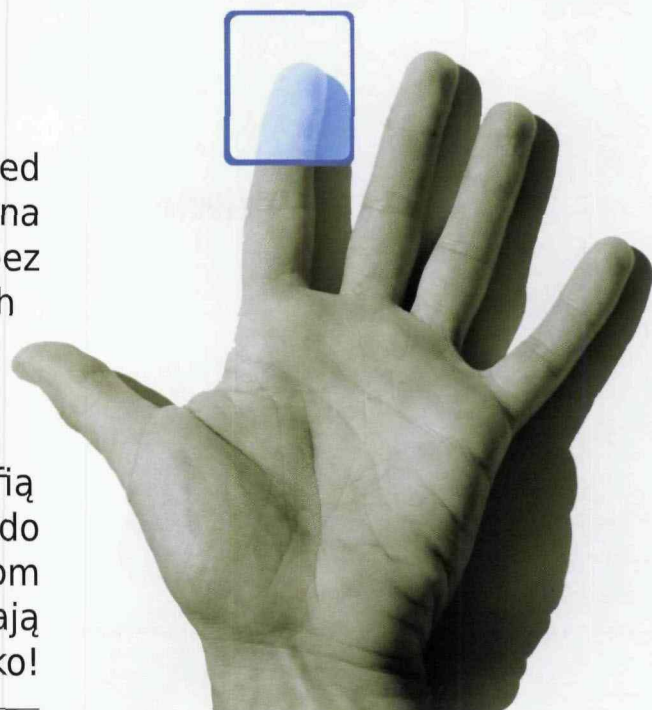


Automatyka w budynku - raport

STRZEC DANYCH JAK ŻRENICY OKA

BEZPIECZEŃSTWO DATA CENTER

Skuteczna ochrona data center przed niepowołanym dostępem jest ważna przede wszystkim dlatego, że bez informacji przechowywanych w serwerowniach wiele firm nie mogłoby normalnie funkcjonować. Z pomocą przychodzą nowoczesne technologie, które już dzisiaj potrafią weryfikować osoby wchodzące do newralgicznych miejsc, dzięki systemom biometrycznym. Eksperti przestrzegają jednak - technologia to nie wszystko!



– Jeszcze kilkanaście lat temu tylko duże firmy posiadały serwerownie, a w większości mniejszych firm serwer stał gdzieś w pomieszczeniu biurowym – zauważa Jan Zalewski, kierownik działu informatyki spółki Aster, dostawcy m.in. telewizji kablowej i dostępu do internetu. – Mało kto myślał wtedy o kwestiach bezpieczeństwa serwera czy danych w nim zawartych w kategoriach innych niż okresowe robienie backupu podstawowych danych.

Dzisiaj jesteśmy już o krok dalej i głównym powodem, dla którego firmy dbają o swoje serwery, jest bezpieczeństwo. Zachowanie ciągłości działania wiąże się bowiem bezpośrednio z uzależnieniem od systemów informatycznych i aplikacji biznesowych działających na serwerach.

– Serwerowni dotyczy pełne spektrum zagrożeń – wyjaśnia Wojciech Darłowski, dyrektor centrum systemów informatycznych w spółce itelligence. – Począwszy od ataku terrorystycznego, poprzez powódzie i inne zdarzenia siły wyższej, aż do trywialnych, wynikających z nieodpowiedzialności pracowników. Żeby zruj-

nować przedsiębiorstwo, naprawdę nie musimy mieć do czynienia z wybuchem bomby, wystarczy proste uszkodzenie infrastruktury trwające kilka godzin. Weźmy przykładowo pod uwagę przerwanie ciągłości działania dużej firmy logistycznej o zasięgu światowym wywołane zniszczeniem infrastruktury serwerowej. W pewnych przypadkach może to oznaczać straty nie do odrobienia lub wręcz bankructwo. Dlatego ochrona serwerowni i skuteczna polityka bezpieczeństwa są kluczowe w biznesie.

Określone zagrożenia

Zabezpieczenie serwerowni jest w istocie zabezpieczeniem informacji zawartych w systemach informatycznych. Dostęp do serwerowni zabezpiecza się po to, aby ograniczyć możliwość utraty danych czy to przez celową kradzież, czy też zniszczenie nośników informacji. W serwerowniach obecnie zlokalizowane są również centra komunikacyjne przedsiębiorstwa, centrale telefoniczne czy węzły sieci przesyłu danych. Awaria sprzętu komputerowego lub telekomunikacyjnego para-

liżuje firmę: uniemożliwia świadczenie usług, sprzedaż produktów, jak i obsługi klientów, czyli zmniejsza przychody i pogarsza wizerunek przedsiębiorstwa. Cel kontroli dostępu do serwerowni jest prosty. Zapewnienie, że tylko autoryzowany personel ma do niej dostęp.

– Łatwo sobie wyobrazić, że osoba postronna uzyskująca fizyczny dostęp do serwerów może nie tylko dokonać aktów wandalizmu, ale np. ukraść dyski twarde, które teraz można usunąć z macierzy bez większego problemu (tzw. hot swap) – stwierdza Michał Ceklarz, szef zespołu internet security systems w IBM Polska.

– Dostęp do serwerowni powinien być monitorowany również z przyczyn czysto technicznych, czyli kto i kiedy uzyskał dostęp oraz jakie czynności wykonał. Brak takiego monitoringu może doprowadzić do sytuacji, w której firma nie będzie w stanie stwierdzić, kto zmienił dane w bazie danych czy wyłączył serwer.

Jednym z aspektów bezpieczeństwa fizycznego jest kontrola dostępu do zasobów IT, w szczególności do pomieszczeń,

raport - Automatyka w budynku

w których znajdują się systemy przetwarzające dane krytyczne. W profesjonalnych centrach przetwarzania danych wydziela się specjalne strefy dostępu, które wymagają odpowiedniego poziomu autoryzacji.

– Ogólna zasada jest prosta. Im mniej osób ma dostęp do najbardziej newralgicznych stref dostępu, tym lepiej – stwierdza Wojciech Darłowski. – Do serwerowni powinni mieć wejście tylko ci, którzy naprawdę tego potrzebują. Istotne jest określenie ról w organizacji i związanych z nimi uprawnień. Ważna jest też zasada, że uprawnienia takie rosną wraz ze stażem pracy. Chodzi głównie o to, by np. nowy pracownik przeszedł pewnego rodzaju weryfikację. Dlatego też w naszej firmie, która zajmuje się opieką nad serwerami, jedynie ok. 30% pracowników ma dostęp do najbardziej newralgicznych obszarów data center.

System idealny?

Jak powinien wyglądać idealnie zaprojektowany system zabezpieczający serwerownię? Pierwsza kwestia to szereg zabezpieczeń przeciwpożarowych, wykrywających zalanie wodą czy podtrzymujących zasilanie. Wszystkie one służą temu, aby w razie zagrożenia mieć czas

na podjęcie działań zabezpieczających. Inne rozwiązania stosuje się, aby zabezpieczyć serwerownię przed niepowołaną osobą, która może, czasem nawet nieświadomie, spowodować awarię jakiegoś urządzenia. Mowa tu o elektronicznych systemach kontroli dostępu. Przeważnie stosuje się zamki elektryczne współpracujące z systemem dostępowym, w ramach którego wyznacza się strefy dostępu i przydziela uprawnienia do poruszania się w tych strefach w określonych godzinach. Z dostępnych rozwiązań stosuje się obecnie karty magnetyczne, zbliżeniowe czy systemy biometryczne.

W przypadku kart magnetycznych zabezpieczenie polega na przeciągnięciu karty z paskiem magnetycznym przez specjalny czytnik połączony z zamkiem otwierającym drzwi. Obecnie ten rodzaj zabezpieczenia nie jest jednak stosowany w nowych obiektach. Jego wadą jest bowiem zużywanie się kart oraz łatwość ich skopiowania. Dodatkowo system ten nie weryfikuje, czy osoba korzystająca z karty jest tą osobą, której kartę wydano.

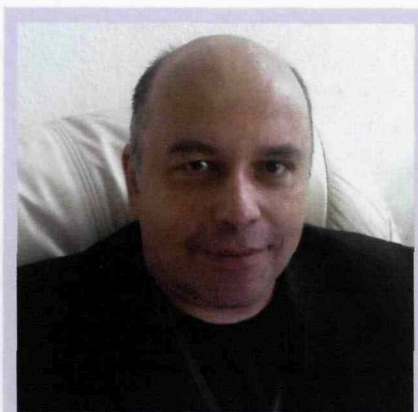
Inny przykład to karty zbliżeniowe, które są ulepszoną wersją poprzedniego zabezpieczenia i bardzo powszechnie wykorzystywane w data center. W tym wypadku karta jest wyposażona w umiesz-



Jakub Żurek, menedżer ds. sprzedaży usług outsourcingowych BCC

Warunki bezpieczeństwa systemów IT w polskich przedsiębiorstwach są bardzo zróżnicowane. Obserwując rynek, możemy powiedzieć, że poziom świadomości z roku na rok rośnie. Coraz częściej nasi klienci zainteresowani są usługami z rodziny rozwiązań tzw. zapasowego centrum przetwarzania danych. Od rezerwacji mocy obliczeniowej i opracowania planów ciągłości działania, pozwalających w przypadku awarii na szybkie przeniesienie systemów IT do naszego centrum przetwarzania danych, do rozwiązań stand-by, czyli równoległe pracujących baz danych czy zapasowych systemów utrzymywanych przez nas w pogotowiu dla sytuacji awaryjnych.

Automatyka w budynku - raport



Paweł Chomicz, dyrektor Centrum Kompetencyjnego Oracle w BizTech Consulting

Idealny system bezpieczeństwa data center powinien w 100% zabezpieczyć dane przed wszystkimi zagrożeniami. Koszty tego typu rozwiązań zależą od rozmiaru obiektu, rodzaju i ilości zastosowanych zabezpieczeń elektronicznych i wahają się od kilku do kilkuset tysięcy złotych.

Zabezpieczenia przed dostępem niepowołanych osób można podzielić na kilka obszarów:

- zabezpieczenia architektoniczne - teren ogrodzony i zamknięty, podzielony na zamknięte strefy o ograniczonym dostępie, szlabany, kółczatki, drzwi pracujące w systemie śluz itd.,
- zabezpieczenia elektroniczne,
- systemy alarmowe, zamki biometryczne, zamki elektroniczne, systemy rejestracji obrazu, czujniki ruchu itd.,
- ochrona fizyczna - dedykowana do ochrony obiektu firma ochroniarska mająca na miejscu załogę wystarczającą do eliminacji ryzyka nieautoryzowanego dostępu do obiektu i potrafiąca obsługiwać systemy zabezpieczeń elektronicznych.

Do tego potrzebne są zabezpieczenia przed zagrożeniami ciągłości działania data center, które zapewniają bieżącą obserwację stanu technicznego budynku i infrastruktury oraz elektroniczny monitoring infrastruktury (zasilanie, klimatyzacja, sprzęt informatyczny) czy parametrów klimatycznych w pomieszczeniach technicznych (temperatura, wilgotność).

czony w niej na stałe chip elektroniczny z unikalnym numerem identyfikacyjnym. Otwarcie drzwi następuje przy zbliżeniu karty do czytnika. Zalety to niski koszt wdrożenia i trudność w podrobieniu karty. Podobnie jak poprzednio system ten również nie weryfikuje jednak osoby, która z niej korzysta.

O wiele bardziej zaawansowaną technologią są systemy biometryczne, które opierają swoje działanie na badaniu indywidualnych części ciała: linii papilarnych palca, całej dłoni i/lub oka. Jest to rozwiązanie znacznie droższe od kart zbliżeniowych, stosowane najczęściej przy wejściu do najbardziej strzeżonych stref. Zaletą jest rzeczywista weryfikacja wchodzącej osoby, ale ograniczeniem wysoki koszt i konieczność uzyskania zgody weryfikowanych osób na przechowywanie i przetwarzanie ich danych biometrycznych.

I ostatnie rozwiązanie - system automatycznej rejestracji obrazu, który umożliwia bieżącą kontrolę i rejestrację działań wykonywanych przez znajdujące się w data center osoby. Nie decyduje przy tym o wejściu bądź odmowie dostępu do pomieszczenia. Jest to dodatkowy element zabezpieczenia, uzupełniający kontrolę osób w data center i w pewnym stopniu kompensujący wady systemów dostępowych opartych na kartach.

A może procedury?

Obecnie systemy kontroli dostępu zmierzają w kierunku rozwiązań opartych na badaniu biometrycznym. Najpopularniejsze (i najtańsze) są systemy oparte na odczycie jednego palca. Bardziej złożone i miarodajne są systemy skanujące całą dłoń. Ze względu na cenę najrzadziej stosowane są systemy do badania tęczy oka, ponieważ weryfikują one osobę na podstawie układu kilkuset tysięcy naczyń krwionośnych, które są unikatowe dla każdego oka. O ile są już bowiem udane próby podrobienia układu linii papilarnych pojedynczego palca i dło-

ni, to nie było jeszcze przypadku podrobienia tęczy oka. Eksperci przestrzegają jednak.

- Oczywiście można stosować bardzo zaawansowane sposoby zabezpieczenia serwerowni, jednak radziłbym podchodzić całościowo do kwestii zabezpieczenia informacji - przekonuje Jan Zalewski. - Inwestować nie tylko w zabezpieczenie serwerowni, ale i pozostałe elementy, jak np. sieć LAN czy punkty Wi-Fi w salach konferencyjnych, które, gdy nie są zabezpieczone, mogą posłużyć do wykradzenia danych firmowych.

Wojciech Darłowski dodaje: - Zbyt duża liczba technicznych elementów powoduje złudne wrażenie bezpieczeństwa. Firma może posiadać nawet najbardziej pancerne drzwi zabezpieczone kodem wejściowym, ale jeśli nie panuje nad tym, komu ten kod jest wydawany, w rzeczywistości nie ma żadnej kontroli nad wejściem. Podobnie w przypadku systemu zabezpieczającego serwerownię przed niepowołanym dostępem.

Eksperti są więc zdania, że rozwój technologii powinien zmierzać w stronę integracji takich technologii, jak kamery, biometryki i systemy eksperckie ze zdrowym rozsądkiem. Tak zintegrowane systemy dają bowiem najmniejsze możliwości oszustwa.

- Nie łudźmy się. Za każdym systemem stoi jakiś człowiek, a w związku z tym idealne zabezpieczenie po prostu nie istnieje - dodaje Darłowski.

Z pomocą przychodzą procedury, które zakładają przewidywanie pewnych sytuacji i sprawdzanie poprawności działania. Wymagają przy tym nieustających usprawnień. Nieprzypadkowo firmy specjalizujące się w usługach data center przechodzą certyfikacje pod kątem norm, np. ISO, a zatem zarządzania ciągłością działania i bezpieczeństwa informacji. Normy te wymuszają bowiem ustalenie i przestrzeganie okresowych procedur.