Uwaga! 360° bezpieczeństwa danych Twojej firmy

Czy zaufanie do pracownika jest wystarczającym powodem, byś jako manager organizacji mógł czuć się bezpiecznie i spełniać obowiązek prawny, jakim jest ochrona informacji?! NIE! Odpowiedziałeś TAK? Zastanów się więc, do czego może być zdolny pracownik w momencie, gdy poczuje się niedoceniony, nie dostanie podwyżki, gdy jego pozycja będzie zagrożona.

ANDRZEJ MACHURA

Inżynier systemów szyfrowania danych UTIMACO. Notariusz podpisu elektronicznego Thawte. Prelegent seminariów z zakresu bezpieczeństwa IT, www.szyfrowaniedanych.pl
Optymista, miłośnik FreeBSD, Audi A4, wypoczynku w katalońskiej Hiszpanii.
andrzej.machura@lanster.com

Każdego dnia budzimy się w świecie coraz większego postępu technicznego. Rozwój ułatwia życie niemal każdemu, przynosząc nowe rozwiązania, pozwalając skuteczniej zarządzać, czyniąc człowieka istotą mobilną. Niestety, wraz z nowymi możliwościami pojawiają się również nowe zagrożenia, ryzyka, niebezpieczeństwa.

Dlatego tak istotne staje się zagadnienie bezpieczeństwa w życiu każdego z nas, bezpieczeństwa, którego potrzebujemy zarówno w życiu osobistym, jako zwykły człowiek, jak również w firmie, jako pracownik, przełożony, manager.

W każdym przedsiębiorstwie zarówno produkcją, jak również instalacjami wewnętrznymi (telefony, klimatyzatory, ogrzewanie, instalacje przeciwpożarowe i alarmowe) sterują systemy informatyczne. Niestety, świadomość własnej zależności od infrastruktury IT i związanej z tym podatności na różne zagrożenia nie jest powszechna.

Owszem, wiele się mówi o zabezpieczaniu danych, mających - istotne, a zarazem krytyczne - znaczenie dla przedsiębiorstwa - danych klientów, danych finansowych, księgowych, itd., jednak nie każdy z nas zdaje sobie sprawę z istoty i wagi problemu. Mimo wielu potencjalnych niebezpieczeństw, chociażby ryzyko pospolitego ataku elektronicznego, można zaobserwować brak odpowiedniego wyczulenia na podobne zagrożenia. Pewnie zastanawiasz się teraz o co tyle zachodu? Zadaj więc sobie pytanie: co dla Ciebie jest największym zasobem w przedsiębiorstwie? Pracownicy, budynki, sprzęt? Z całą pewnością tak, jednak - z punktu widzenia informatycznego - największy zasób przedsiębiorstwa stanowią dane. Tak, to prawda – jeśli nie wierzysz, pomyśl o własnych poufnych i cennych informacjach, ile są warte i co stałoby się, gdyby dostały się w niepowołane ręce i np. zostały umieszczone w prasie, na forum internetowym.

Dlatego o dane warto się troszczyć – właściwie je składować, archiwizować i zabezpieczać. W przypadku każdego z nas poziom stosowanych zabezpieczeń ma bezpośredni wpływ na nasze osobiste korzyści lub też koszty, jakie możemy ponieść – utrata plików, stabilności systemu, kradzież danych, utrata reputacji, etc.

Informacja wciąż nie jest jeszcze traktowana jako właściwy, często najważniejszy, składnik majątku przedsiębiorstwa. A przecież każda dezintegracja takiej informacji lub utrata jej wiarygodności może oznaczać w Twojej sytuacji utratę klientów lub przewagi konkurencyjnej na rynku, co skutkuje brakiem możliwości osiągnięcia w 100 % celu każdego przedsiębiorstwa, jakim jest maksymalizacja zysku i korzyści.

O konieczności stosowania zabezpieczeń powinien więc wiedzieć każdy z nas. Każda firma, organizacja czy też osoba prywatna, aby nie utracić poufności, dostępności, autentyczności i spójności danych, musi stosować odpowiednią koncepcję bezpieczeństwa.

Zbudowanie solidnej koncepcji jest kluczowym elementem funkcjonowania biznesu, opartego na rozwiązaniach informatycznych. Ochrona i bezpieczeństwo danych, a także infrastruktury technicznej i dostępu do informacji zapewni sprawne i ciągłe funkcjonowanie systemów teleinformatycznych Twojego przedsiębiorstwa.

Dla firmy czy instytucji publicznej sytuacja komplikuje się, ze względu na występowanie wielu użytkowników, którzy z reguły w inny sposób dbają o bezpieczeństwo komputerów służbowych niż prywatnych lub używanych wyłącznie w celach prywatnych. Dosłownie chodzi tu o wykorzystywanie komputera służbowego (w większości problem dotyczy laptopów) do celów prywatnych, a tym samym brak zapewnienia poufności danych, haseł dostępu, zostawianie niezabezpieczonego terminala, udostępnianie danych osobom trzecim.

Istnieje kilka kryteriów, jakie musi spełnić koncepcja logiczna bezpieczeństwa informatycznego w przedsiębiorstwie.

Tradycyjne spojrzenie na zabezpieczanie danych – czyli zapewnienie poufności (prywatności) – oznacza, że dostęp do danych powinny mieć wyłącznie osoby uprawnione. Niestaranne zabezpieczenie poufności danych to potencjalne źródło poważnych problemów, więc powinniśmy dążyć do tego, by dane na naszych nośnikach pozostały tajne i nikt bez odpowiedniego uwierzytelnienia nie będzie mógł do nich dotrzeć. Każdy aspekt działalności przedsiębiorstwa wymaga zastosowania niezbędnych środków, które uniemożliwią nieuprawnionym dostęp do informacji w przedsiębiorstwie.

Zapewnienie integralności danych to zapobieganie nieuprawnionym modyfikacjom informacji. Sens tego aspektu jest taki, by określony odbiorca otrzymał dokładnie te dane, które zostały wysłane przez nadawcę. Kryterium integralności obowiązuje również wewnątrz przedsiębiorstwa - pracownik pobierający dane, musi je otrzymać dokładnie w takiej postaci, w jakiej ostatnio zostały zapisane. Niestety, istnieje niebezpieczeństwo, że osoby nieuprawnione mogą dokonywać manipulacji w wewnętrznych zasobach danych przedsiębiorstwa lub dokumenty mogą zostać zmienione – w trakcie ich przesyłania on-line.

Wiarygodność danych oznacza, że odbiorca może ustalić, kto jest rzeczywistym nadawcą dokumentu, zaś nadawca musi mieć pewność, że wysłane dane dotrą do wybranego adresata w sposób nienaruszony.

Istotne wyzwanie bezpieczeństwa informatycznego to dostępność usług informatycznych, funkcjonalności, informacji i danych. Konieczne jest bowiem zagwarantowanie pełnej dostępności przez cały czas. Chcemy wiedzieć, że usługi świadczone przez nasz komputer są w pełni dostępne – w momencie, kiedy ich potrzebujemy.

Pamiętajmy, że stosowanie zabezpieczeń dla danych, jak choćby dane osobowe pracowników, czy dane klientów, nie jest dobrą wolą administratora, lecz jest prawnym wymogiem - są regulowane odpowiednimi normami i regulacjami.

Dzisiejsze, skomplikowane sposoby nieautoryzowanego dostępu do danych, są niebywale zaawansowane i skomplikowane, mają bowiem na celu dotarcie do danych najbardziej wrażliwych, zarówno wewnątrz, jak i na zewnątrz firmy. Wyzwania, dotyczące ochrony zasobów przedsiębiorstwa zmieniają się w błyskawicznym tempie i są zdecydowanie inne niż wyzwania stawiane profesjonalistom kilka lat, miesięcy, tygodni, dni wcześniej.

Istotną kwestię w koncepcji bezpieczeństwa stanowi ochrona mobilnych urządzeń komputerowych, albowiem coraz więcej specjalistów – ponad 40% – spędza swój dzień pracy poza biurem. Pracownicy, opuszczając siedzibę firmy, podróżują z różnorodnymi mobilnymi urządzeniami komputerowymi, włączając w to laptopy, PDA, telefony komórkowe, itp. Na nośnikach tych często przechowywane są ważne informacje, łącznie z wartościami intelektualnymi oraz wrażliwymi danymi. Dane na tych urządzeniach są narażone na ryzyko dopóki, dopóty efektywne techniki ochrony danych nie są w użyciu. Używanie zaawansowanego szyfrowania danych w połączeniu z techniką silnego uwierzytelniania, sprawia, że informacje na urządzeniach mobilnych są efektywnie chronione.

Przedsiębiorstwa w świecie globalnego biznesu, oddziałując na siebie wzajemnie poprzez skomplikowane, ogólnoświatowe połączenia z oddziałami, wymieniając dane z partnerami, dostawcami, kontrahentami, providerami outsourcingowymi, potrzebują bezpieczeństwa współpracy w tak szeroko pojętym łańcuchu biznesowym.

Zaufanie do kontrahentów nie powinno dawać wystarczającego poczucia bezpieczeństwa, albowiem zagrożenia czyhają także na drodze transportu danych. Dlatego też wymagane jest zastosowanie takiej formy ochrony, by ograniczyć dostęp do istotnych informacji.

Centralne zarządzanie szyfrowaniem danych w sieciach i serwerach dostarcza ważnego poczucia kontroli nad systemami, uniemożliwia ujawnienie cennych aktywów firmy, chroni elektroniczne transakcje przed naruszeniem.

Możliwości, oferowane przez model otwartego biznesu, są najlepiej realizowane wówczas, gdy cały zakres danych pozostaje bezpieczny. Pełny 360-stopniowy obwód bezpieczeństwa.

Nieodłącznym elementem operacji biznesowych XXI wieku jest poczta elektroniczna. Jest to również element potencjalnego ataku na dane, dlatego znaczące jest zapewnienie prywatności komunikacji e-mailowej. Typ informacji, krążący wewnątrz czy też na zewnątrz firmy w formie wiadomości e-mail, to przede wszystkim tajemnice, plany biznesowe, strategie rozwoju, prywatne informacje klientów, wrażliwe dane finansowe, jak również informacje poufne. Znaczna część przedsiębiorstw dostrzega poważne i realne ryzyko przechwycenia prywatnej korespondencji e-mailowej przez przestępców lub, co gorsza, przez konkurencję.

Silne metody szyfrowania, wymuszane centralnie, bez ingerencji użytkownika, stanowią najlepszą ochronę bezpiecznej komunikacji za pomocą poczty elektronicznej. Rozwiązanie na tyle sprytne, że adresat wiadomości otrzymuje ją w formie zaszyfrowanej, aby odczytać lub odpowiedzieć nie jest wymagane wdrożenie jakiegokolwiek oprogramowania po jego stronie. E-mail wraca zaszyfrowany!

Zaawansowane rozwiązania szyfrowania w celu zachowania poufności przesyłanych danych są najskuteczniejszą metodą zabezpieczenia informacji w przedsiębiorstwach.

Komfort przenoszenia gigabajtów informacji za pomocą najnowszej generacji nośników danych – pamięci flash, nośniki optyczne czy magnetyczne – musi być zrównoważony do ryzyka ich kradzieży.

Zaleta, jaką jest przenośność, która czyni z tych urządzeń takie funkcjonalne i wygodne, zwiększa jednocześnie prawdopodobieństwo, że wrażliwe informacje przechowywane na tychże nośnikach mogą zostać zagubione lub skradzione. Jeśli jednak na takich nośnikach zastosowane zostanie wymuszane automatyczne szyfrowanie danych, nikt poza właścicielem nie będzie miał dostępu do ich zawartości.

Często zapomina się o przenośnych pamięciach podczas formułowania koncepcji bezpieczeństwa informacji, pomimo, iż zasługują one na poświęcenie pełnej uwagi w tworzeniu tego procesu.

Dane na serwerach korporacyjnych są bardziej narażone na atak ze strony wewnętrznego personelu niż hakerów z zewnątrz.

Firewalle, sieci prywatne VPN są bardzo efektywne do trzymania intruzów z dala od wrażliwych informacji, przechowywanych na serwerach sieciowych, jednak pojedynczy, niezadowolony pracownik lub też tymczasowy kontrahent, przebywający w siedzibie naszej firmy, może znaleźć drogę dostępu do informacji prywatnych lub przejęcia istotnych wartości firmy.

Szyfrowanie danych może jednak zapewnić efektywne ekranowanie informacji, przetrzymywanych na urządzeniach sieciowych, przed groźbą dostępu do zasobów serwerowych przez pracowników – z wewnątrz firmy.

W celu zapewnienia efektywnego bezpieczeństwa danych we własnym przedsiębiorstwie, powinniśmy wybrać najlepszą z możliwych dróg.

Przede wszystkim musimy chronić dane, przechowywane na urządzeniach końcowych, głównie te przechowywane na notebookach. Solidnym punktem startowym dla zapewnienia jakiejkolwiek strategii bezpieczeństwa, jest upewnienie się, że dane przenoszone na laptopach, które często „wędrują" poza siedzibę organizacji, są w pełni chronione – czyt. zaszyfrowane. Ta prosta bowiem we wdrożeniu technika, efektywnie izoluje intruzów oraz pracowników mobilnych przed nieświadomym i niezamierzonym ujawnieniem poufnych danych, informacji o klientach czy też innych informacji, mających wpływ na rozwój przedsiębiorstwa.

Skutecznym rozwiązaniem będzie dla nas – jako prezesów, administratorów, managerów – oprogramowanie, które dostarczy, transparentnego dla użytkownika, szyfrowania danych przechowywanych na urządzeniach i nośnikach przenośnych, dając przy tym użytkownikom (bez ich ingerencji) pełną ochronę przed nieautoryzowanym dostępem, utratą lub kradzieżą.

Po drugie: powinniśmy zapewnić bezpieczeństwo wszystkich danych wymienianych pomiędzy kontrahentami.

Model otwartego biznesu prosperuje pod warunkiem ciągłego udostępniania danych i przekazywania komunikatów drogą elektroniczną, co ulepsza w ten sposób realizację operacji i transakcji biznesowych, a przy tym zwiększa wydajność. Podstawowym, fundamentalnym warunkiem przeprowadzania operacji w takim środowisku jest zapewnienie szyfrowania danych w celu ochrony poufnych informacji, a co za tym idzie zasobów przedsiębiorstwa. Takie rozwiązanie gwarantuje bezpieczną wzajemną wymianę wiadomości z partnerami, dostawcami, klientami czy innymi podmiotami zaangażowanymi we współpracę z naszą organizacją. Zaszyfrowanie danych odbywa się w sposób automatyczny, bez ingerencji i wiedzy pracownika.

Trzeci istotny aspekt w koncepcji ochrony danych to bezpieczna wymiana informacji wewnątrz organizacji.

Wewnętrzne incydenty mogą być dość podstępne i często stanowić nierozpoznawalne ryzyko naruszenia danych. Czy można temu w jakiś sposób zapobiec? Owszem, ryzyko takie może być efektywnie zniwelowane, dzięki zastosowaniu szyfrowania danych zawartości katalogów grup roboczych, korespondencji mailowej, nośników danych i innych zasobów. Taki sposób zabezpieczenia się przed wewnętrznymi intruzami oraz przed świadomymi i nieświadomymi atakami, jest prostym i skutecznym środkiem ograniczenia strat finansowych, jakie pociąga za sobą utrata danych, jak również do wypełnienia obligatoryjnych norm i regulacji prawa.

Efektywnym rozwiązaniem będzie tu więc zaszyfrowanie danych, należących do użytkowników grup roboczych, a także ochrona informacji na dyskach lokalnych czy serwerach sieciowych, zarówno na poziomie plików, jak i katalogów.

Dane – przesyłane wewnątrz sieci – czynią atrakcyjnym obiekt zainteresowania dla potencjalnych intruzów. W związku z tym do danych powinny mieć dostęp tylko i wyłącznie autoryzowane grupy użytkowników, a pozostali pracownicy, administratorzy systemowi nie powinni mieć nawet możliwości oglądania zawartości plików, którymi zarządzają w systemie.

Ogólna koncepcja jest taka, że role administratorów wykluczają się wzajemnie. Admin Bezpieczeństwa Informacji posiada możliwość kodowania/dekodowania ale nie ma fizycznego dostępu do systemów operacyjnych. Z drugiej zaś strony administrator sieci posiada nieograniczony dostęp do systemów plików ale nie ma możliwości dekodowania plików i przeglądania ich zawartości.

Kolejne wyzwanie dotyczy ochrony danych, wychodzących poza naszą organizację, czyli na zewnątrz. Niezależnie od tego, czy pliki są udostępniane w grupie roboczej firmy (Intranet), czy też udostępniane przez Internet, należy zastosować fundamentalny poziom ochrony wszystkich aktywów poprzez wykorzystanie narzędzi szyfrujących w celu zabezpieczenia komponentów sieciowych, jak również serwerów.

Piąty aspekt bezpieczeństwa dotyczy pracowników i współpracowników w naszej organizacji. Czy zaufanie do pracownika jest wystarczającym powodem, by jako administrator IT czy manager organizacji czuć się bezpiecznie i spełniać obowiązek prawny, jakim jest ochrona informacji?! Jeśli odpowiedziałeś TAK to znaczy, że nie zdajesz sobie sprawy, do czego zdolny może być nawet najlepszy pracownik w momencie, gdy poczuje się niedoceniony lub nie dostanie podwyżki. Może zaszkodzić i zniszczyć to, co budowaliście w organizacji wiele lat.

Należy mieć więc również centralną kontrolę nad ustawieniami na stacjach roboczych. Chronić przed złośliwym kodem z prywatnych nośników, używaniem niedozwolonego oprogramowania i niezidentyfikowanych nośników danych (pendrive) czy też nieautoryzowanymi zmianami konfiguracji sprzętu. Potrzebne będzie w tym celu zdefiniowanie, z których urządzeń pracownik na danym stanowisku powinien i może korzystać, a których użycia i korzystania definitywnie zabronić lub domyślnie nie pozwolić na używanie. Oczywiście, dokonywanie ustawień należy wykonywać bez ingerencji użytkownika.

Po szóste, kluczowe jest wymuszenie centralnej polityki zasad na stacjach końcowych. Organizacje z rozmaitą infrastrukturą i skomplikowanymi wymaganiami bezpieczeństwa potrzebują rozwiązania, które łączy i potrafi skoordynować implementację priorytetowej polityki zasad.

Administrator bezpieczeństwa z centralnego, zdalnego punktu wymusza stosowanie zasad na stacjach, bez koniecznej akceptacji użytkowników, zasady zostają zaimplementowane.

Nie ulega więc wątpliwości, iż konieczne jest zabezpieczenie danych na stacjach końcowych i serwerach (dane w spoczynku: serwery, stacje robocze, laptopy, telefony komórkowe, PDA, etc.), w trakcie ich transportu (dane w ruchu: e-mail, CD/DVD, urządzenia Firewire, urządzenia USB, etc.), podczas procesu ich używania (dane w użyciu: personalizacja, zarządzanie dokumentami, e-płatności, procesy e-biznesowe).

Podsumowując, skuteczne zabezpieczenie danych organizacji, pozwoli zarówno zwiększyć wydajność i produktywność pojedynczego pracownika, jak i prowadzić działalność i zarządzać zgodnie z wymogami obowiązującego w Polsce prawa i regulacjami bezpieczeństwa. Wiedząc, iż dane wrażliwe i aktywa przedsiębiorstwa są skutecznie chronione, mając pewność, że w organizacji nie ma „luki bezpieczeństwa", zapewnisz spokój sobie oraz wszystkim pracownikom. ■

BIBLIOGRAFIA:

- Bezpieczne technologie sieciowe, www.lanster.com, 2007
- Data Security 2.0, Utimaco Safeware AG, 2007
- Research by Economist Intelligence Unit, May 2005
- Tomasz Pełech: Stosowanie zabezpieczeń danych w systemach korporacyjnych: dobra wola czy prawny obowiązek?, Gazeta-IT, Warszawa 2003
- Know Your Enemy: Statistics – Analyzing the past. Predicting the future. Honeynet Project
- CSI – Computer Security Institute, 2002. Cyber Crime bleeds
- U.S corporations, survey shows; financial losses from attacks climb for third year in a row.