Piotr Karaś
ptrkaras@univ.rzeszow.pl
Katedra Pedagogiki Medialnej i Komunikacji Społecznej
Uniwersytet Rzeszowski
Rzeszów

Pomiędzy mediami cyfrowymi a technologią. Bezpieczeństwo danych – aspekt edukacyjny

Rozwój technologii informacyjnych, nowych mediów (cyfrowych) [Wrońska, 2012, s. 26] spowodował, iż coraz więcej informacji zostaje utworzonych i zapisanych za pomocą urządzeń elektronicznych, materiały analogowe zostają zdigitalizowane i przechowywane w wersji elektronicznej. Instytucje oświatowe wykorzystują systemy informatyczne do zarządzania swoimi jednostkami, komunikacji oraz wprowadzają je do edukacji. Począwszy od przygotowania dokumentów w edytorze tekstów do programów i systemów wspomagających obieg dokumentacji elektronicznej, a także wykorzystania usług bankowości elektronicznej, zastosowanie mają urządzenia wchodzące w skład infrastruktury informatycznej placówki oświatowej. Przedszkola, szkoły podstawowe, gimnazjalne, średnie, a także uczelnie wyższe tworzą i zarządzają swoimi stronami internetowymi. Uczniowie i studenci korzystają z portali edukacyjnych, zasobów Internetu, wyszukując informacje z różnych dziedzin i obszarów nauki. Internet służy również jako medium do komunikacji i wymiany zasobów. Powstają coraz bardziej złożone struktury informatyczne wymagające specjalistycznych kwalifikacji zawodowych, często wykraczające poza kwalifikacje nauczyciela informatyki i technologii informacyjnych w szkole. Zastosowanie znajduje coraz więcej nowych typów urządzeń informatycznych, np. routerów, switchy zarządzalnych, serwerów NAS (Network Attached Storage*)*, AP (Access Point), kontrolerów, rozwiązań programistycznych np. wirtualizacji serwerów. Użytkownicy, aby korzystać z zasobów i infrastruktury medialnej i multimedialnej szkoły, uczelni stosują urządzenia mobilne (tablety, ultrabooki, netbooki, smartfony), łącząc się z nimi poprzez zabezpieczone sieci bezprzewodowe po uprzedniej autoryzacji (uwierzytelnieniu) użytkownika, np. usługą Radius (*Remote Authentication Dial In User Service*).

Zwiększa się ilość i rodzaj gromadzonych informacji, a także miejsce ich przechowywania. Uczniowie i nauczyciele posiadają wiele kont dostępu do różnych serwisów i usług. Są to konta dostępu do zasobów szkolnych, kont e-mail, dostępu do portali edukacyjnych, serwisów społecznościowych, gier dydaktycznych itp.

(Nie)zawodne technologie

Każdy użytkownik nowoczesnych technologii doświadczył lub z pewnością doświadczy utraty danych lub utraty dostępu do nich. Są to chwile wywołujące stres, połączone z bezradnością wobec „wszechmocnej" technologii, gdzie media cyfrowe stają się niedostępne. Wówczas zdajemy sobie sprawę, jak ważna staje się aktualna kopia danych. Utrata dostępu do Internetu, w tym dostępu do portali społecznościowych, poczty elektronicznej wydaje się być dla niektórych wręcz katastrofą. Innym problemem jest utrata

dostępu do usług wymagających autoryzacji, np. poczty elektronicznej, zasobów dyskowych itp. Odzyskanie dostępu wymaga wypełnienia kolejnych formularzy elektronicznych i nie zawsze kończy się powodzeniem. W dobie telefonii komórkowej i mobilnego Internetu dłuższa awaria (spowodowana uszkodzeniem urządzeń, a w przypadku urządzeń mobilnych rozładowaniem akumulatora) lub brak dostępu do sieci może przynieść ogromne straty. Wielość różnego rodzaju kont, haseł dostępu ustawień i konfiguracji urządzeń, usług powoduje, że w przypadku braku właściwej dokumentacji odtworzenie pełnej funkcjonalności będzie znacznie utrudnione i wydłużone w czasie.

Anonimowość w sieci i cloud computing

Programy i systemy działające w chmurze pozwalają na zapisywanie synchroniczne w co najmniej dwóch lokalizacjach naszych zasobów elektronicznych. Zwiększa to bezpieczeństwo naszych danych. Wzrastająca popularność i ilość aplikacji działających w *cloud computing* powoduje, że z każdym dniem wzrasta liczba użytkowników, m.in.: Dropboxa, Prezi, usług Google, Apple iCloud i innych. Praca w chmurze uniezależnia od konieczności zapisywania danych na lokalnym urządzeniu elektronicznym. Chmura jest źródłem spersonalizowanego dostępu do informacji oraz coraz częściej zawiera odpowiednie narzędzia informatyczne, np. arkusz kalkulacyjny, edytor tekstu, programy do prezentacji multimedialnych, kalendarz, plan zajęć. Nie zawsze zastanawiamy się, czy nasze dane są bezpieczne, czy chmura to dobre miejsce dla przechowywania poufnych danych i czy nikt nie ma do nich dostępu. Przeglądanie stron internetowych może być źródłem takich informacji na temat danego użytkownika, jak:

- adresy oglądanych stron;
- loginy użytkownika zapisane w polu logowania;
- adres IP;
- pliki cookies, dane sprzętu i systemu operacyjnego.

Wykonując zdjęcie aparatem cyfrowym i publikując go w Internecie udostępniamy:

- identyfikator fotografa;
- data i czas utworzenia zdjęcia;
- lokalizacje miejsca wykonania zdjęcia;
- model aparatu fotograficznego;
- ustawienia aparatu (czas migawki, przysłona, ogniskowa obiektywu);
- parametry zdjęcia (wymiary, rozdzielczość, orientacja zdjęcia).

Podczas rozmowy telefonicznej (telefonem komórkowym) udostępniamy:

- numery tel. rozmówców;
- numery IMEI telefonów;
- czasy połączeń;
- lokalizacje rozmówców;
- numery kart SIM.

Jeszcze więcej informacji przekazujemy przy przesyłaniu wiadomości pocztą elektroniczną począwszy od adresów e-mail odbiorcy i nadawcy do adresów serwerów pośredniczących i adresów IP. Powstaje pytanie o zasadność udostępniania i przechowywania informacji w sieci i możliwość zapewnienia sobie anonimowości.

Zgłębiając tajniki technologii pod kątem zwiększenia bezpieczeństwa danych okazuje się, że jest możliwość korzystania z alternatywnych systemów i aplikacji. Zamiast systemu operacyjnego Microsoft Windows można zamienić go na jedną z wersji GNU/Linuxa, np. Debiana, zamiast przeglądarki Microsoft Internet Explorer czy Google Chrom zastosować GNUzilla Ice Cat, Mozilla Firefox, do przeglądarek zainstalować plugin do szyfrowania stron HTTPS Everywere czy Fix Tracking. Do wyszukiwania stron używać zamiast google.pl – duckduckgo.com. Przykładem programu monitorującego dane internautów jest system PRISM.

Hardware i software w placówkach edukacyjnych

Firmy informatyczne przedstawiają szeroką ofertę oprogramowania i sprzętu dla szkół, placówek oświatowych i uczelni wyższych. Zadaniem oprogramowania jest pomoc w zarządzaniu szkołą, wspomaganiu układania harmonogramów zajęć, prowadzeniu kursów e-learningowych, które w ostatnim czasie zdobywają coraz większą popularność ze względu na dużą efektywność nauczania.

Bardzo istotnym elementem jest możliwość działania oprogramowania w środowisku sieciowym, nie tylko lokalnym, ale również w sieci Internet. Nieodzownym elementem infrastruktury informatycznej szkoły/uczelni są komponenty sieciowe:

- firewalle;
- switche zarządzalne z możliwością definiowania VLANÓW, separacją urządzeń wg adresu MAC (Medium Access Control);
- urządzenia dla sieci bezprzewodowej (punkty dostępowe AP);
- kontrolery;
- serwery wirtualne;
- serwery NAS;
- serwery mediów strumieniowych (radio, telewizja internetowa);
- serwery e-learningowe;
- modemy.

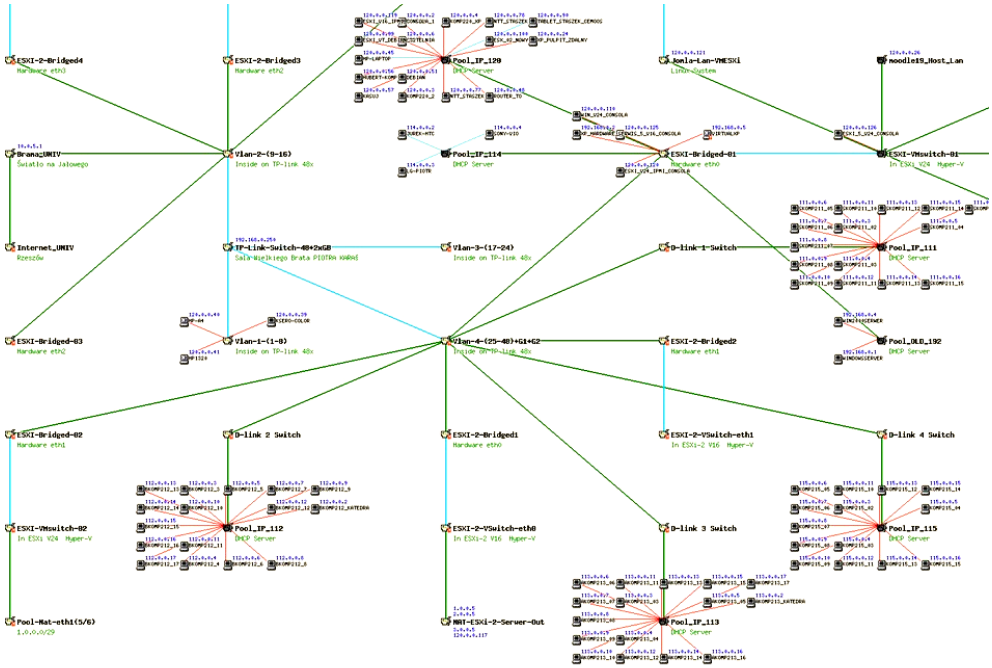
Niezbędne jest wydzielenie specjalnych pomieszczeń dla usytuowania serwerów i urządzeń dostępowych, posiadających klimatyzację i wentylację. Uczelnie, firmy, przedsiębiorstwa zatrudniają na etacie profesjonalnych informatyków, którzy utrzymują ciągłość pracy systemów informatycznych. W szkołach jest to zadanie najczęściej powierzane nauczycielom ICT, których obowiązkiem dodatkowym jest kontrola i usuwanie awarii sprzętu i oprogramowania. Wykonują również typowe zadania związane z instalacją i testowaniem nowych systemów informatycznych. Działania te prowadzą do cyklicznego zwiększania zasobów intelektualnych i materiałów wytwarzanych i zapisywanych na różnego rodzaju nośnikach w postaci elektronicznej. Znaczna część danych ma charakter niejawny, jak np. elektroniczny dziennik ucznia, dane księgowości, dane pracowników szkoły czy osobiste materiały nauczycieli.

System LMS (LAN Managment System)

Rozbudowując informatyczną infrastrukturę w placówce oświatowej można skorzystać z rozwiązania LMS rozprowadzanego na zasadzie Powszechnej Licencji

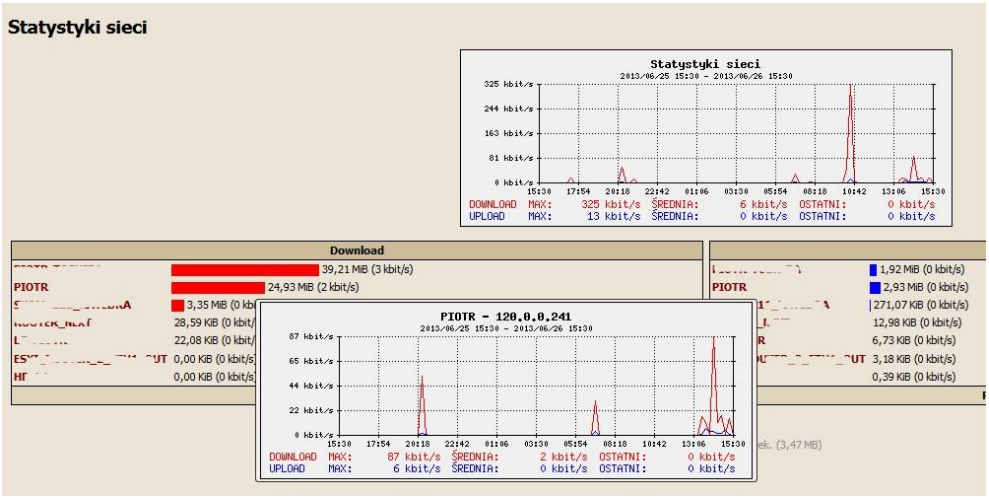
Publicznej GNU (*General Public License*). System napisany jest w PHP, wymaga serwera WWW z interpreterem tego języka, gdzie preferowany jest Apache oraz bazy danych MySQL. Jako podstawę może stanowić system operacyjny Linux/Debian. Wszystkie komponenty posiadają licencje GNU, co jest dobrym atrybutem dla jednostek oświatowych.

LMS jest zintegrowanym systemem zarządzania sieciami. Zadaniem systemu jest między innymi kontrola zasobów jednostki. Udostępnianie zasobów nie powinno odbywać się bez autoryzacji. Problem może stanowić zwiększająca się liczba urządzeń mobilnych i włączenie ich w struktury sieci LAN szkoły, przydzielenie wymaganych uprawnień dostępu.



Rys. 1. Fragment struktury logicznej i fizycznej sieci LAN w systemie LMS

Powyższy schemat ukazuje złożoność i zależność fragmentu struktur informatycznych na przykładzie Instytutu Pedagogiki Uniwersytetu Rzeszowskiego. W przypadku dużej ilości komponentów informatycznych istnieje konieczność zastosowania narzędzi ułatwiających i usprawniających zarządzanie siecią LAN. System LMS pozwala na wygenerowanie raportów aktywności poszczególnych użytkowników i urządzeń potrzebnych w analizie wykorzystania dostępu do zasobów szkoły, nie tylko administratorowi sieci, lecz także kadrze kierowniczej. W uzasadnionych przypadkach w prosty sposób można odłączyć wybrane urządzenia z dostępu do zasobów sieci LAN, uniemożliwić korzystania z sieci Internet w szkole [Karaś, 2013, s. 288].



Rys. 2. Statystyka pracy użytkownika

Od penvdrive'a do macierzy dyskowych

Czy robimy kopię zasobów elektronicznych? Pytanie to nie powinno dotyczyć indywidualnych użytkowników, lecz osób odpowiedzialnych za działanie systemów informatycznych instytucji oświatowych.

Większość użytkowników mediów ma świadomość zagrożeń, stosuje programy antywirusowe, antyspywarowe, zabezpiecza się przed trojanem. Aktualizujemy system operacyjny instalując patche i service packi, wykonujemy kopię pojedynczych plików na płytę CD lub DVD, pendrive'a bądź na dysk zewnętrzny.

Co się stanie w przypadku poważnej awarii całych systemów? Jak się przygotować na utratę dostępu do danych? Scenariuszy jest wiele, od utraty pojedynczych plików do awarii całych systemów w wyniku burzy (przepięć w instalacji elektrycznej), po przypadki zalania bądź spalenia urządzeń.

Backup czy (i) archiwizacja?

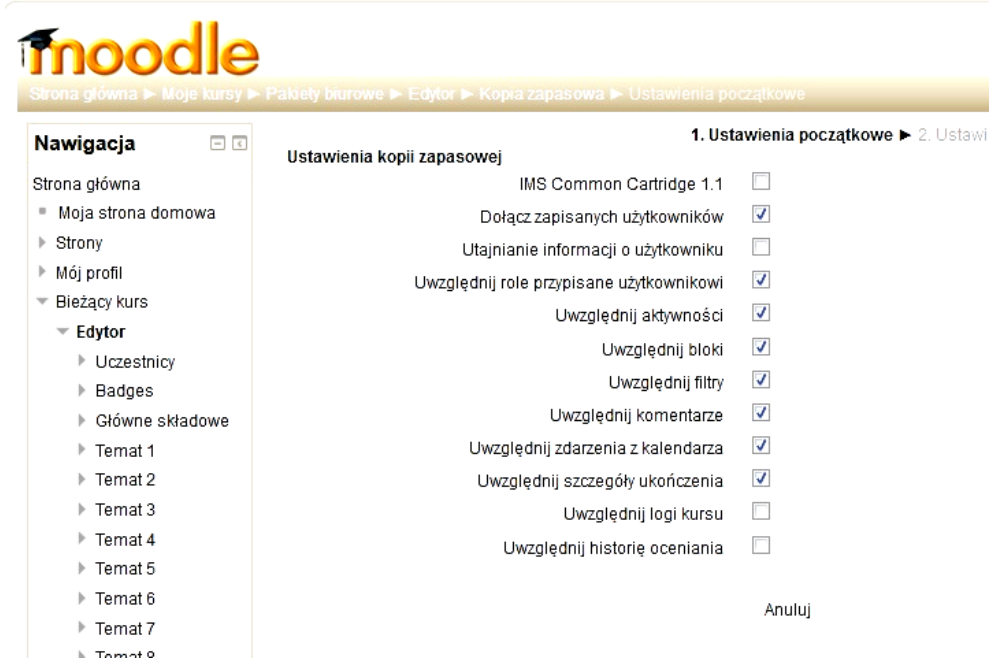
Pojęcie archiwizacji związane jest z wykonaniem kopii plików, natomiast backup uwzględnia wykonanie kopii całego systemu komputerowego łącznie z systemem operacyjnym. Newralgicznym punktem będzie serwer (np. VMware) zawierający kilka lub kilkanaście wirtualizacji. Awaria urządzenia prowadzi do sytuacji, gdzie dostęp do wszystkich zasobów jednostki organizacyjnej lub całej instytucji będzie niemożliwy.

Bardzo ważnym zadaniem jest również skuteczność odzyskiwania i łatwość wyszukiwania danych. Problemem może okazać się odtworzenie aktualnej kopii. Sytuacja komplikuje się, gdy chcemy wykonać kopię „środowiska medialnego", w którym odbywa się np. edukacja elektroniczna.

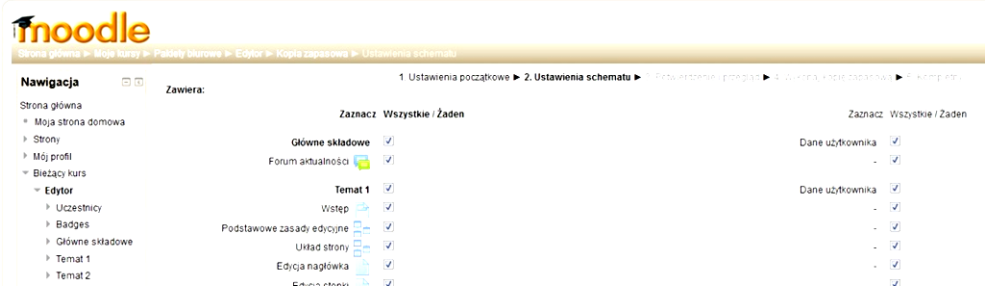
Bardzo popularne są portale oparte o platformę Moodle. Wykonanie kopii w postaci jednego lub ewentualnie kilku plików nie zabezpieczy całej platformy, lecz poszczególne jego elementy, np. wybrane kursy. Moodle to platforma dynamiczna, w każdej chwili zmienia

się jej zawartość, dodawane są nowe elementy. Administrator wykonuje standardowe czynności, wykorzystując swoje najwyższe uprawnienia, dodaje nowych użytkowników przydzielając im odpowiednie role (np. menedżera, prowadzącego, studenta), zakłada nowe kursy, pomaga odblokować konta użytkowników. Studenci przesyłają na bieżąco zadania, rozwiązują quizy, wypełniają ankiety. Moodle rejestruje ich aktywność, którą można przeglądać w raportach systemu [Brzózka, 2011, s. 299].

Wbudowane w platformę funkcjonalności pozwalają na wykorzystanie modułu do tworzenia i odtworzenia kopii kursu. Podczas ustawiania kopii zapasowej określamy jakie elementy mają być w niej zawarte. Do kopii kursu możemy dołączyć zapisanych użytkowników wraz z ich loginami i hasłami dostępu. Pozwoli to po ewentualnej awarii przywrócić kurs wraz z jego użytkownikami, bądź przenieść kurs na inną platformę w przypadku awarii całego systemu. Uwzględniając dynamikę zmian odtworzenie będzie możliwe do czasu wykonania kopii, może się więc okazać, że nie będzie zadań wykonanych przez studentów, które należało oddać w określonym terminie, nowych elementów nie ujętych w procesie tworzenia kopii.



Rys. 3. Pierwszy etap selekcji danych poddanych archiwizacji w kursie



Rys. 4. Dobór elementów składowych kopii zapasowej kursu

Wykonując archiwum czy backup mamy nadzieję, że będziemy mogli go wykorzystać po określonym czasie. Niestety, tak nie jest. Okazuje się, że dynamiczny rozwój technologiczny, pojawiające się nowe wersje programów nie są naszym sprzymierzeńcem. Dobrym przykładem jest platforma Moodle. Wykonanie kopii kursów z wersji np. 1.6 i wcześniejszych nie będziemy mogli wykorzystać w wersjach powyżej 2.0. Podobnie było z tekstami zapisanymi w pierwszych edytorach tekstów, takich jak ChiWriter (z 1986 r.) czy Tag (z 1988 r.). Kopia tych plików jest bezużyteczna, ponieważ standardowe oprogramowanie, takie jak Microsoft Word, LibraOffice nie otworzy tych dokumentów. Programy te były uruchamiane w systemie operacyjnym MS-DOS, który już dawno odszedł do lamusa.

Powstaje więc pytanie o sens archiwizacji elektronicznej dokumentów na długie lata, skoro nie będzie można ich uruchomić.

Rys. 5. Konfiguracja automatycznych kopii na platformie Moodle ver. 2.5

Innym problemem jest miejsce i bezpieczeństwo przechowywania. Jak do tej pory najbardziej popularnym nośnikiem są płyty CD i DVD lub dyski przenośne podłączane do USB lub zlokalizowane w sieci LAN. Najkrótszą żywotność mają płyty CD i DVD, których czas jest przewidziany na kilka lat, w zależności od sposobu ich przechowywania, jakości wykonania. Rozwiązania bardzo proste okazują się czasami bardzo skuteczne. Wymaga to jednak cyklicznych „ręcznych" prac w wykonywaniu kopii zapasowych. Wielką zaletę mają zautomatyzowane rozwiązania wykonujące zadania w sposób automatyczny.

W większych instytucjach i przedsiębiorstwach przechowywanie istotnych plików odbywało się z użyciem sieciowych udziałów dyskowych, lecz tzw. konsumeryzacja (BYOD *Bring Your Own Device*) polegająca na używaniu przez pracowników własnych prywatnych urządzeń uniemożliwia centralizowanie zapisu danych. Rozwiązaniem jest system CDP (*Continuous Data Protection*). Za każdym razem, gdy blok danych się zmienia jest on transferowany do CDP. Tego typu rozwiązanie zachowuje zmiany w logach, dlatego można nawet cofnąć modyfikacje i przywrócić system do określonego czasu. Rozwiązania CDP można budować samodzielnie w oparciu o narzędzia open source i odpowiednio dobrane komponenty serwerowe [Szczepaniak, 2013, s. 36].

Pełne zabezpieczenie systemów i danych instytucji oświatowych z pewnością zostanie docenione w przypadku awarii, gdzie dostęp do danych zostanie utracony.

Rozwiązaniem jest zakup dedykowanych serwerów backupowych (Synology, Qnap, TSMbox, Imation NEXAN)

Jednak stworzenie profesjonalnych zabezpieczeń nie zawsze jest możliwe do wykonania własnymi zasobami ludzkimi. Jednym z rozwiązań jest skorzystanie z ofert firm zewnętrznych, oferujących kompleksowe zabezpieczenie – backup w Cloud Computing. Jednakże to rozwiązanie sprawdza się w niewielkich ilościach danych oraz instytucji posiadających symetryczne łącze internetowe lub dostęp za pomocą wirtualnej sieci prywatnej (IP VPN – Virtual Private Networks).

Ciekawym rozwiązaniem jest seria produktów Storagecraft służąca tworzeniu backupu i odzyskiwaniu zasobów softwarowych. Aplikacja Shadowprotect Desktop pozwala na utworzenie backupu stacji roboczej i w przypadku awarii komputera umożliwia uruchomienie systemu jako wirtualnego na innym komputerze. Praca na kopii wirtualnej jest możliwa natychmiast po jej uruchomieniu wraz z jego aplikacjami i danymi zapisanymi w katalogach roboczych.

Zasady „dobrego" backupu

W celu zabezpieczenia danych i całych systemów medialnych usytuowanych na serwerach i komputerach lokalnych należy:

- zabezpieczyć odpowiednią ilość miejsca na nośnikach najlepiej zewnętrznych (zalecane jest przechowywanie płyt, taśm, dysków przenośnych w innej lokalizacji niż miejsce wykonania kopii);
- zabezpieczyć możliwość odtworzenia kopii poprzez duplikowanie kluczowych urządzeń;
- korzystając z usług outsourcingowych (*Outside-Resource-Using*) zaplanować czas przechowywania danych;
- określić częstotliwość wykonywania kopii;
- określić czas wykonywania kopii (np. po godzinach pracy);
- zabezpieczyć narzędzia do wykonania kopii (w przypadku usług backupu w chmurze usługodawca powinien je dostarczyć);
- dokładnie określić co ma podlegać backupowi i archiwizacji (platformy edukacyjne, bazy danych, programy księgowe, konta użytkowników, wiadomości poczty elektronicznej, katalogi użytkowników, systemy wirtualne itd.).

Po wykonaniu backupu lub archiwizacji należy przeprowadzić test, który potwierdzi, że odtworzenie danych jest możliwe. Należy pamiętać, że nie istnieją systemy wykonujące kopię bezpieczeństwa dające stuprocentową gwarancję zabezpieczenia danych. Nie należy z nich rezygnować i zdecydowanie systematycznie je wykonywać, co może uchronić przed przykrymi konsekwencjami.

Bibliografia

Brzózka P.: *Moodle dla nauczycieli i trenerów*. Wydaw. Helion, Gliwice 2011

Hyla M.: *Przewodnik po e-learningu*. Wydaw. Wolters Kluwer Polska, Kraków 2009

Karaś P.: *Współczesne technologie w edukacji*. [W:] *Współczesne media. Język Mediów*. Red. nauk. I. Hoffman, D. Kępa-Figura. Wydawca: Uniwersytet Marii Curie-Skłodowskiej, Lublin 2013

Serafin M.: *Sieci VPN. Zdalna praca i bezpieczeństwo danych.* Wydaw. Helion, Gliwice 2010

Szczepaniak P.: *Dane lokalnie i w chmurze.* „PC WORLD" 2013, nr 7

Wrońska W.: *Kultura medialna adolescentów. Studium dostępu i zastosowań.* Wydaw. Uniwersytetu Rzeszowskiego, Rzeszów 2012

Zieliński Z.: *E-learning w edukacji. Jak stworzyć multimedialną i w pełni interaktywną treść dydaktyczną*. Wydaw. Helion, Gliwice 2012

Netografia

http://www.lms.org.pl [dostęp 14.06.2013]

http://www.sejfdanych.pl/ [dostęp 14.06.2013]

http://tech.wp.pl/kat,1009785,title,Jakie-dane-na-twoj-temat-zbieraja-sluzby-Zobacz-jak-stac-sie-anonimowym-w-internecie,wid,15740404,wiadomosc.html?ticaid=110d85 [dostęp 14.06.2013]

http://tsmbox.eu/pl [dostęp 14.06.2013]

http://www.storagecraft.pl/ [dostęp 14.06.2013]