PRACOWNICY ZAGRAŻAJĄ BEZPIECZEŃSTWU POUFNYCH DANYCH

Przeprowadzone przez RSA badania ujawniają nieświadome działania pracowników korporacji i administracji rządowej, które zagrażają bezpieczeństwu poufnych danych. Wyniki wskazują potrzebę ścisłego monitorowania zagrożeń informacji.

Prawdziwe zagrożenie tkwi w codziennych czynnościach

Wyniki badań wskazują, że zagrożenia dla danych ze strony zaufanych pracowników należy monitorować równie uważnie jak zagrożenia, stwarzane przez pracowników nieuczciwych, którzy z premedytacją ujawniają poufne dane. Fizyczny i/lub logiczny dostęp do zasobów organizacji mają zarówno pracownicy, podwykonawcy zewnętrzni, dostawcy, partnerzy, goście, jak i konsultanci. Podczas wykonywania swoich rutynowych obowiązków mogą bezwiednie powodować niezwykle poważne i kosztowne ujawnienia danych – czy to przez nieuwagę, poprzez obchodzenie istniejących zabezpieczeń lub też za sprawą nieodpowiednich procedur bezpieczeństwa.

Pracownicy potrzebują technologii i zabezpieczeń dopasowanych do potrzeb biznesowych

Wyniki sondażu wskazują, że upoważnione osoby często ignorują niepraktyczne – ich zdaniem – zasady polityki bezpieczeństwa, jeśli wymaga tego wykonanie zadania. Na przykład pracownicy, pozbawieni zdalnego dostępu do służbowej poczty elektronicznej, mogą wysłać dokument służbowy na prywatne konto pocztowe, by móc kontynuować pracę w domu, choć w większości organizacji takie działanie jest niezgodne z zasadami bezpieczeństwa.
Wyniki badania w tym zakresie są następujące:

- 35% respondentów stwierdziło, że wykonywanie zadań służbowych stwarza niekiedy potrzebę obchodzenia obowiązujących zasad i procedur bezpieczeństwa;
- 63% respondentów często lub sporadycznie wysyła służbowe dokumenty na prywatne konto pocztowe, by móc pracować nad nimi w domu.

Zaufani pracownicy, którzy ignorują politykę bezpieczeństwa, najczęściej czynią to bez złych zamiarów. Jednak, niezależnie od intencji, ich działania stwarzają zagrożenie ujawnienia poufnych danych, a tym samym powodują narażenie całej organizacji, jak i jej klientów, na niepotrzebne ryzyko. To ryzyko można ograniczać poprzez opracowywanie strategii zabezpieczeń zorientowanych na informację, w których uwzględniane są wymogi codziennej pracy z danymi. Po wprowadzeniu takich strategii, firmy powinny na bieżąco śledzić zgodność działań użytkowników z przyjętymi zasadami. Na podstawie analizy tych informacji należy kształtować zabezpieczenia w taki sposób, aby jednocześnie minimalizować ryzyko i maksymalizować produktywność. Wprowadzenie zabezpieczeń jak najmniej uciążliwych dla użytkowników pozwala ograniczać przypadki obchodzenia niewygodnych zasad bezpieczeństwa.

Pracownicy potrzebują zdalnego dostępu do poufnych danych

Zgodnie z oczekiwaniami, badania wykazały, że pracownicy potrzebują zdalnego dostępu do służbowych danych podczas podróży lub zdalnej pracy:

- 87% respondentów często lub sporadycznie wykonuje swoje obowiązki zdalnie przez sieć VPN lub e-mail z dostępem przez przeglądarkę WWW;
- 56% respondentów często lub sporadycznie korzysta ze służbowej skrzynki pocztowej za pośrednictwem publicznie dostępnej sieci bezprzewodowej (np. Wi-Fi w kawiarni, na lotnisku, w hotelu itd.);
- 52% respondentów często lub sporadycznie korzysta ze służbowej skrzynki pocztowej za pośrednictwem ogólnie dostępnego komputera (np. komputera w kafejce internetowej, na lotnisku, w hotelu itd.).

Zdalny dostęp do poufnych informacji wymaga silniejszego uwierzytelnienia niż tylko zabezpieczenie nazwą użytkownika i hasłem, które są stosunkowo łatwe do złamania. Organizacje mogą połączyć elastyczność dostępu zdalnego z zapewnieniem ochrony poufnych danych poprzez wprowadzenie silnego dwuskładnikowego uwierzytelniania: przy dostępie do sieci VPN i korzystaniu z poczty przez przeglądarkę WWW. Ryzyko utraty danych w środowiskach z dostępem mobilnym można dodatkowo ograniczyć poprzez tworzenie, monitorowanie i egzekwowanie polityki zabezpieczeń zorientowanych na informację.

Skuteczne wykorzystanie danych wymaga swobody ich przenoszenia

Wyniki sondażu pokazują, że zapewnienie efektywności pracowników i maksymalizacja wartości zasobów informacyjnych organizacji wymagają swobody przenoszenia danych:

- 65% respondentów często lub sporadycznie wychodzi z miejsca pracy z urządzeniem mobilnym (laptopem, telefonem i/lub pamięcią flash USB), zawierającym poufne dane (np. dane klientów, dane osobowe, dane finansowe firmy, dane kart kredytowych i informacje stanowiące tajemnicę handlową, jak chociażby plany rozwoju produktów);
- 8% respondentów w przeszłości zgubiło laptopa, telefon i/lub pamięć flash USB z danymi dotyczącymi firmy/organizacji.

O ile mobilność ma kluczowe znaczenie dla elastyczności działania, niechronione dane są zawsze zagrożone podczas składowania, przesyłania i użytkowania. Organizacje mogą to ryzyko minimalizować poprzez ograniczenie dostępu do danych poufnych i osobistych, do przypadków rzeczywiście niezbędnych oraz zapewnienie ochrony poufnych informacji niezależnie od miejsca ich gromadzenia: podczas użytkowania na urządzeniach osobistych, składowania w firmowych systemach plików i bazach danych oraz przesyłania przez sieci korporacyjne i publiczne. Przedsiębiorstwa powinny rozważyć wprowadzenie rozwiązań automatycznej kontroli, które w zależności od poziomu poufności danych pozwalają akceptować, śledzić, zawieszać, blokować transmisję danych lub szyfrować dane.

Zaufani pracownicy ufają sobie nawzajem

Bezpieczeństwo fizyczne stanowi fundamentalny element bezpieczeństwa ogólnego. Jednak wyniki badań pokazują, że pracownicy dość często wpuszczają do firmy nieznajome osoby. Podczas badań stwierdzono, że:

- 34% respondentów zdarzyło się w pracy otworzyć drzwi nieznajomej osobie;
- 40% respondentów zostało w przeszłości wpuszczonych do budynku przez nieznajomą osobę, gdy zapomnieli karty lub klucza do drzwi;
- 66% respondentów, pracujących w firmach, przyznało, że w salach konferencyjnych i pokojach dla gości w ich firmie udostępniana jest wewnętrzna sieć bezprzewodowa. Spośród respondentów, w których firmie taka sieć się znajduje, 19% stwierdziło, że dostęp do tej sieci jest całkowicie otwarty, bez konieczności jakiegokolwiek uwierzytelnienia.

Fizyczne zabezpieczenia nie zawsze są wystarczające, by zagwarantować dostęp wyłącznie uprawnionym osobom do pomieszczeń organizacji. Co więcej, nawet jeśli fizyczna kontrola dostępu działa bez zarzutu, niekoniecznie wszyscy – uprawnieni do przebywania w budynku – powinni mieć dostęp do danych w systemach komputerowych. Minimalizacja zagrożenia wymaga połączenia zabezpieczeń fizycznych z logiczną kontrolą dostępu. Organizacje mogą się przyczynić do zwiększenia bezpieczeństwa poufnych danych poprzez wprowadzenie dwuelementowego uwierzytelniania dostępu do wewnętrznych sieci bezprzewodowych, komputerów biurkowych, domen, portów i aplikacji, wraz z kontrolą dostępu.

Pracownicy często zmieniają role

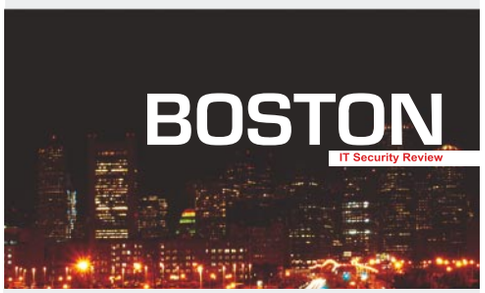
Zmiana jest w organizacjach czynnikiem stałym. Codziennie zachodzą zmiany zarówno w rolach wewnątrz firmy, jak i grupie podwykonawców i konsultantów. Badania pokazały, że aktualizacje zabezpieczeń często nie dotrzymują kroku zmianom.

- 33% respondentów zdarzyło się po wewnętrznej zmianie stanowiska nadal mieć dostęp do nieużywanych już kont lub zasobów;
- 72% respondentów stwierdziło, że w ich firmie/organizacji zatrudniani są pracownicy tymczasowi lub podwykonawcy, których obowiązki wymagają dostępu do kluczowych danych i systemów organizacji;
- 23% zdarzyło się wejść do obszaru sieci korporacyjnej, do którego we własnej ocenie nie powinni mieć dostępu.

Dostęp do danych poufnych lub osobowych powinien być udzielany wyłącznie w zakresie niezbędnym do wykonywania powierzonych zadań. Ograniczenie ryzyka ujawnienia danych można osiągnąć, wprowadzając dla kluczowych informacji kontrolę dostępu opartą na rolach. Istotne jest przy tym zapewnienie szybkiego uwzględniania zmian ról w uprawnieniach dostępu i objęcie kontrolą również wykonawców zewnętrznych i konsultantów. Organizacje mogą też ograniczać zagrożenia dla informacji poprzez scentralizowane i precyzyjne zarządzanie danymi uwierzytelniającymi pracowników, w tym nazwami logowania/hasłami, hasłami jednorazowymi i certyfikatami cyfrowymi oraz śledzenie wykorzystania tych danych w celu wykrywania prób nieuprawnionego dostępu. ■

Pełny raport z wynikami badania i zaleceniami można znaleźć na:
http://www.rsa.com/company/news/releases/pdfs/RSA-insider-confessions.pdf

KONKURS



Wszystkich czytelników zapraszamy do udziału w konkursie związanym z tematyką numeru: „BEZPIECZEŃSTWO KOMUNIKACJI MOBILNEJ".

Wystarczy odpowiedzieć na pytanie:
W JAKI SPOSÓB SYSTEM OPERACYJNY SYMBIAN OS UNIEMOŻLIWIA DOSTĘP DO DANYCH UŻYTKOWNIKA PO KRADZIEŻY JEGO TELEFONU?
Wśród poprawnych odpowiedzi, nadesłanych na adres: *boston@software.com.pl* rozlosujemy trzy programy chroniące przed zagrożeniami; Kaspersky Anty–Virus Mobile.

KONKURS