Czasopismo: Kontroller Info, nr 3/2016

Bezpieczeństwo danych organizacji – polityka kopii zapasowych

Leszek Klich

Wstęp

Eksplozja danych cyfrowych w trwającej obecnie dobie informacyjnej i całodobowa działalność biznesowa powodują coraz większe obawy o bezpieczeństwo danych zgromadzonych w serwerach przedsiębiorstwa. Awarie sprzętu, ataki cyberprzestępców, oprogramowanie złośliwe, szpiegostwo przemysłowe, zakłócenia zasilania, różnorodne zdarzenia losowe o najróżniejszej skali, wywiad przemysłowy oraz błędy personelu powodują wzrost ryzyka dla bezpieczeństwa danych organizacji. Obecnie jednym z najważniejszych wyzwań stojących przed instytucjami jest ochrona własnych zasobów informacyjnych, które muszą być postrzegane jako kolejna kategoria zagrożeń, ponieważ niezależnie od wielkości organizacji, zapewnienie bezpieczeństwa informacyjnego jest jednym z najważniejszych wyzwań.

Jednym z kluczowych elementów bezpieczeństwa w organizacji jest Polityka Bezpieczeństwa, zawierająca zestaw reguł rządzących zachowaniem osób posiadających dostęp do przetwarzania informacji. Oprócz zapisów w Polityce Bezpieczeństwa informacji w zakresie przyznawania uprawnień, osoby odpowiedzialne za bezpieczeństwo teleinformatyczne organizacji, powinny zostać zobligowane do opracowania i modyfikacji scenariuszy na wypadek ryzyka utraty danych, w celu możliwie szybkiego odtworzenia systemów do jak najbardziej aktualnego stanu sprzed awarii. Konieczność zapewnienia bezpieczeństwa przechowywanych danych może wynikać zarówno z troski organizacji w kwestiach bezpieczeństwa, jak i z przepisów prawa.

Badania wykazały, że 60% organizacji posiada udokumentowany plan zachowania ciągłości działania na wypadek awarii systemów, około 14% planuje stworzenie takiego dokumentu, zaś aż 25% przyznaje, że po prostu go nie posiada[1]. Statystyki wypadają jeszcze gorzej w przypadku katastrof oraz klęsk żywiołowych, gdzie aż 19% badanych wykazało niskie przygotowanie na wypadek tego typu zdarzeń[2].

[1] *Bezpieczeństwo. Ryzyko. Dostępność*, HP Polska, Raport specjalny, 2015, s. 9.
[2] Tamże, s. 11.

Koszt nieprzestrzegania zasad bezpieczeństwa danych jest wysoki i nie ma wymiaru jedynie finansowego. Odtwarzanie danych z uszkodzonych nośników w specjalizowanych ośrodkach może okazać się niewspółmiernie wysoki do kosztów opracowania strategii oraz inwestycji w sprzęt do systematycznego składowania kopii zapasowych. Warto jednocześnie podkreślić, że w wielu przypadkach, odtworzenie oryginalnych struktur danych z uszkodzonych nośników może okazać się niemożliwe, a to w konsekwencji prowadzi do nieobliczalnych strat – w szczególnych przypadkach kończących działalność organizacji.

Polskie prawo szczególnie chroni dane osobowe oraz niejawne, których przetwarzanie regulowane jest odpowiednio – przepisami z ustawy o ochronie danych osobowych[3] oraz ustawą o ochronie informacji niejawnych[4].

Niezależnie od tego, czy organizacja przetwarza dane osobowe, podlegające specjalnej ochronie, warto zwrócić uwagę na przepisy ustawy o danych osobowych oraz rozporządzenie MSWiA z dnia 29 kwietnia 2004 r., które oprócz definicji, zawierają bardziej szczegółowe wymagania organizacyjne i techniczne, jakimi powinny odpowiadać urządzenia i systemy informatyczne w zakresie aspektów technicznych przechowywania danych[5].

Ustawa o ochronie danych osobowych oraz rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych regulują warunki organizacyjne, w tym polityki wykonywania i przechowywania kopii zapasowych oraz zarządzania nośnikami w rozdziale 5 „Zabezpieczenie danych osobowych", art. 36 pkt 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**".

Dokumenty prawne nie wyczerpują jednak w pełni warunków technicznych, stąd należy opracować wewnętrzne przepisy zmniejszające do akceptowalnego poziomu ryzyko związane z utratą danych, m.in. poprzez redundancję oraz dywersyfikację przy uwzględnieniu oceny własnych możliwości technicznych, ludzkich oraz finansowych.

[3] Ustawa z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz. U. 1997 Nr 133 poz. 883 tekst jednolity).
[4] Ustawa z dnia 5 sierpnia 2010 (Dz. U. 2010 nr 182 poz. 1228 tekst ujednolicony).
[5] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. *w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych* (Dz. U. z dnia 1 maja 2004 r.).

Nośniki danych przeznaczonych do zabezpieczenia danych

Za nośniki przechowujące dane na bieżąco[6], uznać można dyski twarde lub ich nowsze wersje – dyski SD, ponieważ przechowują one dane aktualnie przetwarzane w systemach informacyjnych organizacji. Wiąże się to z wymaganiami, które nakładane są na tego typu urządzenia, z których jednym z ważniejszych jest szybkość dostępu do danych oraz zapewnienie chwilowego bezpieczeństwa w przypadku awarii. Tego typu wymagania spełniają tzw. macierze RAID (*ang. Redundant Array of Independent Disks*), czyli urządzenia integrujące dwa lub więcej dysków, w zależności od rodzaju połączenia, zapewniając przestrzeń lub redundancję. Połączenie logiczne dysków realizowane jest przez dodatkowe urządzenie (kontroler RAID) lub programowo. Bardziej wymagające środowiska wykorzystują odrębne i autonomiczne urządzenia pełniące funkcję tzw. macierzy dysków. Wyróżnia się kilka poziomów macierzy RAID, które najczęściej mają za zadanie zapewnić odporność systemu na awarię jednego lub więcej dysków. W wielu organizacjach, gdzie liczy się niezawodność działania systemu zapewnioną przy minimalnej inwestycji, stosuje się tzw. lustrzane systemy RAID, składające się z dwóch dysków, z których jeden może ulec awarii i nie spowoduje to utraty danych, a nawet przestoju w pracy organizacji, zaś po wymianie uszkodzonego komponentu na nowy, dane zostaną na niego automatycznie zreplikowane ze sprawnego dysku. W większych systemach stosuje się bardziej zoptymalizowane i wydajne rodzaje RAID, składające się z wielu połączonych ze sobą dysków, co zapewnia jeszcze wyższy poziom bezpieczeństwa[7].

Nośniki informatyczne przechowujące dane na bieżąco, charakteryzują się relatywnie niską żywotnością (degradacja nośnika) przy relatywnie dużej awaryjności na wskutek błędów produkcji, uszkodzeń mechanicznych lub zakłóceń zasilania. Stosowanie macierzy RAID stanowi jedynie chwilowe zabezpieczenie systemu przed utratą danych spowodowaną awarią jednego z dysków, jednak nie chroni przed awarią kontrolera dysków lub serwera, umyślnym lub przypadkowym skasowaniem danych przez użytkownika, uszkodzeniem danych spowodowanym poprzez działanie oprogramowania złośliwego lub też utratą danych spowodowaną zdarzeniami losowymi, jak: powódź, pożar, katastrofa budowlana, itp.

Dobór typu nośnika zależy od kilku czynników, z których jako najważniejsze wymienić można czas dostępu do danych oraz trwałość zapisu. Trwałość zależy nie tylko od

[6] Zwane również danymi aktywnymi.
[7] Ze względu na ograniczenia niniejszej publikacji, poszczególne poziomy RAID będą tu opisywane.

warunków środowiskowych ich przechowywania (temperatury, wilgotności czy ekspozycji na światło), lecz także od technologii wykonania.

W przypadku kopii zapasowych tworzonych w celu szybkiego odzyskiwania systemu, ważniejszym parametrem przy wyborze nośnika jest czas dostępu do danych, zaś trwałość zapisu ma znaczenie drugorzędne. Jednak w przypadku archiwizacji długoterminowej, najistotniejszym parametrem jest trwałości nośnika. Optymalną metodą wykonywania kopii zapasowych jest więc stosowanie różnych rodzajów nośników (np. taśmy magnetyczne oraz urządzenia NAS).

Bardzo popularnym nośnikiem, szeroko wykorzystywanym do archiwizacji w sektorze MŚP[8] i w administracji publicznej pozostaje płyta CD/DVD, jednak należy zaznaczyć, że żywotność tego typu nośnika w praktyce nie przekracza 2-5 lat, zaś w przypadku droższych wersji – do 20 lat. O wiele lepiej na tle tańszych płyt optycznych wypada technologia Blue Ray, pozwalająca na przechowywanie danych na okres około 50 lat. Istnieją także nośniki optyczne typu M-disc, które, jak podaje producent, gwarantują bezpieczeństwo zapisanych danych przez ponad 1000 lat[9]. Niezależnie od technologii nośnika optycznego, wszystkie posiadają poważne ograniczenia pojemności przechowywanych danych, co powoduje problemy przy automatyzacji wykonywania kopii zapasowych lub archiwizacji.

Równie popularnym nośnikiem stosowanym szczególnie do celów tworzenia kopii zapasowych jest pamięć przenośna USB[10] oraz karta SD. Nośnik ten wyróżnia się prostą obsługą oraz odpornością na niektóre czynniki zewnętrzne, stąd urządzenia te zyskały dużą popularność wśród administratorów odpowiedzialnych za zabezpieczanie danych. Jednak oprócz zalet, nośniki te charakteryzuje stosunkowo duża awaryjność oraz wrażliwość na oprogramowanie złośliwe. Warto w tym miejscu wspomnieć o najnowszej technologii kart SD o nazwie WORM, które wykorzystują technologię jednokrotnego zapisu i potrafią przechowywać dane przez okres 100 lat, co w wielu przypadkach jest wystarczającym okresem na potrzeby archiwizacji, jednak nośniki tego typu charakteryzują się niewielką pojemnością, co w wielu przypadkach wyklucza je z wykorzystania.[11]

[8] Sektor małych i średnich przedsiębiorstw, do którego zalicza się podmiot prowadzący działalność gospodarczą. W szczególności są to osoby prowadzące działalność na własny rachunek, firmy rodzinne zajmujące się rzemiosłem lub inną działalnością bądź spółki lub konsorcja prowadzące regularną działalność gospodarczą.
[9] Zob. http://www.mdisc.com/mdisc-technology (dostęp z dnia 08-10-2015).
[10] Inne nazwy tego typu nośnika to: *pendrive, USB Flash Drive, Flash Disk, Memory Stick, USB-Stick, etc.*
[11] Zob. https://www.sandisk.com/about/media-center/press-releases/2010/2010-06-23-sandisk's-write-once-read-many-„worm"-sd-card-stores-images-for-up-to-100-years (dostęp z dnia 08-10-2015).

Badania wykazują, że wciąż najbardziej sprawdzonym i popularnym nośnikiem pozostaje taśma magnetyczna[12], charakteryzująca się dużą pojemnością, przy rozsądnym stosunku ceny do pojemności. Przeprowadzane testy potwierdziły także niezwykle dużą żywotność tego nośnika, ocenianą na okres około 30 lat przy przechowywaniu nośnika w optymalnych warunkach.

Niezależnie od użytego nośnika, dobrą praktyką podczas wykonywaniu kopii zapasowych oraz archiwizacji pozostaje stosowanie kombinacji kilku typów nośników oraz dodatkowo tworzenie ich duplikatów.

Technologia nośników stale ewoluuje, więc w przypadku planowania wieloletniej archiwizacji, oprócz kwestii fizycznego starzenia się nośników, dostrzec należy konsekwencje zmian w urządzeniach archiwizujących na przestrzeni lat, co może w przyszłości przyczynić się do zakłócenia odtwarzania zasobów. Problem ten jest nierozerwalnie związany z dokonującym się postępem w sferze technologii nośników informatycznych oraz sposobem zapisu danych, w konsekwencji wymagając migracji danych archiwalnych do urządzeń i nośników opracowanych w nowszej technologii.

W przypadku archiwizacji skomplikowanych struktur danych, jak np. bazy danych, rozwiązań autorskich lub innych zamkniętych formatów plików, szczególnego znaczenia zyskuje nie tylko możliwość odtworzenia w przyszłości struktury danych, lecz równie ważną kwestią jest zapewnienie możliwości zdekodowania informacji. Przy dynamicznie zmieniających się bibliotekach obsługi,[13] zmianach w silnikach bazodanowych czy innych – autorskich rozwiązaniach, samo odczytanie danych z archiwum nie gwarantuje ich poprawnej interpretacji, ponieważ musi być równocześnie zapewniona kompatybilność wsteczna środowiska. W takich przypadkach może przyjść z pomocą coraz bardziej popularna technologia wirtualizacji, ponieważ wirtualizacja archiwalnych systemów, w wielu przypadkach eliminuje konieczność przechowywania przestarzałego sprzętu, dla zapewnienia kompatybilnego środowiska dla danych archiwalnych. Podczas planowania procesu archiwizacji długoterminowej, niezmiernie ważnym aspektem jest więc migracja zarówno danych, jak i utworzenie dodatkowych archiwów zawierających środowisko systemowe wraz z instrukcją dotyczącą obsługi archiwalnych systemów.

[12] Standardem zapisu na pamięciach taśmowych jest LTO (Linear Tape Open).
[13] Biblioteka w ujęciu informatycznym jest zbiorem funkcji, z której korzysta oprogramowanie, pozwalającej w tym przypadku na dostęp do plików lub rekordów w bazie danych.

Kopia zapasowa a archiwizacja – zasadnicze różnice

Ze względu na często spotykane w literaturze przedmiotu mylne lub zamienne używanie terminów „kopia zapasowa" oraz „archiwizacja", celowym wydaje się opisanie obu terminów dla wykazania, że pojęcia te nie są jednoznaczne, co stanowi podstawę dla projektowania polityki bezpieczeństwa danych w organizacji.

Kopia zapasowa (*ang. backup*) służy ochronie bieżąco przetwarzanych danych, zaś w przypadku ich uszkodzenia lub utraty, umożliwia ich szybkie odtworzenie. Proces tworzenia kopii może polegać na replikacji pojedynczych obiektów (plików) lub złożonych struktur danych z lokalizacji źródłowej do wyodrębnionej lokalizacji docelowej. Zadaniem kopii zapasowej jest zapewnienie spójności danych źródłowych i zapasowych. Do kopii zapasowej zalicza się także technologię klonowania, która zapewnia pełne odzwierciedlenie struktury dysku na nośniku docelowym. Kopia zapasowa ma charakter krótkoterminowy, ale umożliwia szybkie odtworzenie systemu lub danych, minimalizując przestój w pracy organizacji. Dane kopii zapasowych składowane są najczęściej na macierzach dyskowych, serwerach NAS,[14] zewnętrznych dyskach USB lub na taśmach magnetycznych, co umożliwia ich szybkie odtworzenie (*ang. disaster recovery*).

Archiwizacja zaś jest procesem warstwowania[15] danych, polegającym na ich podziale, a następnie zapisaniu ich w odpowiednich obszarach systemu teleinformatycznego. Ma to na celu zapewnienie bezpieczeństwa nieużywanych danych, a jednocześnie zwolnienie zajmowanych zasobów pamięci masowej poprzez proces migracji. Archiwizowane dane nie wymagają szybkiego dostępu, jak w przypadku kopii zapasowych. Priorytetem jest zapewnienie bezpieczeństwa składowanych danych przez dłuższy okres, stąd archiwizacji najczęściej dokonuje się na nośnikach magnetooptycznych, magnetycznych lub wyselekcjonowanych nośnikach optycznych, ze względu na ich dużą pojemność oraz relatywnie niski koszt. Zarchiwizowane dane nadal podlegają zasadom sporządzania kopii zapasowych, lecz w tym przypadku kopie zapasowe materiałów archiwalnych można wykonywać z mniejszą częstotliwością niż w przypadku danych przetwarzanych na bieżąco, ponieważ ich zawartość nie podlega modyfikacji.

[14] NAS - (*ang. Network Access Server*) to urządzenie udostępniające strzeżony zasób sieciowy.
Klienci łączą się do serwera NAS. Ten z kolei łączy się do odpowiedniego serwera zasobów (NFS, HTTP, FTP, RADIUS itp.) pytając czy dany klient ma uprawnienia do skorzystania z tych zasobów. Na tej podstawie NAS zezwala lub odmawia klientowi dostępu do danych zasobów.

[15] Warstwowanie danych oznacza ich podział danych na aktywne, nieaktywne i referencyjne oraz zapisanie ich w odpowiednich obszarach. W zależności od zapisu, dane aktywne charakteryzują się szybkim czasem dostępu, zaś dane historyczne – długim, co w praktyce zależy od sposobu ich zapisania na różnego rodzaju nośnikach.

Polityka tworzenia kopii zapasowych i archiwizacji danych

Najskuteczniejszą metodą zabezpieczenia się przed skutkami awarii – a w konsekwencji utraty danych jest wprowadzenie polityki wykonywania kopii zapasowych oraz archiwizacji jako elementu planowania kryzysowego i wdrożenie jej zapisów w życie. Sformalizowanie procesów zabezpieczania danych daje wiele korzyści w porównaniu do często chaotycznego i nieprzemyślanego wykonywania tych czynności przez informatyka. Wprowadzenie polityki wprowadza ład, rozliczalność i zastępowalność, pozwalając także na kontrolowanie procesu przez personel innego szczebla.

Programowanie bezpieczeństwa danych w organizacji jest procesem, który nigdy się nie kończy, lecz podlega stałemu doskonaleniu. Planowanie musi więc przebiegać wieloetapowo i opierać się na komunikacji pomiędzy decydentem – osobą odpowiedzialną za bezpieczeństwo informacji w organizacji oraz administratorem systemu, ponieważ każda z tych osób dysponuje inną kategorią uprawnień, zaś cel (zwiększenie poziomu bezpieczeństwa) pozostaje wspólny.

Bezpieczeństwo wymaga nakładów finansowych ze strony organizacji nie tylko na zakup profesjonalnych urządzeń, nośników czy specjalistycznego oprogramowania do automatyzacji procesów zabezpieczania danych. Oprócz tego, niezwykle istotnym elementem bezpieczeństwa musi być edukacja kadr w zakresie bezpieczeństwa, co może generować kolejne koszty. Część planowanego budżetu na zwiększenie bezpieczeństwa danych musi być zarezerwowana na zapewnienie szkoleń podnoszących kwalifikacje kadry informatycznej oraz kierowników komórek zajmujących się aspektami bezpieczeństwa w organizacji.

Rozważania, które należy przeprowadzić przed utworzeniem polityki ochrony danych z zakresu kopii bezpieczeństwa i archiwizacji dotyczą zarówno aspektów prawnych, jak i organizacyjnych, wynikających ze specyfiki organizacji, jednak w większości przypadków można odnaleźć punkty wspólne. Podstawowe założenia w niewielkim środowisku mogą być zupełnie inne niż w przypadku dużego ośrodka i dotyczy to zarówno wymagań jak i nakładów czasowych oraz finansowych. W praktyce wymagania dla obu ośrodków okazują się być identyczne, więc pewne zasady i procedury są bardzo podobne[16].

[16] Zob. http://www.zpcir.ict.pwr.wroc.pl/~witold/unixintro/bkupintro_d.pdf (stan na 16-02-2016).

Pierwszym z etapów planowania jest identyfikacja obszarów, polegająca na wyodrębnieniu zakresu danych istotnych z punktu widzenia organizacji, które podlegają procesom wykonywania kopii zapasowej. Głównym obszarem są bazy danych systemów informacyjnych i w tym wypadku listę baz należy utworzyć po inwentaryzacji oprogramowania działającego w organizacji. Na tym etapie można uwzględnić fakt wynikający z polityki bezpieczeństwa organizacji, który do każdego zbioru danych przypisuje określonych użytkowników. Dzięki temu, na podstawie wytycznych, osoby te mogą dokonać klasyfikacji przetwarzanych danych. Podczas konsultacji warto przy okazji ocenić dodatkowe potrzeby dotyczące zabezpieczania wskazanej grupy danych.

Podczas planowania wykonywania kopii zapasowych, warto stosować podział na system oraz dane, ponieważ kopia systemu[17] zabezpiecza środowisko przetwarzania danych, które nie podlega tak dynamicznym zmianom jak przetwarzane na bieżąco dane.

Wyodrębnianie danych wymagających długiego okresu archiwizacji może wynikać zarówno z przepisów prawa, jak i z polityki organizacji. W obszarze podmiotów państwowych[18], realizujących zadania publiczne oraz prowadzące dokumentację elektroniczną, świadczącą o wykonywaniu własnej działalności, w przypadku, gdy dane te odzwierciedlają przebieg załatwienia i rozstrzygania spraw, podlegają ewidencjonowaniu w systemie teleinformatycznym. Jeśli ewidencjonowane dokumenty zostały zakwalifikowane jako materiały archiwalne (posiadają wartość historyczną)[19], wymagane jest opracowanie procedur ich przechowywania przez okres nie krótszy niż 10 lat, z uwzględnieniem warunków technicznych oraz organizacyjnych dla ich bezpiecznego przechowywania w archiwum zakładowym[20].

Podstawowym założeniem podczas wyboru metod wykonywania kopii zapasowych oraz archiwizacji jest świadomość, że żadna technologia nie daje pełnej gwarancji bezpieczeństwa. W praktyce stosuje się więc dywersyfikację źródeł danych, czyli systematyczne wykonywanie kolejnych kopii – przy zastosowaniu różnych technologii.

[17] W tym przypadku systemu operacyjnego.
[18] Tj. organy państwowe i państwowe jednostki organizacyjne, organy jednostek samorządu terytorialnego i samorządowe jednostki organizacyjne. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. *w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi* (Dz. U. Nr 206, poz. 1518).
[19] Zob. Art. 1 Ustawy z dnia 14 lipca 1983r *o narodowym zasobie archiwalnym i archiwach* (Dz. U. 1983 Nr 38 poz. 173 tekst jednolity).
[20] Rozporządzenie MSWiA reguluje wymagania m.in. dla systemów teleinformatycznych, gdzie w §6 ujęto wymagania archiwum zakładowego lub składnicy akt.

Warto więc rozważyć zakup zarówno urządzeń taśmowych, jak i zewnętrznych dysków twardych lub lepiej – urządzeń sieciowych typu NAS.

Częstotliwości tworzenia kopii zapasowych (harmonogram) należy dobrać w zależności od kilku czynników związanych między innymi z istotnością dostępu do przetwarzanych danych, co wynika z charakteru działalności organizacji oraz możliwości finansowych. W przypadku kopii zapasowej systemu oraz danych, najlepszą metodą zabezpieczenia jest utworzenie tzw. obrazu – w tym na nośniku szybkiego dostępu, co umożliwi jego natychmiastowe użycie w przypadku konieczności odtworzenia środowiska produkcyjnego. W większych organizacjach kopie zapasowe systemu oraz danych tworzone są co godzinę lub częściej i wykonywane na nośnikach szybkiego dostępu, co umożliwia szybkie przywrócenie sprawności systemu, nawet po całkowitej awarii. Mniejsze jednostki, których działalność nie polega wyłącznie na przetwarzaniu danych w systemach informacyjnych, mogą wykonywać kopię zapasową rzadziej. Harmonogram powinien uwzględniać jednocześnie czas wykonywania kopii zapasowych. Jest to szczególnie ważne w silnie obciążonych środowiskach, gdzie planowanie wykonywania kopii danych należy zaplanować poza godzinami pracy. Jednocześnie czas zakończenia tworzenia kopii musi kończyć się wcześniej od rozpoczęcia pracy przez użytkowników, co umożliwi reakcję na ewentualne problemy wynikłe z procesu kopiowania danych. Częstotliwość archiwizacji długoterminowej wynikać może bezpośrednio z wymagań organizacji lub z przepisów prawa. Fundamentem są w tym przypadku wytyczne dla osób odpowiedzialnych za tworzenie procedur ze strony osób decyzyjnych, w których uwzględniono klasyfikację danych wrażliwych, wymagających częstszej archiwizacji lub też konieczności zwolnienia zasobów pamięci z nieużywanych danych.

Niedoskonałość technologii generuje nie tylko ryzyko utraty aktywnych danych, lecz może przyczynić się do powstawania potencjalnych błędów pojawiających się podczas kopiowania na nośniki zapasowe lub też niespodziewane awarie samych nośników. Stąd ważnym elementem polityki musi być zapis o cyklicznym testowaniu posiadanych kopii zapasowych oraz kontrolnych odczytach zgromadzonych archiwów – w tym testy pełnego odzyskiwania systemu oraz danych. Warto podkreślić, że samo posiadanie nośników zawierających dane zapasowe może okazać się nieprzydatne, jeśli nie są opracowane metody ich użycia. Wewnętrzne przepisy muszą więc zawierać opracowane scenariusze odtwarzania środowiska z kopii zapasowych – w tym scenariusze uwzględniające awarię części nośników, w których wymagane jest użycie kopii off-site. Zapis powinien regulować jednocześnie

harmonogram testowego odtwarzania danych z wykorzystaniem opracowanej instrukcji opisującej krok po kroku ten proces. Oprócz względów kontrolnych (cykliczne raporty z testowego odzyskiwania przekazywanych do osób odpowiedzialnych), tego typu działania znacząco usprawniają proces odtwarzania środowiska w warunkach stresu, wynikłego z potencjalnych awarii w przyszłości.

Nośniki wykorzystywane do przechowywania kopii zapasowych wymagają cyklicznej i zaplanowanej wymiany dla zachowania najwyższego poziomu bezpieczeństwa przechowywanych na nich danych. Polityka powinna więc szczegółowo określać postępowanie z nośnikami wycofanymi z eksploatacji, ponieważ przepisy dotyczące sposobów postępowania z zapisanymi nośnikami wskazują odpowiedzialność karną bądź cywilną z tytułu niedopełnienia odpowiednich obowiązków ochrony informacji[21]. Z przepisów wynika, by dane znajdujące się na nośnikach przeznaczonych do likwidacji zostały usunięte za pomocą metod uniemożliwiających ich odtworzenie. Przepisy nie wskazują jednak metod bezpiecznego usuwania danych, co znacznie komplikuje podjęcie decyzji o wyborze skutecznych sposobu.

Do metod niszczenia danych zaliczyć można metody logiczne (programowe), polegające na wielokrotnym nadpisywaniu danych przypadkowymi wartościami[22] lub metody fizyczne, oparte na fizycznym niszczeniu nośnika. Niestety żadna z metod nie gwarantuje pełnego bezpieczeństwa, choć ich odzyskanie w tym przypadku może się wiązać ze znacznymi nakładami środków. Skuteczną metodą niszczenia nośników jest 4-etapowa metoda nadpisywania, demagnetyzacji, wiórkowania oraz rozpuszczenia pozostałości za pomocą metody chemicznej, która wykonywana jest przez specjalistyczne firmy.

Jednym z zasadniczych punktów planowania zabezpieczania danych w organizacji jest uwzględnienie ryzyka związanego z uszkodzeniami nośników poprzez siły wyższe, tj. pożar, woda, katastrofa budowlana, itp. Ryzyko to wymusza planowanie rozmieszczenia kopii nośników zawierających identyczne dane w co najmniej kilku pomieszczeniach[23], a najlepiej także w innym budynku. Kopie tego typu mogą być wykonywane np. z wykorzystaniem

[21] Zob. więcej https://www.niszczenie.pl/przepisy-prawne (stan na 16-02-2016).
[22] Specjalistyczne oprogramowanie nadpisuje wielokrotnie (nawet 35-krotnie) sektory nośnika poprzez losowo wygenerowane ciągi liczbowe za pomocą algorytmów, które mają gwarantować bezpieczne usuwanie danych np. metodą US DOD 5220.22-M.
[23] Tzw. kopia off-site.

transmisji sieciowej lub przenoszeniem nośników do ich miejsca przeznaczenia. Warto w tym miejscu zwrócić uwagę na nowe metody archiwizacji „chmurowej”[24], w której zaszyfrowane dane przesyłane są do data-center zlokalizowanego w odrębnym mieście lub nawet kraju – z uwzględnieniem aktualnych przepisów prawnych. Proces przenoszenia danych do usługi chmury, powinien być poprzedzony analizą skutków tego typu operacji, zarówno od strony prawnej, jak i ekonomicznej oraz sformalizowany za pomocą obustronnej umowy między dostawcą a klientem, w której regulowane są kwestie praw autorskich czy własności oraz bezpieczeństwa informacji[25]. Niestety, prawo nie nadąża za szybko rozwijającą się technologią i należy w tej kwestii zachować szczególną ostrożność[26].

Kolejną kwestią, nierozerwalnie związaną z wykonywaniem kopii zapasowych jest wybór dedykowanego oprogramowania. Punkt ten należy dokładnie skonsultować z działem IT organizacji, ponieważ komórka ta jest w wielu przypadkach elementem wykonawczym, odpowiedzialnym za zapewnienie prawidłowego funkcjonowania tego systemu. Raporty wskazują, że aż 85% organizacji boryka się z poważnymi problemami związanymi z wysokimi kosztami kopii zapasowych oraz odtwarzania, wskazując na braki funkcjonalne, zaś w przypadku 83% jako problem wskazano zbyt wysoki poziom skomplikowania systemów automatyzacji kopii zapasowych[27]. Warto też przytoczyć negatywne statystyki dotyczące odtwarzania danych, z których wynika, że aż 1 na 6 operacji odtwarzania danych kończy się niepowodzeniem[28]. Podsumowując – wybór oprogramowania do wykonywania kopii zapasowych stanowi jeden z kluczowych czynników bezpieczeństwa i nie warto w tej kwestii oszczędzać.

Uwzględniając powyższe rozważania, polityka bezpieczeństwa danych w zakresie kopii oraz archiwizacji danych musi zawierać:

- szczegółowy zakres czynności operatorów wykonujących kopie zapasowe przy zachowaniu rozliczalności;

[24] W tym miejscu należy wskazać, że istnieją „chmury” publiczne (zarządzane przez zewnętrznego dostawcę), prywatne (zarządzana przez autonomicznego dostawcę) oraz hybrydowe (w której część infrastruktury klienta pracuje w chmurze prywatnej, zaś część jest umieszczona w chmurze publicznej).
[25] Zob. http://di.com.pl/prawo-pozwala-bezpiecznie-korzystac-z-chmury-obliczeniowej-53880 (stan na 16-02-2016).
[26] Obecnie brak jest odrębnych przepisów regulujących przechowywanie, archiwizowanie, przetwarzanie oraz zarządzanie danymi w „chmurze”. Przepisy, które ustalają ramy prawne w tym zakresie to Dyrektywa o ochronie danych 95/46/WE oraz Ustawa z dnia 29 sierpnia 1997 o ochronie danych osobowych (tj. Dz. U. z 2002 r. Nr 101, poz. 926 ze zm.).
[27] Zob. http://websecurity.pl/tag/kopie-zapasowe/ (stan na 17-02-2016).
[28] Tamże.

- wykaz danych podlegających zabezpieczeniu na nośnikach zewnętrznych;
- wykaz nośników danych wraz z ich opisem oraz numerami seryjnymi, datą pierwszego użycia oraz datą wymiany;
- wykaz oprogramowania stosowanego do wykonywania kopii zapasowych;
- wykaz lokalizacji przechowywania nośników – w tym off-site;
- szczegółowy zakres i sposób wykonywania kopii zapasowych, rodzaj (pełny, przyrostowy, różnicowy), okresy rotacji oraz szczegółowy harmonogram wykonywania kopii;
- instrukcje wykonywania kopii;
- kompleksowe scenariusze odtwarzania danych – w tym również uwzględniające awarię jednego z nośników;
- wykaz personelu posiadającego dostęp do przechowywanych danych;
- wzory raportów: testowego odtwarzania, archiwizacji (opcjonalnie w wersji elektronicznej), likwidacji uszkodzonych lub zużytych nośników.

Zakończenie

Statystyki wykazują braki w podejmowaniu pojawiających się wyzwań z zakresu zabezpieczania danych oraz sukcesywnego projektowania oraz implementacji rozwiązań technicznych, adekwatnych do istniejących zagrożeń, które w konsekwencji mogą prowadzić do sankcji prawnych oraz ekonomicznych. Zabezpieczanie danych poprzez tworzenie kopii zapasowych jest procesem ciągłym i czasochłonnym, stąd kierownictwo organizacji nie powinno traktować tych czynności jako kolejnych zadań przypisanych do pracowników działów IT zaabsorbowanych innymi zadaniami wynikającymi z obowiązków administratorów aplikacji czy serwerów. Zamiast tego, o ile jest to możliwe, należy tworzyć dedykowane stanowisko służbowe operatora kopii zapasowych, jednak w przypadku niewielkich organizacji może być to nieakceptowane ze względów ekonomicznych. Tymczasem jak wynika z badań, jedynie w 11% przypadków bezpieczeństwem w organizacji zajmuje się wydzielona komórka organizacyjna, zaś pomimo ogólnych deklaracji o priorytetowym traktowaniu bezpieczeństwa, aż w 45% badanych organizacji, bezpieczeństwo jest kompetencją działu IT[29]. Jak wykazują wyniki badań, w przypadkach, gdzie bezpieczeństwem zajmuje się niezależna komórka lub zewnętrzna firma, standardy

[29] *Bezpieczeństwo. Ryzyko. Dostępność*, HP Polska, Raport specjalny, 2015, s. 7.

jakości bezpieczeństwa są wyższe, gdyż 73% tych organizacji posiada plany działania na nieprzewidziane okoliczności[30]. Należy więc mieć świadomość, że nadmierne oszczędności w tej kategorii ryzyka mogą okazać się złudne, a nawet katastrofalne w skutkach.

Abstract

One of the key elements of security in an organization is a Security Policy, containing a set of rules governing the behaviour of people having access to the processing of information. In addition to the Information Security Policy provisions regarding granting permission, people responsible for the information security of the organization should be required to develop and modify scenarios against the risk of data loss in order to restore the system to the most current state from before the crash as quickly as possible. The need to ensure the security of the stored data may stem both from the organization's care regarding security issues and from the provisions of the law.

[30] Tamże, s. 9.