7 etapów zwiększania bezpieczeństwa sieci

Alan Mark

www.novell.pl

STRATEGIA BEZPIECZEŃSTWA
SYSTEMÓW IT W BIZNESIE

Novell®

Z powodu wydarzeń z 11 września 2001 r. ludzie na całym świecie zaczęli na nowo zastanawiać się, co znaczy dla nich bezpieczeństwo. Wiele osób boi się latać, ponieważ uważają to za zbyt ryzykowne. w końcu jeśli często podróżuje się z samolotami, to zna się bardzo dobrze problemy, z jakimi borykają się pracownicy lotnisk, próbując zapewnić bezpieczeństwo swoim placówkom.

Również firmy informatyczne musiały zrewidować swoje poglądy na temat znaczenia bezpieczeństwa dla życia ludzkiego. 24 września ubiegłego roku podano w „New York Times", że ataki terrorystyczne spowodowały m.in. „zniszczenie ważnych połączeń z komputerami stanowymi, które służą rozdzielaniu środków z opieki społecznej i paczek żywnościowych oraz wspomagają działanie systemu Medicaid, w wyniku czego tysiące biednych mieszkańców Nowego Jorku i okolic zostało pozbawionych normalnego dostępu do zapomóg, żywności i opieki medycznej" — patrz artykuł Niny Bernstein pt. Destroyed Computer Links Leave Thousands of Poor People Without Welfare Benefits (Tysiące biednych pozostaje bez zapomóg z opieki społecznej z powodu zniszczenia łączy komputerowych), „New York Times", 24 września 2001, www.nytimes.com). Bez wątpienia infostrada jest równie ważna jak budynki, w których przechowywane są dokumenty urzędowe.

Zabezpieczenia zawsze stanowiły integralny składnik infrastruktury informatycznej i podobnie jak pracownicy portów lotniczych, borykamy się z olbrzymimi problemami, próbując zapewnić pełną ochronę sieciom komputerowym naszych firm. Zagrożenia dla bezpieczeństwa mogą mieć charakter elektroniczny i fizyczny. Te pierwsze są powodowane przez hakerów i intruzów, którzy atakują strony internetowe, systemy poczty elektronicznej lub wewnętrzne oprogramowanie firm. Zagrożenia fizyczne są powodowane przez nieuczciwych administratorów sieci, pracowników i kontrahentów, jak również przez pożary, ładunki wybuchowe, powodzie i trzęsienia ziemi.

Naruszenie bezpieczeństwa zawsze powoduje straty, nawet jeżeli nie zostaną wyrządzone żadne szkody. Jeżeli np. nastąpi naruszenie bezpieczeństwa lotniska, to wszyscy pasażerowie zostają ewakuowani, co często prowadzi do opóźnień w całym systemie transportu lotniczego. Jeżeli jakaś firma odkryje włamanie do swojej wewnętrznej sieci, to zamyka wszystkie drogi dostępu do Internetu, aby zapobiec dalszym atakom hakerów. Oczywiście wyłączenie dostępu do Internetu uniemożliwia także przeprowadzanie elektronicznych transakcji handlowych z klientami, dostawcami i biurami terenowymi. Jak my, informatycy, możemy ograniczyć do minimum przypadki naruszenia bezpieczeństwa i powodowane przez nie straty?

Stawianie czoła zagrożeniom

Nasze reakcje w obliczu dramatycznych wydarzeń nie zawsze bywają rozsądne: np. nie można obecnie zabierać ze sobą na pokład samolotów pasażerskich scyzoryków, pilników do paznokci i innych małych narzędzi. Co więcej, metalowe noże używane przy posiłkach zostały usunięte ze wszystkich samolotów i lotnisk. Pasażerowie otrzymują do dyspozycji metalowy widelec i plastikowy nóż (nawet w restauracjach na lotniskach). Zakaz posiadania metalowych noży przy spożywaniu posiłków nie zapobiegłby tragediom z 11 września, ale wszelkiego rodzaju noże są teraz uważane za niebezpieczne.

W branży informatycznej jest natomiast tak, że niektóre pakiety oprogramowania mają stale luki w zabezpieczeniach. Na przykład wirus Code Red, który wykorzystywał lukę w zabezpieczeniach serwerów Microsoft Internet Information (IIS), kosztował przedsiębiorstwa, zdaniem analityków z Computer Economics, ok. 2,62 mld USD — patrz artykuł Economic Impact of Malicious Code Attacks (Skutki ekonomiczne wirusów) pod adresem www.computereconomics.com. Mimo że Netcraft wskazuje na niewielki spadek liczby serwerów Microsoft IIS na jesieni 2001 r. (po ataku wirusa Code Red), i tak w listopadzie 2001 r. w użyciu pozostawało ich ciągle ponad 3 mln (Netcraft szacuje, że w listopadzie wykorzystywano o 300 tys. mniej serwerów Microsoft IIS niż w październiku; więcej informacji można znaleźć pod adresem www.netcraft.com).

Poziom ryzyka, które podejmujemy we wszelkich sferach życia, zależy od tego, jakie przewidujemy zagrożenia, oraz co możemy zrobić, by usunąć ewentualne szkody. Bez wątpienia musimy zmienić naszą ocenę poziomu zabezpieczeń, który wydawał się wystarczający przed 11 września. Nastały czasy, kiedy proste hasła i systemy tworzenia kopii zapasowych nie zapewniają wystarczającego bezpieczeństwa. Jesteśmy obecnie zmuszeni do opracowania systemów komputerowych, które ograniczają do minimum ryzyko utraty bezpieczeństwa, oraz do przygotowania planów działań, jakie należy podjąć w razie awarii.

Przy projektowaniu lub sprawdzaniu zabezpieczeń specjaliści ds. bezpieczeństwa stosują się do trzech ważnych zasad:

1. **O skuteczności zabezpieczeń decyduje najsłabsze ogniwo łańcucha systemów.** Należy stosować skuteczne zasady bezpieczeństwa w całym systemie. w przeciwnym wypadku wprowadzanie zasad bezpieczeństwa jest bezcelowe.

2. **Bezpieczeństwo nigdy nie jest pełne.** w świecie rzeczywistym nie można zabezpieczyć wszystkiego. Należy jednak stale wdrażać i testować nowe procedury, aby osiągać najwyższy możliwy poziom bezpieczeństwa.

3. **Komuś trzeba zaufać.** Np. ochrona punktów kontroli pasażerów na lotniskach przez uzbrojonych żołnierzy jest skuteczna tylko wtedy, gdy wojskowi zostali wcześniej skrupulatnie sprawdzeni. w przypadku systemu informatycznego zaufanymi ludźmi muszą być administratorzy sieci, którzy będą pielęgnować systemy, kontrolować dostęp do danych i dbać o działanie wewnętrznej infrastruktury informatycznej.

Jak zagwarantować uczciwość administratorów sieci? Można stworzyć krąg zaufania i rezerw personalnych, gdzie grupa administratorów sieci jest odpowiedzialna za pielęgnowanie systemów. Ponadto okresowo przeprowadzają oni wzajemne szkolenia. Należy również zadbać o to, aby administratorzy sieci zamieniali się co jakiś czas obowiązkami. Dzięki temu gdy jeden z administratorów sieci zrobi coś niewłaściwego, inny prawdopodobnie zauważy to i zgłosi próbę naruszenia bezpieczeństwa.

Nikt nie jest w pełni zabezpieczony przed sabotażem i awariami. Nawet przed 11 września Biały Dom stał się ofiarą ataku typu denial-of-service (odmowa usługi), przeprowadzonego za pomocą wirusa Code Red. Trzeba postawić sobie trudne pytanie: jeżeli nie da się na raz w pełni zabezpieczyć firmowej sieci, to jakie kroki należy podjąć, aby rozpocząć ten proces?

Tutaj opisano pierwsze działania, jakie należy wykonać, aby zwiększyć bezpieczeństwo firmowej sieci i ograniczyć do minimum słabości systemu zabezpieczeń.

Etap 1: ocena środowiska informatycznego firmy

Powiedzenie „jeżeli coś nie jest zepsute, to nie trzeba tego naprawiać" nie sprawdza się w branży informatycznej. Jeżeli ktoś stosowałby się do tej maksymy, to nigdy nie zainstalowałby programów usuwających luki w zabezpieczeniach ani narzędzi antywirusowych, dopóki użytkownicy mieliby dostęp do swoich aplikacji. Oczywiście nie można lekceważyć bezpieczeństwa sieci, dopóki nie jest ono wystarczające.

Najtrudniejszym aspektem wprowadzania zabezpieczeń jest ich ścisłe określenie. Podstawą wszelkich programów bezpieczeństwa są trzy zasady: integralność, poufność i dostępność.

Inaczej mówiąc, program bezpieczeństwa powinien:

1) zapobiegać umyślnemu manipulowaniu danymi w niecnych celach,
2) umożliwiać wyświetlanie danych wybranej grupie osób oraz
3) udostępniać dane tylko tym osobom, którym są one potrzebne.

Kilka firm specjalizuje się w przeprowadzaniu kompleksowych kontroli bezpieczeństwa (nazywanych również oszacowaniami słabości lub ryzyka). Ci usługodawcy w dziedzinie zabezpieczeń (Managed Security Service Provider — MSSP) mogą ocenić niemal każdy aspekt środowiska informatycznego firmy, m.in. sprawdzić, kto może mieć fizyczny dostęp do systemów przetwarzających dane o znaczeniu krytycznym (dla zabawy można sobie wypożyczyć film „Sneakers", aby zobaczyć jak firma Roberta Redforda sprawdziła system zabezpieczeń banku). Koszt tej usługi może wynosić od dziesiątków do setek tysięcy dolarów, a proces szacowania może trwać kilka miesięcy.

Czy taka kontrola warta jest pieniędzy i wysiłku? Podobnie jak w życiu osobistym, należy odpowiedzieć sobie na pytanie, czy zasoby firmy są tego warte. Oczywiście trzeba brać pod uwagę również przedmioty nie mające wartości materialnej, np. zdjęcia czy inne obiekty, których nie da się zastąpić. Jeżeli kupuje się np. dom za 150 tys. USD, to wykupuje się również ubezpieczenie o odpowiedniej wysokości. Jeżeli odliczenie wynosiłoby 500 USD, to zainstalowanie systemu alarmowego za 300 USD miałoby sens. Co ważniejsze, alarm chroniłby również przedmioty nieobjęte ubezpieczeniem.

Jak można oszacować prawdziwą wartość firmowych danych? Niestety jest to trudne. Proszę sobie wyobrazić, że nagle traci się książkę adresową poczty elektronicznej. Jak wiele czasu trzeba będzie poświęcić na odtworzenie jej zawartości? Albo pomyślmy, co mogłoby się stać, gdyby firmowy system obsługujący bazę danych dotyczącą sprzedaży został zarażony wirusem? Jeżeli odtworzenie wszystkiego z kopii zapasowych potrwałoby jeden dzień (co nie jest wcale przesadą, biorąc pod uwagę wielkość współczesnych baz danych), to jaką część przychodów utraciłaby firma?

W przypadku wdrażania większości rozwiązań w dziedzinie bezpieczeństwa nie można również w prosty sposób wyliczyć zwrotu z inwestycji, z wyjątkiem tych aplikacji, które zwiększają funkcjonalność obecnie wykorzystywanego systemu. Na przykład, jeżeli domowa instalacja alarmowa jest wyposażona w kamerę, służącą do obserwowania posiadłości za pośrednictwem Internetu, to system alarmowy zapewnia podwójną korzyść. w świecie biznesu, gdzie zmniejszenie liczby zgłoszeń do działu pomocy technicznej wpływa na osiągnięcie oszczędności, można liczyć na nadejście łatwiejszych czasów, jeśli sprzedaje

się wyższemu kierownictwu firm rozwiązania zapewniające jednokrotną rejestrację w sieci.

Nie można trzymać pieniędzy w miejscu pozbawionym należytej ochrony, ponieważ jest to po prostu niebezpieczne. Czy istnieją miasta, w których ludzie nie zamykają swoich drzwi na noc? w dobie Internetu drzwi firmy są zawsze otwarte, a u progu stoi cały świat.

Chociaż nie da się w prosty sposób oszacować wartości firmowych danych, to można określić, co by się stało, gdyby one nagle zaginęły. Przy takim oszacowaniu należy rozważyć najgorszy scenariusz (np. pożar i całkowite zniszczenie) oraz bardziej prawdopodobny przebieg wydarzeń (np. sabotaż dokonany przez intruzów i hakerów).

Zależnie od rodzaju działalności prowadzonej przez firmę, może występować kolejny powód do troski: szpiegostwo przemysłowe. Typowy haker (nazywany również „łamaczem zabezpieczeń" [cracker] lub „adeptem skryptów" [script kiddie]) chce, aby go widziano i słyszano, natomiast celem szpiega przemysłowego jest niewykrywalna kradzież informacji. Nie istnieją żadne dowody, dzięki którym można by się dowiedzieć, jak dużo występuje przypadków szpiegostwa, ponieważ wiele kradzieży pozostaje niezauważonych.

Dokonanie oceny środowiska informatycznego firmy może być bardzo uciążliwym zadaniem. Najlepszą metodą jest przeprowadzanie analizy krok po kroku, zaczynając od aktualnego schematu architektury wewnętrznej sieci. Dokument „Lista kontrolna służąca ocenie infrastruktury informatycznej" (Checklist for Evaluating Your IT Infrastructure - http://www.nwconnection.com/2002_01/security12/checklist.html pomoże oszacowaniu firmowej sieci pod kątem punktów wejściowych i procesów o znaczeniu krytycznym. Ta lista kontrolna pomoże również w rozstrzygnięciu zagadnień dotyczących bezpieczeństwa, np. w sprawdzeniu, jak uzyskuje się dostęp do poufnych danych i kto może to zrobić.

Chyba najbardziej zaniedbywaną częścią procesu analizy bezpieczeństwa jest ustalanie zasad. Powinno się np. ustalić zasady, które zagwarantują, że programy korygujące zostaną zainstalowane, że tylko upoważnieni użytkownicy mogą dostać się do centrum przetwarzania danych oraz że korzystanie z systemu obsługującego księgowość wymaga zastosowania karty procesorowej.

Gwarancja instalowania programów korygujących ma rzeczywiście krytyczne znaczenie. Zdumiewa mnie, gdy czytam o firmach, które podłączają do Internetu systemy niezaktualizowane o programy korygujące, które często usuwają słabe punkty w zabezpieczeniach. Bez programów korygujących systemy firmy mogą mieć „dziurawe" zabezpieczenia. Programy monitorujące (tzw. skanery) odnajdują słabo zabezpieczone systemy i powiadamiają o tym hakerów.

Nie powinno się podłączać do Internetu żadnego systemu, wobec którego nie zastosowano wszelkich dostępnych programów korygujących. Aby zapewnić pełną aktualność oprogramowania działającego w firmowej sieci, należy utrzymywać dobre kontakty z dostawcami i odnawiać z nimi umowy gwarantujące określony poziom usług (service level agreement — SLA).

Zasady mają postać zarówno elektroniczną, jak i pisemną. Można wykorzystać pakiet ZENworks for Desktops (www.novell.com/zenworks) lub inny podobny produkt do narzucenia zasad elektronicznych, np. typu „użytkownicy mogą uzyskać dostęp tylko do określonych aplikacji za pośrednictwem określonych stacji roboczych". Należy zapisać zasady, aby poinformować pracowników, że nie powinni nikomu ujawniać haseł ani korzystać ze stacji roboczej innej osoby bez przeprowadzenia procedury uwierzytelniania dostępu do sieci lub samej stacji roboczej (więcej informacji o wprowadzaniu zasad bezpieczeństwa można znaleźć w dokumencie Generally Accepted System Security Principles (Powszechnie przyjęte zasady bezpieczeństwa systemów komputerowych – http://web.mit.edu/security/www/gassp1.html).

Wydarzenia z 11 września nauczyły nas, że służby bezpieczeństwa nie mogą same zapewnić bezpieczeństwa całemu światu. Wszyscy muszą brać w tym udział i mieć się na baczności. Trzeba wyjaśnić pracownikom, jak ważne jest dla nich powiadamianie innych, gdy zauważą, że ktoś postępuje niewłaściwie lub gdy odkryją naruszenie bezpieczeństwa. Można nawet założyć anonimową skrzynkę pocztową dla użytkowników, na którą można by kierować swoje sugestie lub wysyłać informacje o naruszeniu zabezpieczeń.

Należy również ostrzec użytkowników przed zagrożeniami, jakie powodują wiadomości poczty elektronicznej. Podobnie jak Poczta Polska radzi ludziom, aby nie otwierali listów od nieznanych adresatów, trzeba zalecić użytkownikom nieotwieranie wiadomości poczty elektronicznej od nieznanych nadawców — szczególnie wiadomości z załącznikami. Ponieważ pokusa otwarcia takich wiadomości może być zbyt silna dla niektórych użytkowników, trzeba wprowadzić filtrowanie podejrzanych listów poczty elektronicznej w bramce, zanim trafią do odbiorców.

Kolejnym ważnym systemem, który należy wdrożyć, jest kontrola elektroniczna. Niektóre znakomite produkty monitorują zarówno NetWare, jak i eDirectory: Novell ZENworks for Servers (www.novell.com/products/zenworks/servers), DSMeter i DSRazor firmy Visual Click (www.visualclick.com), LT Auditor+ firmy Blue Lance (www.bluelance.com) i DirectoryAlert firmy NetVision (www.netvision.com). Program NetTrend firmy AdRem Software

(www.adremsoft.com) monitoruje działanie wielu urządzeń sieciowych.

Programy te sporządzają szczegółowe raporty na temat niemal wszystkich działań dotyczących eDirectory lub serwera. Za pomocą jednego z tych narzędzi można np. dowiedzieć się, którzy użytkownicy mają uprawnienia administratora i czy są one zapisane w listach kontroli dostępu (access control list — ACL) z parametrem „ukryte". Można ponadto sporządzać raporty dotyczące ustawień haseł i nieudanych prób rejestracji w eDirectory.

W szczególności DSMeter sporządza dziennik modyfikacji zabezpieczeń eDirectory i systemu plików NetWare, a DSRazor kontroluje bezpieczeństwo eDirectory i udostępnia ponad 100 wbudowanych szablonów raportów. DirectoryAlert i LT Auditor+ oferują bieżące ostrzeganie przed intruzami i sporządzanie dzienników kontroli bezpieczeństwa. Wdrożenie któregoś z tych systemów ma decydujące znaczenie dla możliwości sprawdzenia, co dzieje się w firmowej sieci.

Etap 2: identyfikowanie użytkowników

Podstawowym elementem systemu komputerowego jest mechanizm identyfikowania użytkowników. Główny problem polega na tym, że każdy system korzysta z innej procedury identyfikacji. w związku z tym użytkownik o identyfikatorze ROBERT w jednym systemie może być inną osobą niż użytkownik o tym samym identyfikatorze w innym systemie.

Przez całe lata firmy bezskutecznie próbowały konsolidować konta użytkowników. Większość systemów nie komunikuje się ze sobą, a firmy nie mogły zastępować oprogramowania starszego typu nowocześniejszymi aplikacjami zgodnymi ze standardami. Co zatem może zrobić administrator sieci?

Na początek można wypróbować rozwiązania Novella w dziedzinie dostępu i bezpieczeństwa, które koordynują wykonywanie nużących zadań tworzenia, usuwania i identyfikowania użytkowników. Rozwiązania te umożliwiają firmom bezpieczne zarządzanie dostępem do aplikacji, baz danych i platform użytkowników korzystających z komunikacji internetowej i bezprzewodowej, komputerów-klientów, wirtualnych sieci prywatnych (VPN) i łączy komutowanych. Dzięki tym rozwiązaniom niezależnym od platformy użytkownicy mają tylko jeden zestaw danych uwierzytelniających, który mogą stosować w celu uzyskania dostępu do wszystkich zasobów sieciowych, z jakich mają prawo korzystać. i oczywiście nie ma znaczenia, na jakiej platformie znajdują się te zasoby. Listę tych rozwiązań można znaleźć w załączonym do tego atykułu dokumencie pt. Rozwiązania Novella w dziedzinie dostępu i bezpieczeństwa.

W przypadku dowolnego systemu można zastosować najróżniejsze procedury identyfikacji: od prostego podawania identyfikatora użytkownika i hasła, aż po używanie wyrafinowanych identyfikatorów biometrycznych. Jak wyglądało bezpieczne laboratorium w pierwszej części filmu „Mission Impossible"? Pokazano tam, że CIA używa różnych czujników, urządzeń biometrycznych i kart procesorowych do ochrony systemu zawierającego najbardziej poufne informacje.

W świecie rzeczywistym większość firm nie może sobie oczywiście pozwolić na tak wymyślne techniki. z drugiej strony stosowanie samych haseł do ochrony informacji o znaczeniu krytycznym jest już niewystarczające. Na szczęście można usprawniać metody identyfikowania użytkowników.

Identyfikacja użytkownika może obejmować sprawdzenie trzech podstawowych warunków rejestracji: hasła (posiadanie odpowiedniej wiedzy), żetonu (posiadanie odpowiedniego przedmiotu) i danych biometrycznych (posiadanie odpowiednich cech fizycznych). Połączenie tych elementów umożliwia zastosowanie uwierzytelniania wieloetapowego, które jednoznacznie potwierdza tożsamość użytkownika. Poziom kontroli (nazywany również stopniem) jest przypisany danemu użytkownikowi, a dostęp do danych jest ograniczany z uwzględnieniem właśnie poziomu kontroli.

Można np. tak skonfigurować dany system, aby użytkownik, który uwierzytelnia swoją tożsamość za pomocą identyfikatora i hasła, mógł uzyskać dostęp tylko do podstawowych aplikacji i danych. Jeżeli natomiast uwierzytelnienie nastąpi poprzez sprawdzenie odcisku palca, to użytkownik uzyska dostęp do bardziej poufnych informacji, np. przetwarzanych przez system do naliczania płac.

Novell Modular Authentication Service

Enterprise Edition (NMAS) (www.novell.com/products/nmas) wykorzystuje moduły opracowane przez Novella i firmy niezależne, aby umożliwić stosowanie jednej z tych metod rejestracji lub nawet wszystkich naraz (NMAS to rozwiązanie Novella w dziedzinie dostępu i bezpieczeństwa; więcej informacji o modułach NMAS można znaleźć pod adresem www.novell.com/products/nmas/partners). Przy doborze metod rejestracji należy brać pod uwagę poziom zaufania, jakiego wymaga się przyznając dostęp do danego zasobu, koszt wdrożenia określonej metody oraz możliwość jej ewentualnego wykorzystania do innych celów. Można wybierać spośród następujących opcji:

Hasło

Hasło NDS jest podstawą uwierzytelniania od 1993 r. Dostępne są dwie dalsze opcje: hasło proste

i rozbudowane. Proste hasło przechowuje zaszyfrowany ciąg znaków w drzewie katalogowym eDirectory i jest stosowane w przypadku różnych produktów Novella (np. Native File Access Pack). Proste hasło może być również wykorzystywane na potrzeby różnych zasobów internetowych. z drugiej strony hasło NDS nie jest nigdy przesyłane łączami sieciowymi i aplikacje nie mają do niego dostępu (więcej informacji można znaleźć pod adresem http://developer.novell.com/research/appnotes/1994/october/02/04.htm). Hasło rozbudowane pozwala na ustalanie reguł dotyczących haseł (np. że hasła muszą zawierać wielkie i małe litery, cyfry lub znaki specjalne). Ponadto osobisty numer identyfikacyjny (Personal Identification Number — PIN) może służyć do uaktywniania kart procesorowych lub, w połączeniu z żetonami, do identyfikowania użytkownika. Hasła świetnie nadają się do uwierzytelniania za pośrednictwem Internetu, ponieważ nie wymagają stosowania specjalnych urządzeń. w porównaniu z pozostałymi metodami są one jednak łatwiejsze do wykradzenia i wykorzystania przez hakerów, a ponadto użytkownicy mogą je gdzieś zapisywać.

Żeton

Większość żetonów wymaga spełnienia dwóch warunków: posiadania pewnej wiedzy (znajomość hasła lub kodu PIN) i posiadania pewnego przedmiotu (urządzenia). Niektóre czytniki kart procesorowych są ponadto wyposażone w czytniki linii papilarnych, co dodatkowo zwiększa bezpieczeństwo. Dostępnych jest obecnie kilka rodzajów żetonów. Najpopularniejszym jest SecureID firmy RSA Security (www.rsasecurity.com). w tym przypadku żeton synchroniczny wyświetla co 30 sekund nowy 6-cyfrowy kod. w celu uwierzytelnienia tożsamości użytkownik wprowadza uzyskany kod oraz własny numer PIN. Podobne urządzenie oferuje firma Vasco (www.vasco.com). Jej żeton Digipass wyświetla również 6-cyfrowy kod, ale dopiero wtedy, gdy użytkownik wprowadzi odpowiedni numer PIN. Urządzenie to oferuje także opcję hasło-odzew, która nie wymaga precyzyjnej synchronizacji z serwerem. Tak jak SecureID, żeton Digipass dobrze nadaje się do wykorzystania na potrzeby Internetu lub intranetu. Firma Rainbow Technologies (www.rainbow.com) oferuje mały żeton USB, który przechowuje dane uwierzytelniające i certyfikaty użytkowników. Uaktywnienie żetonu następuje po podaniu hasła. Ponieważ żeton USB wymaga instalacji specjalnego oprogramowania na komputerze PC, nie można go używać w kawiarenkach internetowych. Większość kart procesorowych działa w podobny sposób. Użytkownik wsuwa kartę do czytnika, uaktywnia ją, wprowadzając numer PIN, a znajdujące się na karcie dane uwierzytelniające potwierdzają jego tożsamość. Karty procesorowe i żetony USB pod dwoma względami przewyższają inne urządzenia: stacja robocza może zostać zablokowana po odłączeniu urządzenia, a zapisany w nim klucz prywatny można wykorzystać do cyfrowego podpisywania transakcji (np. wiadomości poczty elektronicznej). Dostępne jest również nowe urządzenie, tzw. karta zbliżeniowa (proximity card). Do stacji roboczej przymocowany jest czujnik, który automatycznie rozpoznaje kartę, którą ma przy sobie użytkownik, gdy tylko zbliża się on do komputera. Aby uniemożliwić złodziejowi przejście automatycznej procedury uwierzytelniania przy wykorzystaniu skradzionej karty, wymagane jest dodatkowo podanie pewnego rodzaju identyfikatora (jego rolę pełni zwykle odcisk palca). Rozwiązanie to stosuje się w niektórych szpitalach na potrzeby szybkiego dostępu do terminali.

Biometria

Jak w zwykłym świecie identyfikuje się osobę? Na podstawie jej wyglądu. w małych firmach ludzie z łatwością rozpoznają swoich współpracowników. w dużych przedsiębiorstwach lub urzędach polega się jednak na kartach identyfikacyjnych. Karty identyfikacyjne mają trzy wady. Po pierwsze, wygląd ludzi (np. kolor włosów, zarost, zmarszczki) zmienia się wraz z upływem czasu, co powoduje konieczność aktualizowania kart identyfikacyjnych. Po drugie, bardzo łatwo zapomnieć o zabraniu ze sobą karty identyfikacyjnej. Po trzecie, kart identyfikacyjnych ze zdjęciami nie można w łatwy sposób wykorzystać na potrzeby systemów elektronicznych. Oczywiście potrzebny jest inny rodzaj identyfikatorów dla użytkowników sieci. Techniki biometryczne stosowano już od jakiegoś czasu, ale do niedawna nie były one wystarczająco niezawodne. Obecnie urządzenia biometryczne mogą dokładnie zidentyfikować użytkownika na podstawie jego odcisku palca. Można również zastosować inne metody, np. rozpoznawanie głosu i rysów twarzy. Firma SAFLINK (www.saflink.com) zapewnia obsługę całego szeregu urządzeń biometrycznych (www.saflink.com/bsp.html) i używa oprogramowania NMAS jako platformy do uwierzytelniania. Rzecz jasna trik polega na tym, że czytnik biometryczny nie może dać błędnych wyników. Inaczej mówiąc, czytnik nie może pomyłkowo zidentyfikować osoby jako kogoś innego i uwierzytelnić tożsamość, przyznając niewłaściwy identyfikator. TLC Care Hospital w Las Vegas stosuje czytnik kształtu dłoni do uwierzytelniania pracowników, gdy przychodzą do szpitala i wychodzą z niego. System ten gwarantuje, że nikt nie przedostanie się do kliniki ani jej nie opuści, udając inną osobę. Ponadto 55 tys. pracowników lotnisk w Chicago będzie

wkrótce korzystać przy wkraczaniu do stref bezpieczeństwa z uwierzytelniania za pomocą odcisków palców. Rozwiązanie to zostanie wdrożone przez firmę SecuGen, kolejnego naszego partnera, który używa oprogramowania NMAS.

Etap 3: skuteczne zarządzanie kontami użytkowników

Większość użytkowników ma wiele kont. Załóżmy np., że Alicja ma konto o nazwie Alicja w systemie Windows na swojej stacji roboczej i rejestruje się w eDirectory jako Alicja. Jednak jej identyfikator poczty elektronicznej to AlicjaZ, a kiedy korzysta z aplikacji do naliczania płac działającej w systemie UNIX, jest znana jako AlicjaZimecka. Jej identyfikator w komputerze mainframe to AZ09379 (inicjały i identyfikator pracownika). Oczywiście przy każdym koncie jest inne hasło. Co ma zrobić Alicja?

Wszyscy wiemy aż nazbyt dobrze, że wielość kont sprawia problemy zarówno administratorom, jak i użytkownikom, których kontami oni zarządzają. Zapomniane hasła oznaczają wzrost liczby zgłoszeń do działu pomocy technicznej, z których każde kosztuje, według szacunków firmy IDC, 50–80 USD (więcej informacji można znaleźć pod adresem www.idc.com). a co dzieje się, jeśli „Alicja już tu nie mieszka”? Jak szybko można wyłączyć wszystkie jej konta?

Systemy starszego typu odeszły być może w cień, ale nigdy nie da się ich usunąć całkowicie, ponieważ ich wymiana jest zbyt kosztowna. Drepcze się więc w miejscu, próbując uczyć stare systemy nowych sztuczek. Na szczęście istnieje kilka rozwiązań, które mogą pomóc w zarządzaniu danymi identyfikacyjnymi użytkowników na wielu platformach.

Novell Account Management jest aplikacją ułatwiająca i jednolicąca zarządzanie profilami użytkowników na serwerach NetWare 4.x i nowszych, Windows 2000, Windows NT, Solaris i Linux. Zamiast zarządzania osobnymi kontami dla każdej platformy, wystarczy zarządzać jednym kontem w eDirectory. Użytkownicy mają dzięki temu tylko jeden zestaw danych uwierzytelniających i jedno hasło, które mogą stosować w celu uzyskania dostępu do wszystkich zasobów sieciowych, z jakich mają prawo korzystać.

NDS Authentication Services jest kolejnym z tych rozwiązań (http://developer.novell.com/nss_profile.jsp?product_key=79958). Synchronizuje ono hasła wykorzystywane na potrzeby kont znajdujących się na następujących systemach (nawet jeżeli identyfikatory użytkownika różnią się miedzy sobą): AIX, FreeBSD, HP-UX, Linux, OS/390, Solaris, Windows NT/2000.

Dzięki NDS Authentication Services Alicja używa tego samego hasła — swojego hasła z eDirectory — w celu uzyskania dostępu do niezbędnych jej systemów. Niektóre aplikacje mogą ponadto uzyskać dostęp do właściwości użytkownika eDirectory, np. członkostwa w grupie czy poziomu bezpieczeństwa.

Novell eDirectory i DirXML to kolejne rozwiązanie. Novell DirXML (www.novell.com/products/nds/dirxml), synchronizuje nie tylko identyfikatory, ale także inne informacje dotyczące użytkowników. Na przykład po zmianie adresu i numeru telefonu użytkownika, zapisanych w bazie danych Oracle, Novell DirXML może przesłać te modyfikacje do eDirectory oraz innych baz danych i programów, m.in. firmowego systemu poczty elektronicznej. Dzięki temu zmiany wprowadza się tylko raz, a wszystkie firmowe bazy danych i książki adresowe zawierają zawsze aktualne informacje. Możemy również dodać moduły DirXML do synchronizacji haseł (DirXML Password Synchronization for Windows 2000/NT).

eDirectory i DirXML są podstawą przedsięwzięcia Zero Day Start firmy Novell. To rozwiązanie w dziedzinie elektronicznego zaopatrywania wyznacza standard synchronizowania systemów wykorzystywanych w firmie. Dzięki Zero Day Start nowi pracownicy Novella mogą rozpocząć wykonywanie swoich obowiązków już od pierwszego dnia, w którym pojawili się w firmie. Zamiast wprowadzania informacji o pracownikach do wielu systemów (operacja ta może trwać kilka dni, a nawet tygodni), Novell może pozwolić sobie na jednokrotne wpisanie tych danych. Informacje są następnie synchronizowane w odpowiednich systemach.

Równie ważne jest to, że omawiane rozwiązanie umożliwia natychmiastowe usunięcie informacji o zwalnianych pracownikach (Zero Day Stop). Jak wiemy, szybkie usuwanie lub wyłączanie kont użytkowników może być koszmarem. Dzięki Novell DirXML można wyłączać konta użytkowników jednym kliknięciem przycisku myszki.

Etap 4: ochrona haseł

Trzeba to otwarcie przyznać: w przypadku większości systemów — systemów UNIX, komputerów mainframe i serwisów internetowych — hasło jest jedyną metodą uwierzytelniania. Pomimo tego wszystkiego, co napisano wyżej o żetonach, kartach procesorowych i urządzeniach biometrycznych, niewybaczalnie słabe hasła dla wielu są najgorszym koszmarem.

Gdzie użytkownicy trzymają listę swoich haseł? Może ona być zapisana na karteczce przyklejonej do klawiatury lub monitora. Może być także przechowywana w pliku na komputerze przenośnym lub w urządzeniu kieszonkowym. Skoro nie istnieje proste rozwiązanie, które umożliwiałoby uporządkowanie chaosu towarzyszącego stosowaniu haseł, to użytkownicy samodzielnie wymyślą sposób — nawet ryzykując kradzież haseł.

Novell SecureLogin służy do rozwiązania tych problemów (www.novell.com/products/securelogin), chroniąc firmę przed nadmiarem kłopotów, jakie powodują niewyrafinowane zbiory znaków, zwane hasłami. Po pierwsze, Novell SecureLogin oferuje usługi jednokrotnej rejestracji dostępu do komputerów centralnych i mainframe, stron internetowych, sesji terminali Citrix i aplikacji Windows. Po drugie, Novell SecureLogin pozwala na tworzenie opartych na usługach katalogowych zasad dotyczących haseł. i wreszcie, dzięki przechowywaniu danych uwierzytelniających użytkowników w drzewie katalogowym, są one dostępne za pośrednictwem dowolnej stacji roboczej, na której działa oprogramowanie Novell SecureLogin.

Dzięki Novell SecureLogin dziesiątki aplikacji są przystosowane do automatycznego wykrywania hasła. w takim przypadku Novell SecureLogin automatycznie zapisuje i zapamiętuje dane uwierzytelniające użytkownika przy jego minimalnym udziale.

Jeżeli dana aplikacja nie jest odpowiednio przystosowana, Novell SecureLogin udostępnia kreator, który pomaga użytkownikowi skonfigurować ją pod kątem jednokrotnej rejestracji. w przypadku rejestracji za pośrednictwem Internetu pakiet Novell SecureLogin pyta użytkownika, czy chce, aby jego dane uwierzytelniające (identyfikator, hasło i inne informacje) były zapamiętywane, czy nie.

Tradycyjnie obawiano się stosowania jednokrotnej rejestracji, gdyż uważano, że jedno hasło odblokowuje wszystkie pozostałe. Jeżeli zostanie skradzione lub „złamane" hasło eDirectory, to ktoś może uzyskać dostęp do aplikacji o znaczeniu krytycznym, ponieważ identyfikator użytkownika i hasło są wprowadzane automatycznie. Aby uchronić się przed tym problemem, można zastosować oprogramowanie NMAS, które wymusi skuteczniejsze uwierzytelnianie dostępu do eDirectory. Zanim Novell SecureLogin wprowadzi dane uwierzytelniające użytkownika do aplikacji o znaczeniu krytycznym, musi zostać sprawdzony innego rodzaju identyfikator (np. żeton lub odcisk palca).

A jeżeli użytkownik uwierzytelni swój dostęp do eDirectory i pójdzie po kawę? Ze stacji roboczej może wówczas skorzystać dowolna przechodząca osoba. w tym przypadku dostępne są co najmniej dwa rozwiązania: można tak skonfigurować pakiet NMAS, aby blokował stację roboczą po upływie określonej liczby minut braku aktywności użytkownika, albo zastosować do jej ochrony kartę procesorową lub żeton. Jeżeli karta lub żeton są odłączone, to stacja robocza zostaje automatycznie zablokowana. Ten ostatni sposób wymaga, aby pracownik zabierał ze sobą żeton, odchodząc od stacji roboczej. Przymocowanie żetonu do kółka z kluczami lub karty identyfikacyjnej pozwala zagwarantować odpowiednie postępowanie pracowników.

Corocznie dyskutuję z tysiącami administratorów sieci na różne tematy dotyczące bezpieczeństwa i jestem zdumiony, że wielu z nich nie używa produktów oferujących jednokrotną rejestrację. Narzędzia te nie tylko zwiększają bezpieczeństwo haseł, ale również oszczędzają mnóstwo czasu. Warto je wypróbować. Wystarczy pobrać bezpłatną wersję demonstracyjną Novell SecureLogin ze strony internetowej pod adresem www.novell.com/products/securelogin i zainstalować ją na swojej stacji roboczej w trybie autonomicznym. Na swojej stacji roboczej mam zapisanych ponad 50 zestawów danych uwierzytelniających do aplikacji i stron internetowych.

Etap 5: zabezpieczenie stacji roboczych i konsol serwerów

Na współczesnych stacjach roboczych przechowuje się więcej danych niż jeszcze pięć lat temu na serwerach i na tym właśnie polega problem: jeżeli przestrzeń dyskowa jest natychmiast dostępna na napędzie C, użytkownicy nie mają powodów, aby zapisywać dane gdzie indziej.

Przechowywanie danych na dyskach lokalnych stwarza dwa problemy: nie są prawdopodobnie tworzone kopie zapasowe, a ponadto dane można z łatwością odczytać po kradzieży stacji roboczej lub włamaniu się na nią.

Novell ZENworks for Desktops (www.novell.com/products/zenworks) wykorzystuje eDirectory do wprowadzenia zasad dotyczących stacji roboczych. Dzięki ZENworks for Desktops użytkownicy i stacje robocze stają się łatwymi w zarządzaniu obiektami, które są powiązane z dziedzicznymi zasadami. Można np. utworzyć zasadę, która nakazuje przeprowadzanie kontroli antywirusowej stacji roboczej i sporządzanie zapasowych kopii przechowywanych na niej danych — niezależnie od tego, czy użytkownik jest aktualnie zarejestrowany w sieci, czy nie. Dzięki mechanizmowi Wake-Up On LAN komputer można uruchomić poprzez zdalne wydanie odpowiednich poleceń.

Zasady ZENworks for Desktops mogą ponadto dynamicznie tworzyć użytkowników eDirectory na stacjach roboczych Windows. Profil użytkownika jest następnie kopiowany na stację roboczą z jego katalogu macierzystego, a inna zasada decyduje o tym, co użytkownik może zobaczyć i wykonać. Na przykład po uwierzytelnieniu Alicji w eDirectory, wykorzystywane przez nią środowisko i ustawienia pulpitu są odtwarzane na stacji roboczej. Zasada ZENworks for Desktops uniemożliwia Alicji dostęp do poleceń Explorer, Run i Registry, nie pozwalając jej zatem na korzystanie z zewnętrznych aplikacji. Kiedy Alicja wylogowuje się, jej profil jest uaktualniany na serwerze i usuwany ze stacji roboczej, co uniemożliwia innym osobom korzystanie z jej konta.

Kluczowe znaczenie dla ZENworks for Desktops ma system eDirectory, który przechowuje informacje o użytkownikach i stacjach roboczych oraz zasady decydujące o ich funkcjonowaniu. Jeżeli konto Alicji w eDirectory jest zablokowane, to nie będzie ona mogła zalogować się na żadnej stacji roboczej.

ZENworks for Desktops udostępnia ponadto narzędzie Application Launcher, które instaluje, dystrybuuje, uruchamia, konfiguruje, naprawia i usuwa niemal dowolne aplikacje działające pod kontrolą systemu Windows. Najważniejszą opcją zabezpieczeń zastosowaną w Application Launcher jest to, że jeżeli użytkownik nie ma uprawnień do korzystania z danej aplikacji, to nie zobaczy nawet ikony, którą mógłby kliknąć dwukrotnie. Hakerzy mają bardzo trudne zadanie przy włamywaniu się do systemów, których nawet nie widzą.

Oczywiście trzeba zapewnić również ochronę konsoli serwera. Tradycyjne narzędzie RCONSOLE jest uważane za niezbyt bezpieczne w użyciu, ponieważ hasła nie są skutecznie szyfrowane. Aby rozwiązać ten problem, program **sfConsole 4.0 firmy AdRem** zapewnia bezpieczny dostęp do zarówno lokalnych, jak i zdalnych konsol serwerów. Dzięki sfConsole wystarczy po prostu uwierzytelnić się w eDirectory i zainicjować bezpieczne połączenie chronione 128-bitowym kluczem.

sfConsole 4.0 chroni ponadto konsolę serwera za pomocą zabezpieczonego hasłem wygaszacza ekranu i blokady klawiatury. Można także ograniczyć użytkownikom uprawnienia dostępu do konsoli serwera i dokładnie określić, z których poleceń mogą oni korzystać.

Etap 6: zabezpieczenie danych

Zabezpieczenie danych to skomplikowane przedsięwzięcie. w końcu dane muszą być łatwo dostępne, co oznacza możliwość ich wydrukowania lub wyświetlenia na monitorze. w przypadku sieci komputerowych informacje można także z łatwością kopiować, a jeżeli wszyscy mają dostęp do sieci, to jakiś podsłuchiwacz może przechwycić dane przesyłane jej łączami.

Można zastosować dwie metody zabezpieczania danych: uniemożliwić nieupoważnionym osobom dostęp do danych oraz zaszyfrować dane na wypadek przechwycenia ich przez niepowołane osoby.

W środowisku NetWare można zastosować kontrolę dostępu do woluminów, katalogów i plików. eDirectory pozwala natomiast na szczegółowe określenie, które obiekty i atrybuty mogą być wyświetlane lub modyfikowane. Jeżeli jednak intruz wykradnie hasło — a może nawet serwer — to dane zostaną przechwycone. Należy zastosować szyfrowanie danych przesyłanych łączami sieciowymi i przechowywanych na dyskach twardych.

Jak już wcześniej wspomniano, NMAS może przypisać woluminowi NetWare etykietę zabezpieczania, wymagającą od wszystkich użytkowników — nawet użytkownika ADMIN — przeprowadzenia ściśle określonej procedury uwierzytelniania przed uzyskaniem dostępu do danych przechowywanych na tym woluminie. Jeżeli np. wolumin FINANSE ma etykietę Hasło&Żeton (Password&Token), to użytkownik musi mieć co najmniej ten poziom kontroli, aby móc wyświetlić informacje o akcjach firmy. Ów poziom kontroli oznacza, że użytkownik będzie musiał skorzystać z żetonu, np. karty procesorowej, i podać PIN. Dzięki NMAS sposób uwierzytelniania tożsamości decyduje o tym, co będą mogli zrobić użytkownicy — więcej informacji na temat wykorzystania stopni kontroli można znaleźć w dokumencie Taipei County Government Secures Access to Its Assets (Placówki administracji państwowej w okręgu Taipei zabezpieczają dostęp do swoich zasobów - http://www.nwconnection.com/2002_01/tcg12/index.html).

Novell iFolder (www.novell.com/products/ifolder) bezpiecznie synchronizuje dane przechowywane na stacjach roboczych i serwerach. Pliki zapisane w określonym folderze są szyfrowane przed wysłaniem na serwer. Nawet jeżeli ktoś ukradłby serwer, zaszyfrowane dane będą dla niego bezwartościowe. Natomiast użytkownicy mający odpowiednie uprawnienia mogą bezpiecznie uzyskać dostęp do plików za pośrednictwem dowolnej przeglądarki internetowej. Do ochrony przesyłania danych iFolder wykorzystuje protokół Secure Sockets Layer (SSL) — więcej informacji można znaleźć w artykule Novell iFolder: Your Data Where You Want It, When You Want It (Novell iFolder: dostęp do danych w dowolnym miejscu i czasie, www.nwconnection.com/2001_05/ifolder51/), „Novell Connection", maj 2001 r., s. 6–20).

Szyfrowanie danych to skuteczny sposób na pokrzyżowanie szyków złodziejom. Ale skąd można mieć pewność, że dane nie zostały zmodyfikowane? Szyfrowanie zapewnia bezpieczeństwo danych; natomiast podpisy cyfrowe pomagają zagwarantować ich integralność.

Jeśli wiadomość poczty elektronicznej lub plik są podpisane cyfrowo, odbiorca może mieć pewność, że faktycznie pochodzą od nadawcy i nie zostały „po drodze" zmodyfikowane. Największym problemem przy szyfrowaniu i podpisywaniu dokumentu jest pobranie danych uwierzytelniających (kluczy publicznych) nadawcy i odbiorcy. Szczegółowe zagadnienia dotyczące podpisów cyfrowych nie są przedmiotem tego artykułu, ale ogólnie można powiedzieć, że aby Alicja mogła wysłać zaszyfrowaną wiadomość do Roberta, musi ona dysponować jego kluczem publicznym. i odwrotnie, jeśli Robert chce sprawdzić, czy dana wiadomość została rzeczywiście wysłana przez Alicję, musi mieć jej klucz publiczny.

Novell GroupWise 6 (http://www.novell.com/products/groupwise) oferuje nowe opcje, które ułatwiają znajdowanie klucza publicznego danego użytkownika. Zanim Alicja wyśle swoją wiadomość, GroupWise poprosi ją o skorzystanie z prywatnego lub publicznego drzewa katalogowego LDAP w celu odszukania klucza Roberta. Po jego znalezieniu odpowiedni certyfikat (zawierający klucz publiczny Roberta) jest zapisywany w książce adresowej Alicji.

Jeżeli szuka się oprogramowania do ochrony wiadomości poczty elektronicznej, to warto sięgnąć po produkt firmy PGP Security Business, będącej działem Network Associates. Narzędzie to umożliwia szyfrowanie i podpisywanie plików i wiadomości poczty elektronicznej na wielu platformach. Bardzo wielu użytkowników korzysta z tego bezpłatnego programu (więcej informacji o produktach opartych na PGP można znaleźć pod adresem www.pgp.com).

Nowa metoda szyfrowania danych polega na stosowaniu dwuetapowej lub dłuższej procedury uwierzytelniania przy szyfrowaniu plików, folderów lub całych dysków twardych. Po uwierzytelnieniu tożsamości użytkownika w systemie lokalnym jego hasło jest przesyłane do oprogramowania szyfrującego. Firma PC Guardian (www.pcguardian.com) oferuje kilka produktów do ochrony danych, a obecnie opracowuje wersje działające z eDirectory.

Chociaż komputery przenośne znacznie ułatwiają wykonywanie pracy w podróży, są one najmniej bezpiecznymi urządzeniami, jakie znajdują się w posiadaniu firm. Co roku kradzione są setki tysięcy laptopów (1 na 14 wyprodukowanych) i założę się, że większość znajdujących się na nich danych nie jest chroniona (więcej informacji można znaleźć pod adresem www.ztrace.com/zLab1.asp; dane statystyczne dotyczące kradzieży komputerów znajdują się pod adresem www.safeware.com/losscharts.htm).

Nawet jeżeli system operacyjny komputera przenośnego wymaga podania hasła, haker dysponujący odpowiednimi narzędziami może w końcu złamać zabezpieczenia. Jeżeli nie sporządza się kopii zapasowych informacji przechowywanych na laptopie, to traci się je razem ze sprzętem. Wykorzystanie ZENworks for Desktops do wprowadzenia zasad dotyczących stacji roboczych, które wymuszą tworzenie kopii zapasowych danych przechowywanych na laptopach, oraz użycie Novell iFolder do synchronizowania informacji znajdujących się na stacjach roboczych i serwerach może zwiększyć bezpieczeństwo komputerów przenośnych.

Aż nazbyt dobrze wiadomo, że wirusy, robaki i inne odrażające „stworzonka" mogą zarazić stacje robocze, a nawet spowodować ich niezdatność do użytku. Jeszcze gorsze jest to, że wirusy mogą przesyłać poufne dane do jakiegoś komputera centralnego podłączonego do Internetu. Wirusy przedostają się do systemów trzema głównymi drogami: poprzez luki w zabezpieczeniach programów-klientów (np. Microsoft Windows, Outlook czy Word), uzyskując dostęp do usług internetowych (za pośrednictwem serwera Microsoft IIS lub aplikacji działającej w systemie UNIX) albo za pośrednictwem poczty elektronicznej.

I w tym wypadku można wykorzystać ZENworks for Desktops w celu wymuszenia regularnych kontroli antywirusowych oraz wprowadzić odpowiednią zasadę bezpieczeństwa, która poinformuje użytkowników, że nie należy otwierać wiadomości poczty elektronicznej i załączników od nieznanego nadawcy. Można również kontrolować wiadomości poczty elektronicznej na bramce.

Etap 7: zabezpieczenie dostępu do Internetu

Zarządzanie użytkownikami i systemami wewnętrznymi może być kłopotliwe, ale powody do zdenerwowania pojawiają się dopiero wtedy, gdy użytkownicy potrzebują dostępu do systemów wewnętrznych za pośrednictwem Internetu. a kiedy dostawcy i klienci również zechcą mieć taki dostęp, to już można zacząć sięgać po środki uspokajające.

Pierwsza linia obrony to tzw. zapora (firewall). Tak, to jedno urządzenie potrafi wszystko: od zapobiegania katastrofom po zapewnienie ochrony przed złoczyńcami. Nadaje blask podłogom i połysk butom! Przepraszam za ten sarkazm, ale zapora to najmniej trafnie używane słowo w branży sieci komputerowych. Żadne urządzenie nie chroni całej sieci i nie powinno się powierzać tego zadania jednemu urządzeniu. Należy myśleć o zaporze jako

o zbiorze systemów, usług i zasad, które chronią wewnętrzną sieć przed intruzami i utratą danych.

Zatem na rozwiązanie stanowiące zaporę składa się sprzęt i oprogramowanie znajdujące się na serwerach, bramkach internetowych, a nawet na stacjach roboczych. Kompleksowe rozwiązanie powinno obejmować systemy wykrywania intruzów, mechanizmy kontroli uwierzytelniania, narzędzia nadzorujące, zarządzanie dostępem do sprzętu i centrów przetwarzania danych, oprogramowanie antywirusowe i zasady wymuszające odpowiednie zachowania pracowników.

Przed otwarciem sieci dla świata zewnętrznego trzeba określić, które systemy mają być udostępniane. Okaże się prawdopodobnie, że użytkownicy Internetu powinni mieć dostęp do niemal wszystkich systemów firmy. Ponieważ wiele systemów jest lub będzie opartych na komunikacji internetowej, trzeba przeprowadzać identyfikację użytkowników za pośrednictwem interfejsu przeglądarki WWW.

Novell iChain (http://www.novell.com/products/ichain) umieszcza fronton przed zasobami firmowymi, wymagając od użytkowników uwierzytelnienia tożsamości za pomocą hasła, żetonu lub certyfikatu przed przyznaniem im dostępu do systemów wewnętrznych. Ponadto dane przesyłane za pośrednictwem protokołu HTTP są automatycznie szyfrowane w ramach sesji SSL uaktywnionej przez iChain. Dzięki temu cała komunikacja pomiędzy użytkownikiem Internetu a wewnętrznym serwerem WWW jest szyfrowana bez zmiany serwera WWW.

Novell BorderManager (http://www.novell.com/products/bordermanager) zapewnia inny rodzaj bezpiecznej komunikacji, oferując wirtualną sieć prywatną. Przy jej zastosowaniu każdy program-klient uaktywnia bezpieczne połączenie z serwerem. Po uwierzytelnieniu użytkownicy uzyskują dostęp do intranetu, jak gdyby znajdowali się w biurze. Wirtualne sieci prywatne łączące ze sobą serwery szyfrują przesyłane pomiędzy nimi dane, wykorzystując Internet jako środek komunikacji.

Dane muszą być bezpieczne w każdym miejscu. Chociaż zabezpieczanie transakcji internetowych jest ważne, to ochrona systemów wewnętrznych ma charakter priorytetowy. Nie odnotowano jeszcze potwierdzonego przypadku wykradzenia numeru karty kredytowej przy okazji pojedynczej transakcji. Wielokrotnie informowano natomiast o przykładach włamań do baz danych, w których przechowywano numery kart kredytowych. iChain i BorderManager mogą skutecznie blokować dostęp do systemów wewnętrznych.

Łączenie wszystkiego ze sobą, bit po bicie

Dysponując eDirectory (http://www.novell.com/products/edirectory/) jako podstawą firmowej sieci, można się dowiedzieć, kim jest użytkownik (tożsamość), gdzie się znajduje (miejsce), jak się zalogował (uwierzytelnienie) i co będzie mógł zobaczyć (kontrola dostępu). Poniższy rzeczywisty scenariusz demonstruje możliwości eDirectory w połączeniu z innymi rozwiązaniami wymienionymi w tym artykule.

Robert siada przy swoim biurku i loguje się w eDirectory. Konto Roberta działa, więc jego profil zostaje przesłany do stacji roboczej. Jest poniedziałek rano, a w weekend został odkryty nowy wirus. ZENworks Application Launcher konfiguruje menu Start i pasek zadań Roberta, pobiera najnowszy plik z charakterystykami wirusów oraz uruchamia program antywirusowy. Ponieważ Robert pracuje w dziale sprzedaży, zasada ZENworks umożliwia mu niemal pełny dostęp do stacji roboczej (chociaż nie może używać polecenia Regedit).

Robert uruchamia emulator terminala, aby uzyskać dostęp do bazy danych dotyczących sprzedaży. Jego identyfikator na komputerze mainframe to RobertT. Wpisuje zatem swój identyfikator i hasło (które zostało zsynchronizowane z jego hasłem w eDirectory).

Robert chce następnie zajrzeć do systemu finansowego, aby sprawdzić wyniki sprzedaży na podległym mu obszarze. System finansowy wymaga kontroli biometrycznej, więc Robert uwierzytelnia ponownie swoją tożsamość za pomocą wbudowanego w klawiaturę czytnika linii papilarnych. Po odświeżeniu dokonanym przez narzędzie Application Launcher, na pulpicie Roberta pojawia się ikona systemu finansowego.

Teraz Robert chce sprawdzić swoje akcje. Uruchamia przeglądarkę i przechodzi na odpowiednią stronę internetową. Novell SecureLogin automatycznie wprowadza tam jego identyfikator i hasło. Pojawia się okienko z ofertą bezpłatnych lekcji gry w golfa i Robert klika je. Jednak nie może wejść na tamtą stronę internetową. Administrator sieci użył BorderManagera, aby zablokować dostęp do stron o tematyce sportowej.

Następnie Robert uruchamia GroupWise. Novell SecureLogin automatycznie wprowadza jego identyfikator użytkownika GroupWise, ale pojawia się okno dialogowe, informujące Roberta, że już czas na zmianę hasła. Novell SecureLogin automatycznie pomaga Robertowi utworzyć nowe hasło, zgodne z zasadami ustalonymi przez administratora sieci.

Robert pisze wiadomość do swojego szefa. Przed wysłaniem szyfruje ją i podpisuje. Dzięki temu wiadomość zostaje wysłana poufną drogą, a szef ma pewność, że pochodzi ona od Roberta. w domu Robert uzyskuje dostęp do firmowego intranetu, uwierzytelniając najpierw swoją

tożsamość na serwerze Novell iChain. Od tego momentu cała komunikacja między jego komputerem domowym a intranetem jest zabezpieczona przez SSL, a rejestracja w firmowych aplikacjach internetowych przebiega automatycznie.

Podsumowanie

Przyznajmy: bezpieczeństwo to nie zabawa. Większość projektów zabezpieczeń przewiduje zacieśnienie kontroli nad użytkownikami, stacjami roboczymi i budynkami. Już choćby z tego powodu wprowadzanie silnych zabezpieczeń martwi niektórych administratorów sieci, ponieważ wychodzą na złych pracowników.

Każda firma zawsze będzie musiała się liczyć z zagrożeniami dla bezpieczeństwa, zarówno wewnętrznymi, jak i zewnętrznymi. Celem jest ograniczanie ryzyka do minimum. Trzeba pamiętać, że dbanie o bezpieczeństwo to proces, który nigdy się nie skończy. Stale trzeba uaktualniać systemy za pomocą najnowszych programów korygujących luki w zabezpieczeniach, szukać słabości środowiska informatycznego oraz wdrażać najlepsze systemy zabezpieczeń, na jakie firma może sobie pozwolić.

I wreszcie nie można zapominać o najważniejszych zasobach, czyli pracownikach. Użytkownicy mogą sprawiać kłopoty, ale mogą również stanowić pierwszą linię obrony. Trzeba namówić ich do czynnego dbania o bezpieczeństwo. Na przykład kiedy w listopadzie wracałem samolotem z targów Comdex, współpasażer zapytał mnie, czy pomógłbym załodze, gdyby wystąpiła sytuacja kryzysowa. w tej nowej erze nieoczekiwanych wydarzeń wszyscy muszą dbać o bezpieczeństwo.

Alan Mark jest głównym strategiem ds. zabezpieczeń w firmie Novell. Pracuje w niej już od 11 lat i udziela porad dużym przedsiębiorstwom z całego świata.

Jeżeli zainteresują Państwa prezentowane tu rozwiązania, obszerniejsze informacje na ich temat możecie Państwo uzyskać dzwoniąc do bezpłatnej infolinii firmy Novell Polska: 0-800 22 66 85 (0-800 22 NOVL) lub zamówić je elektronicznie wysyłając e-mail na adres: infolinia@novell.pl