanego dostępu do plików. Udaną penetrację sieci zawsze poprzedza kilka nieudanych prób — i to one mogą wskazać napastnika.

Systemy wykrywania włamań (IDS)

Przeglądanie dzienników zdarzeń systemowych jest przydatne, ale ma swoje wady. Przede wszystkim przegląd dotyczy zdarzeń, które już się dokonały — więc o przypadku jakiegoś nadużycia w twojej sieci dowiesz się już po fakcie. Po drugie, na proces analizy dzienników zużywa się części mocy obliczeniowej, na której stratę czasami nie możesz sobie pozwolić. I wreszcie po trzecie, w sieci znajduje się tak wiele urządzeń, że przeglądanie dziennika każdego z nich nie zawsze jest wykonalne, a w niektórych przypadkach niemożliwe jest wykorzystanie analizatora składniowego automatycznie dokonującego analizy (gdyż takiego po prostu nie ma). Pierwszy powód wydaje się najistotniejszy. Jeżeli ktoś włamuje się na twój serwer sieciowy bądź jeżeli jakiś pracownik próbuje dotrzeć do chronionych informacji o sprzedaży, z pewnością nie chcesz dowiedzieć się o tym klika godzin lub kilka dni po fakcie. Chciałbyś o tym wiedzieć już teraz, w czasie rzeczywistym, tak abyś mógł zareagować, zanim napastnikowi uda się to, co zaplanował. Wad, o których była mowa w kontekście procesu przeglądania dzienników zdarzeń, nie mają systemy wykrywania włamań (IDS).

IDS można porównać do antywłamaniowego systemu alarmowego ochraniającego siedzibę firmy. Podobnie jak jego odpowiednik w rzeczywistym świecie (który wykorzystuje kamery, czujniki ruchu, podczerwieni, ciepła, ciśnienia itp.) IDS stosuje różne metody, szukając nietypowych lub podejrzanych zachowań użytkowników sieci (np. próby wykorzystania znanej wady lub luki systemu czy podszywania się pod adres IP wewnętrznej sieci mające na celu oszukanie zapory sieciowej). IDS, podobnie jak alarm antywłamaniowy, ostrzega cię o fakcie dokonywanego ataku w czasie rzeczywistym, tzn. w momencie, w którym napad ma miejsce.

System wykrywania włamań monitoruje ruch w sieci (dzięki czujnikom sieciowym, jest to tzw. *network-based IDS* — IDS sieciowy) lub uruchamia programy na każdym z serwerów, które wyszukują przypadki ataków wymierzonych przeciwko pojedynczym serwerom (tzw. *host-based IDS* — IDS systemowy). Każda z metod ma swoje dobre strony, ale jest coś, co łączy je wszystkie: IDS działa poprawnie tylko wtedy, gdy ktoś monitoruje to, co się dzieje na ekranie komputera. Pamiętaj — hakerzy nie atakują tylko w godzinach pracy. Tutaj poruszamy zagadnienie, które jest charakterystyczne dla wielu niepoprawnych implementacji systemów IDS: pracownicy obsługujący systemy kontroli włamań często pracują w niepełnych godzinach i nie zawsze są obecni, gdy następuje atak (fałszywy bądź rzeczywisty). Pamiętaj, że kiedy IDS wykryje zagrożenie, nie powie ci, co należy robić — jego zadaniem jest tylko raportowanie o działaniach potencjalnych intruzów. I jeżeli nie planujesz zatrudnienia grupy specjalistów bezpieczeństwa, którzy będą pracować przez cały czas (trzeba osiem osób pracujących na pełnym etacie, aby zabezpieczyć tydzień działania systemu IDS), nie będziesz mógł dobrze wykorzystać zainstalowany system. Jest to argument, który przemawia za skorzystaniem z outsourcingu, tzn. stałego podwykonawstwa usługi monitorowania systemów IDS. Jeżeli nie dysponujesz sporym zespołem doświadczonych pracowników, których zadaniem już teraz jest kontrola bezpieczeństwa sieci, tworzenie specjalnej grupy jest po prostu nieopłacalne i nieefektywne. Kwestiami zalet i wad systemów wykrywania włamań zajmiemy się dokładniej w rozdziale 10. Tymczasem ważne jest, abyś wiedział, że IDS jest przydatnym i niezbędnym narzędziem, w przypadku gdy chcemy stworzyć solidny system bezpieczeństwa.

Fuzja danych

Siłą metody polegającej na przeglądaniu dzienników zdarzeń jest to, że możesz poddać dokładnej analizie dane o ruchu w sieci przesyłane przez wszystkie urządzenia. Zaletą systemów IDS jest to, że nie wymagają one monitorowania każdego urządzenia z osobna, a informacje o prawdopodobnym ataku otrzymujesz w czasie rzeczywistym. Jednak najlepszą metodą jest synteza dwóch omawianych wcześniej rozwiązań. Z braku lepszego określenia nazwijmy ją fuzją danych.

Określenie może tłumaczyć fakt, że w przypadku tej metody wykorzystuje się sygnały płynące z systemów IDS, które łączy się z informacjami pochodzącymi z innych urządzeń w sieci, i wszystko to daje razem pełniejszy obraz sytuacji. Pozwala to na bardziej kompleksowe podejście do zagadnienia bezpieczeństwa, bo teraz analizowany jest cały łańcuch zdarzeń, które osobno mogą nie wydawać się istotne. Przypuśćmy, że w dzienniku rutera został zauważony fakt dokonania skanowania portów, potem z miejsca, z którego nastąpiło skanowanie, dokonane zostało połączenie niezerwane

przez zaporę sieciową i wreszcie na jednym z serwerów sieciowych uruchomiono pewien nowy proces. Każde z tych zdarzeń, rozpatrywane z osobna, nie musiałoby wcale wzbudzić podejrzeń. Jednak, jeżeli zbierze się te informacje w jedną całość, oznaczają one, że ktoś dokonał wstępnego przeglądu topologii sieci, połączył się z serwerem sieciowym i uruchomił jakiś program, który —wykorzystując lukę systemu — pozwolił mu prawdopodobnie na uzyskanie praw administratora systemu. Metoda polegająca na połączeniu przeglądania dzienników i IDS jest więc skuteczną bronią w rękach administratora. W niektórych systemach IDS (tych z „górnej półki") możliwe jest dokonywanie analizy połączonej tego rodzaju. Jest to obecnie rozwiązanie najnowsze i stanowi cel, ku któremu zmierza większość twórców narzędzi służących do monitorowania systemu. Jest to też najlepsza broń przeciwko napastnikom w sieci.

Reakcja i odzyskiwanie danych

Nawet jeśli wszystko zostało zrobione tak jak trzeba i wszystkie etapy (od etapu tworzenia polityki, przez fazę implementacji, po fazę monitorowania) zakończyły się sukcesem, prawdopodobnie znajdzie się ktoś, kto jest wystarczająco zdeterminowany i dostatecznie bystry, aby pokusić się o przyprawienie cię o ból głowy. Nawet najlepsze zabezpieczenia mogą zostać złamane. Sprawcą może być ktoś z wewnątrz firmy, kto będzie miał szczęście i wykorzysta jakąś niekonsekwencję w procedurze bezpieczeństwa bądź odnajdzie jakąś lukę w systemie, której istnienie nikomu dotąd nie przyszło do głowy. Nawet jeśli twój program bezpieczeństwa jest solidny, zawsze powinieneś być przygotowany na najgorsze, tj. ostatnią fazę procesu — fazę reakcji i odzyskiwania danych.

Na temat odzyskiwania danych napisano już wiele książek i nie chcielibyśmy, aby ta w jakiś sposób próbowała z nimi konkurować. Z uwagi na fakt, że ten rozdział ma uczulić czytelników na istotność całego procesu bezpieczeństwa, ważne jest, aby wspomnieć o znaczeniu planowania i gotowości na atak. Poniższy przykład dobrze obrazuje wagę elementu planowania.

Dwa dni po odkryciu zagrożenia ze strony wirusa o nazwie Melissa odwiedzaliśmy jedną z agencji, która stała się ofiarą ataku. Rozmawialiśmy z głównym administratorem, który był miedzy innymi odpowiedzialny za ochronę antywirusową. Poinformował nas, że odkrył obecność wirusa wcześnie rano, gdyż zwrócił uwagę na zadziwiająco dużą liczbę wiadomości elektronicznych, które oczekiwały w kolejce do serwera pocztowego. Mniej więcej w tym samym czasie główny specjalista IT usłyszał o istnieniu wirusa i domyślił się, że to właśnie on może być przyczyną obecnej sytuacji. Dyrektor działu IT zwołał zebranie, aby zastanowić się nad tym, co należy czynić. Spotkanie trwało godzinę, podczas której wszyscy pracownicy rozpoczęli już pracę, zalogowali się na swoje komputery i… ich komputery zostały zaatakowane przez wirusa. Administrator, z którym rozmawialiśmy, bardzo żałował straty czasu, bo gdyby pozwolono mu odpowiednio szybko wyłączyć usługi pocztowe, mógłby zapobiec większości strat, zanim pracownicy rozpoczęliby pracę. Jednak dyrektor działu IT stanowczo nalegał na zwołanie posiedzenia i przedyskutowanie sposobu poradzenia sobie z problemem.

Przytoczony przypadek jest typowym przykładem braku przygotowania. Jeśli martwisz się potencjalnymi zagrożeniami, wirusami i stratą połączenia z siecią, jednym z imperatywów powinno być stworzenie procedur reakcji i odzyskiwania danych przed zajściem a nie w trakcie jego trwania bądź dopiero po fakcie. Plany określające sposób reagowania niekoniecznie muszą dotyczyć wyłącznie kwestii technicznych. Częścią tego planu może być na przykład powiadomienie prezesa przedsiębiorstwa i działu PR po to, aby byli odpowiednio przygotowani na kontakt z prasą. Konieczne jest, aby procedura reagowania i odzyskiwania danych była poddawana regularnym testom. W trakcie fałszywego alarmu może się na przykład okazać, że pomimo tego, iż procedura zakłada powiadomienie prezesa przedsiębiorstwa o aktach nadużycia związanych z witryną internetową przedsiębiorstwa, w dokumencie nie ma ani numeru domowego prezesa, ani numeru telefonu komórkowego, ani nawet numeru pagera.

Reagowanie i odzyskiwanie danych to właściwie ostatnia faza i, miejmy nadzieję, najrzadziej wykorzystywany komponent procesu zapewnienia bezpieczeństwa. W przypadku zaistnienia nadużycia ostatnią częścią fazy odzyskiwania danych powinna być ponowna ocena mechanizmów bezpieczeństwa, która może naprowadzić nas na nowe rozwiązanie umożliwiające takie ulepszenie systemu bezpieczeństwa, że incydent w przyszłości już się nie powtórzy.

Przygotowanie na incydent

Podczas przeprowadzania testów architektury sieci pewnej dużej firmy działającej w Internecie naszym celem było przeprowadzenie ataku DoS. Intensywność ataku miała stopniowo rosnąć, co w założeniu pozwalałoby ocenić stabilność i odporność sieci klienta. Z uwagi na fakt, że trudno jest przeprowadzić rozproszony atak DoS, jeśli nie posiada się tysięcy przejętych komputerów, do naszych celów miał przysłużyć się jeden laptop, którego zadaniem miało być wysyłanie 100 Mb segmentów danych bezpośrednio do rutera. Przy pomocy specjalnie stworzonego oprogramowania mogliśmy stopniowo zwiększać siłę ataku DoS i wielkość przesyłanych pakietów, podczas gdy zadaniem administratorów była ocena możliwości wykrycia ataku i jak najlepsza reakcja na incydent. W wyniku późniejszych przemyśleń zmieniliśmy listy kontroli dostępu rutera, włączyliśmy kilka jego funkcji bezpieczeństwa, przekonfigurowaliśmy urządzenie służące do rozkładania obciążenia sieci i, ogólnie mówiąc, wypróbowaliśmy działanie procedur reagowania na incydent obowiązujących w firmie. Okazało się, że zespół pracowników dużo nauczył się o atakach typu DoS, poznał metody reagowania, a cały plan reakcji na incydent obowiązujący w przedsiębiorstwie został odpowiednio uaktualniony i ulepszony.

Przy okazji okazało się, że jeden jedyny laptop może unieruchomić całą infrastrukturę sieci. Jak to możliwe? Podczas testów nasi specjaliści odkryli pewną lukę w systemie operacyjnym zarządzającym ruterem. Wezwano zespół roboczy producenta, który ostatecznie stworzył specjalną łatkę programową usuwającą błąd systemowy. Jaka stąd płynie lekcja? Nie wszystkim atakom można zapobiec.

Podsumowanie

Jak niejednokrotnie podkreślaliśmy, założeniem tego rozdziału było przedstawienie czytelnikowi szerszego obrazu zagadnienia bezpieczeństwa, który znacznie wykracza poza ten widziany z perspektywy serwerów i zapór sieciowych. Próbowaliśmy pokazać

czytelnikom, że bezpieczeństwo zaczyna się na najwyższym, organizacyjnym poziomie. Kolejnym etapem po tym, jak zostaną określone role i zakres odpowiedzialności za IA, powinna być ogólna ocena organizacji, zdefiniowanie i kategoryzacja krytycznych zasobów. Wartość względna tych zasobów, oszacowana na podstawie trzech atrybutów: poufności, integralności i dostępności, powinna pozwolić na zdefiniowanie polityki bezpieczeństwa. Dopiero polityka bezpieczeństwa, jako dokument wzorcowy, powinna stać się podstawą do rozważań na temat budowy właściwej struktury sieci i decyzji o wykorzystaniu konkretnych produktów, technologii i procesów.

Architektura sieci powinna mieć taką formę, jaka byłaby w zgodzie z zasadami zdefiniowanymi w polityce bezpieczeństwa i potrzebami biznesowymi firmy. Bezpieczeństwo systemu powinno opierać się przede wszystkim na zabezpieczeniach tkwiących w najprostszych urządzeniach sieciowych, tj. serwerach, ruterach i przełącznikach, a zaawansowane narzędzia bezpieczeństwa takie, jak zapory sieciowe i serwery proxy powinny być stosowane tam, gdzie są potrzebne i niezbędne. I wreszcie, system powinien być monitorowany za pomocą właściwych urządzeń do tego celu służących takich, jak systemy IDS, ale także powinna być wykorzystywana analiza dzienników zdarzeń systemowych. W przypadku gdy będzie miało miejsce jakieś naruszenie bezpieczeństwa, istotne jest, aby specjalnie przeszkolony zespół reagował zgodnie z procedurami zawartymi w planie reakcji na incydent. Jeśli to konieczne, powinien on dokonać natychmiastowego odzyskania utraconych danych. Całość infrastruktury i system bezpieczeństwa powinna być okresowo sprawdzana poprzez testy penetracyjne, kierowany audyt itp. W momencie odkrycia nowych słabości czy luk systemowych program bezpieczeństwa należy usprawniać automatycznie. Czy to wszystko to nie bułka z masłem?

Nawet jeżeli nigdy nie będziesz musiał zdefiniować polityki bezpieczeństwa, zająć się przeprowadzeniem audytu czy zareagować na naruszenie bezpieczeństwa, dobrze by było gdybyś wiedział, jakie jest twoje miejsce w całym procesie zapewnienia bezpieczeństwa i jak te wszystkie elementy, które się na niego składają, powinny razem współpracować. W kolejnym rozdziale zagłębimy się w zagadnienia specyfiki Internetu i spróbujemy przedstawić charakterystyczne wady i słabości wielu protokołów i usług, które wspólnie składają się na gigantyczną sieć.