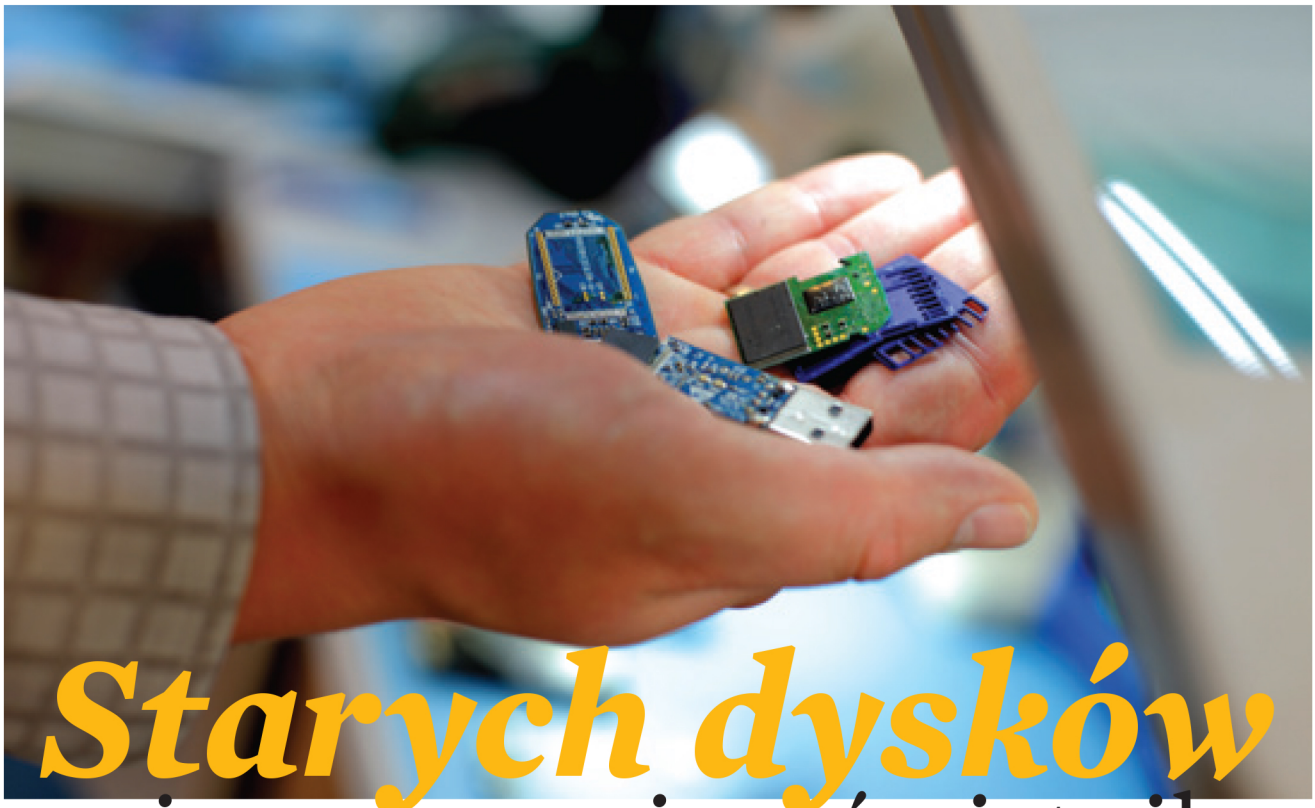

Starych dysków nie wyrzucaj na śmietnik

Praktycznie każdy podmiot prowadzący działalność biznesową musi w swoich planach uwzględnić strategię bezpieczeństwa pojmowaną nie tylko w zakresie bezpieczeństwa sieciowego, ale również w kwestii przechowywania kopii i archiwów.

DARIUSZ HAŁAS

Nawet najdoskonalsza strategia archiwizacji i backupu nie będzie nic warta, jeżeli dojdzie do zniszczenia, zgubienia czy choćby pomieszania nośników zawierających dane archiwalne i kopie zapasowe. Problem jednak w tym, że o ile samo wykonywanie kopii zapasowych jest już dziś traktowane poważnie nawet w najmniejszych, wręcz jedno- bądź kilkuosobowych mikrofirmach, to kwestia zarządzania nośnikami zawierającymi zabezpieczone dane zazwyczaj nie jest już tak oczywista. Sama świadomość tego, że został wykonany backup, może prowadzić do złudnego poczucia bezpieczeństwa. Co z tego, że będziemy dysponować kopią danych, gdy w chwili awarii lub w innych okolicznościach – wymagających zwykle jak najszybszego odtworzenia danych – nie będziemy wiedzieć, gdzie potrzebna kopia się znajduje?

Generalnie polityka archiwizacji i składowania danych w firmie zawsze powinna być dostosowana do faktycznych potrzeb i racjonalna ekonomicznie. W wielu firmach „strategią" przechowywania nośników jest wydzielona szafa z odpowiednio oznaczonymi nośnikami. Owszem, samo uporządkowanie woluminów (podpisanie, skatalogowanie i ich odpowiednie rozmieszczenie) znacznie ułatwi i przyśpieszy proces dostępu do zarchiwizowanych danych. Jednak od kompleksowych systemów składowania zwykle wymaga się więcej.

Oprócz uporządkowania danych z punktu widzenia bezpieczeństwa informacji istotne jest także uwzględnienie różnych możliwych scenariuszy. Należą do nich przypadkowe (bądź celowe) skasowanie danych przez użytkownika/pracownika, ich utrata wskutek błędu oprogramowania lub w wyniku uszkodzenia sprzętu, w tym również fizycznego uszkodzenia nośników, zdarzenia losowe (pożar, powódź itp.), kradzieże sprzętu i/lub nośników danych itp.

Trzeba też pamiętać, że zarządzanie nośnikami to nie tylko kwestia archiwizacji i kopii zapasowych, ale jest ono powiązane również z zarządzaniem licencjonowanym oprogramowaniem wykorzystywanym w firmie, które przecież nadal w znacznej części dostarczane jest na odpowiednich nośnikach danych.

Wreszcie nie sposób pominąć tego, że strategia zarządzania danymi w większości firm jest – przynajmniej częściowo – narzucona przez ustawodawcę.

Polskie prawo wymusza przechowywanie wielu rodzajów danych (księgowych, osobowych) w odpowiedni sposób, a to oznacza konieczność dysponowania zarówno infrastrukturą przystosowaną do ich przechowywania (dotyczy to zarówno nośników własnych oraz wynajmowanych), jak i rozwiązaniami umożliwiającymi sprawne zarządzanie szybko rosnącym zbiorem informacji.

Fizyczna ochrona danych

Kontrola dostępu do danych znajdujących się w stałym obiegu musi obejmować również nośniki archiwizacyjne. O ile nikogo dziś nie dziwi konieczność uwierzytelniania użytkownika podczas próby dostępu do udostępnionego dokumentu na firmowym serwerze, o tyle kwestia fizycznej ochrony nośników przechowujących danych oraz informacji na nich zapisanych dla wielu podmiotów nie jest w pełni oczywista.

Na polskim rynku jest wiele rozwiązań, które zapewniają bezpieczne przechowywanie nośników zawierających wrażliwe dane, kopie zapasowe i inne wartościowe dane. Sejfy na nośniki zapewniają nie tylko fizyczną ochronę dostępu, ale także zabezpieczają dane przed różnymi czynnikami zewnętrznymi: wodą, ogniem, impulsem elektromagnetycznym, upadkiem itp.

Warto jednak przy tym pamiętać, że np. ognioodporność nie jest pojęciem równoznacznym z żaroodpornością. O ile ognioodporna szafa na nośniki danych może się sprawdzić w przypadku krótkotrwałej emisji ognia (szybko ugaszonego za pomocą automatycznych systemów ppoż. instalowanych w nowoczesnych biurowcach), o tyle niekoniecznie ochroni nośniki w razie długotrwałego narażenia na wysoką temperaturę. Niektóre z firm oferują urządzenia stanowiące połączenie klasycznego sejfu i serwera NAS bądź dysku zewnętrznego podłączanego do stacji roboczej przez popularne interfejsy wymiany danych (USB 2.0/3.0, eSATA itp.).

Transport nośników

Przechowywanie nośników z danymi wyłącznie w jednym miejscu nigdy nie jest optymalnym rozwiązaniem. Nie ma tu znaczenia skala działania firmy. Bez względu na to, czy chodzi o kilkuosobową działalność gospodarczą, czy międzynarodową korporację, polityka bezpieczeństwa powinna uwzględniać możliwość przechowywania dwóch kopii ważnych danych – zarówno w siedzibie firmy, jak i poza macierzystą lokalizacją.

Oprócz zapewnienia bezpieczeństwa nośników z wrażliwymi danymi/kopiami zapasowymi – zarówno w siedzibie firmy, jak i w zapasowej lokalizacji – równie ważne jest odpowiednie zabezpieczenie ich podczas transportu. Ułatwiają to specjalne walizki dostosowane do różnego typu nośników (np. taśm DLT, LTO Ultrium, DDS 4 mm, MTC, Titanium i wielu innych). Tego typu urządzenia produkują m.in. firmy ProDevice, Imation oraz Turtle Case. Oprócz odpowiedniego wyprofilowania przestrzeni ładunkowej dla różnych typów nośników walizki dodatkowo zapewniają zabezpieczenie przed wilgocią czy wręcz wodoodporność, a także amortyzację wstrząsów i wibracji.

> Zawsze należy szyfrować poufne dane na nośnikach.

Dla bardziej wymagających klientów przeznaczone są pojemniki o znacznie podwyższonej wytrzymałości na wstrząsy bądź zabezpieczające przed zmianami temperatury (hermetyzacja) oraz wyładowaniami elektrostatycznymi. Dodatkowym wyposażeniem pojemników transportowych może być moduł GPS gwarantujący śledzenie w czasie rzeczywistym lokalizacji nośników danych.

Szyfrowanie i pułapki implementacji

Nawet najbardziej bezpieczne scenariusze w zakresie przechowywania i transportu danych powinny zakładać możliwość utraty nośników (np. w wyniku kradzieży). Dlatego nieodzowne w skutecznym zabezpieczaniu wrażliwych danych przed niepowołanym dostępem jest szyfrowanie.

Funkcje kryptograficzne są obecnie implementowane niemal w każdym rozwiązaniu umożliwiającym przechowywanie danych, wykonywanie kopii zapasowych czy archiwizację. W przypadku biznesowych stacji roboczych szyfrowanie nośników może być jedną z funkcji danej maszyny, w czym pomagają stanowiące integralną część konstrukcyjną danego sprzętu układy TPM (Trusted Platform Module) z zaimplementowanymi funkcjami kryptograficznymi. Bardzo użyteczne są pamięci USB z wbudowanym układem TPM, który chroni dane przed niepowołanym dostępem.

Zwolennicy bardziej otwartych rozwiązań mogą zdecydować się na użycie oprogramowania do szyfrowania danych. Niestety, przykład popularnego i bezpłatnego oprogramowania TrueCrypt, przez wielu użytkowników mylnie uważanego za aplikację o otwartym kodzie źródłowym, pokazuje, że zaufanie do rozwiązań udostępnianych bezpłatnie może słono kosztować. De facto TrueCrypt – chociaż nawet polska Wikipedia kwalifikowała go jako oprogramowanie open source – nigdy nie był programem opublikowanym zgodnie z zasadami otwartej licencji. Projekt ten został porzucony praktycznie z dnia na dzień, a ostatnia wersja programu ma niewiele wspólnego z narzędziem zabez-

pieczającym dane i jest wręcz pozbawiona funkcji szyfrujących. Dlatego reseller powinien oferować klientowi komercyjne produkty, które zapewniają szyfrowanie danych. To umożliwia unikanie ryzyka, że w którymś momencie rozwiązanie się zdezaktualizuje, a firma zostanie zmuszona do zmiany metod szyfrowania, co oznacza dodatkowe koszty.

Niszczenie danych i nośników

Nośniki, podobnie jak urządzenia służące do ich odczytu i zapisu, zużywają się w trakcie eksploatacji. W efekcie bardzo istotną kwestią, która powinna być uwzględniona w każdej strategii zarządzania nimi jest bezpieczne usunięcie zużytych nośników i zniszczenie ich wraz ze wszystkimi danymi, które mogłyby się na nich znajdować.

Przekonanie potencjalnego klienta do tego, że nie powinien po prostu wyrzucać zużytych nośników, jest o tyle proste, że media na całym świecie bardzo często nagłaśniają przypadki „wycieków" wrażliwych danych, spowodowane prostymi błędami w zakresie bezpiecznego zarządzania nośnikami danych.

W sprzedaży jest wiele niszczarek dysków, taśm i innych nośników danych wykonanych z twardych materiałów. Urządzenia spełniające odpowiednie normy i certyfikaty (w Polsce Certyfikat Akredytacji Bezpieczeństwa Teleinformatycznego jest wydawany przez Służbę Kontrwywiadu Wojskowego) są bardzo drogie. Dlatego mniejszym firmom, które rzadko potrzebują całkowitej dezintegracji nośników z danymi, należy raczej zaproponować usługę niszczenia danych.

Ciekawe rozwiązanie oferuje firma BOSSG Data Security. Opracowana przez tę polską spółkę technologia LiquiData jest autorską, zgłoszoną do opatentowania, metodą chemicznego niszczenia nośników danych. W przeciwieństwie do powszechnie stosowanych na rynku niszczarek mechanicznych, mielących nośniki, technologia LiquiData oprócz rozdrobnienia (zgodnie z normą DIN 32 757, klasa tajności 4) dosłownie rozpuszcza nośniki. Cały proces niszczenia może być zrealizowany za pomocą tzw. Mobilnego Centrum Utylizacji Danych, bezpośrednio w siedzibie klienta bądź w miejscu przez niego wskazanym.

Tomasz Filipów
dyrektor, Diskus

W firmach posiadających dużą liczbę nośników mogą sprawdzić się rozwiązania automatyzujące poszczególne etapy zarządzania nimi. Klientowi można zaproponować np. usługę etykietowania zgodnie z przyjętą przez niego strategią numeracji. Etykietowanie może być przeprowadzone zarówno w siedzibie klienta, jak i u usługodawcy oraz połączone z nabywaniem nowych nośników. Jednak gdy nośniki mają być transportowane w celu wykonania takiej operacji, należy także zadbać o odpowiednie ich zabezpieczenie podczas tego procesu.

Oczywiście zniszczenie danych nie zawsze musi oznaczać również dezintegrację samego nośnika. W przypadku nośników magnetycznych (np. klasycznych dysków twardych) urządzeniami szybko likwidującym wszelki zapis na dysku, co uszkadza napęd i uniemożliwia dalsze korzystanie z niego, są różnego typu demagnetyzery (zwane też degausserami). Ich zaletą jest szybkość operacji – całkowite usunięcie danych z dowolnego dysku to kwestia kilkudziesięciu sekund. Urządzenia te są jednak drogie, np. Degausser ProDevice ASM120 Basic jest oferowany przez firmę Diskus w cenie ok. 15 tys. zł netto. Najtańszą metodą skutecznego usunięcia danych jest skorzystanie z odpowiedniego oprogramowania, dostępnego w wersjach płatnych (zgodnych ze standardami, drukujących odpowiednie raport z procesu niszczenia), jak też bezpłatnych. „Kosztem" jest tu jednak czas – proces ten może trwać nawet kilka godzin, a dla zwiększenia pewności usunięcia danych cykl nadpisywania trzeba kilkukrotnie powtórzyć. Dlatego sens korzystania z tej metody jest tylko wtedy, gdy do usunięcia danych przeznaczone są małe ilości nośników.

Odzyskiwanie danych dla firm

Nawet najbardziej dopracowana strategia zarządzania danymi musi uwzględniać wariant „katastrofy", czyli scenariusz, w którym część danych jest tracona, a ich odzyskanie może wymagać wsparcia wyspecjalizowanych firm. Takich, które dysponują profesjonalnym laboratorium, umożliwiającym operowanie na nośnikach w sterylnych warunkach.

W Polsce zdecydowanym liderem w zakresie tego typu usług jest katowicki Kroll Ontrack (firma ma własny kanał partnerski zrzeszający około 2 tys. firm), ale świadczą je też HDLab, Mediarecovery, Dabi, DataLab, DataMax Recovery, TRS System czy Akte. Wiele z tych firm zajmuje się również wspomnianymi wcześniej usługami outsourcingu informatycznego w zakresie bezpiecznego przechowywania i kasowania danych.

Dla resellera oferującego sprzęt i usługi związane z bezpieczeństwem informatycznym oferowanie usług przechowywania, transportu, archiwizacji danych, zarządzania nośnikami, niszczenia danych, niszczenia nośników czy wreszcie – odzyskiwania danych po awarii to dodatkowe, niemal gwarantowane i – co ważne – stałe źródło dochodu. Danych przetwarzanych w przedsiębiorstwach będzie coraz więcej, a to oznacza rosnące wymagania w zakresie zarządzania dużymi zbiorami informacji, również przez zarządzanie nośnikami zawierającymi kopie zapasowe i archiwa. Tymczasem wciąż w wielu firmach nie archiwizuje się danych i nie wykonuje kopii zapasowych, można więc zaproponować takie usługi kolejnym klientom. ■