Jerzy Piskor

Bezpieczeństwo szkolnej infrastruktury informatycznej

Ważnym elementem komputeryzacji pracy szkoły jest szacowanie i kontrola ryzyka związanego z wykorzystaniem komputerów w zakresie zachowania przez nie poufności, łatwości dostępu i integralności.

W 1994 roku utworzyłem w szkole podstawowej informacyjny system wspierania edukacji i zarządzania, który jest ciągle modyfikowany i doskonalony, a doświadczenia z jego funkcjonowania stały się podstawą niniejszego artykułu.

Celem moich działań było zbudowanie bezpiecznego systemu, ale ze względu na złożoność i czasochłonność wielu jego elementów i procesów, poważnym problemem stały się istniejące i pojawiające się nowe luki w zabezpieczeniach.

Prawdziwie bezpieczny system, zgodnie z powszechną definicją, jest idealnym urządzeniem, które poprawnie i w całości realizuje tylko i wyłącznie cele zgodne z intencjami właściciela. W rzeczywistości, w związku z ryzykiem powstania prozaicznych błędów i usterek oraz w wyniku sprzecznych oczekiwań użytkowników, właściciela czy projektanta, tak naprawdę zapewnienie bezpieczeństwa skupia się na zarządzaniu ryzykiem mogących wystąpić zagrożeń i powstających ewentualnie w związku z tym strat. Trzeba zatem podejmować racjonalne kroki zapobiegawcze, mając na uwadze możliwości techniczne i finansowe. Dotychczasowe wsparcie szkół poprzez fundowanie im pracowni komputerowych nie uwzględniało wystarczająco tego problemu. W miarę rozbudowy infrastruktury (sieci rozległe, Internet) coraz większym problemem stają się osoby trzecie mogące wchodzić w interakcje z systemem w sposób niezamierzony ani oczekiwany przez właściciela. Ważnym aspektem tego zagadnienia są błędy i pomyłki (np. techniczne) popełniane najpierw przez programistów, potem przez administratorów (wynikające z niezrozumienia dokumentacji, niestaranności czy niepełnych kwalifikacji) czy wreszcie operatorów (użytkowników nierozumiejących zagadnień prawidłowej i bezpiecznej obsługi – np. uruchamianie załączników od niepewnych nadawców, ignorowanie komunikatów ostrzegawczych czy przypadkowa zmiana np. opcji programów). Innym aspektem tego zagadnienia są kłopoty ze spamem, wynikające historycznie z budowy protokołu SMTP.

Choć wyeliminowanie błędów zabezpieczeń praktycznie nie jest możliwe (nieekonomiczne), można starać się je zminimalizować. Ważne jest, aby budować struktury w sposób ograniczający ewentualne skutki naruszenia zabezpieczeń czy niepożądanej aktywności uprawnionego użytkownika. W efekcie będzie możliwe zminimalizowanie ewentualnych strat i szybka identyfikacja problemów. Kluczem do sukcesu może być ograniczenie do niezbędnego minimum uprawnień użytkowników, wyłączanie zbędnych usług sieciowych na platformach czy stosowanie zapór sieciowych.

Zapewnienie bezpieczeństwa wymaga ciągłych nakładów pracy i nakładów finansowych oraz edukacji użytkowników, aby np. rezygnowali z oglądania niebezpiecznych stron WWW. Konieczna jest więc permanentna aktualizacja oprogramowania oraz zachowanie ostrożności przy korzystaniu z Internetu. Ogromną rolę spełnia też odpowiedni tryb informowania użytkowników o nieprawidłowościach i zagrożeniach, żeby mogli im w porę zapobiec. Należy zatem najpierw budować możliwie najbezpieczniejszą infrastrukturę, a potem ustawicznie pracować nad edukacją jej użytkowników dla bezpieczeństwa.

Początkowo, 20 lat temu, zaczynałem od budowy prostych sieci P2P na skrętce pomiędzy komputerami stosowanymi w zarządzaniu szkołą. Ograniczenia tego rozwiązania i potrzeba połączenia ze sobą grup komputerów w sieć LAN oraz postęp technologiczny wpłynęły na decyzję budowy sieci o topologii pierścieniowo-gwiaździstej (kabel koncentryczny – skrętka). Do tak połączonych stacji w sieci zostały podpięte dwa serwery plików Novell NetWare 3.12 – osobno dla zarządzania i dla edukacji – wraz z aktywnymi urządzeniami sieci (hubami). To rozwiązanie zaspokoiło początkowe potrzeby zbudowanego wówczas informacyjnego

systemu wspierania edukacji i zarządzania. Uruchomienie w Lublinie akademickiej sieci komputerowej stworzyło możliwość podłączenia struktury szkolnej do globalnego systemu sieciowego, jakim stawał się Internet. Szkolna sieć komputerowa oparta o 25-stanowiskowy Novell NetWare została zbudowana w 1995 roku, a następnie rozbudowana o następny 50-stanowiskowy NetWare. W tym samym roku sieć szkolna została podłączona dzierżawionym łączem stałym do sieci Internet Lubmana. Głównym pretekstem do podłączenia się do światowej pajęczyny była możliwość ściągania z Biblioteki Narodowej w Warszawie informacji o pozycjach książkowych w reorganizującej się bibliotece szkolnej. Ówczesne połączenia modemami z providerem za pomocą stałych linii dzierżawionych o bardzo małej przepustowości zostały z czasem zastąpione szybszymi modemami, by w końcu uzyskać dostęp światłowodowy.

W początkowym okresie, ze względu na niszowy w tym czasie charakter rozwiązań technicznych, sprawy bezpieczeństwa sieci były drugoplanowe. Jednak wraz z upowszechnieniem Internetu wzrastała liczba zagrożeń. Wymagało to ciągłej modernizacji parku sprzętowego nie tylko ze względu na zużycie, ale i nowoczesność oraz pewność rozwiązań. Serwer Uniksowy Novella był drogi, więc do sieci zewnętrznej został podłączony za pomocą komputera działającego w systemie Linuks. Były tam uruchomione m.in. usługi typu router, firewall, serwer DNS, Proxy itd., które obecnie wykonywane są za pomocą dedykowanych rozwiązań sprzętowych. Na serwerze Novell NetWare uruchomiony został również serwer WWW.

Oczywiście, przy braku środków finansowych, rozważana była koncepcja wdrożenia w szkole Linuksa. Podjęte próby z czasem zaniechano, gdyż wymagało to dodatkowych umiejętności od posługujących się sprzętem pracowników i nauczycieli. Trudno im było uczyć się obsługi oprogramowania innego od tego, które mieli w domu. Rotacje kadrowe w szkole i hobbystyczna (*non profit*) działalność pracowników w zakresie pracy z Linuksem samoistnie ograniczyły liczbę urządzeń działających w tym systemie do wybranych rozwiązań w niektórych kategoriach. Pomimo że rozwiązania linuksowe są, jak się wydaje, najtańsze, to biorąc pod uwagę określone możliwości kadry szkoły oraz brak odpowiednio dużego i taniego wsparcia technicznego, szkoła wycofała się z Linuksa na rzecz systemów droższych, ale sprawdzonych i posiadających pełne i łatwo dostępne wsparcie techniczne.

Teza, aby w świetlicy zapoznawać uczniów z Linuksem, w kształceniu zintegrowanym z komputerami Macintosh, a dopiero potem z systemem Windows na razie nie może doczekać się realizacji, choć dzięki temu uczniowie nie mieliby w przyszłości żadnych kłopotów i obaw związanych z posługiwaniem się jakimikolwiek komputerami.

Mając na uwadze również wyżej wymienione względy, szkoła starała się o pracownie MEN z wyposażeniem w system Windows, gdyż Linuks jako darmowy system zawsze można było dodatkowo w komputerach doinstalować.

Od momentu otrzymania pierwszej pracowni w 2002 roku z programu MEN w szkole zaprzestano rozwoju systemów oferowanych przez firmę Novell, przechodząc na systemy firmy Microsoft. Zgodnie z programami ministerialnymi nauczyciele zostali objęci szkoleniami w zakresie użytkowania i administracji otrzymanych SBS-ów (*Small Business Server*).

Oferowane szkolenia pomagały w początkowej fazie użytkowania. Aby jednak w pełni wykorzystywać posiadane możliwości sprzętowe, administrator musiał poświęcić wiele czasu i pracy, która nie była dodatkowo opłacana.

Wzrastająca liczba komputerów i pracowni SBS wymagała dostosowania eksploatacji do zwiększającego się zapotrzebowania na rozwiązania szybkie, łatwe i nieskomplikowane w korzystaniu z nowych możliwości, jakie dawały coraz nowsze wersje pracowni.

Dużo więcej uwagi należało poświęcić zarówno zagrożeniom zewnętrznym, jak i wewnętrznym w szkolnej sieci. Już w 2004 roku podczas wystąpienia/warsztatów na III Ogólnopolskim Zjeździe Opiekunów Szkolnych Pracowni Internetowych w Mrozach na temat „Bezpieczeństwa dzieci w sieci" zwróciłem uwagę na wiele aspektów bezpieczeństwa wewnętrznego sieci – poczynając od wychowania uczniów dla bezpieczeństwa, na zabezpieczeniach sprzętu przed nieuprawnionym korzystaniem z treści internetowych kończąc.

Bezpieczeństwo szkolnej infrastruktury obejmuje zatem zarówno bezpieczeństwo informacji krążących w sieci, jak i tych zgromadzonych w bazach danych dostępnych za jej pośrednictwem. Zagrożenia związane z włamaniami do systemów wewnątrzszkolnych są tak znaczące, że środki ochrony poprzez ograniczenie dostępu do zasobów zgodnie z ustaloną polityką ochronną w szkole oraz utajnianie informacji za pomocą kryptografii są niezbędne i konieczne.

Zanim jednak poniesiemy duże nakłady finansowe na zabezpieczenia sprzętowe, musimy pamiętać, że sama technologia nie może zapewnić

pełnego bezpieczeństwa. Ochrona to przede wszystkim właściwe zarządzanie i organizacja.

Właściwa organizacja systemu ochrony obejmuje rozpoznanie jego obszaru oraz określenie (uświadomienie sobie), jak wygląda schemat sieci, punkty dostępowe, kto oraz jak z nich korzysta oraz jakie zasoby są na tyle ważne, aby je chronić, i gdzie są zlokalizowane?

Szkolenia wszystkich użytkowników sieci w szkole w zakresie takiej ochrony jest sprawą bezdyskusyjną, choć często nieuświadomioną (przez co zaniedbaną). Niezbędna jest zarówno stała współpraca agend szkolnych, jak również wspomaganie, zrozumienie i elastyczność wobec użytkowników końcowych – ucznia i nauczyciela. Proces edukacyjny powinien być dostosowany do oczekiwań i potrzeb każdej grupy w szkole, w przeciwnym razie ochrona będzie pomijana, ignorowana lub wyłączana.

Idealny system ochrony szkolnej sieci powinien być zdolny do wykrywania niektórych działań i zachowań pochodzących z zewnątrz i z wewnątrz, które mogą być uznane za podejrzane. Wykrywanie intruzów jest szczególnie ważne, gdy korzystamy z Internetu, choć, jak wynika z badań, prawdopodobnie połowa ataków jest powodowana przez osoby kiedyś związane z daną siecią od wewnątrz. Dlatego zawsze należy pamiętać o nadawaniu uprawnień użytkownikom stosownie do ich pozycji w szkole. Poza dyskusją powinno być włączanie beneficjentów systemu do ochrony, a nie czynienie z nich potencjalnych przeciwników. Przykładem może być tutaj sytuacja, w której dane księgowe i kadrowe są odłączone od sieci dla edukacji i Internetu. Pracownicy mają dodatkowy dostęp do tych zasobów z innych komputerów lub sieci. Koszty zapewnienia bezpieczeństwa są wtedy ułamkiem ewentualnych kosztów wynikłych ze strat powstałych przez brak zapewnienia pełnej ochrony. Jest to kolejny przykład, że technologia nie stanowi o wszystkim, a problem często można rozwiązać prostym działaniem organizacyjnym.

W sieciach rozległych jest wiele miejsc, z których hakerzy mogą penetrować sieć podsłuchem, rozprzestrzeniać wirusy, wykradać informacje, czy zakłócać ich pracę. Nie istnieją metody pełnej ochrony, a utrzymywanie całego arsenału środków nie jest rozsądne i przysparza kłopotów mających swe źródło w zmienności technologii i standardów. Dlatego należy ograniczyć się do ochrony ich granic.

Wraz z rozwojem Internetu i wzrostem liczby użytkowników uzyskujących dostęp do jego zasobów szczególnego znaczenia nabiera ochrona danych metodą kryptograficzną. Oprócz stosowania kart identyfikacyjnych, zamków elektronicznych czy zapór ogniowych, niezbędne staje się szyfrowanie znaczących informacji. Dostęp przez Internet do szkolnych zasobów edukacyjnych powoduje konieczność wprowadzania coraz lepszych zabezpieczeń (nie tylko poprzez odpowiednio spreparowane hasło do zasobów).

Oto aktualne elementy szkolnej infrastruktury informatycznej:

1. Serce infrastruktury – **serwer z Hyper-V 2008 R2 do wirtualizacji serwerów** (zdalnie zarządzany) znajduje się w klimatyzowanej serwerowni zabezpieczonej przed postronnymi osobami kontrolą dostępu i monitoringiem wejść. Umieszczone są w niej dwie szafy 42U 19". Zastosowany został UPS 5kVA do zasilania awaryjnego serwerowni i komputerów. Z każdego pomieszczenia doprowadzono bezpośrednio skrętkę komputerową. W szkole położono łączenie ponad 10 km skrętki. W całej szkole jest ponad 320 gniazd RJ45 umożliwiających dostęp do Internetu. Do połączenia światłowodowego wykorzystano 6-włóknowy kabel światłowodowy o łącznej długości 120 m. Pracownie komputerowe zostały połączone z serwerownią kablem światłowodowym (3 tory dwuwłóknowe).
   Wirtualizacja umożliwia oddzielenie wykorzystywanych zasobów sprzętowych od systemów i aplikacji, które z tych zasobów korzystają. Uruchomienie kilku wirtualnych maszyn na jednym serwerze fizycznym pozwala na zaoszczędzenie miejsca w serwerowni, ograniczenie kosztów zakupu nowych serwerów, redukcję kosztów zasilania i chłodzenia oraz lepsze wykorzystanie mocy obliczeniowej serwerów. W najbliższym czasie wszystkie serwery szkolne będą działał jako maszyny wirtualne.
2. **SBS 2003 i ISA Server**
3. **Router DUAL-WAN ETHERNET Draytek 2930 Vn**
4. **Routery bezprzewodowe: Draytek 2910 VG, Linksys WRT54GL**
5. **Zarządzalne switche**
6. **Pakiet przejścia (Transition Pack) Microsoft**
   Obecnie w szkole działa 5 serwerów SBS. Integracja pracowni jest tak przeprowadzana, aby wszystkie komputery uczniowskie były podłączone do jednego serwera. W tym celu został zakupiony pakiet przejścia dla systemu MS Windows SBS 2003 R2 Premium Edition z licencjami dostępowymi, który umożliwia zamianę

zainstalowanego (skonfigurowanego i działającego) serwera SBS na pełną wersję systemu serwerowego Windows Server 2003 R2 Standard Edition. Tym samym znosi wbudowane do systemu SBS ograniczenia, czyniąc go pełnoprawnym systemem serwerowym, dającym znaczne możliwości skalowalności w zależności od potrzeb. W szkolnych warunkach główną zaletą zastosowania pakietu przejścia jest zniesienie ograniczenia licencyjnego, niepozwalającego podłączyć do jednego serwera więcej niż 75 stacji roboczych.

7. **PCinfo MagicEYE 5.5**
Szkoła podsiada licencje na 120 stanowisk PCinfo® MagicEYE. W wersji STANDARD zawiera moduły:
– audyt i ewidencja oprogramowania,
– audyt i ewidencja sprzętu,
– zarządzanie licencjami,
– zdalne instalacje,
– zdalne sterowanie.
Jest to rozbudowany system do audytu oprogramowania i zarządzania zasobami IT. PCinfo® MagicEYE umożliwia przeprowadzanie bardzo szczegółowej ewidencji posiadanych komputerów, podzespołów komputerowych i innych urządzeń informatycznych, a także precyzyjne wykrywanie zainstalowanego w komputerach oprogramowania (opcjonalnie także plików graficznych, muzycznych czy filmów). Wszelkie dane pobierane są z instalowanych zdalnie agentów rezydujących na poszczególnych końcówkach sieci i wyświetlane na stanowisku administratora. Możliwe jest także sprawdzanie komputerów pracujących pod kontrolą systemu Linuks. Program umożliwia wprowadzenie liczby posiadanych licencji na oprogramowanie, dzięki czemu można w łatwy sposób wychwycić ewentualne różnice, a także sprawdzić, w których konkretnie komputerach zainstalowane jest dane oprogramowanie.

MagicMONITOR umożliwia:
• monitoring wykorzystania aplikacji
– które uruchomił konkretny użytkownik,
– jak długo były one uruchomione,
– jak długo użytkownik z nich korzystał (były „on top"),
– z jakimi plikami pracował,
– liczba uderzeń w klawiaturę i kliknięć myszką w każdej aplikacji,
– z kim czatowano przez komunikatory internetowe,
• monitoring WWW:
– jakie serwery i strony odwiedzał użytkownik PC,
– ile czasu z nich korzystał,
– z jakiej przeglądarki internetowej korzystał.

8. **Program antywirusowy – wersja sieciowa**
Moduły wchodzące w skład aplikacji:
– serwer,
– moduł zarządzający ochroną antywirusową sieci,
– administrator,
– aplikacja zarządzająca modułem serwera,
– WebAdministrator,
– aplikacja do zarządzania ochroną sieci przez WWW,
– klient AntiVirus,
– moduł chroniący komputery końcowe.
Antywirus oferuje w pełni automatyczną ochronę sieci przed wirusami i złośliwym oprogramowaniem. Umożliwia zdalną instalację, automatyczną aktualizację, a także zdalną modyfikację ustawień ochrony antywirusowej. Antywirus rozpoznaje i blokuje wirusy, rootkity, robaki, spyware, trojany, backdoory. Chroni prywatność podczas wykonywania płatności online, blokując wszelkie próby wyłudzenia danych. Uniemożliwia zainfekowanie systemu, dzięki czemu komputer zawsze działa szybko i stabilnie.

9. **Technologia iPAT 3.1**
Technologia iPAT chroni, po włączeniu, zawartość dysku twardego (wybranych partycji) przed nieupoważnionymi trwałymi zmianami. W czasie użytkowania komputera działanie zabezpieczenia jest niewidoczne (transparentne) – po każdym restarcie komputera oryginalna chroniona zawartość jest automatycznie przywracana. Niestety iPAT 3.1 działa tylko z płytą główną INTEL D946GZAB (pracownia EFS z roku 2008 – 10 komputerów).

10. **Karta przywracania**
Karta ta, to urządzenie montowane w slocie PCI, zabezpieczające twardy dysk przed niekontrolowanymi zmianami. Posiada kilka elastycznych trybów przywracania: automatyczny, manualny, cykliczny, rezerwowania danych. Może chronić wiele partycji.
Posiada funkcję modernizacji/uaktualniania danych – w każdej chwili można dodawać nowe programy komputerowe, które muszą być koniecznie chronione. Posiada funkcję zabezpieczania przed zmianami konfiguracji BIOS – tutaj również działa funkcja przywracania.
Niestety, karta nie była jeszcze dopracowana – testy zakończyły się utratą systemu i koniecznością jego ponownej instalacji. Nie z każdą płytą główną działa poprawnie.

11. Uczniowie są chronieni przed niepożądanymi treściami z Internetu następującymi programami zabezpieczającymi:
   – Beniamin,
   – Opiekun ucznia,
   – NetSupport School NSS 10".

   Beniamin oraz Opiekun Ucznia blokują, dzięki zaawansowanym filtrom, dostęp do niepożądanych stron. Programy te wymagają szczególnego nadzoru i mogą wprowadzać problemy w codziennym korzystaniu z komputerów, które chronią. NetSupport School został zainstalowany na 27 stanowiskach komputerowych i pozwala na zdalny podgląd komputerów, z których korzystają uczniowie, kontrolę użytkowanych aplikacji i stron internetowych. Dzięki temu nauczyciel, nie wstając od biurka, ma kontrolę nad pracą uczniów. NetSupport School jest programem do wspomagania nauczania w skomputeryzowanej klasie, zapewniającym nauczycielowi możliwość nauczania, nadzorowania oraz współpracy z uczniami, zarówno indywidualnie, jak i grupowo.

Infrastruktura informatyczna powinna nadążać za wzrastającymi potrzebami społeczności szkolnej, która świadomie rozszerza krąg swoich zainteresowań o coraz to nowe możliwości zastosowania komputera w edukacji. Szkoła już od ponad roku dostosowuje do własnych potrzeb platformę edukacyjną Fronter, badamy funkcjonalność Microsoft Live@edu, wykorzystujemy Moodle. A więc poprzeczka bezpieczeństwa musi być zawieszona bardzo wysoko.

Autor jest dyrektorem Szkoły Podstawowej nr 21 im. Królowej Jadwigi w Lublinie
http://piskor.pl

◄

Przemoc występująca w grze ma bardziej dosadny charakter, skierowana jest jednak na postaci fantastyczne lub w nierealistyczny sposób przedstawia przemoc skierowaną na postaci ludzkie, jak np. w grach RPG (komputerowa gra fabularna), osadzonych w fantastycznych światach. Ewentualne wulgaryzmy muszą mieć łagodny charakter i nie mogą zawierać odwołań do seksu.

Przykładowe gry z tej grupy: Cywilizacja IV, Guitar Hero III, World of Warcraft.

◄

Przedstawione w grze przemoc i aktywność seksualna bohaterów wyglądają jak w prawdziwym życiu. Pojawia się bardziej dosadny język, sceny spożywania alkoholu i tytoniu, zażywania narkotyków oraz popełniania przestępstw.

Przykładowe gry z tej grupy: Star Wars: TFU, Final Fantasy XII, Far Cry 2.