Ochrona firm przed kradzieżą tożsamości

Wydajne sieci

Przy tylu głośnych informacjach prasowych na całym świecie na temat kradzieży tożsamości wydaje się nieprawdopodobne, że firmy w dalszym ciągu padają ofiarą tego przestępstwa. Eksperci twierdzą, że nie powinnyśmy być tym zbytnio zaskoczeni. Wyrafinowanie i natężenie ataków w połączeniu z tym, że wiele rozwiązań ochronnych jest ogromnie skomplikowane technicznie, może prowadzić do przerażających sytuacji.

Niedawne bardzo głośne wpadki w zakresie bezpieczeństwa, na przykład w brytyjskim resorcie podatków i ceł (HM Revenue & Customs service - HMRC) uświadomiły wszystkim, jakie zagrożenia niesie za sobą kradzież tożsamości – zarówno dla przedsiębiorstw, jak i dla konsumentów. W samym tylko ubiegłym roku z [brytyjskich] urzędów, funduszu zdrowia, banków, firm ubezpieczeniowych i placówek handlu detalicznego wyciekły – w co aż trudno uwierzyć – dane osobowe aż 37 milionów osób. A spokojnie można założyć, że to działo się nie tylko w Wielkiej Brytanii i że z podobnymi problemami borykają się także pozostałe kraje europejskie bez wyjątku. Tak więc polityki zapewniania bezpieczeństwa, w szczególności te, które na pierwszy rzut oka mogą się wydawać trudno egzekwowalne z punktu widzenia infrastruktury, powinny wszystkich bardzo zainteresować.

Ale, pomimo że nagłaśniane są przede wszystkim naruszenia bezpieczeństwa informatycznego w systemach publicznych, nie ma wątpliwości, że ogólnie bezpieczeństwo informatyczne – a w szczególności ochrona danych – jest stałym problemem przedsiębiorstw na całym świecie.

W każdej organizacji dane są drugim najcenniejszym zasobem, zaraz po pracownikach. Niestety wraz z pojawieniem się nielegalnych aukcji, na których sprzedaje się informacje osobiste, na takich „przedsięwzięciach" można zarobić duże pieniądze. A przez to, zagrożenie ze strony oszustów jest cały czas poważne.

Bezprawne wtargnięcia

Jakikolwiek element informacji o charakterze osobowym, na przykład „loginy" do sieci i nazwiska, i informacje o pracownikach, mogą umożliwić nieuprawnione wejście do sieci i otworzyć przed przestępcą drzwi do skarbnicy informacji. Dane te mogą być sprzedane najwyżej licytującemu w przetargu lub wykorzystane bezpośrednio do wejścia do krytycznych baz danych firm, zawierających informacje finansowe, gospodarcze lub dane klientów. I to w tym obszarze powstają największe szkody. Ponieważ obecnie powszechnie są atakowane firmy niezależnie od wielkości i rodzaju działalności, zapobieganie zagrożeniom wymaga stosowania właściwych mechanizmów zapobiegawczych.

Ponieważ ustawodawcy zaczynają coraz surowiej traktować kradzieże tożsamości, techniki ataków również ewoluują. Współcześnie cyberprzestępcy działają inteligentnie. Brutalna „kradzież z włamaniem" do sieci bez wątpienia zwróci uwagę służb informatycznych firmy i spowoduje szybkie działania naprawcze. Znacznie lepiej jest dostać się do sieci niezauważenie i skopiować z niej cenne dane finansowe i o klientach, zanim przedsiębiorstwo zda sobie sprawę z tego, że pada ofiarą ataku.

A jak najprościej dostać się do sieci? Przez pracownika. Niezależnie od tego, czy ściąga on niedopuszczalne programy z Internetu, odpowiada na pozornie zasadną prośbę o podanie hasła pocztą elektroniczną czy tylko nieodpowiednio chroni informacje potrzebne do logowania się w sieci, zagrożenia płynące ze strony własnego personelu firm mogą być duże.

Spójrzmy na niedawną wpadkę służby celnej i podatkowej HMRC w Wielkiej Brytanii. Stracono 25 milionów rekordów danych, wcale nie w drodze złośliwego ataku, a przez niezamierzony, choć lekkomyślny błąd. W tym wypadku pracownik niskiego szczebla wysłał niezaszyfrowany dysk zawierający nazwiska, adresy i informacje o rachunkach bankowych milionów rodzin w UK przesyłką kurierską. Dysk, a także kolejny wysłany później, zaginął w drodze – co wywołało burzę w mediach podsycających panikę i zachęciło ponad milion osób do zmiany haseł dostępu do rachunków bankowych i kodów PIN.

Jakikolwiek element informacji o charakterze osobowym, na przykład „loginy" do sieci i nazwiska, i informacje o pracownikach, mogą umożliwić nieuprawnione wejście do sieci i otworzyć przed przestępcą drzwi do skarbnicy informacji.

To konkretne zdarzenie jest przykładem niezadziałania polityki bezpieczeństwa na styku infrastruktury przetwarzania danych i fizycznego przemieszczania danych. Warto także przy tej okazji zauważyć, że kompletna baza danych (25 milionów rekordów!) znalazła się na dyskach, czyli cała zaginęła, dlatego że system nie był w stanie określić, jaki podzbiór danych należy przesłać. Innymi słowy, lepsza polityka określałaby, że należy z bazy danych wybrać tylko niezbędne rekordy i je przesłać, dzięki czemu w razie utraty informacji sytuacja byłaby znacznie mniej bolesna i uniknięto by narażenia danych tak wielu milionów ludzi na wykorzystanie w celach przestępczych.

Rozległość problemu, przed którym stoją współcześnie firmy, powoduje, że w większości krajów wprowadzono odpowiednie przepisy – na przykład w Wielkiej Brytanii Ustawę o ochronie danych – wymagające, aby urzędy przestrzegały pewnych norm „higieny" danych oraz zapewniania ich ochrony i bezpiecznego przetwarzania. Ich złamanie może pociągać za sobą konsekwencje karne, utratę wiary-

godności i gniew klientów. W grudniu 2007 roku firma ubezpieczeniowa Norwich Union została ukarana rekordowej wysokości karą 1,26 miliona funtów za to, że nieszczelność zabezpieczeń w jej centrach telefonicznej obsługi klientów umożliwiła oszustom dostęp do danych osób ubezpieczonych, co spowodowało narażenie prawie siedmiu milionów klientów na możliwość poniesienia strat finansowych.

Oczywiście prawdziwego kosztu kradzieży tożsamości nie da się wyrazić w samym pieniądzu, choć według niektórych szacunków w samej Wielkiej Brytanii określa się go na 1,7 miliarda funtów rocznie. Ale w takich szacunkach należy również uwzględniać uszczerbek reputacji, który znacznie trudniej jest skwantyfikować, choć może nawet doskonale prosperującą firmę doprowadzić do upadłości.

Mając przed sobą takie perspektywy, co firmy powinny robić, by chronić siebie, pracowników i klientów? I jak, dążąc do zapewnienia pełnej ochrony sieci, mają doprowadzić do tego, by inwestycje w infrastrukturę w tym zakresie zwiększały także wydajność i sprawność pracy?

Policja polityczna

Podstawą działania jest skuteczne zabezpieczenie „styków" sieci, a sprawą krytyczną - wprowadzenie polityk odciążających pracowników od odpowiedzialności za decydowanie, co jest, a co nie jest „godne zaufania". Dobrym punktem wyjścia jest tu kontrola dostępu, a system oparty na realizacji polityki może być dobrym rozwiązaniem.

Potrzebę stosowania takiego rozwiązania doskonale podkreślają programy komunikacyjne współcześnie powszechnie wykorzystywane w biurach, takie jak błyskawiczne komunikatory (ang. - Instant Messaging - IM), Web 2.0 i programy peer to peer (P2P). Chociaż ruch IM trudno jest kontrolować i monitorować, całkowite zablokowanie pracownikom dostępu do komunikatorów to w pewnym sensie wylewanie dziecka z kąpielą, ponieważ takie rozwiązania bez wątpienia często zwiększają wydajność i sprawność pracy. Wdrożenie systemu ochrony opartego na polityce jest dobrym kompromisem – szkoli się pracowników, jak unikać błędów ludzkich, a jednocześnie wprowadza się funkcję nadzorczą właścicieli firmy pozwalającą im na egzekwowanie praktycznego przestrzegania tej polityki w sieci.

Dlatego pociągającą strategią jest stosowanie systemów ujednoliconej kontroli dostępu, umożliwiających granularną kontrolę nad punktami dostępu do sieci i weryfikację tożsamości (osoby usiłującej wejść do sieci, a także sprawdzenie czy urządzenie, z którego korzysta, nie stwarza zagrożenia)

oraz integrację z grodzią ogniową, urządzeniami wirtualnych sieci prywatnych, przełącznikami i punktami dostępowymi, wymuszającymi przestrzeganie przyjętej polityki.

Ponadto w firmach musi istnieć sposób rozpoznawania aplikacji pracujących w sieci (na przykład systemu CRM) i tego, kto usiłuje uzyskać do nich dostęp. Oznacza to dokładną analizę ruchu połączeń VoIP (głosowych po IP) i komunikatorów błyskawicznych pod kątem wykorzystywania i sprawdzania tożsamości użytkowników przed udostępnieniem im tych usług. Lepsze procedury rozpoznawania umożliwią firmom nie tylko większą kontrolę nad takimi aplikacjami, ale także wymuszenie stosownego poziomu bezpieczeństwa i jakości usług, zamiast zwykłego otwierania kanału, który może zostać wykorzystany przez niepożądaną aplikację do pokonania zabezpieczeń.

Powyższe w połączeniu z bramką ochrony na poziomie warstwy aplikacji, działającą jak sito przepuszczające autoryzowany ruch bez zakłóceń przy jednoczesnym blokowaniu ruchu pozostałego powinno zdecydowanie polepszyć bezpieczeństwo sieci konwergentnych. Jednakże przedsiębiorstwa nie powinny zapominać o istotności szyfrowania przesyłanego ruchu. W ten sposób będzie on „zakodowany" tak, że nawet w razie przechwycenia będzie bezwartościowy dla nieuprawnionego użytkownika.

Firmy są zobowiązane do ochrony własnego personelu i klientów poprzez dołożenie należytej staranności i zapewnienie maksymalnych możliwych zabezpieczeń. Ale polityka bezpieczeństwa będzie skuteczna tylko wtedy, jeżeli będzie rygorystycznie egzekwowana w całej organizacji i wspomagana stosownymi rozwiązaniami technicznymi zapewniającymi maksymalne ograniczenie ryzyka i skutków „czynnika ludzkiego".

Tego rodzaju działania prewencyjne umożliwią firmom osiąganie wysokiej sprawności działania, eliminując „czynnik strachu" i maksymalizując zalety gospodarcze stwarzane przez nowe techniki komunikacyjne. Jednakże osiągnięcie stanu wysokiej sprawności bezwzględnie wymaga zadbania o to, by zapewnienie bezpieczeństwa sieci nie ograniczało szybkości działania sieci, aplikacji, a także sprawności pracy pracowników. I tutaj ogromnie istotne jest przemyślane wybranie takiego rozwiązania i dostawcy, żeby zabezpieczenie sieci nie było kompromisem z jej użytecznością dla firmy.

Większe bezpieczeństwo to lepsza firma

Nie ma wątpliwości co do tego, że ataki są coraz częstsze i bardziej wyrafinowane, a zwalczanie takich zagrożeń wydaje się być sprawą skomplikowaną. Jednakże bolesne konsekwencje zaniechań w tym obszarze nie pozostawiają miejsca na bierność. Dobre rozwiązania zabezpieczające – czyli takie, które choć wewnętrznie są ekstremalnie rozbudowane technicznie, to są proste we wdrożeniu i obsłudze – są dostępne na rynku i firmy powinny poważnie się zastanowić nad ich wdrażaniem.

Na przykład wprowadzenie zunifikowanego systemu ochrony dostępu pozwoli firmie na sprawniejsze i bardziej otwarte udostępnianie informacji handlowych, przy jednoczesnej ochronie danych wewnątrz sieci przedsiębiorstwa przed atakami z wewnątrz i z zewnątrz.

Sieci o wysokiej wydajności pozwalają znacznie łatwiej spełniać ostre rygory bezpieczeństwa, a jasna co do kierunku polityka pozwala pracownikom skupić się na pracy zawodowej, bez dodatkowego obciążenia koniecznością pilnowania, by niezamierzenie nie otworzyć drzwi złodziejom tożsamości. Firmy, które dojdą do tego etapu rozwoju, będą mogły działać szybciej, bezpieczniej, wchodząc na drogę prowadzącą do stania się prawdziwie „wysoko,wydajnymi firmami sieciowymi".

dr Anton Grashion
Strateg ds. Bezpieczeństwa
na region Europy, Środkowego Wschodu i Afryki
w firmie Juniper Networks