Bezpieczeństwo informatyczne szkół i instytucji publicznych - poradnik

Paweł Krawczyk pawel.krawczyk@hush.com

Licencja: Creative Commons Uznanie autorstwa-Na tych samych warunkach 3.0 Polska License.

Spis treści

Wstęp

Poradnik ten został napisany przez praktyków dla praktyków i mamy nadzieję, że w takim modelu będzie rozwijany. Jego cel jest bardzo prosty - pokazać osobom zarzadzającym nowoczesnymi technologiami w administracji, że bezpieczeństwo nie jest kosztownym kaprysem tylko podstawową potrzebą, którą na dodatek można zapewnić stosunkowo tanim kosztem.
Większość opisywanych przez nas poniżej technik jest darmowa, część z nich jest dostępna w modelu *open-source*. Wielu dostawców komercyjnych oferuje darmowe wersje swoich usług i produktów, które, choć nieco uboższe od płatnych odpowiedników, często będą zupełnie wystarczające na potrzeby szkół. Inni dostawcy oferują specjalne licencje edukacyjne w bardzo atrakcyjnych cenach.
Chcielibyśmy aby głównym wnioskiem jaki nasunie się Państwu po lekturze tego poradnika był ten, że bezpieczeństwo to ciągła zmiana a zarządzanie bezpieczeństwem to racjonalne kontrolowanie tych zmian. Bezpieczeństwo w XXI wieku to nie jednorazowy zakup urządzenia za kilkadziesiąt tysięcy, które podłączamy do sieci i ono nas chroni - bezpieczeństwo to przede wszystkim sprawnie działający proces, dzięki któremu komputery są regularnie aktualizowane a administratorzy na czas zauważą próby ataku.
Pamiętajmy też, że najsłabszym ogniwem w bezpieczeństwie są ludzie. Utartym zwyczajem w dużych instytucjach jest przedkładanie inwestycji w dobra “namacalne”, takie jak sprzęt komputerowy, zamiast w “miękkie” umiejętności personelu. Tymczasem żaden sprzęt, a już na pewno nie komputery, nie będzie poprawnie działał, jeśli nie będzie z niego korzystał świadomy użytkownik.

Bezpieczeństwo organizacyjne

Zabezpieczenia techniczne są podstawą, która jednak będzie nieszczelna i nieskuteczna jeśli nie będzie koordynowana przy pomocy środków organizacyjnych. Inicjatywa na rzecz bezpieczeństwa musi pochodzić z góry, czyli od dyrekcji, która musi przynajmniej dać jej “zielone światło” i wspierać w przypadku nieuniknionych przeszkód.
Dyrekcja ustala jakie priorytety ma dana organizacja w zakresie bezpieczeństwa i opisuje je w polityce bezpieczeństwa (którą szczegółowo omawiamy poniżej). Polityka bezpieczeństwa jest przekładana przez specjalistów na język techniczny - w postaci standardów, minimalnych wymagań i procedur.
Bezpieczeństwo organizacyjne ma to do siebie, że zapomina się o jego istnieniu tak długo jak nic złego się nie dzieje. Tymczasem w razie awarii czy włamania do sieci od zarządu i

specjalistów oczekuje się udzielenia w trybie pilnym odpowiedzi na szereg pytań. Na przykład: co się stało i kogo należy natychmiast powiadomić? Na to pytanie odpowiadać będzie procedura reagowania na incydenty. Gdzie są kopie zapasowe? Tu przyda się procedura ciągłości działania - i tak dalej.
Ale co jeśli osoby wskazane w procedurze dawno są na emeryturze, a kopie zapasowe ostatnio testowano pięć lat temu? Dlatego tak istotne jest by nad formalną poprawność polityk i procedur przedkładać ich faktyczną przydatność i regularną (co najmniej raz w roku) aktualizację oraz testowanie.

Polityka bezpieczeństwa

W tym poradniku skupiamy się przede wszystkim na **bezpieczeństwie technicznym**, które jest zazwyczaj pierwszą formą aktywności, na której skupiają się instytucje zaczynające jakiekolwiek działania związane z bezpieczeństwem. W przypadku instytucji mogących podlegać jakiejś formie nadzoru ze względu na obowiązujące przepisy[1] niemniej ważne jest jednak **bezpieczeństwo organizacyjne**.
Narzędzia techniczne odpowiadają na pytanie **jak** się zabezpieczać i zwykle opieramy się tutaj na szeroko pojętych dobrych praktykach i zdrowym rozsądku. Możemy być być świadomi naszego poziomu bezpieczeństwa i znać jego silne oraz słabe strony. W momencie pojawienia się audytora musimy jednak być w stanie odpowiedzieć także na pytanie **dlaczego** zabezpieczamy się w taki, a nie inny sposób i jaki był powód wybrania konkretnych rozwiązań[2].
Polityka bezpieczeństwa jest dokumentem, który definiuje to pytanie i udziela na niego odpowiedzi w sposób uzystematyzowany i formalny. Z polityki bezpieczeństwa wynika cała reszta - to na jej podstawie podejmujemy decyzję co ma być chronione hasłem i jakie pliki mają być dostępne dla kogo.
Brak jest także łatwo dostępnych wzorców polityk bezpieczeństwa dla instytucji działających według podobnych procedur - np. szkół. Dlatego dobrym punktem wyjścia do stworzenia polityki bezpieczeństwa jest norma PN ISO-IEC 27001, zawierająca wszystkie kluczowe punkty, jakie powinny się w niej znaleźć.
Nie twórzmy jednak polityk bezpieczeństwa, które składają się z samych pobożnych życzeń jak wyglądałaby nasza sieć, gdybyśmy mieli więcej pieniędzy. Nie kopiujmy polityk bezpieczeństwa z Internetu, z książek lub z polityk innych, większych instytucji. Będzie to wtedy dokument martwy, nie mający żadnego przełożenia na rzeczywistość.
Każda instytucja ma swój specyficzny profil ryzyka, który nalezy wziąć pod uwagę przy tworzeniu takiej polityki. Oznacza to z jednej strony, że pewne aspekty należy potraktować priorytetowo, ale inne z kolei możemy świadomie pominąć - na przykład wątpliwe, by szkoły przetwarzały transakcje finansowe kartami kredytowymi, co przysparza problemów wielu firmom.

---

[1] Wystarczy choćby ustawa o ochronie danych osobowych.
[2] Pytanie o poziom bezpieczeństwa pojawi się niechybnie ze względu na koszty. Wyższy poziom bezpieczeństwa jest przeważnie droższy. Jeśli potrafimy uzasadnić nasze wymagania związane z bezpieczeństwem przy pomocy faktów i liczb, to nie powinniśmy mieć problemu z ich obronieniem np. we wniosku o dofinansowanie czy przetargu.

W dalszej części poradnika postaramy się wskazać na punkty istotne w środowisku szkolnym.

Bezpieczeństwo haseł

Hasła są od dawna najpopularniejszą metodą uwierzytelniania użytkowników i to pomimo faktu, że można je podsłuchać, przechwycić lub zgadnąć. Hasła mają jedną, dużą zaletę - do ich wprowadzenia wystarczy klawiatura i monitor (albo ekran dotykowy), czyli coś co jest dostępne "zawsze" (w odróżnieniu np. od czytnika kart czipowych).
Najłatwiejszą metodą włamań na cudze konto jest zgadnięcie hasła. Użytkownicy nie wykazują szczególnej inwencji w wymyślaniu haseł - najpopularniejsze to imiona (na dodatek pisane małymi literami - "monika", "maciek") i popularne kombinacje klawiszowe ("qwerty", "12345", "q1w2e3"). Za szczyt przebiegłości uchodzi utworzenie prostej kombinacji słowno-liczbowej, na przykład "marysia123".
Takie hasła są jednak bardzo słabe. Przy pomocy szybkich programów, testujących hasła w tempie kilku milionów na sekundę (!) te najprostsze można zgadnąć w kilkanaście minut. Dłuższe - w kilka godzin lub kilka dni. Ale to żaden problem dla zdeterminowanego włamywacza - uruchamia program i czeka aż jakieś konto "puści".
Tymczasem hasła mogą być i łatwe do zapamiętania, i trudne do zgadnięcia. Oto kilka zasad:

- Hasła od dawna nie muszą już mieścić się ośmiu znakach. Kiedyś "bezpieczne hasło" kojarzyło się z niezrozumiałą zbitką znaków. Obecnie hasła mogą zawierać spacje i znaki przestankowe, a nawet polskie litery, i mieć długość nawet całych zdań (zwykle do 128 znaków).
- O ile polskich liter lepiej unikać bo nie wiemy z jakiej klawiatury przyjdzie nam się logować, o tyle ze spacji i innych znaków przestankowych możemy korzystać do woli. Każde taki znak to znaczne utrudnienie dla włamywacza.
- Dlatego najbezpieczniejszym hasłem jest dzisiaj po prostu fraza lub całe zdanie. Na przykład "*Litwo ojczyzno moja!!!*" jest praktycznie nie do zgadnięcia przy pomocy słownika[3].

Ale o tych zasadach użytkownicy muszą wiedzieć - musimy im o tym powiedzieć, zachęcić do korzystania z takich "długich haseł" i przełamać nawyki wyniesione ze starych książek i regulaminów, mówiące o ośmioznakowych hasłach składających się z losowych znaków. Trzeba im o tym wprost powiedzieć, pokazać na przykładach - i zdać się na ich kreatywność oraz oczytanie.
Kolejnym problemem, z którymi borykamy się dzisiaj jest **zarządzanie hasłami do wielu serwisów**. Jedno do banku, drugie do poczty, trzecie do szkolnej strony i tak dalej. Łatwo się w tym pogubić i wiele osób rozwiązuje ten problem używając wszędzie tego samego hasła. Ale jeśli ktoś go ukradnie, będzie mógł wejść do wszystkich naszych stron. Tylko jak zapamiętać tyle haseł?
Tutaj z pomocą przychodzą **programy do zarządzania hasłami** (*password managers*)**,** które

[3] Oczywiście, o ile wszyscy nie zaczną nagle korzystać z tego konkretnego fragmentu. Z uwagi na sam fakt publikacji tę konkretną frazę należy uznać za "spaloną" :)

umożliwiają bezpieczne zapamiętywanie i przechowywanie nawet setek haseł. Muszą być one zawsze zabezpieczone jednym hasłem głównym, które chroni wszystkie pozostałe. Jeśli są wbudowane w przeglądarki internetowe to tym lepiej, bo zapamiętają hasła po pierwszym wpisaniu na danej stronie, a przy kolejnym logowaniu wkleją je za nas.
Wśród popularnych narzędzi można wymienić:

- Funkcje zapamiętywania haseł wbudowane w przeglądarki - Google Chrome, Mozilla Firefox, Internet Explorer. We wszystkich zapamiętane hasła mogą być dodatkowo chronione "hasłem głównym" - należy z tej funkcji korzystać, inaczej dowolny wirus będzie mógł za jednym zamachem ukraść wszystkie hasze hasła. Przeglądarki zapamiętają tylko hasła do aplikacji webowych.
- LastPass - program zaintegrowany z większością przeglądarek, o bardzo rozbudowanych funkcjach bezpieczeństwa. Może zapamiętywać dowolne hasła i notatki.
- KeePass - otwarte oprogramowanie pozwalające na edytowanie i bezpieczne przechowywanie listy haseł w zaszyfrowanym pliku, ale nie zintegrowane z przeglądarkami. Może zapamiętywać dowolne hasła i notatki.
- KeePassX - wersja dostępna dla Linuksa, MacOS i Windows
- PwdHash - wtyczka do popularnych przeglądarek, która na podstawie jednego hasła głównego ustawi nam różne (ale wywodzące się z niego) hasła w każdym serwisie, z którego korzystamy.

Bezpieczna pracownia komputerowa

Dotychczas tradycyjnymi ośrodkami "komputerowymi" były pracownie internetowe w szkołach. Obecnie komputery dynamicznie coraz częściej pojawiają się już w klasach czy na biurkach uczniów, są także obecne w sekretariatach i w pokojach nauczycielskich. Szkoły stają się instytucjami zinformatyzowanymi na normalnym, światowym poziomie - ale za tym musi iść też dostosowanie poziomu bezpieczeństwa. Poniższa lista dotyczy więc wszystkich zastosowań, gdzie komputery są stosowane w szkołach jako stacje robocze, nie tylko pracowni.

Złośliwe oprogramowanie

Złośliwe oprogramowanie (*malware*) to czarnorynkowa branża przynosząca obecnie krociowe zyski. Obecnie rzadko spotykamy wirusy komputerowe, których celem jest samo powielanie się lub niszczenie danych. Współczesne programy tego typu służą przede wszystkim zarabianiu pieniędzy przez kradzież haseł, adresów email, wyłudzanie pieniędzy (na "zaszyfrowany dysk", na fałszywego antywirusa) lub wykorzystywanie zainfekowanych komputerów jako "stacji przesiadkowych" (*zombie*) do innych ataków.
W powszechnym przekonaniu głównym narzędziem ochrony są tutaj programy antywirusowe. To błąd - antywirusy mają często skuteczność nie przekraczającą 50% wobec nowych zagrożeń. Oznacza to, że w początkowym (i najbardziej intensywnym) okresie dystrybucji danego wirusa użytkownik jest praktycznie bezbronny jeśli opiera się tylko na antywirusie.
Jak się bronić? Zarażenie komputera wymaga spełnienia dwóch warunków:

- użytkownik musi **uruchomić** zarażony plik - może on przyjść emailem, być wystawiony na stronie jako fałszywa “aktualizacja bezpieczeństwa” lub być ukryty na stronie WWW;
- w celu dalszego opanowania komputera wirus musi uzyskać **prawa administratora**; jeśli użytkownik pracuje na koncie administratora to wirus ma je podane na tacy; jeśli nie, to może zaatakować przez znane dziury w systemie lub aplikacjach; na tym etapie pomoże ograniczenie uprawnień

Typowymi technikami infekcji są błędy w przeglądarkach internetowych oraz dodatkach do nich - zwłaszcza wtyczkach **Java** i **Flash**. Dlatego dla uniknięcia powtarzających się infekcji kluczowe jest wdrożenie następujących zasad:

- ogranicz dostęp do konta administratora
  - dla uczniów i nauczycieli stwórz konta z ograniczonymi uprawnieniami,[4]
  - nie udostępniaj hasła administratora bez potrzeby,
  - nie pracuj na codzień na koncie administratora,
  - wiele czynności administracyjnych w Windows możesz nadal wykonać przy pomocy funkcji Run As.[5]
- włącz wszędzie automatyczne aktualizacje
  - w systemie operacyjnym (Aktualizacje Windows),
  - we wszystkich programach, które mają taką funkcję.[6]
- zainstaluj program antywirusowy
  - włącz automatyczne aktualizacje sygnatur
  - nie używaj na stałe wersji demonstracyjnych i testowych[7]

Opisane powyżej techniki to absolutne podstawy, które uszeregowaliśmy według ich ważności. Pamiętajmy jednak, że żadne z wymienionych zabezpieczeń nie ma stuprocentowej skuteczności i jedynie wiele “warstw” zabezpieczeń zmniejszy szansę infekcji. Dlatego warto również stosować następujące zalecenia:

- Zawsze aktualizuj przeglądarkę internetową do najnowszej wersji. Jest ona pierwszą linią obrony, a nowe wersje przeglądarek zawierają zawsze udoskonalone mechanizmy bezpieczeństwa.
- Bazy groźnych stron WWW wbudowane w nowe wersje przeglądarek Chrome, Firefox (Google SafeBrowsing) oraz Microsoft Internet Explorer (SmartScreen). Powinny być domyślnie włączone.
- Ochrona przed wykonywaniem danych (DEP) wbudowana w Windows XP od wersji

---

[4] Takie konta są domyślnie zakładane w Windows Vista, Windows 7 oraz w Linuksie. W systemie Windows XP trzeba stworzyć je po założeniu domyślnego konta administratora. Instrukcja dostępna jest np. w serwisie YouTube.

[5] W systemach Windows XP używaj Run As, w Windows Visa i 7 - funkcji UAC.

[6] Przeglądarki są najbardziej narażone na ataki ze strony złośliwych stron internetowych i należy je bezwzględnie aktualizować. Funkcje automatycznej aktualizacji mają także popularne programy typu Adobe Flash, Adobe Reader, Open Office itd.

[7] Testowe (*evaluation, trial*) wersje nawet najlepszych antywirusów po okresie testowym często wyłączają funkcje aktualizacji. Antywirus bez aktualizacji jest bezużyteczny. Jeśli nie możesz kupić pełnej wersji, wybierz produkt, który z założenia jest darmowy. Jeśli podejmujesz decyzję o zakupie, kieruj się wynikami niezależnych testów skuteczności, np. AV Comparatives, AV-Test, Virus Bulletin

Service Pack 2 zmniejsza szanse na wykorzystanie przez złośliwe oprogramowanie luk w systemie. Domyślnie ochrona jest włączona tylko dla podstawowych usług systemowych, należy ją włączyć dla wszystkich programów.[8]

- W systemie Windows Vista i 7[9] pojawiły się zabezpieczenia znacznie skuteczniejsze niż DEP, są one jednak domyślnie wyłączone. Należy je włączyć przy pomocy darmowego programu Microsoft EMET.[10] Jest to prawdopodobnie najskuteczniejsza obecnie metoda ochrony Windows przed nowymi atakami (tzw. ataki zero-day).
- UTM - omawiamy je szczegółowo w rozdziale Urządzenia klasy UTM

Przydatne programy:

- Secunia PSI oraz OSI - sprawdzają Windows i aplikacje pod kątem brakujących poprawek - także te, które nie mają wbudowanej automatycznej aktualizacji
- Darmowe, w pełni funkcjonalne antywirusy to na przykład Microsoft Security Essentials, Avira, Agnitum, BitDefender, ClamAV[11], Avast. Pełne wersje z tańszymi licencjami dla edukacji to na przykład Avast, G Data. Bardzo przydatne administratorm będą także darmowe usługi VirusTotal oraz Anubis, które pozwalają na przesłanie podejrzanych programów. Pierwsza przeskanuje go przy pomocy ok. ~40 różnych antywirusów, druga - uruchomi go w zamkniętym środowisku i opisze podejrzane czynności.
- CloneZilla - narzędzie do tworzenia obrazów całego systemu operacyjnego, umożliwiające odtwarzanie szybkie jego odtwarzanie na jednym lub wielu komputerach w razie infekcji lub awarii.

Niepożądane treści

Internet w szkole jest postrzegany jako zagrożenie ze względu na możliwość uzyskania przez uczniów dostępu do treści nie przeznaczonych dla dzieci i młodzieży. Ochrona przed tego typu treściami jest o tyle kłopotliwa, że mogą one pojawiać się w bardzo wielu źródłach informacji a problematyczne jest samo zdefiniowanie pojęcia “nieodpowiednich treści”.
Stosunkowo łatwo i skutecznie można wyeliminować treści, które bez wątpienia nie powinny pojawiać się w wynikach wyszukiwania w Google - jak np. pornografia. Wszystkie popularne wyszukiwarki mają mechanizmy filtrujące takie wyniki (piszemy o nich poniżej).
Żaden z opisanych mechanizmów nie jest w stu procentach skuteczny, a zdeterminowany uczeń może każdy z nich obejść. Celem działań ochronnych szkoły powinno być zatem zapewnienie takich środków, by uczniowie nie napotykali się na treści nieodpowiednie w wynikach wyszukiwania w Google czy podczas przeglądania filmów w YouTube.
Praktycznie niemożliwe jest uzyskanie pewności, że uczniowie nie natkną się na wulgaryzmy lub nawoływanie do przemocy w komentarzach pod artykułami prasowymi na portalach czy

---

[8] Patrz opis konfiguracji DEP w artykule Microsoft KB875352

[9] Zabezpieczenia dostępne w systemach Windows 7 wykraczają dalece poza zakres tego dokumentu. Można o nich więcej przeczytać w obszernym poradniku “Zalecenia Microsoftu dla systemu operacyjnego Windows 7” opublikowanym przez polski CERT.

[10] Zestaw narzędzi rozszerzonego środowiska ograniczającego ryzyko (EMET)

[11] ClamAV umożliwia skanowanie plików do dysku, ale nie zapewnia bieżącej ochrony podczas uruchamiania plików.

blogach[12].
Od strony technicznej filtrowanie treści (ang. *content filtering*, kontrola rodzicielska) można i należy prowadzić w następujących lokalizacjach:

- na indywidualnych komputerach czy tabletach
    - za pomocą specjalnych, dodatkowych programów;,
    - za pomocą funkcji samych przeglądarek internetowych;
- na poziomie całej sieci,
    - za pomocą filtrów wbudowanych w urządzenia sieciowe (routery, firewalle);
    - za pomocą odpowiednich ustawień sieci.

Większość filtrów treści działa na dwa sposoby:

- przez analizowanie **adresu** strony, którą ładuje użytkownik (np. youtube.com) i sprawdzenie jak została ona sklasyfikowana przez producenta filtra; nieskuteczne, jeśli strona nie jest w ogóle sklasyfikowana - wymaga dostępu do aktualnej bazy klasyfikacji, która jest zwykle usługą płatną;
- przez analizowanie **treści** strony i sprawdzenie, czy nie zawiera ona słów lub wyrażeń zabronionych; może prowadzić do niesłusznego blokowania stron z błahych powodów (np. nazwa “Essex” zawiera zakazane słowo “sex”); nieskuteczne wobec filmów i treści w językach nieprzewidzianych przez autorów narzędzia;

Wybierając rozwiązanie do filtrowania treści należy pamiętać, że jego skuteczność zależy przede wszystkim od aktualności bazy zawierającej klasyfikacje poszczególnych adresów w Internecie. W związku z tym naprawdę skuteczne rozwiązania będą miały charakter usługi z subskrypcją i regularnymi, automatycznymi aktualizacjami, a nie produktu, który kupuje się jednorazowo. Oczywiście, możliwy jest jednorazowy zakup licencji z wliczonymi w cenę aktualizacjami przez jakiś okres czasu.
W przypadku zakupu komercyjnego narzędzia do filtrowania treści należy wziąć pod uwagę następujące kryteria:

- Jaką metodę filtrowania obsługuje - po treści, czy po klasyfikacji adresów? Najlepiej jeśli używane są obie.
- Jak duża jest baza sklasyfikowanych adresów i jak często jest aktualizowana? Liczba stron w Internecie jest liczona w miliardach.
- Na ile elastyczne są kryteria blokowania stron? Najprostsze narzędzia rozróżniają jedynie strony “dobre” i “złe”, a kryteria definiowania tych ostatnich są wewnętrzną sprawą producenta. Narzędzia z najwyższej półki klasyfikują miliony stron na jasno określone kategorie (np. “narkotyki”, “pornografia”) i administrator ma pełną dowolność w definiowaniu, które z nich mają być blokowane.
- Czy narzędzie umożliwia selektywne odblokowywanie stron, które zostały błędnie sklasyfikowane jako niepożądane? Bez tego niemożliwe będzie wejście na “dobre” strony, które narzędzie błędnie uznało za “złe”.
- Czy narzędzie umożliwia blokowanie stron, które nie zostały sklasyfikowane? Podobnie jak wyżej, brak takiej funkcji to luka w ochronie.

[12] Nawet takie treści mają jednak wartość edukacyjną - każdy portal umożliwia zgłaszanie ich jako niestosownych, co jest jednym z elementów aktywnej postawy obywatelskiej. Nie siedźmy i nie czekajmy, aż “ktoś” jest skasuje - róbmy to sami.

- Czy producent oferuje wsparcie techniczne i możliwość zgłaszania błędnie sklasyfikowanych stron?

Poniżej opisujemy kilka popularnych narzędzi, które można wykorzystać do filtrowania stron w szkołach.

Oprogramowanie instalowane na komputerach:[13]

- K9 Web Protection - darmowy filtr treści dostępny dla systemów Windows, MacOS, iOS oraz Android, udostępniany przez firmę BlueCoat, jednego z wiodących producentów korporacyjnych filtrów. Jako taki posiada jedną z najbardziej rozbudowanych i często aktualizowanych baz stron i rozbudowane funkcje chroniące przed wyłączaniem przez użytkowników.
- Microsoft Family Safety - korzysta z klasyfikacji stron zarządzanej przez Microsoft, darmowej dla użytkowników Windows Vista i 7. Umożliwia także filtrowanie gier.
- Google SafeSearch - ustawienie wyszukiwarki Google, darmowe dla wszystkich użytkowników tej wyszukiwarki. Łatwe do obejścia lub wyłączenia, dość skutecznie chroni przed przypadkowym zetknięciem z treściami nieodpowiednimi. Działa także w innych serwiach Google - np. YouTube. Analogiczne ustawienie istnieje w wyszukiwarce Microsoftu - Bing SafeSearch.
- Polskie programy Cenzor i Strażnik Ucznia, ukierunkowane głównie na rynek edukacyjny i domowy, ze stosunkowo niedrogimi licencjami dla szkół. Dobrze dostosowane do specyfiki języka polskiego, stosunkowo łatwe do obejścia.

Rozwiązania działające na poziomie całej sieci:

- OpenDNS FamilyShield, usługa działająca na poziomie DNS, chroniąca zarówno przed stronami dla dorosłych jak i stronami zawierającymi wirusy itd.[14]
- DansGuardian - darmowy system filtrujący dla systemu Linux, zintegrowany z serwerem proxy, a więc przeznaczony do instalacji na serwerach służących jako zapora i brama do Internetu. Ma wbudowane filtrowanie po słowach kluczowych oraz możliwość ładowania klasyfikacji stron, które są dostępne komercyjnie (np. URLBlacklist, koszt ok. 200 zł rocznie). Wymaga administratora znającego się na obsłudze Linuksa. Trudny do obejścia jeśli jest to jedyna brama do Internetu w sieci szkolnej.
- UTM - najskuteczniejsze i najbardziej rozbudowane, ale równocześnie kosztowne. Omawiamy je szczegółowo w rozdziale Urządzenia klasy UTM

Większość narzędzi sieciowychmożna łączyć z narzędziami działającymi na komputerach w celu zwiększenia skuteczności.

Sieci bezprzewodowe

[13] Należy pamiętać, że większość programów instalowanych na komputerach uczniów może zostać stosunkowo łatwo wyłączona i w Internecie można znaleźć mnóstwo poradników obchodzenia popularnych w polskich szkołach programów. Istnieją specjalne strony służące jako pośrednicy do ładowania innych zablokowanych stron - np. nkac.pl.

[14] Cała konfiguracja OpenDNS sprowadza się do przestawienia na komputerach i routerze adresów serwerów DNS na 208.67.220.123 oraz 208.67.222.123. Usługa zablokuje odwołania do stron o nazwach sklasyfikowanych jako strony pornograficzne lub niebezpieczne, ale także do stron służących obchodzeniu filtra (w tym wymieniony powyżej nkac.pl).

Sieci bezprzewodowe (WiFi) są obecnie standardową technologią sieci komputerowych, szybko wypierającą tradycyjne sieci kablowe (Ethernet). Główną ich zaletą jest właśnie brak konieczności kładzenia kosztownego okablowania, co jest problemem zwłaszcza w instytucjach zajmujący budynki zabytkowe. Wiele współczesnych urządzeń w ogóle nie ma gniazd dla sieci kablowej i mogą się łączyć z Internetem głównie przez WiFi.
Najczęściej spotykanym układem jest podłączenie bezprzewodowego urządzenia dostępowego (*Access Point* - AP) bezpośrednio do sieci lokalnej (LAN) tak, by osoby uprawnione do korzystania z WiFi miały dostęp do szkolnych zasobów. W takim przypadku zagrożenie jest oczywiste - dostęp do sieci musi być właściwie zabezpieczony. Na szczęście większość dostępnych na rynku urządzeń, nawet tych najtańszych, oferuje wystarczający poziom bezpieczeństwa - wystarczy je poprawnie skonfigurować.
Kluczowe dla bezpieczeństwa sieci WiFi są następujące parametry konfiguracyjne:

- Szyfrowanie połączeń bezprzewodowych. Należy zawsze ustawiać szyfrowanie **WPA2** lub **WPA**. Nie należy w ogóle udostępniać sieci nieszyfrowanych (*Open*, *Shared*). Nie należy pod żadnym pozorem korzystać z szyfrowania WEP gdyż jest ono słabe i zostało dawno złamane.
- Obie zalecane metody (WPA2 i WPA) są bezpieczne wyłącznie pod warunkiem użycia **dobrego hasła** (patrz rozdział Bezpieczeństwo haseł).

Popularne w przypadku większych instytucji jest zakładanie dwóch sieci bezprzewodowych - pierwszej, przeznaczonej do użytku wewnętrznego i podłączonej do sieci lokalnej szkoły, oraz drugiej, dla gości.
W przypadku sieci bezprzewodowych mających połączenie z siecią lokalną szkoły zalecane jest podłączanie ich przez zaporę sieciową (*firewall*) oraz wykorzystanie indywidualnych danych do logowania (nazwa uzytkownika i hasło) dla każdego użytkownika.
Sieć dla gości (np. rodziców lub osób korzystających z pomieszczeń wynajmowanych przez szkołę) nie powinna mieć żadnego połączenia z siecią lokalną - daje ona po prostu dostęp do Internetu. Powinna być ona również szyfrowana, wspólne dla wszystkich hasło można udostępniać uprawnionym osobom np. za pośrednictwem tablicy ogłoszeń, recepcji itd.
Pod żadnym pozorem nie należy udostępniać sieci pozbawionych całkowicie kontroli dostępu (czy to za pomocą szyfrowania, czy to logowania typu hot-spot). W przeciwnym razie sieć zostanie szybko wykorzystana jako darmowy dostęp do Internetu przez okolicznych mieszkańców i firmy, a w przypadku ewentualnych przestępstw dokonywanych za jej pośrednictwem pierwszym podejrzanym będzie operator czyli szkoła.

Urządzenia mobilne

Urządzenia mobilne - tablety i smartfony - z systemami operacyjnymi Android oraz Apple iOS są atrakcyjnymi celami dla złośliwego oprogramowania. Bardziej są na niego narażeni użytkownicy systemu Android, ponieważ model dystrybucji oprogramowania nie jest tak scentralizowany i sformalizowany jak w przypadku Apple.

Android

Z punktu widzenia użytkownika tabletu lub smartfonu z systemem Android instalacja oprogramowania jest bardzo łatwa. Wystarczy uruchomić domyślnie zainstalowaną aplikację Google Play by móc znaleźć i zainstalować jedną z tysięcy gier i innych "fajnych" programów. Pomimo, że Google stara się usuwać ze sklepu programy ewidentnie złośliwe, to i tak są one tam nieustannie dodawane[15].
Programy na Androida można także instalować z dowolnego innego źródła w postaci plików instalacyjnych APK. Wymaga to jedynie *wyłączenia* opcji "Zezwól na instalację aplikacji z nieznanych źródeł" (domyślnie jest *włączona*).
Wiele złośliwych stron będzie próbowało wykorzystać ten fakt i "podrzucić" zainfekowany plik APK użytkownikowi, który miał pecha na nie trafić. Dlatego istotne jest, by opcja ta była zawsze włączona. Bardzo istotne jest także edukowanie użytkowników, aby czytali "ze zrozumieniem" regulamin użytkowania aplikacji; bardzo często użytkownik klika "OK" bez zastanowienia się, jakie może to nieść za sobą konsekwencje.
Dla Androida jest dostępnych także wiele programów antywirusowych, które działają podobnie jak ich "pecetowe" odpowiedniki. W styczniu 2013 organizacja konsumencka AV-Test jako najskuteczniejszy wskazała darmowy program TrustGo, a w maju - komercyjny BitDefender. Najlepszym rozwiązaniem wydaje się więc monitorowanie aktualnych rankingów antywirusów dla urządzeń mobilnych AV-Test i wybranie narzędzia o najlepszym stosunku ceny do jakości. Pewnym rozwiązaniem może być też stworzenie lokalnego źródła instalacji sprawdzonych i zaufanych plików APK i zablokowanie możliwości pobierania innych aplikacji[16]. W takim przypadku przydatna będzie darmowa usługa ApkScan, która umożliwia skanowanie plików APK pod kątem ewentualnych zagrożeń.

Szkolne zasoby w Internecie

Wszystkie ankietowane przez nas szkoły mają swoje własne strony internetowe, połowa z nich umieszcza również swoje dane na stronach firm trzecich - na przykład w dziennikach internetowych. We wszystkich tych przypadkach istnieje realne ryzyko, że osoby z zewnątrz znajdą w tych stronach błędy programistyczne i wykorzystają je z niekorzystnymi konsekwencjami dla szkoły. W najlepszym przypadku będzie to wandalizm - np. umieszczenie na szkolnej stronie wulgaryzmów lub haseł politycznych, w najgorszym - kradzież danych osobywych lub inne ataki skutkujące wymiernymi stratami finansowymi.
Rynek przestępczości komputerowej od początku XXI wieku szybko się profesjonalizuje. Zanikają ataki na strony wykonywane "dla zabawy", obecnie jest to przede wszystkim biznes. Przejęte przez włamywaczy komputery szybko zaczynają służyć jako darmowe "stacje przesiadkowe" do wysyłania spamu i innych ataków. Dlatego niezbędna jest maksymalna

[15] Na przykład w kwietniu 2013 przestępcom udało się umieścić w sklepie ponad 30 atrakcyjnych aplikacji zainfekowanych wirusem BadNews, który wyłudzał pieniądze za pomocą połączeń telefonicznych i SMSów na numery premium. Zanim zostały one usunięte użytkownicy pobrali je ponad 2 mln razy.
[16] Do blokowania instalacji niezatwierdzonych aplikacji w systemie Android można wykorzystać aplikacje SureLock, AppProtectorPro i inne. Można także zablokować pobieranie plików APK na zaporze sieciowej lub serwerze *proxy*. Należy jednak pamiętać, że w urządzeniach z Wi-Fi lub 3G będzie można je nadal pobrać z pominięciem sieci lokalnej.

ochrona komputerów używanych w szkole przez nauczycieli i uczniów. Bardzo dobrym przykładem może być tutaj system operacyjny Linux, na którym praktycznie nie ma w chwili obecnej wirusów ani innego złośliwego oprogramowania[17] - zatem może być idealnym rozwiązaniem dla szkół.
Bezpieczeństwo stron internetowych szkoły należy planować od samego początku, przed podjęciem jakichkolwiek innych działań. Nie jest to bynajmniej "czarna magia" i większość osób, które umieją programować bez problemu przyswoi sobie opisane poniżej zasady. Większość włamań na strony ma miejsce w instytucjach, które nie zdawały sobie z tych zasad pojęcia!.
Przystępując do budowy własnej strony internetowej należy zadać sobie następujące pytania:

1. Czy wiemy w jaki sposób **programować bezpiecznie** w wybranej technologii? Większość pułapek programistycznych skutkujących później włamaniem to błędy oczywiste, łatwe do uniknięcia - jeśli się o nich wie.
2. Samo uruchomienie strony to dopiero początek pracy. Czy jest wyznaczona **osoba odpowiedzialna** za późniejsze utrzymanie serwera i strony? Oprogramowanie serwera obsługującego stronę musi być bezwzględnie **aktualizowane** - co najmniej w cyklu miesięcznym. Serwer pozostawiony sam sobie z pewnością padnie ofiarą włamywaczy.
3. Czy **testujemy bezpieczeństwo** naszej strony? Powinniśmy to zrobić co najmniej raz, tuż przed jej umieszczeniem w Internecie i oficjalną publikacją. Testy należy następnie powtarzać przynajmniej co kilka lat, ze względu na pojawiające się nowe ataki na strony [18].

Zarządzanie bezpieczeństwem stron umieszczanych w Internecie przez szkołę nie musi być procesem kosztownym. Niezależnie od tego, czy są one wykonywane siłami nauczycieli lub uczniów, czy zlecane na zewnątrz, przestrzeganie kilku prostych zasad pozwoli uniknąć problemów w przyszłości.

Zamawiać czy budować własnymi siłami?

Większość szkół ma strony internetowe - czy wręcz całą infrastrukturę komputerową - zbudowaną siłami własnymi pracowników, uczniów i rodziców. Jest to rozwizanie najtańsze i pozwalające maksymalnie wykorzystać dostępny sprzęt, często pochodzący z "demobilu" z firm i innych instytucji.
Samodzielna budowa strony internetowej przez szkolną wspólnotę jest doskonałą metodą budowania kompetencji technicznych, które później procentują w całym życiu zawodowym. Ponieważ do pracy biorą się jednak amatorzy, może to być proces długotrwały a efekt niekoniecznie musi odpowiadać oczekiwaniom.

Zalety	**Wady**

[17] Znane są tylko przypadki wirusów "laboratoryjnych"
[18] Bezpieczeństwo strony internetowej nie zależy wyłącznie od kodu HTML, w którym została napisana oraz aplikacji, która ją obsługuje. Wprowadzanie do przeglądarek nowych funkcji języka HTML skutkuje pojawianiem się nowych metod ataku nawet na stronach, które wcześniej były bezpieczne.

● Niski koszt kapitałowy - głównym nakładem jest czas poświęcony nauczycieli i uczniów ● Przyswajanie nowych kompetencji takich jak zarządzanie projektami, praca w zespole, programowanie, tworzenie stron WWW ● Możliwość wielokrotnych zmian, budowania prototypów i dowolnego rozszerzania oraz dopasowywania do potrzeb szkoły	● Stworzenie w pełni funkcjonalnej strony może zająć sporo czasu ● Strona może zawierać liczne błędy i podatności ● Trudne określenie jednoznacznych wymagań funkcjonalnych i jakościowych

Zlecając wykonanie strony na zewnątrz unikamy długotrwałego i pracochłonnego procesu uczenia się nowych technologii, w zamian dostając konkretny produkt - działającą stronę. Działa tutaj jednak zasada, że zamawiający dostaje to co sobie zamówił. Wiele instytucji ma problemy z poprawnym opisaniem swoich wymagań funkcjonalnych, nie mówiąc już o jakościowych (i w tym bezpieczeństwa).

Zalety	**Wady**
● W pełni funkcjonalna wersja strony dostępna w ustalonym terminie ● Możliwość egzekwowania wymagań jakościowych i funkcjonalnych	● Konieczność zapewnienia od kilku do kilkudziesięciu tysięcy złotych na stworzenie strony ● Konieczność jednorazowego, precyzyjnego opisania wymagań funkcjonalnych i jakościowych ● Strona może nadal zawierać błędy i podatności ● Samo zamówienie strony bez umowy na jego utrzymanie i braku kompetentnych osób wewnątrz instytucji gwarantuje, że po paru latach strona będzie podatna na ataki.

Podsumowując, zatrudnienie zewnętrznej firmy zwiększa prawdopodobieństwo uzyskania produktu wysokiej jakości (i bezpiecznej), ale w żadnym wypadku go nie gwarantuje. Rynek ten jest wciąż stosunkowo niedojrzały, brak jest na nim utrwalonych standardów jakości czy opisu wymagań projektowych.
Zamawiający musi wiedzieć czego chce i musi umieć to poprawnie nazwać oraz opisać. Jeśli takich umiejętności nie mamy to możemy poszukać produktu gotowego (“z półki”), który mniej

więcej będzie odpowiadał naszym potrzebom. Jeśli wymagamy produktu dostosowanego do naszych potrzeb to należy zamówienie zrealizować dwuetapowo:

- Najpierw zamawiamy usługę polegającą na **analizie potrzeb** i przełożeniu ich na język projektów informatycznych oraz dokumenty przetargowe (SIWZ).
- Na tej podstawie zamawiamy właściwy **system informatyczny**. Podmioty wykonujące oba zamówienia powinny być od siebie niezależne. Podmiot sporządzający dokumentację warto również wykorzystać przy odbiorze finalnego produktu.

Poniżej skupiamy się na typowych projektach informatycznych w edukacji - każdy z nich ma swoją specyfikę.

Ryzyka związane z serwisami internetowymi

Strony internetowe szkół spełniają najczęściej rolę informacyjną - stanowią publicznie dostępną witrynę ogłoszeniową, zawierającą dane kontaktowe, kalendarze, aktualności czy zdjęcia z uroczystości.

Strony tego typu od strony technicznej oparte są o najczęściej o oprogramowanie do zarządzania treściami (CMS. *Content Management System*). Nazwą tą określa się aplikacje internetowe, których główną funkcją jest zarządzenie publikacją stron w różnej postaci. W edukacji dominują darmowe aplikacje dostępne z kodem źródłowym (*open-soure*)[19]. Jeśli chodzi języki programowania to dominuje język PHP, który jest stosunkowo łatwy w nauce i elastyczny. Jest to także język, który dzięki swojej elastyczności wybacza wiele błędów popełnianych przez niedoświadczonych programistów. Niestety, ma to poważne konsekwencje dla bezpieczeństwa stron kiedy już zostaną one opublikowane w Internecie

Ryzyko	**Przyczyna**	**Zabezpieczenia**
Przejęcie kontroli nad panelem administracyjnym	Słabe hasła	Stosuj silne hasła
Przejęcie kontroli nad aplikacją CMS	Nowoodkryte błędy w CMS, które nie zostały załatane na czas. Łatwe do znalezienia błędy w samodzielnie napisanej aplikacji.	Regularnie czytaj aktualne ogłoszenia o nowych dziurach w swojej aplikacji CMS[20]. **Poprawiaj błędy natychmiast po publikacji**.
Przejęcie kontroli nad całym systemem operacyjnym serwera	Brak aktualizacji systemu operacyjnego.	Zawsze włączaj automatyczne aktualizacje w systemie operacyjnym serwera.

[19] Do popularnych darmowych CMS należy Drupal, WordPress, Joomla (wszystkie w języku PHP). Systemem tej klasy jest też Microsoft SharePoint (komercyjny) oraz darmowe Windows SharePoint Services (programowane w ASP.NET).

[20] Każdy szanujący się projekt CMS prowadzi listę z informacjami o nowych błędach:Drupal, Joomla.

Serwisy informacyjne i transakcyjne

Z punktu widzenia funkcjonalności serwisy internetowe możemy podzielić na **informacyjne** i **transakcyjne**. Te pierwsze są z zasady dostępne dla wszystkich - zawierają ogólnodostępne informacje i ogłoszenia. Serwisy transakcyjne są dostępne dla uprawnionych użytkowników i służą do wykonywania określonych operacji.
Najprostszym przykładem serwisu informacyjnego jest publiczna strona szkoły. Jeśli strona ta bedzie zawierać specjalny panel administracyjny to ta część serwisu będzie przykładem części transakcyjnej. Serwisem transakcyjnym będzie również osobny dziennik internetowy, system obiegu dokumentów czy poczta elektroniczna.
Rozróżnienie to ma dość istotne konsekwencje z punktu widzenia **skutków** ewentualnego włamania i związanych z nim strat.

Serwis informacyjny	**Serwis transakcyjny**
● Zmiana treści strony ● Szkody wizerunkowe	● Wyciek danych ● Szkody finansowe, kontraktowe i karne

Jak widać, utrzymanie serwisów transakcyjnych wiążą się ze znacznie większymi potencjalnymi stratami niż utrzymanie prostego serwisu informacyjnego.
Ze względu na to, że dzienniki internetowe zyskują obecnie popularność i jest to oprogramowanie praktycznie zawsze zamawiane w firmach zewnętrznych, należy zwrócić szczególną uwagę na poprawne określenie wymagań bezpieczeństwa wobec tych serwisów.

Określanie wymagań bezpieczeństwa

W przypadku stron zamawianych u zewnętrznych dostawców zamawiający musi wprost wskazać następujące wymagania związane z bezpieczeństwem. Poniżej “serwis” oznacza całość stron składających się na daną witrynę internetową wraz z oprogramowaniem, “strony” oznaczają pojedyncze podstrony serwisu.

- Wykonawca stosuje dobre praktyki bezpiecznego programowania i tworzenia oprogramowania, takie jak OWASP Development Guide (2005), Microsoft SDL lub równoważne.
- Wykonawca stosuje dobre praktyki bezpieczeństwa dla wybranej platformy programistycznej, udostępnione przez producenta lub społeczność programistów, takie jak OWASP Developer Cheatsheets dla danej platformy.
- Serwis jest, wedle najlepszej wiedzy wykonawcy, odporny na ataki przeciwko aplikacjom sklasyfikowanym w WASC Threat Classification, NIST Common Weakness Enumeration (CWE) lub równoważnych klasyfikacjach.
- Serwis zawiera listę stron wyłączonych z indeksowania przez wyszukiwarki zgodną z Robots Exclusion Standard (robots.txt), zawierającą co najmniej adresy stron

zastrzeżonych do użytku osób uprawnionych w danym serwisie[21].

- Odporność na ataki jest potwierdzona za pomocą testu penetracyjnego lub skanu bezpieczeństwa serwisu, przeglądu lub skanu kodu źródłowego oprogramowania wykonanego przez osoby inne niż zespół projektujący i tworzący dany serwis (patrz Testowanie bezpieczeństwa).
- Usługa wsparcia technicznego lub gwarancji na dany serwis obejmuje również bezzwłoczną instalację poprawek błędów bezpieczeństwa opublikowanych lub zgłoszonych wykonawcy.

Powyższe wymagania mają charakter wytycznych, które należy dostosować do specyfiki zamawianego serwisu oraz specyfiki polskiego prawa zamówień publicznych, zgodnie z wytycznymi do zamawiania systemów informatycznych opublikowanymi przez Urząd Zamówień Publicznych.

Serwery i chmury obliczeniowe

Rynkowa oferta dla instytucji chcących utrzymywać swoje strony w Internecie jest bardzo bogata. Typowymi usługami są:

- Serwery wirtualne (VPS) - maszyna wirtualna z wybranym przez zamawiającego systemem operacyjnym, działający w ramach fizycznego serwera, współdzielony z wieloma innymi użytkownikami. Z punktu widzenia użytkownika VPS jest całkowicie autonomicznym systemem operacyjnym, jednak izolacja od innych maszyn wirtualnych ma charakter wyłącznie logiczny, nie fizyczny.
- Serwery dedykowane - fizyczny serwer umieszczony w serwerowni dostawcy, przydzielony na wyłączoność zamawiającemu. Izolacja od serwerów innych klientów ma charakter fizyczny.
- Chmura obliczeniowa - wyższa forma wirtualizacji, do której klient ładuje wyłącznie aplikację i nie ma dostępu do systemu operacyjnego serwera. Chmury obliczeniowe oferują w standardzie proste usługi bazodanowe, a opłacie podlega np. maksymalna liczba procesów, miejsce na dysku lub ruch sieciowy generowany przez aplikację.

Wszystkie wymienione usługi są oferowane przez licznych dostawców krajowych i zagranicznych, w Unii Europejskiej i poza nią. Rozpiętość cen jest bardzo duża i pozwala znaleźć dostawcę dostępnego dla instytucji praktycznie z każdym budżetem i potrzebami. Wybór tych metod ma istotne znaczenie z punktu widzenia bezpieczeństwa. W każdym przypadku ktoś - albo właściciel serwisu albo platformy hostingowej - musi być odpowiedzialny za bezpieczeństwo serwisu i jego danych ale zakres tej odpowiedzialności może być różny. W przypadku serwera lokalnego sprawa jest jasna - jego właścicielem i operatorem jest szkoła. W przypadku utrzymania na serwerze zewnętrznym odpowiedzialność ta nie jest już tak jednoznaczna i jej konkretny zakres musi wynikać z umowy:

---

[21] Kontrola właściciela strony nad wyszukiwarkami internetowymi jest często lekceważona. Tymczasem to właśnie wyszukiwarki są często pierwszym narzędziem, przy pomocy którego włamywacze wyszukują ofiary. Wyszukiwarki także przez jakiś czas “pamiętają” strony nawet jeśli skasowano je z oryginalnego serisu (GIODO przypomina jak zabezpieczać serwisy przed wyciekiem). Najprostszą metodą jest stworzenie pliku robots.txt, zalecane jest zarejestrowanie strony w Google Webmaster Tools i Bing Webmaster Tools.

- Kto odpowiada za tworzenie kopii zapasowych oprogramowania serwera, aplikacji i bazy danych?
- Jaka jest częstotliwość ich tworzenia?
- Kto odpowiada za ich odtworzenie w razie awarii?
- Po jakim czasie zostaną one odtworzone, a serwis przywrócony do stanu poprzedniego?
- Kto odpowiada za instalowanie aktualizacji systemu operacyjnego?
- Jak szybko po ich publikacji przez producenta zostaną one zainstalowane?
- Jakie gwarancje daje dostawca jeśli chodzi o bezpieczeństwo fizyczne serwerów?

Serwisy utrzymywane w chmurze obliczeniowej należy traktować podobnie jak utrzymywane na zewnętrznych serwerach hostingowych, z kilkoma różnicami. Operatorzy chmur oferują zwykle kilka standardowych abonamentów, w których opisane wyżej warunki są z góry określone.
Jeśli w danej aplikacji chcemy przetwarzać dane osobowe to musimy mieć możliwość określenia geograficznej lokalizacji danych. W przypadku chmur może to być utrudnione (patrz też Ochrona danych osobowych).
W praktyce dane wrażliwe utrzymywane są wyłącznie na serwerach fizycznych będących w wyłącznej dyspozycji właściciela, czyli w jego własnej serwerowni. Dane mniej wrażliwe można utrzymywać na serwerach dedykowanych pod warunkiem zawarcia w umowie z dostawcą odpowiednich gwarancji dotyczących dostępu do serwerów i zawartych na nich danych. Dane jawne można z powodzeniem przetwarzać na serwerach wirtualnych i chmurach.

Obowiązki prawne

Ochrona danych osobowych

Ustawa o ochronie danych osobowych nakłada na instytucje przetwarzające dane osobowe - w tej liczbie także szkoły i dane uczniów - szereg obowiązków związanych z ich należytym zabezpieczeniem.
Z punktu widzenia bezpieczeństwa obowiązki te nie powinny stanowić dla nikogo szczególnego zaskoczenia. Są one jawnym, sformalizowanym ustanowieniem zasad dobrze znanych w branży bezpieczeństwa. W szczególności należy zadbać o poufność przetwarzanych danych osobowych za pomocą:

- środków organizacyjnych zgodnie z zasadą wiedzy koniecznej - dostęp do danych wrażliwych powinny mieć tylko osoby, którym ten dostęp jest niezbędny ze względu na wykonywane obowiązki; należy opisać procedury:
    - przyznawania tego dostępu,
    - jego odbierania (np. w razie zwolnienia lub przeniesienia do innego działu),
    - cyklicznego weryfikowania listy uprawnionych osób;
- uwierzytelnienie użytkowników mających dostęp do danych - na przykład za pomocą loginu i hasła lub odpowiednich uprawnień dostępu w systemie operacyjnym;
- szyfrowania danych osobowych oraz haseł przesyłanych przez sieć - np. za pomocą protokołu HTTPS, jeśli chodzi o serwisy internetowe..

Przydatne odnośniki:

- GIODO Opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36−39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
- GIODO: Ochrona prywatności w systemach teleinformatycznych

Cookies (“ciasteczka”)

W 2009 roku weszła w życie nowelizacja europejskiej dyrektywy o prywatności (2009/136/WE), co skutkowało koniecznością nowelizacji polskiego prawa telekomunikacyjnego. W rezultacie od 2013 roku operatorzy polskich stron są zobowiązani do przedstawiania odwiedzającym szczegółowej informacji o danych zapisywanych przez stronę w ich przeglądarkach (tzw. ciasteczkach - “cookies”)[22].
Konkretny sposób realizacji tego obowiązku jest różnie interpretowany. Większość stron komercyjnych - dla uniknięcia ewentualnych sporów interpretacyjnych - wyświetla wyraźne okno z informacjami o stosowaniu ciasteczek, zasłaniajace część strony i wymagające kliknięcia. Z drugiej strony większość stron rządowych realizuje ten obowiązek przez umieszczenie dobrze widocznego (na górze strony) odnośnika do podstrony, zawierającej szczegółowe informacje o stosowanych ciasteczkach[23].
Nie ma zatem powodu by stosować techniki dalej idące niż te stosowane np. na stronach GIODO.

Testowanie bezpieczeństwa

O ile samo tworzeniem aplikacji i stron internetowych można się zajmować praktycznie wyłącznie przy pomocy narzędzi całkowicie darmowych lub bardzo tanich, o tyle z testowaniem ich bezpieczeństwa jest pewien problem.
Rynek ten jest zdominowany przez dostawców profesjonalnych usług i produktów, które są niestety dość kosztowne. Stosunkowo niewiele jest na nim narzędzi darmowych lub ze średniej półki - a przynajmniej takich, które dają miarodajne rezultaty.
Dostępne techniki testowania bezpieczeństwa aplikacji i stron internetowych można podzielić na statyczne i dynamiczne.

Analiza statyczna

Analiza statyczna to analiza bezpieczeństwa kodu źródłowego[24]. Jest to metoda pozwalająca na wyeliminowanie potencjalnie największej ilości błędów z aplikacji, zanim jeszcze ujrzy ona światło dzienne. Analiza kodu źródłowego wymaga oczywiście dysponowania tym kodem, stąd jest stosowana głównie przez właścicieli aplikacji pisanych na ich wyłączne zamówienie, lub

---

[22] Paweł Krawczyk, *“Cookies - niedźwiedzia przysługa”*, Computerworld, 27 kwietnia 2012
[23] Jednym z obowiązków nakładanych przez nowe przepisy jest poinformowanie odwiedzających o rodzaju i przeznaczeniu ciasteczek stosowanych przez naszą stronę. W zebraniu tych informacji pomoże serwis WebCookies.info.
[24] Analiza kodu jest określana jako “analiza statyczna” - SAST (*static application security testing*) lub SCA (*static code analysis*) - ze względu na to, że skanowany jest “statyczny” kod źródłowy, dla odróżnienia od “analizy dynamicznej” czyli testowania działającego prototypu aplikacji.

producentów oprogramowania rynkowego. W przypadku zakupu tego ostatniego nic nie stoi na przeszkodzie, by jednym z kryteriów zamówienia uczynić wykonywanie takich analiz. Analiza kodu źródłowego może być wykonywana:

- **ręcznie** (*manual code review*) - jest procesem kosztownym ze względu na czasochłonność i wysokie kwalifikacje zatrudnionych przy tym specjalistów. Daje wysoki poziom precyzji i umożliwia wskazanie błędów trudnych do znalezienia innymi metodami.
- **automatycznie** - pozwala na szybkie, częste i cykliczne skanowanie kodu źródłowego w poszukiwaniu błędów, nie tylko związanych z bezpieczeństwem. Na rynku dostępnych jest wiele narzędzi, zarówno komercyjnych jak i darmowych, jednak ich poziom jest bardzo nierówny. Obszerną ich listę można znaleźć na Wikipedii, zaś na uwagę zasługują:
    - Yasca - darmowy, napisany w PHP skaner
    - Brakeman - darmowy skaner dla aplikacji napisanych w Ruby on Rails.
    - RIPS - darmowy skaner dla aplikacji napisanych w PHP
    - CAT.NET (ASP.NET), MSSCASI (ASP) - dwa darmowe narzędzia Microsoftu.
    - Armorize CodeSecure - najtańszy (ok. 10 tys. zł rocznie) skaner komercyjny, obsługujący wiele języków, w tym Javę i ASP.NET. Ceny innych dostawców w tej klasie zaczynają się ok. 10x wyżej.

Analiza statyczna ma jedną istotną przewagę na analizą dynamiczną opisaną poniżej - może być prowadzona od pierwszej linijki kodu, zanim powstanie jakikolwiek działający prototyp aplikacji. Narzędzia do analizy statycznej często są zintegrowane ze środowiskiem programistycznym, wskazując programistom błędy od razu po ich popełnieniu[25].

Analiza dynamiczna

Analiza dynamiczna polega na testowaniu bezpieczeństwa **działającego prototypu aplikacji** wraz z całym otaczającym ją środowiskiem - bazą danych, serwerem itd. Podobnie jak analiza statyczna może ona być wykonywana dwoma metodami:

- **ręcznie** - czyli przez zespół specjalistów. W takim przypadku określa się ją mianem **testów penetracyjnych**. Podobnie jak w przypadku analizy statycznej, ręczne testy penetracyjne zapewniają o wiele wyższy poziom dokładności - umożliwiają znalezienie większej ilości błędów przy mniejszej ilości fałszywych alarmów. Testy ręczne umożliwiają także wskazanie subtelnych błędów, niemożliwych do znalezienie przez narzędzia automatyczne (tzw. błędów logiki biznesowej). Na rynku polskim należy liczyć się z cenami rzędu kilkudziesięciu tysięcy złotych za test pojedynczej aplikacji. Testowanie bezpieczeństwa aplikacji jest samo w sobie bardzo pouczające i dostępnych jest wiele darmowych narzędzi, które takie testy wspomagają:
    - BurpSuite
    - Zed Attack Proxy

[25] Doskonałym, darmowym narzędziem tego typu jest Lapse+ czyli dodatek do popularnego narzędzia progamistycznego Eclipse, znajdujący błędy w programach w języku Java.

    - WebScarab
- **automatycznie** - czyli przez narzędzia (skanery), symulujące ataki na aplikację. Narzędzia te charakteryzują się niższą zdolnością do znajdowania błędów i większą ilością fałszywych alarmów, mają jednak szereg zalet: niższy koszt niż testy ręczne, stosunkowo szybkie skanowanie nawet bardzo rozbudowanych aplikacji i możliwość skanowania dużej liczby serwisów w stosunkowo krótkim czasie. Przeważnie nie mają one problemów ze znalezieniem poważnych, "ziejących" dziur, łatwych do znalezienia także przez włamywaczy.
    - CERT.GOV.PL - komórka rządowa działająca przy ABW na rzecz bezpieczeństwa teleinformatycznego jednostek polskiej administracji; świadczy darmowe szkolenia z bezpieczeństwa dla urzędników (najbliższe planowane na 2013 rok), testowanie bezpiczeństwa stron oraz - przede wszystkim - pomoc w przypadkach włamań i innych incydentów związanych z bezpieczeństwem
    - Qualys Free Scan - darmowa usług stanowiaca "próbkę" komercyjnego skanera Qualys; skupia się na bezpieczeństwie serwera, trochę dotykając także aplikacji;
    - Detectify, ScanMyServer, WebGuard, GamaSec, 6Scan, ArmorHub - usługi skanowania bezpieczeństwa stron pod kątem typowych podatności. W przypadku Detectify pierwszy skan jest darmowy (użytkownik przy rejestracji otrzymuje 1 darmowy kupon kredytowy, kolejne trzeba kupić).
    - Norton Safe Web, Sucuri SiteCheck - darmowe usługi polegająca na przeskanowaniu naszej strony pod kątem obecności złośliwego oprogramowania zainstalowanego w wyniku wcześniejszych udanych ataków.
    - iViz Free Website Security Testing - darmowa oferta indyjskiego dostawcy komercyjnego skanera iViz, z długim czasem oczekiwania na skan;
    - WebCookies.info - prosty skaner ciasteczek ustawianych przez daną stronę sprawdzający także kilka opcji bezpieczeństwa.
    - Netsparker Community Edition, N-Stalker Free Edition - darmowe wersje popularnych skanerów komercyjnych (instalowane jako aplikacje dla Windows).
    - w3af, sqlmap, xsser, skipfish, metasploit - darmowe narzędzia do testowania bezpieczeństwa stron i serwerów wymagające wiedzy specjalistycznej.

Dynamiczna czy statyczna?

Analiza dynamiczna **nie** jest równoważną alternatywą dla analizy statycznej. Analiza dynamiczna ma znacznie szerszy zakres - obejmuje nie tylko samą aplikację, ale całe działające środowisko, w tym konfigurację serwera, w której rónież można popełnić wiele błędów.
Obie metody należy zatem stosować równocześnie. Tu pojawia się jednak nieuniknione pytanie - skąd brać na to wszystko pieniadze?
Powyżej wskazane jest co najmniej kilka darmowych lub tanich narzędzi do analizy zarówno statycznej jak i dynamicznej. Dostępność, skuteczność i cena tych narzędzi jest bardzo różna dla różnych języków programowania, a dostawcy z reguły bez problemu zgadzają się na darmowe testy.

Należy zamówić narzędzie lub usługę o najlepszym stosunku ceny do jakości dla danego środowiska, a równocześnie samemu wykorzystać do maksimum dostępne narzędzia darmowe. Nawet darmowy skaner kodu źródlowego pozwala często wyłapać krytyczne błędy, które nigdy nie zostaną ujawnione w teście penetracyjnym. Nawet jeśli nie będą to **wszystkie** błędy, to nasz poziom ryzyka i tak się zmniejszy.

Audyty, testy penetracyjne...?

Branża testów bezpieczeństwa aplikacji jest wciąż niezbyt dojrzała i panuje na niej spore zamieszanie, zwłaszcza jeśli chodzi o terminologię. Dostawcy prześcigają się w wymyślaniu coraz bardziej rozbudowanych nazw oferowanych przez siebie usług i narzędzi. W praktyce wszystkie sprowadzają się do tych opisanych powyżej. W uporządkowaniu terminologii pomocne mogą być następujące uwagi:

- **test penetracyjny** jest wykonywany przez ludzi, którzy mogą korzystać z narzędzi automatycznych, ale większość testów jest wykonywana ręcznie; jeśli stosowane są głównie narzędzia to mamy do czynienia ze **skanem bezpieczeństwa**;
- **audyt bezpieczeństwa** nie jest synonimem testu penetracyjnego lub skanu; audyt musi być prowadzony *w odniesieniu* do *czegoś* - polityki bezpieczeństwa, normy (np .ISO 27001), przepisów; ponieważ brak jest ścisłych standardów bezpieczeństwa aplikacji, więc testy penetracyjne są prowadzone na podstawie najlepszej, aktualnej wiedzy wykonawców a nie standardów - nie należy więc ich nazywać audytami[26];

Profilaktyka bezpieczeństwa stron internetowych

Testy pozwalają na wyłapanie i naprawienie błędów bezpieczeństwa zanim aplikacja zostanie udostępniona publicznie. Na tym jednak nie koniec - nowe błędy są często odkrywane już w trakcie jej eksploatacji. Nie muszą to być błędy w samej stronie (które powinny wyjść w testach) - mogą one wystąpić w systemie operacyjnym i komponentach używanych do budowy strony. Dlatego bezpieczeństwo serwisu musi mieć charakter wielopoziomowy.

- Do systemów operacyjnych i innego oprogramowania na serwerach stosujmy dokładnie te same zasady, o których pisaliśmy wyżej w rozdziale Złośliwe oprogramowanie. Kluczowe są **częste aktualizacje** oraz dodatkowe zabezpieczenia na poziomie systemu operacyjnego, takie jak EMET dla Windows czy AppArmor dla Linuksa.
- Hasła do paneli administracyjnych muszą być odpowiednio silne (patrz rozdział Bezpieczeństwo haseł). W styczniu 2012, gdy doszło do włamania na stronę Kancelarii Prezesa Rady Ministrów, włamywacze ujawnili, że panel administracyjny miał login "*admin*" i hasło "*admin1*" - nie powtórzmy tego błędu.
- Zarejestrujmy stronę w dostępnych darmowych usługach związanych z bezpieczeństwem:
    - Google Webmaster Tools oraz Bing Webmaster Tools - panele administracyjne popularnych wyszukiwarek dają znacznie większą kontrolę nad wynikami

[26] Audyt na zgodność z normą ISO 27001 ma zakres znacznie szerszy niż same tylko testy aplikacji - obejmuje aspekty organizacyjne i wiele innych. Norma ISO 27001 w jednym z punktów wymaga prowadzenia testów penetracyjnych, należy ją więc traktować jako nadzbiór a nie synonim testów.

wyszukiwania dla naszych stron. Rejestracja naszej strony umożliwi np. szybkie usunięcie z wyszukiwarki niefortunnie opublikowanych danych.

- CloudFlare - usługa ochrony stron przed przeciążeniem i atakami (zwłaszcza *denial of service*), oferuje także licencję darmową. CloudFlare nie wymaga instalacji po stronie serwera, "instalacja" polega na podmianie serwerów DNS dla naszej strony. Dla CloudFlare dostępnych jest wiele rozszerzeń oferujących dodatkową ochronę serwera - np. darmowa wersja Dome9.
- ModSecurity - zaawansowana, bezpłatna zapora przeznaczona dla aplikacji webowych opartych o serwer Apache oraz URLScan dla serwera Microsoft IIS.

Bibliografia

- *"Bezpieczeństwo informacyjne"*, Krzysztof Liderman, PWN, 2012
- *"OWASP Application Security Verification Standard Project"*, OWASP, 2009