Ochrona informacji w firmie – archiwizacja danych

W obecnych czasach, rzetelna informacja niejednokrotnie stanowi o tym, czy dana organizacja przetrwa na rynku oraz zapewni sobie właściwy rozwój, czy też będzie zmuszona ogłosić upadłość i zwolnić swoich pracowników. W warunkach wysokiej konkurencyjności największymi dobrami firmy są jej pracownicy oraz posiadane informacje. W niniejszym opracowaniu uwaga została skupiona głównie na informacji, a w szczególności na prawidłowym jej zabezpieczeniu.

Obecnie wiele organizacji wdraża tak zwany System Zarządzania Bezpieczeństwem Informacji – ISMS (ang. *Information Security Management System*) – jest to zjawisko nad wyraz pozytywne i świadczące o dojrzałości danej organizacji jako całości, a w szczególności jej zarządu. Przy wdrażaniu ISMS należy pamiętać, że powinno być to działanie kompleksowe i ciągle udoskonalane. Nie można systemu tego typu wdrożyć, a następnie zapomnieć o nim – działanie takie jest z góry skazane na porażkę i utratę już zainwestowanych środków finansowych. Wszystkie systemy bezpieczeństwa podlegają pewnej zasadzie, a mianowicie – powinny być wdrożone kompleksowo, zaś ISMS nie jest wyjątkiem od tej reguły. Należy zwrócić uwagę na fakt, że cały system jest tak wytrzymały, jak jego najsłabsze ogniwo! Ze względu na swoją złożoność, dokładny opis systemu zarządzania bezpieczeństwem informacji może stanowić nawet kilkusetstronicową książkę, dlatego też w artykule tym uwaga została skupiona na wybranych aspektach jednego z wielu ogniw, stanowiących kompleksowy ISMS, a mianowicie na archiwizacji danych. W dalszej części artykuł ten składa się z trzech bloków tematycznych, odnoszących się do archiwizacji danych. Blokami tymi są: aspekty organizacyjne, aspekty techniczne oraz aspekty prawne archiwizacji danych.

ROBERT DEKOWSKI
Urodził się w 1977 r. w Warszawie. Obecnie doktorant w Instytucie Badań Systemowych Polskiej Akademii Nauk na kierunku Informatyka w Finansach i Zarządzaniu. W 2005 r. ukończył Wyższą Szkołę Informatyki Stosowanej i Zarządzania w Warszawie na wydziałach sieci komputerowe i inżynieria programowo-sprzętowa oraz w 2001 r. Szkołę Nauk Ścisłych na makrokierunku matematyka, fizyka, chemia. Od stycznia 2006 r. pracuje jako analityk w Biurze Bezpieczeństwa Informacji i Systemów Informatycznych w Raiffeisen Bank Polska SA, zajmując się głównie kwestiami: audytów bezpieczeństwa teleinformatycznego, oceną ryzyka aplikacji i systemów IT, testami bezpieczeństwa, opiniowaniem projektów, zarządzaniem incydentami bezpieczeństwa oraz opracowywaniem specjalistycznej dokumentacji i prowadzeniem szkoleń. Posiada certyfikat Generalnego Inżyniera Bezpieczeństwa IsecMan oraz zdane egzaminy CISA i CCNA. Jako swoje zainteresowania wskazuje żeglarstwo i fotografię. Wszelkie opinie i uwagi na temat artykułu można kierować bezpośrednio do autora na adres kontaktowy *robertde@wp.pl*.

Aspekty organizacyjne archiwizacji danych

Zapewnienie właściwej archiwizacji danych powinno być procesem ciągłym oraz dokładnie dostosowanym do potrzeb i możliwości konkretnej organizacji. Oczywistym jest, że instytucje finansowe, takie jak banki czy korporacje ubezpieczeniowe posiadają inne potrzeby na tej płaszczyźnie niż urzędy administracji publicznej czy służba zdrowia. Dlatego też niezmiernie istotnym jest opracowanie (a także stałe korygowanie w celu uaktualnienia) odpowiednich dokumentów, odnoszących się do archiwizacji danych. Do najważniejszych należy zaliczyć:

- Politykę przeprowadzania archiwizacji danych;
- Standard odnoszący się do archiwizacji danych;
- Zalecenia (*guidelines*), zawierające odpowiednie wskazówki dla osób tworzących stosowne procedury;
- Procedury archiwizacji danych, a także odtwarzania ich z kopii zapasowych i kopii bezpieczeństwa.

Dokumenty te stanowią fundament, umożliwiający przeprowadzanie archiwizacji danych w sposób zoptymalizowany pod względem potrzeb konkretnej organizacji. Dlatego też powinny one zostać stworzone przez osoby, posiadające odpowiednią wiedzę oraz doświadczenie w tej tematyce. Bardzo niewłaściwym podejściem do problemu jest dokładne skopiowanie cudzych rozwiązań. Pomijając aspekty prawne i moralne takiego działania, należy stwierdzić, że jest to rozwiązanie najgorsze z możliwych i to z wielu powodów. Po pierwsze, każda organizacja jest inna – po-

trzeby, struktura organizacyjna, kompetencje i liczba pracowników, posiadany budżet, itd. Przykładowo, filtr powietrza z samochodu A nie będzie pasował (z bardzo dużym prawdopodobieństwem) do samochodu B, mimo że i A, i B są podobnymi urządzeniami (każdy ma kierownicę, koła, silnik, itd.). Podobnie jest z dokumentacją, odnoszącą się do archiwizacji danych. Po drugie, złe i nietestowane procedury są gorsze niż ich brak! Generalnie, ludzie zachowują się znacznie rozsądniej, gdy nie posiadają żadnych wytycznych, niż w sytuacji, gdy posiadają niesprawdzone i wątpliwej jakości instrukcje. Po trzecie, ktoś w organizacji może użyć tych dokumentów jako pewnego rodzaju wzorca odniesienia – jaka będzie jakość „dokumentu", tworzonego na podstawie złej jakości wzoru, pozostaje pytaniem zarówno retorycznym, jak i otwartym. Celem tego podrozdziału nie jest przeprowadzenie ekspresowego kursu tworzenia dokumentacji korporacyjnej (osobiście uważam, że kurs taki byłby z góry skazany na niepowodzenie), lecz przedstawienie najważniejszych zagadnień, na które należy zwrócić szczególną uwagę podczas opracowywania wyżej wymienionych dokumentów oraz w trakcie stosowania opracowanych procedur. Do kwestii tych zaliczyć należy:

- Wybór informacji, które powinny być archiwizowane;
- Właściwy dobór odpowiedniego czasu i cyklu archiwizacji;
- Odpowiedni wybór nośnika oraz oprogramowania służącego do archiwizacji;
- Właściwy wybór metody przeprowadzania archiwizacji oraz liczby kopii;
- Ustalenie czasu i sposobu przechowywania archiwów;
- Określenie sposobu postępowania z informacją zapisaną w formie innej niż elektroniczna (na papierze, folii, kliszach, itp.);
- Właściwy dobór metody zapewnienia poufności i integralności archiwizowanych danych;
- Oszacowanie oraz umieszczenie w budżecie odpowiednich środków finansowych.

Wybór informacji, które powinny być archiwizowane

Planując archiwizację danych, należy dokładnie zastanowić się, jakie informacje należy archiwizować. Przy podejmowaniu takiej decyzji pomocna okazuje się klasyfikacja informacji. Zgodnie z „regułami sztuki", do każdej informacji powinien zostać przypisany jej właściciel, który, na podstawie znormalizowanych i spójnych dla całej organizacji wytycznych, dokonuje jej klasyfikacji. Istotnym jest, że jedna osoba może być właścicielem wielu informacji, natomiast dana informacja może należeć tylko do jednego właściciela. Przykładowe poziomy klasyfikacji informacji mogą być następujące: tajne, poufne, do użytku wewnętrznego, jawne. W zależności od potrzeb i specyfiki danej organizacji, zarząd (po przeprowadzeniu konsultacji z osobami, posiadającymi odpowiednią wiedzę) może (powinien) podjąć decyzję, jakie informacje należy archiwizować, np. te informacje, które zostały sklasyfikowane jako tajne lub poufne.

Właściwy dobór odpowiedniego czasu i cyklu archiwizacji

Czas przeprowadzania archiwizacji, rozumiany jako czas rozpoczęcia tworzenia kopii (*backup'u*) danej informacji, powinien być tak zaplanowany, aby w jak najmniejszym stopniu proces archiwizacji wpływał na funkcjonowanie systemu, w którym informacja ta jest przechowywana lub przetwarzana. Dla przykładu, jeżeli dział księgowości pracuje w godzinach 8.30-17.00, to dobrym rozwiązaniem jest przeprowadzanie archiwizacji w godzinach 17.30–6.00. Ważnym jest, aby czas jej planowanego zakończenia wypadał dużo wcześniej niż rozpoczęcie użytkowania systemu, dając tym samym możliwość reakcji w sytuacji awaryjnej, czyli „gdy coś pójdzie nie tak, jak powinno". Osobnego rozważenia wymagają tzw. systemy 24/7, czyli pracujące bez przerwy. W sytuacji takiej zalecanym rozwiązaniem jest przeprowadzenie analizy obciążenia systemu i na tej podstawie ustalenie czasu archiwizacji w okresach, gdy system jest najmniej obciążony. Drugim alternatywnym podejściem do tego zagadnienia jest przełączenie systemu (o ile to możliwe) w tryb tylko do odczytu, na czas wykonywania archiwizacji lub całkowite przełączenie na system zapasowy (w przypadku tym należy w odpowiedni sposób zapewnić integralność i spójność danych w systemie podstawowym i zapasowym). Kolejną istotną kwestią jest cykl archiwizacji informacji, tzn. jak często i w jaki sposób konkretne informacje powinny być archiwizowane. Częstotliwość archiwizacji powinna zostać określona przez odpowiednich właścicieli poszczególnych informacji – właściciel jest (powinien być) osobą najlepiej znającą daną informację, to znaczy wymagania, co do jej wrażliwości oraz dostępności (także wymagania odnośnie integralności i poufności). Najczęstszymi rozwiązaniami są archiwizacje codzienne lub cotygodniowe.

> **Zapewnienie właściwej archiwizacji danych powinno być procesem ciągłym oraz dokładnie dostosowanym do potrzeb i możliwości konkretnej organizacji... sposobów na archiwizację jest kilka.**

Odpowiedni wybór nośnika oraz oprogramowania służącego do archiwizacji

Zarówno wybór nośników, jak i oprogramowania zależy od potrzeb oraz możliwości danej organizacji. W małych firmach może okazać się całkowicie wystarczające archiwizowanie informacji za pomocą narzędzi wbudowanych, np. w system operacyjny Windows 2000, 2003 czy XP, z wykorzystaniem dedykowanych dysków twardych (w sytuacji takiej na ogół jeden komputer, zaopatrzony w odpowiednio dużej pojemności dyski, staje się dedykowaną maszyną do przechowywania archiwów) lub płyt DVD/CD. Innym alternatywnym rozwiązaniem są zestawy skryptów (pisane np. w SHELL'u, Perl'u, itd.), przeprowadzające automatycznie proces archiwizacji. Wraz z rozbudową organizacji, pojawiają się potrzeby bardziej scentralizowanego podejścia do archiwizacji danych. Z pomocą przychodzą tu rozwiązania, np. TSM (*Tivoli Storage Manager*). Wzrasta również zapotrzebowanie na pojemność nośników. Obecnie najczęściej stosowanymi nośnikami są taśmy magnetyczne, których pojemność należy do przedziału od 30 do 980 GB. Niestety, nie jest to rozwiązanie tanie, zarówno przy zakupie, jak i podczas eksploatacji.

Właściwy wybór metody przeprowadzania archiwizacji oraz liczby kopii

Sposobów, w jaki można archiwizować informacje, jest kilka i to zarówno technicznych, jak i organizacyjnych. Sposoby techniczne zostały opisane w dalszej części tego artykułu w podrozdziale zatytułowanym „Aspekty techniczne". Natomiast kwestia, w jaki sposób organizacyjnie przeprowadzać ten proces, zależy od różnych czynników, jak: wrażliwość informacji, aspekty prawne, posiadane zasoby. Oczywistym jest, że informacje bardziej wrażliwe powinny być archiwizowane częściej, dodatkowo regulacje prawne mogą wymuszać określony sposób postępowania z archiwami, zaś możliwości finansowe organizacji także nie pozostają bez znaczenia. Jedną z popularniejszych metod przeprowadzania archiwizacji jest tworzenie raz w tygodniu (np. w piątek) pełnych kopii, zaś w pozostałe dni robocze kopii przyrostowych. W cyklu takim potrzebne są cztery rotowane nośniki na kopie przyrostowe (ze względu na awaryjność oraz małą trwałość nie zaleca się tworzenia kilku kopii przyrostowych na jednym nośniku) oraz dodatkowo nośniki na kopie pełne. Liczba nośników przeznaczonych na składowanie kopii pełnych zależy od tego, jak daleko wstecz zachodzi potrzeba dostępu do archiwizowanych danych. Potrzeba ta może być podyktowana względami biznesowymi lub/i wymogami

prawnymi. Dla informacji mało wrażliwych i dających się w prosty lub szybki sposób odtworzyć, powinna wystarczyć jedna kopia, natomiast informacje strategiczne z punktu widzenia konkretnej organizacji (należy także uwzględnić wymogi prawne) powinny być archiwizowane w przynajmniej w dwóch egzemplarzach, przy czym każdy z nich powinien znajdować się w innym miejscu (przynajmniej innym budynku albo nawet i mieście). Rozdzielenie kopii ma na celu zagwarantowanie przetrwania chociażby jednej z nich w przypadku np. pożaru, kradzieży czy aktu sabotażu.

Ustalenie czasu i sposobu przechowywania archiwów

Jak zostało napisane wcześniej, czas przechowywania archiwów jest zależny od tego, jak daleko wstecz zachodzi potrzeba dostępu do informacji. Różne informacje najprawdopodobniej będą wymagały różnych czasów przechowywania, dlatego warto tak zaplanować rozkład informacji na nośnikach, aby wszystkie dane zapisane na pojedynczym nośniku ulegały „przedawnieniu" niemalże jednocześnie, zwalniając tym samym cały nośnik. W przypadku nośników zapisu jednorazowego, po upłynięciu czasu przechowywania informacji, nośnik taki powinien być utylizowany w specjalnej niszczarce. W celu zapewnienia odpowiedniej dostępności archiwizowanych informacji, zawierające je nośniki, powinny być przechowywane w wyznaczonym do tego celu miejscu. Miejsce to powinno gwarantować odpowiedni poziom ochrony przechowywanych informacji, przy czym poziom ten powinien być adekwatny do wagi składowanych informacji. Dodatkowo, należy rozważyć zastosowanie zabezpieczeń przed czynnikami środowiskowymi, takimi jak pożar czy powódź. Dobrym miejscem na magazyn archiwów jest kasa pancerna, która najczęściej jest ognio- i wodoodporna, a także posiada stałe mocowanie do podłoża lub ściany. Należy pamiętać, że chaos destabilizuje pracę organizacji, dlatego każdy nośnik powinien być zaopatrzony w odpowiedni numer inwentarzowy. Ponadto w miejscu przechowywania archiwów, powinien znajdować się odpowiedni wykaz, zawierający następujące informacje: numer inwentarzowy nośnika, krótki opis informacji, jakie się na nim znajdują, imię i nazwisko oraz podpis osoby wykonującej kopię, datę wykonania kopii, inne informacje.

Określenie sposobu postępowania z informacją, zapisaną w formie innej niż elektroniczna (na papierze, folii, kliszach, itp.)

Archiwizowanie informacji, przechowywanych w formie innej niż elektroniczna, wymaga znacznych przestrzeni (miejsca w szafach, szufladach, itd.), dlatego też może okazać się, że lepszym rozwiązaniem jest skanowanie materiałów, a następnie archiwizowanie ich już w formie elektronicznej. Oczywiście, nie każdy dokument można po zakończeniu skanowania zniszczyć – chociażby z powodów prawnych, dlatego też nie da się całkowicie wyeliminować dokumentów nieelektronicznych. Mając na uwadze charakter prowadzonej działalności, każda organizacja indywidualnie powinna wypracować odpowiedni punkt równowagi.

Właściwy dobór metody zapewnienia: poufności i integralności archiwizowanych danych

Oprócz zapewnienia dostępności, integralność archiwizowanych informacji jest ich najważniejszym atrybutem. Informacje, które zostały (celowo lub przypadkowo) zmodyfikowane, tracą swoją wartość i będą wprowadzać w błąd. Dlatego też należy rozważyć wdrożenie pewnych mechanizmów, zapewniających weryfikację integralności, takich jak np. naliczanie sum kontrolnych. To, czy sumy te będą naliczane dla poszczególnych plików, katalogów czy całego dysku lub archiwum, zależy od wrażliwości archiwizowanych informacji. Należy tu wykorzystać wspomnianą wcześniej klasyfikację informacji, na podstawie której można wyznaczyć poziom wrażliwości poszczególnych archiwizowanych danych. Szczególnie wrażliwe informacje powinny dodatkowo być podpisywane cyfrowo przez upoważnioną do tego osobę. Jeżeli archiwizowane dane wymagają zapewnienia poufności, to należy je w odpowiedni sposób zaszyfrować, lecz przy stosowaniu szyfrowania pojawia się problem zarządzania kluczami szyfrującymi. Ponieważ zagadnienie szyfrowania znacznie przekracza tematykę oraz ramy tego artykułu, dlatego zostało ono jedynie wspomniane jako propozycja zapewnienia poufności archiwizowanych informacji.

Oszacowanie oraz budżetowanie odpowiednich środków finansowych

Często spotykanym błędem jest traktowanie archiwizacji jako kolejnej czynności przypisywanej do obowiązków administratorów aplikacji czy serwerów, itp. W małych organizacjach może być to jedyne rozsądne rozwiązanie, lecz w średnich i dużych jest nie do zaakceptowania. O ile to możliwe, powinno istnieć dedykowane do tego celu stanowisko służbowe, a to, oczywiście, generuje dodatkowe koszty dla organizacji. W sytuacji takiej niezbędnym staje się umieszczenie w budżecie odpowiednich środków finansowych, w tym także na sprzęt i materiały. Nadmierne oszczędności mogą okazać się pozorne i prowadzić do utraty informacji, np. poprzez używanie tych samych taśm wiele lat. Utrata taka może skutkować sankcjami prawnymi, a na pewno odtworzenie (o ile się uda) informacji nie będzie tanie.

Aspekty techniczne

Ze względu na zakres oraz tematykę tego artykułu, aspekty techniczne i prawne zostały ograniczone jedynie do krótkiego opisu najważniejszych kwestii. Przede wszystkim należy zastanowić się, czy system archiwizowania powinien być scentralizowany czy rozproszony, generalnie małe organizacje posiadają systemy rozproszone, a duże scentralizowane. Zaletą systemu rozproszonego jest jego niski koszt, natomiast scentralizowanego – lepsze, w porównaniu do rozproszonego, zarządzanie cyklem wykonywania i magazynowania archiwów. Kolejnym etapem jest wybór odpowiedniego sprzętu i oprogramowania. Zasada jest następująca – sprzęt powinien być dobrany pod konkretnie przyjęty system (rozproszony, scentralizowany lub hybrydowy), a nie odwrotnie. Ze względu na olbrzymią liczbę dostępnych na rynku różnego rodzaju rozwiązań, zarówno sprzętowych jak i programowych oraz dużą dynamikę zmian, dokładniejszy ich opis w tym artykule staje się bezzasadny. Dodatkowo, należy zapewnić odpowiedni poziom wyszkolenia osoby odpowiedzialnej za wykonywanie kopii, nie ulega wątpliwości, że osoba ta powinna posiadać techniczne podstawy oraz wiedzę z obszaru IT.

Aspekty prawne

Każda organizacja, bez względu na rozmiar czy zakres działalności, w mniejszym lub większym stopniu podlega różnym regulacjom prawnym. Część z nich dotyczy także archiwizacji danych. To, jakie ustawy i rozporządzenia obejmują daną organizację, zależy od wielu czynników, m.in. od rodzaju prowadzonej działalności. Z tego względu opis aspektów prawnych, odnoszących się do archiwizacji danych, został przedstawiony jedynie w sposób ogólny. W interesie każdej z firm jest określenie, jakim podlega regulacjom, dla przykładu – dla instytucji finansowych mamy Bazylee II, dla służby zdrowia HIPPA, w USA obowiązuje Sarbanes-Oxley (SOX), itd. W prawodawstwie polskim „Ustawa o ochronie danych osobowych" (Dz. U. Nr 133, poz. 883) także odnosi się do archiwizacji danych, np. rozdział 5 pt. „Zabezpieczenie danych osobowych", Art. 36. punkt 1.: „Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne, zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem".

Zakończenie

Należy pamiętać, że nawet najlepiej przygotowany system archiwizacji danych, a następnie „zapomniany" i nieudoskonalany, nie na wiele się zda. System ten powinien „żyć" i w sposób cykliczny być dostrajany do zmieniających się realiów. Dodatkowo należy np. raz na miesiąc przeprowadzać testy odtwarzania wybranych losowo danych. Archiwum, którego nie można odtworzyć, stwarza pozorne poczucie bezpieczeństwa, a to z kolei jest gorsze niż świadomość jego braku. W parze ze zmianami powinna być przeprowadzana aktualizacja dokumentacji. Wiele organizacji traktuje dokumentację jako „zbędną makulaturę", a to właśnie ta „makulatura" może zaoszczędzić dużo czasu i pieniędzy w przypadku, np. niedostępności administratora, podejrzanego działania systemu, odbudowy systemu po awarii, itd. Reasumując, prawdziwą wartość archiwów docenia się dopiero wtedy, gdy ich brakuje!