

Z roku na rok wzrasta ryzyko wycieku z firm strategicznych informacji. Ważną rolę w systemie ochrony odgrywa szeroko rozumiane zarządzanie dostępem oraz troska o zabezpieczanie i uwierzytelnianie dokumentów. Jak można się lepiej chronić?

Bezpieczeństwo jest obecnie jednym z podstawowych kryteriów korzystania z systemów informatycznych. Potwierdza to badanie firmy Cisco przeprowadzone wśród społeczności 970 posiadaczy certyfikatu CCIE (Cisco Certified Internetworking Expert) z 79 krajów, którzy pracują w firmach z listy Fortune 500 oraz małych i średnich przedsiębiorstwach. Z raportu wynika, że w ciągu najbliższych pięciu lat najważniejsze z punktu widzenia informatyków obszary to wirtualizacja oraz zarządzanie zabezpieczeniami i ryzykiem.

Jakie obszary i w jaki sposób powinny być szczególnie chronione? Z całą pewnością warto uszczelniać dostęp do newralgicznych dla firmy obszarów: fizycznych – pomieszczeń, budynków oraz cyfrowych – danych zgromadzonych w systemach IT. Istotnym aspektem bezpieczeństwa jest sprawowanie kontroli nad firmowymi dokumentami. Każdy dokument ważny dla firmy powinien być przypisany do konkretnej osoby, podobnie jak każda dokonana na nim zmiana powinna być kojarzona z pracownikiem, który jej dokonał i oznaczona znacznikiem czasu.

Biometryczny dokument identyfikacyjny

Jak wynika z badań firmy Mediarecovery zajmującej się odzyskiwaniem danych, 37 proc. specjalistów od spraw bezpieczeństwa IT obawia się defraudacji i nadużyć dokonywanych przez własnych pracowników. Są to słuszne obawy, gdyż to właśnie pracownicy w 66 proc. incydentów naruszali bezpieczeństwo wewnętrzne. Równie poważna w skutkach jak przestępczość korporacyjna może być beztroška zatrudnionych, gubiących sprzęt lub przesyłających istotne dokumenty jako zwykłe załączniki poczty.

Dobrym sposobem na zwiększenie ochrony danych może okazać się zastosowanie systemów biometrycznych do kontroli dostępu nie tylko do pomieszczeń, ale też aplikacji informatycznych. Uwierzytelnianie za pomocą rozpoznawania cech biometrycznych gwarantuje, że do stref i systemów chronionych będzie miała dostęp konkretna osoba, a jej tożsamość zostanie potwierdzona ponad wszelką wątpliwość. Rozwiązania takie potrzebne są w bankach i w administracji państwowej w celu ochrony zastrzeżonych informacji, sprawdzają się także w zakładach przemysłowych, w których wydzielone strefy fizyczne czy informatyczne powinny być chronione ze względów bezpieczeństwa. Jednak aby stosować zabezpieczenie biometryczne trzeba w firmie wdrożyć odpowiednie rozwiązanie, które pozwoli na pobieranie, gromadzenie, przechowywanie i weryfikowanie danych identyfikacyjnych. System taki niezbędny jest wszędzie tam, gdzie istnieje konieczność produkcji identyfikatorów biometrycznych, ich użycia lub ich obsługi. Jedną z dostępnych na rynku platform do budowy rozwiązań biometrycznych jest PentaBIDS firmy Pentacomp Systemy Informatyczne S.A. Posiada ona strukturę modułową, co ułatwia dostosowanie do indywidualnych potrzeb użytkującej organizacji. PentaBIDS jako cechy biometryczne wykorzystuje wizerunki twarzy, w tym odwzorowania trójwymiarowe twarzy, oraz rysunek żył nadgarstka lub palca. Są to metody o małej skali błędów, znacznie mniej podatne na czynniki środowiskowe niż odcisk palca, gdyż zabrudzony lub skaleczony palec może spowodować, że użytkownik nie zostanie rozpoznany przez system. „PentaBIDS obsługuje cały proces prowadzący do wydania biometrycznego dokumentu identyfikacyjnego, począwszy od pobierania danych biometrycznych, przez gromadzenie ich w repozytorium, aż do wydania biometrycznej karty identyfikacyjnej lub tokenu biometrycznego, służących użytkownikowi do uwierzytelniania się i autoryzacji dostępu do chronionych pomieszczeń i systemów informatycznych. PentaBIDS składa się z komponentów pozwalających tworzyć w firmie kompleksowe rozwiązania. Jest przeznaczone dla tych, którzy chcą uwierzytelniać konkretne osoby, a nie karty dostępu, którymi te osoby się posługują” - mówi Bartłomiej Klinger zastępca dyrektora ds. Technologii i Rozwoju w Pentacomp.

Podpis elektroniczny – zrób to sam

Coraz częściej w firmach pracownicy pracują zdalnie, przesyłając wyniki swojej pracy do firmowej sieci. Nie zawsze są to bezpieczne kanały VPN, nieraz przesyłka wędruje po niezabezpieczonych łączach. Zresztą szyfrowanie dokumentów nie rozwiązuje problemu przypisania ich do konkretnego pracownika. Z kolei wewnątrz firm, szczególnie

w dużych organizacjach, także tych rozproszonych, zachodzi potrzeba elektronicznego podpisywania dokumentów, tak by ich obieg był szybki i wszelkie decyzje mogły być podejmowane natychmiast. Jeśli dokumenty krążą w wewnętrznym obiegu i nie wychodzą poza organizację niekoniecznie trzeba kupować i wdrażać kwalifikowany podpis elektroniczny. Można przy pomocy odpowiedniego rozwiązania informatycznego stworzyć sobie podpis do wewnętrznego użytku. Pentacomp już w 2005 roku rozpoczął prace nad takim oprogramowaniem. Obecnie jest to dojrzały produkt – PentaSCAPE – platforma do obsługi infrastruktury klucza publicznego. „Rozwiązanie oferuje wszystko, czego potrzeba do wydawania pracownikom certyfikatów cyfrowych nawet w najmniejszej organizacji. Certyfikaty takie mogą służyć do cyfrowego podpisywania dokumentów czy poczty elektronicznej, szyfrowania danych oraz uwierzytelniania się w systemach informatycznych” dodaje Bartłomiej Klinger. Pentacomp w 2008 roku wdrożył całą platformę PentaSCAPE w Urzędzie Marszałkowskim Województwa Małopolskiego. Urząd korzysta z wytwarzanych dzięki niej certyfikatów i podpisów cyfrowych w swoich wewnętrznych procedurach, w tym przy wymianie informacji z innymi jednostkami samorządowymi na terenie województwa małopolskiego.

W 2011r. mają wejść w życie nowe regulacje prawno-organizacyjne związane z projektem pl.ID i wydaje się, że administracja państwowa czy samorządowa, która była naturalnym klientem dla rozwiązań typu PentaSCAPE straci potrzebę ich zakupu. Obywatel będzie miał certyfikat elektroniczny zaimplementowany w swoim dowodzie osobistym, wydawanym przez jeden centralny organ państwowy, a jednostki administracji będą wyposażone w narzędzia do obsługi tego certyfikatu. Dla tego typu rozwiązań będzie jednak miejsce w organizacjach, które wolą stworzyć infrastrukturę zaufanych certyfikatów na własnym terenie i nie chcą korzystać z certyfikatów „urzędowych”.

O platformie PentaBIDS

Platforma PentaBIDS składa się z trzech zintegrowanych i jednocześnie niezależnych strukturalnie podsystemów. Pierwszy z nich, PentaBIDS-ES, wspomaga pracę biur lokalnych i punktów obsługi w zakresie elektronicznej rejestracji wniosków, wydawania oraz unieważniania biometrycznych dokumentów identyfikacyjnych. Umożliwia pobranie i zarejestrowanie danych biograficznych oraz biometrycznych (m.in.: zdjęcia twarzy, rysunku żył, odcisków palców). Drugi o nazwie PentaBIDS-BDPS – odpowiada za graficzną oraz elektroniczną personalizację dokumentów. Oprogramowanie steruje procesem produkcji dokumentów, w tym zaawansowanymi maszynami personalizującymi (drukarki, grawerki laserowe, urządzenia do perforacji obrazów, urządzenia do personalizacji elektronicznej mikroprocesorów itp.) Trzeci: PentaBIDS-BDMS – to centralny rejestr dokumentów biometrycznych. Może obsługiwać dane biometryczne dowolnego typu. Administratorem danych jest zawsze przedsiębiorstwo wdrażające rozwiązania. Należy pamiętać, że cechy fizyczne poszczególnych osób przetworzone w postać cyfrową są pod względem prawnym danymi osobowymi i jako takie podlegają ustawie o ochronie danych osobowych.

O platformie PentaSCAPE

Platforma PentaSCAPE zapewnia pełną infrastrukturę klucza publicznego (PKI), dzięki czemu pozwala stworzyć lokalne Centrum Certyfikacji, wydawać certyfikaty cyfrowe i zaufane znaczniki czasu oraz na bieżąco weryfikować ważność wydawanych poświadczeń cyfrowych. Uwierzytelnianie dostępu, zabezpieczanie danych oraz kanałów komunikacyjnych w PentaSCAPE (Secure Communication and Application Portal Environment) odbywa się z wykorzystaniem indywidualnych certyfikatów cyfrowych użytkowników, zapisanych na kartach mikroprocesorowych oraz certyfikatów cyfrowych wydawanych dla urządzeń będących elementami infrastruktury komunikacyjnej.

Marek Massalski

Optimum PR