Urząd Komunikacji Elektronicznej

we współpracy

FUNDACJA bezpieczna cyberprzestrzeń

BEZPIECZEŃSTWO KOMPUTEROWE SZKOŁY. PORADNIK.

Warszawa, grudzień 2016 r.

Spis treści

1. DLACZEGO SZKOLNE SYSTEMY TELEINFORMATYCZNE WYMAGAJĄ OCHRONY 4

2. PODSTAWOWE ZASADY BEZPIECZEŃSTWA. W SZKOLE I NIE TYLKO…..... 6

2.1. NIE WCHODŹ NA PODEJRZANE STRONY INTERNETOWE 6

2.2. NIE KLIKAJ W LINKI, KTÓRYCH NIE ZNASZ 6

2.3. NIE OTWIERAJ PODEJRZANYCH ZAŁĄCZNIKÓW 7

2.4. NIE KLIKAJ W „WŁĄCZ OBSŁUGĘ MAKR”, „OPCJE”, „ENABLE CONTENT” W DOKUMENTACH 7

2.5. NIE WYSYŁAJ SWOICH POUFNYCH DANYCH ZWYKŁYM MAILEM 7

2.6. INSTALUJ PROGRAMY Z ZAUFANYCH ŹRÓDEŁ 7

2.7. AKTUALIZUJ WSZYSTKO..... 7

2.8. UŻYWAJ ANTYWIRUSA..... 7

2.9. SKONFIGURUJ ZAPORĘ SIECIOWĄ (FIREWALL)..... 8

2.10. UWAŻAJ NA SIECI PUBLICZNE 8

2.11. PAMIĘTAJ, ŻE DANYCH Z INTERNETU JUŻ NIE USUNIESZ..... 8

2.12. SZYFRUJ DANE SWOJE 8

2.13. ZADBAJ O SWOJĄ PRZEGLĄDARKĘ 8

2.14. WYKONUJ KOPIE ZAPASOWE..... 8

2.15. PROFIL ADMINISTRATORA TO NIE PROFIL NA CO DZIEŃ 8

2.16. USTAL MOCNE HASŁO. WSZĘDZIE..... 8

3. ORGANIZACJA BEZPIECZEŃSTWA W SZKOLE..... 10

3.1. POLITYKA BEZPIECZEŃSTWA 11

4. BEZPIECZNA PRACOWNIA SZKOLNA..... 13

4.1. JAK, CO I PO CO ATAKUJĄ CYBERPRZESTĘPCY 13

4.2. JAK SIĘ BRONIĆ 13

4.2.1. Przydatne oprogramowanie 15

4.3. JAK OCHRONIĆ UCZNIA PRZED NIEPOŻĄDANYMI TREŚCIAMI 16

4.3.1. Filtrowanie treści ... 17
4.3.2. Przydatne oprogramowanie ... 18
5. WIFI W SZKOLE ... 20
5.1. KONFIGURACJA ... 20
5.2. DOBRE PRAKTYKI ... 21
6. SZKOLNE ZASOBY W SIECI ... 23
6.1. STRONA INTERNETOWA SZKOŁY ... 23
6.2. ZAMAWIAĆ CZY BUDOWAĆ WŁASNYMI SIŁAMI? ... 24
6.2.1. Zagrożenia dla stron internetowych ... 25
6.2.2. Porady ... 26
6.3. DZIENNIK ELEKTRONICZNY I INNE INTERNETOWE SERWISY TRANSAKCYJNE ... 28
6.3.1. Zagrożenia ... 28
6.3.2. Porady – czego wymagać od dostawców ... 28
6.4. DZIAŁANIA PROFILAKTYCZNE ... 31
6.4.1. KOPIE ZAPASOWE ZASOBÓW ... 32
6.5. OBOWIĄZKI PRAWNE ... 33
6.5.1. Ochrona danych osobowych ... 33
6.5.2. Cookies (“ciasteczka”) ... 33
7. HASŁA ... 35
7.1.1. Zarządzanie hasłami ... 36
7.1.2. Uwierzytelnianie wieloskładnikowe ... 36
8. EDUKACJA I UŚWIADAMIANIE UŻYTKOWNIKÓW ... 38
9. STUDIUM PRZYPADKÓW ... 39
10. LITERATURA PRZEDMIOTU ... 39

1. Dlaczego szkolne systemy teleinformatyczne wymagają ochrony

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. Szkolne systemy to także dane. Dane to informacja. Informacja to dzisiaj wartość komercyjna. Tam, gdzie wartość komercyjna, tam też i złodzieje – cyberprzestępcy, którzy chcą ukraść jak najwięcej i jak najszybciej – szkolne zasoby nadają się do tego procederu idealnie. Dlatego niezbędna jest **skuteczna** ochrona komputerów używanych w szkole przez nauczycieli i uczniów.

Ten poradnik został napisany przez praktyków dla praktyków. Jego cel jest bardzo prosty – pokazać osobom zarządzającym nowoczesnymi technologiami w szkołach, że bezpieczeństwo informatyczne nie jest kosztownym kaprysem, lecz podstawową potrzebą, którą można zrealizować stosunkowo tanim kosztem.

Większość opisywanych narzędzi jest darmowa, a część z nich dostępna w modelu *open source*. Wielu producentów komercyjnego oprogramowania zabezpieczającego oferuje również jego darmowe odpowiedniki, które – choć nieco uboższe od płatnych wydań – często będą całkowicie wystarczające na potrzeby szkół. Istnieją też dostawcy, którzy opatrują sprzedawane produkty licencjami edukacyjnymi w bardzo atrakcyjnych cenach.

Chcielibyśmy, aby głównym wnioskiem jaki nasunie się Państwu po lekturze tego poradnika był taki, że bezpieczeństwo to ciągłe zmiany, a zarządzanie bezpieczeństwem to racjonalne kontrolowanie tych zmian. **Racjonalne - czyli odpowiednie do potrzeb.**

Bezpieczeństwo w XXI wieku to nie jednorazowy zakup urządzenia za kilkadziesiąt tysięcy złotych, które wystarczy podłączyć do sieci – to przede wszystkim sprawnie działający **proces**, dzięki któremu systemy komputerowe są regularnie aktualizowane, a administratorzy w porę zauważają próby ataków.

Pamiętajmy też, że najsłabszym ogniwem w procesie zapewniania bezpieczeństwa są **ludzie**. Utartym zwyczajem w dużych instytucjach jest inwestowanie w dobra materialne, takie jak sprzęt komputerowy czy oprogramowanie, a wydatki na rozwój zawodowy personelu są często traktowane jako coś mniej istotnego. Tymczasem żaden sprzęt, a już z pewnością nie komputery, nie będzie poprawnie działał, jeśli nie będzie z niego korzystał świadomy użytkownik.

Większość opisanych przez nas wspaniałych, darmowych narzędzi i aplikacji jest owocem wieloletniej pracy ludzi o dużym doświadczeniu i często niewielkich środkach finansowych. Z kolei wiele spektakularnych "katastrof" z branży informatycznej, o których czytaliśmy w prasie dotyczyła instytucji, którym nie brakło pieniędzy - tylko właśnie kompetencji.

Dlatego wydaje nam się, że zwłaszcza w dziedzinie bezpieczeństwa każda złotówka wydana na szkolenie dyrekcji, nauczycieli, pracowników i uczniów będzie mieć znacznie większy wpływ na efekt finalny niż wydatki na sprzęt i oprogramowanie.

2. Podstawowe zasady bezpieczeństwa. W szkole i nie tylko…

W dalszej części poradnika przedstawiamy rozwiązania i narzędzia, których zastosowanie uodporni szkolne zasoby na ataki cyberprzestępców. Jednak żadne z nich nie będzie w pełni skuteczne, jeśli nie zachowamy podstawowej higieny w naszych działaniach w cyberprzestrzeni. Warto je stosować nie tylko w odniesieniu do systemów szkolnych, ale też i tych domowych. Jeśli zachowamy zasady spisane poniżej, możemy śmiało powiedzieć, że zrobiliśmy dużo dla naszego bezpieczeństwa. Stuprocentowej ochrony mieć nigdy nie będziemy. W cyberprzestrzeni ona po prostu nie istnieje.

2.1. Nie wchodź na podejrzane strony internetowe

Jeśli nie jesteś pewny reputacji strony internetowej – nie wchodź na nią. Sprawdź wcześniej w wyszukiwarce jakie są opinie na jej temat. Skorzystaj z serwisów (np. www.virustotal.com), które przeskanują podejrzany adres.

Trzeba pamiętać, że nawet samo odwiedzenie „zawirusowanej" strony może doprowadzić do zainstalowania złośliwego oprogramowania na naszych komputerach.

2.2. Nie klikaj w linki, których nie znasz

Jeśli ktoś przysyła Ci link – bądź czujny. Po pierwsze sprawdź nadawcę (czy go znasz i czy spodziewałaś się tej wiadomości). Pamiętaj, że ktoś mógł podszyć się pod nadawcę. Jeśli nie jesteś pewny – zadzwoń do nadawcy i się upewnij. Zwróć uwagę, że treść samego linku może być zupełnie inna od lokalizacji do której prowadzi. Możesz spróbować wskazać kursorem na link (uwaga: bez kliknięcia) i w większości programów pojawi się obok lub w rogu okna prawdziwa destynacja linku. Jeśli link prowadzi do strony lub pliku ze złośliwym oprogramowaniem: klikasz – przegrywasz.

2.3. Nie otwieraj podejrzanych załączników

Jeśli dostałeś wiadomość e-mail z dziwnie wyglądającym załącznikiem, tzn. z dziwną nazwą, z rozszerzeniem, którego nie znasz (.js, .zip, .rar etc.) nie otwieraj! Jeśli dodatkowo w treści maila znajdziesz ponaglenia, żądania zrobienia czegoś jak najszybciej – bądź wyjątkowo czujny, możesz być ofiarą kampanii phishingowej. To znaczy, ktoś chce, żebyś koniecznie wykonał czynność kliknięcia w link lub otworzenia załącznika. Jeśli wiadomość jest napisana bez składu i ładu, z błędami gramatycznymi, bez polskich znaków – możesz być pewien, że jest to próba manipulacji.

2.4. Nie klikaj w „Włącz obsługę makr", „Opcje", „Enable content" w dokumentach

Jeśli postanowiłeś otworzyć załącznik Worda czy Excela (najczęściej spotykane) i wyskakuje Ci informacja, by „włączyć obsługę makr" lub wyłączyć zabezpieczenia klikając „opcje" lub cokolwiek podobnego – nigdy nie klikaj! Klikasz, znaczy pozwalasz na wykonanie się dołączonego skryptu – przeważnie złośliwego.

Nawet jeśli załącznik pochodzi od zidentyfikowanego nadawcy, żądaj od niego by dostarczył go bez makr. To jego problem, nie Twój!

2.5. Nie wysyłaj swoich poufnych danych zwykłym mailem

Ilekroć ktoś prosi Cię o przesłania danych osobowych, identyfikacyjnych, uwierzytelniających do konta bankowego – odmawiaj. Chcesz przesłać poufne dane – zaszyfruj je (patrz PGP). A danych do konta używaj tylko w serwisach bankowych – wcześniej upewnij się czy to na pewno serwis banku, a nie podstawiona, łudząco podobna strona (punkt 2.1).

2.6. Instaluj programy z zaufanych źródeł

Tak jak możesz zainstalować nieświadomie złośliwe oprogramowania wchodząc na skompromitowaną stronę, czy klikając w link dostarczony Ci wiadomością e-mail, tak możesz je sobie zainstalować, jeśli ściągasz programy z niezaufanych źródeł.

2.7. Aktualizuj wszystko

Bezpieczeństwo to wyścig. Kiedy tylko przestępca zauważy lukę (błąd) w dowolnym programie, od razu będzie chciał ją wykorzystać do przejęcia kontroli nad Twoim komputerem. Jednocześnie programiści odpowiedzialni za daną aplikację, tak szybko jak to możliwe, będą takie luki łatać, czyli dopisywać odpowiednie fragmenty kodu, aby niemożliwe było wykorzystanie zidentyfikowanego błędu. Zatem tak szybko jak to możliwe – instaluj aktualizacje wszystkich programów. Nigdy nie wiadomo, którędy przestępca będzie chciał się włamać – a będzie próbował wszystkiego.

2.8. Używaj antywirusa

To prawda, że oprogramowanie antywirusowe nie uchroni nas przed wyrafinowanym atakiem, ale spowoduje, że większość znanych już wirusów nie będzie dla nas problemem. Zdecydowana większość oprogramowania, które wykorzystują przestępcy jest stara, dlatego też antywirus ciągle pozostaje jedną z podstawowych form zabezpieczenia.

2.9. Skonfiguruj zaporę sieciową (firewall)

Zapora sieciowa musi być włączona. Jeśli jakiś program chce zmienić ustawienia zapory sieciowej – zastanów się dwa razy nim to zrobisz. Lepiej „wyciąć" trochę więcej ruchu sieciowego niż dopuścić do nieuprawnionego dostępu do sieci lokalnej z zewnątrz.

2.10. Uważaj na sieci publiczne

Sieci publiczne są słabo zabezpieczone i zazwyczaj jeden użytkownik może łatwo „podsłuchać" innego. Nie musisz – nie korzystaj. Musisz – szyfruj komunikację.

2.11. Pamiętaj, że danych z Internetu już nie usuniesz

Jeśli upublicznisz jakiekolwiek dane musisz zakładać, że zostaną one w Internecie już na zawsze. Internet też ma swoje archiwum.

2.12. Szyfruj dane swoje

Szyfrowanie to dzisiaj podstawa. Nie tylko w komunikacji (np. https, PGP). Powinieneś również zaszyfrować swoje dyski. Wtedy nawet po kradzieży sprzętu dostęp do danych nie będzie prosty.

2.13. Zadbaj o swoją przeglądarkę

Przeglądarka internetowa to Twoje okno na świat i podstawowe narzędzie pracy. Warto pomyśleć o jej bezpieczeństwie, korzystając zawsze z najbardziej aktualnej wersji. Pamiętaj też, że o ile możesz znaleźć wiele wtyczek poprawiających jej i Twoje bezpieczeństwo, to możesz też zainstalować rozszerzenie, które może być złośliwe.

2.14. Wykonuj kopie zapasowe

Należy liczyć się z tym, że prędzej czy później zostaniemy zaatakowani, utracimy nasze dane i naszym jedynym ratunkiem będzie sięgnięcie po kopię zapasową danych. Po prostu trzeba je mieć.

2.15. Profil administratora to nie profil na co dzień

Dobrą praktyką jest używanie profilu administratora tylko wtedy, kiedy jest to potrzebne. Do codziennej pracy lepiej stworzyć osobny profil użytkownika.

2.16. Ustal mocne hasło. Wszędzie.

O hasłach napisano już wiele (np. w poradniku UKE), ale wciąż jest to najsłabsze ogniwo systemu zabezpieczeń. Dlatego przypominamy o nich jeszcze raz.

Hasła są od dawna najpopularniejszą metodą uwierzytelniania użytkowników i to mimo faktu, że można je podsłuchać, przechwycić lub odgadnąć. Hasła mają jedną, dużą zaletę – do ich wprowadzenia wystarczy klawiatura i monitor (lub ekran dotykowy), czyli coś, co jest w zasięgu ręki niemal zawsze (np. w odróżnieniu od czytnika kart czipowych).

Najłatwiejszą metodą włamań na cudze konto jest odgadnięcie 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”*. **Ale złamanie takich haseł to “pestka”.**

3. Organizacja bezpieczeństwa w szkole

Zabezpieczenia techniczne są podstawą ochrony przed zagrożeniami, jednak będą one nieskuteczne, jeśli ich stosowanie nie będzie skoordynowania przez odpowiedni proces organizacyjny. Nazwa “proces” brzmi tutaj niezwykle poważnie, ale w praktyce sprowadza się do rzeczy prostych i tak oczywistych, że często pomijanych - gdy kupimy urządzenie do zapisywania kopii zapasowych, to będzie ono bezwartościowe, jeśli nie powiemy pracownikom jak często mają z niego korzystać i kto jest za to odpowiedzialny.

Inicjatywa zwiększania poziomu bezpieczeństwa musi pochodzić od dyrekcji, która powinna przynajmniej się na nią zgodzić, wspierać w przypadku nieuniknionych przeszkód, ale przede wszystkim samemu dawać przykład jej stosowania. Nie ma nic bardziej demoralizującego niż dyrektor, który ma hasło przyklejone na kartce do monitora.

Priorytety każdej szkoły w zakresie bezpieczeństwa ustala jej dyrekcja i opisuje w polityce bezpieczeństwa. Jest to znowu pojęcie, wokół którego narosło wiele mitów, ale w praktyce sprowadza się on do dokonania konkretnych wyborów - na przykład kto jest za co odpowiedzialny albo co wolno robić w naszej sieci lokalnej. Wybory te są następnie przekładane na techniczny język 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 dyrekcji i specjalistów oczekuje się udzielenia w trybie natychmiastowym odpowiedzi na szereg pytań. Na przykład o to, co się stało i kogo należy powiadomić. Na tę kwestię odpowiedzieć pomoże procedura reagowania na incydenty. “Gdzie są kopie zapasowe?” – tu przyda się procedura ciągłości działania; i tak dalej…

Co jednak w wypadku, gdy osoby wskazane w procedurze dawno przeszły na emeryturę, a kopie zapasowe ostatnio sprawdzano kilka lat temu? I dlatego istotne jest, aby nad formalną poprawność zasad i procedur przedkładać ich faktyczną przydatność i regularną (co najmniej raz do roku) aktualizację oraz testowanie w bieżących warunkach.

3.1. Polityka bezpieczeństwa

W tym poradniku skupiamy się przede wszystkim na **bezpieczeństwie technicznym**, które jest zazwyczaj pierwszym procesem przyjmowanym przez instytucje zaczynające jakiekolwiek działania związane z ochroną informacji. W przypadku organizacji podlegających jakiejś formie nadzoru ze względu na obowiązujące przepisy[1] równie ważne jest **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 świadomi poziomu bezpieczeństwa i znać silne oraz słabe strony systemu obiegu informacji. 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 wyboru konkretnych rozwiązań[2].

Polityka bezpieczeństwa jest dokumentem, który definiuje to pytanie i udziela na niego odpowiedzi w sposób systematyczny i formalny. Z jej zapisów wynika cała reszta – to na ich podstawie podejmujemy decyzję, **co ma być chronione hasłem i które pliki mają być dostępne dla kogo.**

Brak jest 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 27002:2014, zawierająca wszystkie kluczowe punkty, jakie powinny się w niej znaleźć.

Każda instytucja ma swój specyficzny profil ryzyka, który należy wziąć pod uwagę przy tworzeniu polityki bezpieczeństwa. Oznacza to z jednej strony, że pewne aspekty należy potraktować priorytetowo, ale inne z kolei możemy świadomie pominąć – na przykład wątpliwe, by szkoły obsługiwały płatności kartami kredytowymi, co przysparza problemów wielu firmom.

Polityka bezpieczeństwa nie musi być stustronicowym dokumentem napisanym prawniczym językiem. **Lepiej by miała dwie strony, ale za to faktycznie osadzone w rzeczywistości danej instytucji np. szkoły.** Jeśli nie wiemy czy dana kwestia jest dla nas istotna to nie umieszczajmy jej w polityce “na zapas”.

Nie róbmy z niej także “koncertu życzeń” - czyli jak mogłaby hipotetycznie wyglądać sieć, gdyby na jej rozbudowę i unowocześnienie było 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.

Aby polityka bezpieczeństwa była stosowana, użytkownicy muszą o niej wiedzieć. Politykę mocno osadzoną w kontekście naszej organizacji można podsumować w **kwadrans na cotygodniowej odprawie - “róbcie to, nie róbcie tamtego, w razie pytań zgłaszajcie się do X”**. Rozesłanie mailem dwustustronicowego dokumentu to gwarancja, że nikt go nigdy nie przeczyta, a już na pewno nie będzie wiedział o co w nim w ogóle chodzi.

---

[1] Na przykład ustawie o ochronie danych osobowych czy ustawie o informatyzacji.

[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 w przetargu.

W dużych instytucjach często istnieje konieczność rozbicia polityki, zawierającej zapisy ogólne i rzadko zmienianej, na mniejsze dokumenty - standardy (np. jakiego programowania używamy), minimalne wymagania (np. z jakich haseł korzystamy) i procedury (np. co robimy w razie wykrycia wirusa). W mniejszych instytucjach mogą być one zawarte w jednym dokumencie.

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

4. Bezpieczna pracownia szkolna

4.1. Jak, co i po co atakują cyberprzestępcy

Dotychczas tradycyjnymi ośrodkami komputerowymi w placówkach edukacyjnych były pracownie internetowe. Obecnie komputery coraz częściej pojawiają się już w salach lekcyjnych i na biurkach uczniów, są też obecne w sekretariatach i w pokojach nauczycielskich. Szkoły stają się instytucjami zinformatyzowanymi, ale za tym musi iść też dostosowanie poziomu bezpieczeństwa. Poniższy tekst dotyczy więc wszystkich zastosowań, gdzie komputery są stosowane w szkołach jako stacje robocze, nie tylko pracowniach (zasady korzystania z pracowni powinny być także ujęte w polityce bezpieczeństwa).

Szkodliwe oprogramowanie (ang. *malware*) to rodzina produktów czarnorynkowej branży przynoszącej obecnie krociowe zyski. Obecnie rzadko spotykamy wirusy komputerowe, których celem jest wyłącznie powielanie się lub niszczenie danych. **Współczesne programy tego typu służą przede wszystkim zarabianiu pieniędzy na skradzionych hasłach, adresach e-mailowych, wyłudzaniu pieniędzy lub wykorzystywaniu zainfekowanych komputerów jako stacji przesiadkowych do innych ataków (tzw. *zombie*).**

W powszechnym przekonaniu głównym narzędziem ochrony są tutaj programy antywirusowe. Jest to błąd – antywirusy często rozpoznają nie więcej niż 50% nowych zagrożeń. Oznacza to, że w początkowym (a więc najbardziej intensywnym) okresie dystrybucji danego “szkodnika” użytkownik jest praktycznie bezbronny, jeśli opiera się **tylko** na antywirusie.

4.2. Jak się bronić

Infekcja komputera wymaga spełnienia dwóch warunków:

- użytkownik musi **wykonać jakąś akcję**, np. wejść na stronę (tak, czasem tylko to wystarczy!) lub otworzyć zainfekowany plik, który przyjdzie mailem lub zostanie ściągnięty z Internetu; ten kanał ograniczamy za pomocą edukacji użytkowników;

- w celu dalszego opanowania komputera wirus musi uzyskać **uprawnienia administratora**;

jeśli użytkownik pracuje na koncie administratora, to szkodliwy program ma je podane na tacy, jeśli nie, to może wykorzystać znane usterki w systemie lub w aplikacjach – na tym etapie pomoże ograniczenie uprawnień.

Typowymi technikami infekcji są błędy w przeglądarkach internetowych oraz dodatkach do nich, zwłaszcza we wtyczkach **Javy** (sprawdź) i **Flasha** (sprawdź). Dzięki nim potencjalny napastnik jest w stanie wprowadzić dowolne polecenia i wykonać je z uprawnieniami użytkownika obsługującego komputer.

Dla uniknięcia powtarzających się zarażeń wirusami kluczowe jest wprowadzenie następujących zasad:

- ograniczenie dostępu do konta administratora:
  - dla uczniów i nauczycieli tworzymy konta z ograniczonymi uprawnieniami[3],
  - nie udostępniamy hasła administratora bez potrzeby,
  - konto administratora służy wyłącznie do zarządzania systemem,
  - wykonywanie wybranych czynności administracyjnych w Windows z użyciem funkcji `Run As`[4];

- włączenie automatycznych aktualizacji:
  - w systemie operacyjnym (Aktualizacje Windows),
  - we wszystkich programach, które mają taką funkcję[5];

- instalacja programu antywirusowego:
  - włączenie automatycznego aktualizowania sygnatur wirusów,
  - nie korzystamy na stałe z demonstracyjnych i testowych wersji[6].

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 aktualizujmy przeglądarkę internetową do najnowszej wersji**. Przeglądarka jest na pierwszej linii frontu i pada zawsze jako pierwsza. Nowe wersje przeglądarek zawierają poprawki znanych błędów i udoskonalone mechanizmy bezpieczeństwa.

- Korzystajmy z baz złośliwych stron WWW wbudowanych w nowe wersje przeglądarek Chrome, Firefox (*Google SafeBrowsing*) oraz Microsoft Internet Explorer (*SmartScreen*).

---

[3] Takie konta są domyślnie zakładane w Windows Viście, Windows 7, 8 i 10 oraz w GNU/Linuksie. W systemie Windows XP trzeba stworzyć je po założeniu domyślnego konta administratora. Instrukcja dostępna jest np. w serwisie YouTube.

[4] W systemach Windows XP należy użyć Run As, w Windows Viście, 7, 8 i 10 funkcji UAC.

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

[6] Testowe (ang. *evaluation, trial*) wersje nawet najlepszych antywirusów po okresie testowym często wyłączają funkcje aktualizacji. Antywirus bez aktualizacji jest bezużyteczny. Jeśli nie można nabyć pełnej wersji, warto wybrać produkt, który z założenia jest darmowy. Jeśli podejmujemy decyzję o zakupie, kierujmy się wynikami niezależnych testów skuteczności, np. AV Comparatives, AV-Test, Virus Bulletin

- Ochrona przed wykonywaniem danych (ang. *Data Execution Prevention,* skr. DEP) wbudowana w Windows XP od wersji Service Pack 2 zmniejsza szanse na wykorzystanie systemowych luk przez szkodliwe oprogramowanie. Fabrycznie ochrona jest włączona tylko dla podstawowych usług systemowych, należy ją włączyć także dla wszystkich programów[7].

- W systemie Windows Vista, 7, 8 i 10[8] pojawiły się zabezpieczenia znacznie skuteczniejsze niż DEP, są one jednak domyślnie wyłączone. Należy je aktywować z użyciem darmowego programu Microsoft EMET[9]. **Jest to prawdopodobnie najskuteczniejsza obecnie metoda ochrony Windows przed nowymi atakami** (tzw. atakami zero-day), darmowa i o wiele skuteczniejsza niż jakikolwiek antywirus. Tu warto wspomnieć, że od 2013 roku Microsoft w Polsce uruchomił specjalny program licencyjny przeznaczony dla instytucji edukacyjnych, obejmujący szkoły podstawowe, średnie i wyższe.

4.2.1. Przydatne oprogramowanie

Przydatne programy:

- Secunia PSI oraz OSI – sprawdzają Windows i zainstalowane aplikacje pod kątem brakujących poprawek. Jest to istotne zwłaszcza w przypadku tych programów, które nie mają wbudowanej funkcji automatycznej aktualizacji;

- darmowe, w pełni użyteczne antywirusy: Microsoft Security Essentials, ClamAV[10] oraz darmowe do użytku prywatnego - Avast, Avira, BitDefender - instalacja w instytucji wymaga wykupienia licencji, ale cześć z nich oferuje tańsze wersje dla placówek edukacyjnych (Avast, G Data);

- darmowe usługi VirusTotal – pozwalają na przesłanie podejrzanych programów (pierwsza przeskanuje go przy pomocy ok. 40 różnych antywirusów, a druga uruchomi w zamkniętym środowisku i opisze podejrzane zachowania); stosujmy, jeśli dostaliśmy podejrzany plik a nasz antywirus nie zgłasza nic podejrzanego[11];

- CloneZilla - narzędzie do tworzenia obrazów całego systemu operacyjnego, umożliwiające szybkie jego odtwarzanie na jednym lub wielu komputerach w razie infekcji lub awarii.

---

[7] Patrz opis konfiguracji DEP w artykule Microsoft KB875352

[8] 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. Użytkownikom i administratorom Windows 10, CERT.GOV.PL zaleca zapoznanie się z Przewodnikiem Zabezpieczeń systemu Windows 10 dostępnym w dziale Zalecenia konfiguracyjne/Microsoft Windows

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

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

[11] Jest to o tyle istotne, że większość antywirusów, także tych "renomowanych", ma problemy z wykrywaniem wirusów, które dopiero co zostały wpuszczone do sieci. Niektóre z nich wykryją go po codziennej aktualizacji, niektórej po kilku dniach - a wtedy będzie już zwykle za późno. Tego typu pliki wygenerują zwykle co najmniej kilka ostrzeżeń na VirusTotal, a z każdym dniem ich liczba będzie rosła w miarę jak zainstalowane w nim antywirusy będą się aktualizować.

4.3. Jak ochronić ucznia przed niepożądanymi treściami

Internet w szkole jest postrzegany jako zagrożenie ze względu na możliwość uzyskania przez uczniów dostępu do treści nieprzeznaczonych dla dzieci i młodzieży. Ochrona przed tego typu zawartością jest o tyle kłopotliwa, że mogą one pojawiać się w bardzo wielu źródłach (serwisach), a problematyczne jest samo zdefiniowanie pojęcia “nieodpowiednie treści”.

Stosunkowo łatwo i skutecznie można wyeliminować te, które bez wątpienia nie powinny pojawiać się w wynikach wyszukiwania w Google, jak np. pornografia. Wszystkie popularne wyszukiwarki wyposażone są w mechanizmy filtrujące tego typu wyniki (piszemy o nich niżej).

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, by **uczniowie nie napotykali się na nieodpowiednie treści przypadkowo**, w wynikach wyszukiwania czy podczas przeglądania klipów wideo (np. w usługach *YouTube* czy *Vimeo*).

Praktycznie niemożliwe jest przy tym uzyskanie pewności, że uczniowie nie natkną się na wulgaryzmy lub nawoływanie do przemocy w komentarzach pod artykułami prasowymi na portalach czy w blogach[12].

[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.

4.3.1. Filtrowanie treści

Od strony technicznej filtrowanie treści (ang. *content filtering*) czy tzw. kontrolę rodzicielską (ang. *parental controls*) można i należy prowadzić w następujących lokalizacjach:

- na indywidualnych komputerach i tabletach
  - z użyciem specjalnych programów,
  - z użyciem funkcji przeglądarek internetowych;

- na poziomie całej sieci:
  - z użyciem filtrów wbudowanych w urządzenia sieciowe (routery i firewalle),
  - z użyciem odpowiednich ustawień sieci.

Większość filtrów treści działa na dwa sposoby:

- przez analizowanie **adresu** strony, którą ładuje użytkownik (np. *youtube.com*) i sprawdzanie jak została ona sklasyfikowana przez producenta filtra – nieskuteczne, jeśli strona nie jest w ogóle sklasyfikowana, poza tym 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 oprogramowanie 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 – badanie treści czy klasyfikacja 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 oznaczone jako dobre lub 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 strony, które narzędzie błędnie uznało za niepożądane.
- Czy narzędzie umożliwia blokowanie stron, które nie zostały sklasyfikowane? Podobnie jak wyżej, brak takiej funkcji to luka w ochronie.
- Czy producent oferuje pomoc techniczną i możliwość zgłaszania błędnie sklasyfikowanych stron?

Poniżej opisujemy kilka popularnych narzędzi, które można wykorzystać do filtrowania stron w szkołach i innych miejscach, w których z komputerów korzystają osoby niepełnoletnie lub w inny sposób nieuprawnione do odwiedzania stron o pewnym charakterze.

4.3.2. Przydatne oprogramowanie

Lista zawiera dwie grupy aplikacji filtrujących – pierwsza to oprogramowanie przeznaczone do pracy na komputerze użytkownika, a druga to usługi sieciowe, które analizują przepływające dane i są w stanie zablokować dostęp do podejrzanych lokalizacji niezależnie od tego, czy przyłączony komputer wyposażono w odpowiednie narzędzie, czy też nie (bo na przykład jest to laptop lub inteligentny telefon z przeglądarką przyniesiony przez ucznia).

Oprogramowanie instalowane na komputerach:[13]

- K9 Web Protection – darmowy filtr treści dostępny dla systemów Windows, Mac OS-a X, iOS-a oraz Androida, udostępniany przez firmę BlueCoat – jednego z wiodących producentów korporacyjnych filtrów. Posiada jedną z najbardziej rozbudowanych i często aktualizowanych baz stron oraz rozbudowane funkcje chroniące przed wyłączaniem przez użytkowników. Całkowicie darmowy.
- Microsoft Family Safety – korzysta z klasyfikacji stron zarządzanej przez Microsoft, darmowej dla użytkowników Windows Visty i 7. Umożliwia filtrowanie gier. Darmowy dla posiadaczy legalnych licencji Windows 7 i nowszych.
- Google SafeSearch – mechanizm wyszukiwarki Google, darmowy dla wszystkich użytkowników. Zabezpieczenie łatwe do obejścia lub wyłączenia, dość skutecznie chroni przed przypadkowym zetknięciem z treściami nieodpowiednimi. Działa także w innych serwisach Google'a, np. YouTube'ie. Analogiczne ustawienie istnieje w wyszukiwarce Microsoftu i nazywa się Bing SafeSearch.
- Polskie programy Cenzor i Strażnik Ucznia, ukierunkowane głównie na rynek edukacyjny i domowy, że stosunkowo niedrogimi licencjami dla szkół. Dobrze dostosowane do specyfiki języka polskiego, stosunkowo łatwe do obejścia.

Narzędzia działające na poziomie sieci:

- SafeDNS oraz OpenDNS FamilyShield – usługi działająca na poziomie systemu nazw domenowych (ang. *Domain Name System*, skr. DNS), chroniąca zarówno przed stronami dla dorosłych jak i stronami zawierającymi wirusy itd[14].
- DansGuardian – darmowy system filtrujący dla systemu GNU/Linux, zintegrowany z serwerem pośredniczącym (ang. *proxy*), a więc przeznaczony do instalacji na serwerach służących jako zapora i brama do Internetu. Ma wbudowane filtrowanie słów kluczowych oraz możliwość wprowadzania klasyfikacji stron, które są dostępne komercyjnie. Wymaga obsługi przez administratora zaznajomionego GNU/Linuksem. Trudny do obejścia, jeśli jest to jedyna brama do Internetu w szkolnej sieci.

---

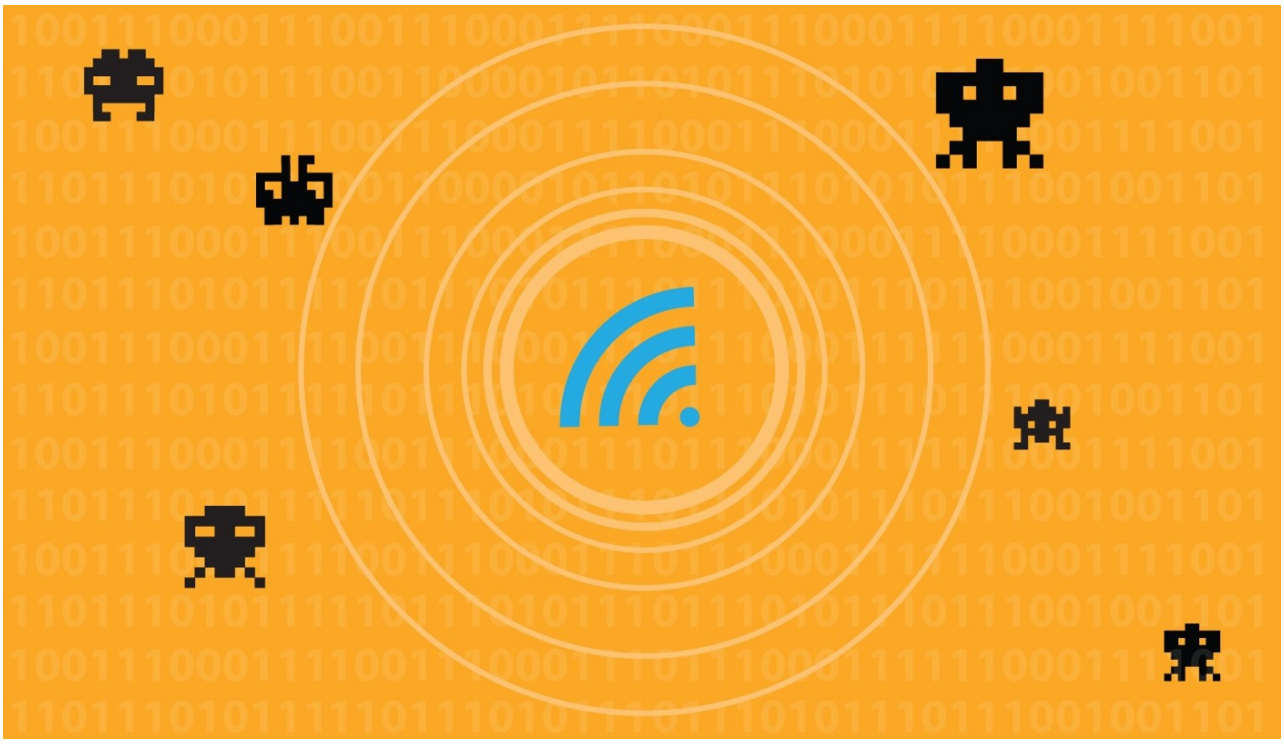
[13] Pamiętajmy, że większość programów instalowanych na komputerach uczniów może zostać stosunkowo łatwo wyłączona i w Internecie można znaleźć mnóstwo poradników obchodzenia popularnych w polskich szkołach programów. Istnieją specjalne strony służące jako "pośrednicy" do ładowania innych zablokowanych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

[14] Cała konfiguracja obu usług sprowadza się do przestawienia na komputerach i routerze adresów serwerów domenowych na wskazane przez każdego z operatorów. 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).

- UTM (ang. *Unified Threat Management*) – najskuteczniejsze i najbardziej rozbudowane, ale równocześnie kosztowne narzędzie. Są to urządzenia stawiane na styku między Internetem a siecią lokalną, zapewniające funkcje zapory sieciowej (ang. *firewall*), systemu wykrywania włamań, antywirusa, filtra treści niepożądanych itd. Koszt jednostkowy zaczyna się od kilku tysięcy złotych, ale w dużych sieciach rozwiązanie takie może się szybko zwrócić ze względu na wysoką skuteczność oraz niższe koszty obsługi niż przy zabezpieczeniach instalowanych na każdym z komputerów oddzielnie[15].

Większość narzędzi sieciowych można łączyć z oprogramowaniem ochronnym działającym na komputerach w celu zwiększenia skuteczności.

[15] Gorąco polecamy projekt OpenWRT. Jest to specjalizowana wersja Linuksa, przeznaczona do instalacji w popularnych urządzeniach sieciowych (routerach, AP) zamiast oryginalnego oprogramowania. Dla OpenWRT jest dostępne mnóstwo modułów dodatkowych, umożliwiających przerobienie AP za kilkaset złotych na zaawansowaną zaporę sieciową, router, bramę VPN, filtr treści czy serwer plików zastępujący do pewnego stopnia profesjonalne UTM.



5. WiFi w szkole

Sieci bezprzewodowe (WiFi) są obecnie standardową technologią sieci komputerowych, szybko wypierającą tradycyjne sieci kablowe (bazujące na standardzie Ethernet). Główną ich zaletą jest brak konieczności umieszczania kosztownego okablowania, co jest problemem zwłaszcza w instytucjach zajmujących budynki zabytkowe. Wiele współczesnych urządzeń w ogóle nie ma gniazd sieci kablowej i mogą łączyć się z Internetem głównie przez WiFi.

Najczęściej spotykanym układem jest podłączenie bezprzewodowego urządzenia dostępowego (ang. *Access Point*, skr. 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, zapewnia wystarczający poziom bezpieczeństwa – wystarczy je poprawnie skonfigurować.

5.1. Konfiguracja

Kluczowe dla bezpieczeństwa sieci WiFi są następujące parametry konfiguracyjne:

- Szyfrowanie połączeń bezprzewodowych. Należy zawsze włączać szyfrowanie **WPA2** lub **WPA**. Nie należy w ogóle udostępniać sieci nieszyfrowanych (otwartych – ang. *open* i współdzielonych – ang. *shared*). **Nigdy nie należy włączać szyfrowania WEP**, gdyż jest ono słabe i złamanie go zajmuje kilka-kilkanaście minut. W warunkach laboratoryjnych zajęło to trzy i pół:

```
[0:10:00] preparing attack "Users" (E8:[redacted])
[0:10:00] attempting fake authentication (1/5)... success!
[0:10:00] attacking "Users" via arp-replay attack
[0:03:26] started cracking (over 10000 ivs)
[endless] captured 19980 ivs, iv/sec: 45  [endless] captured 18335 ivs, iv/sec: 28

[endless] cracked Users (E8:ED:F3:60:0B:D0)! key: "2B[redacted]"
```

Łamanie hasła WEP. Fot. Paweł Krawczyk.

- Obie zalecane metody (WPA2 i WPA) są bezpieczne, ale tylko jeśli będziemy używać **dobrego hasła**. WiFi to sieć radiowa więc podczas każdego logowania nowego użytkownika zaszyfrowane hasło jest widoczne dla **wszystkich** nasłuchujących komputerów w zasięgu sieci. Łamanie tak przechwyconych komunikatów za pomocą wyczerpującego przeszukiwania (ang. *brute-force*), które jest o wiele trudniejsze niż łamanie WEP, ale w przypadku prostych haseł jak najbardziej możliwe. W warunkach laboratoryjnych złamanie hasła WPA2 składającego się z ośmiu cyfr zajęło autorowi około kwadransa. Należy tutaj zatem stosować wszystkie zasady opisane w rozdziale o hasłach.

- Warto upewnić się, że AP pracuje na **najnowszym oprogramowaniu** (ang. *firmware).* W urządzeniach popularnych producentów - m.in. D-Link (aktualizacje) i TP-Link (aktualizacje) - wykrywano w przeszłości tylne furtki (ang. backdoor), które umożliwiały przejęcie kontroli nad siecią.

- Zawsze **wyłączaj funkcję WPS** (ang. *Wi-Fi Protected Setup*). Miała ona w założeniu służyć łatwemu podłączaniu nowych urządzeń do sieci, ale zawiera poważny błąd umożliwiający złamanie hasła do sieci w ciągu kilku godzin.

5.2. Dobre praktyki

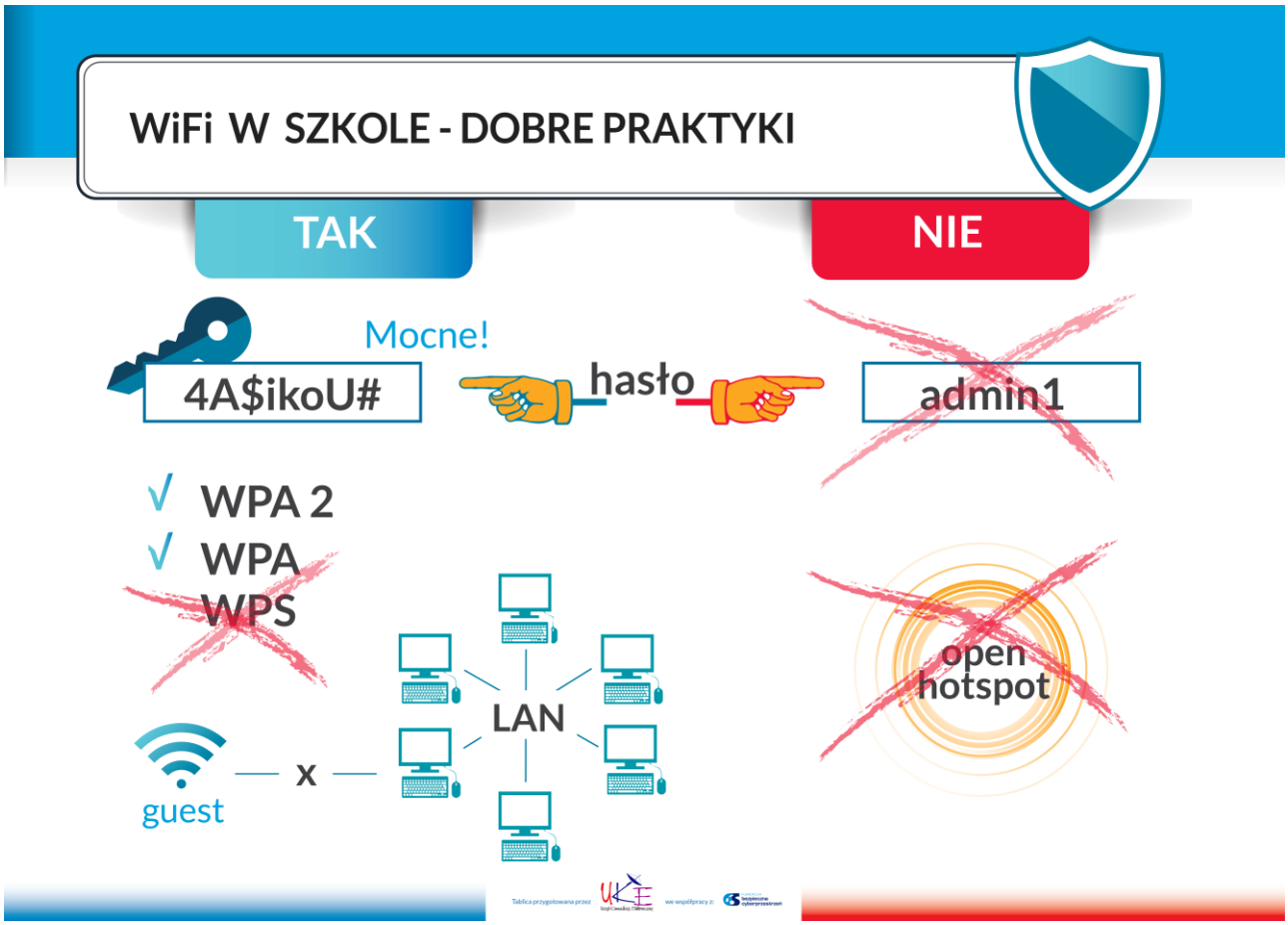
W przypadku większych instytucji zalecane jest uruchamianie **dwóch** sieci bezprzewodowych – pierwszej, przeznaczonej do użytku wewnętrznego i podłączonej do sieci lokalnej (a przez nią do Internetu), oraz drugiej dla gości. Ta ostatnia jest podłączona do Internetu, ale już nie do sieci lokalnej.

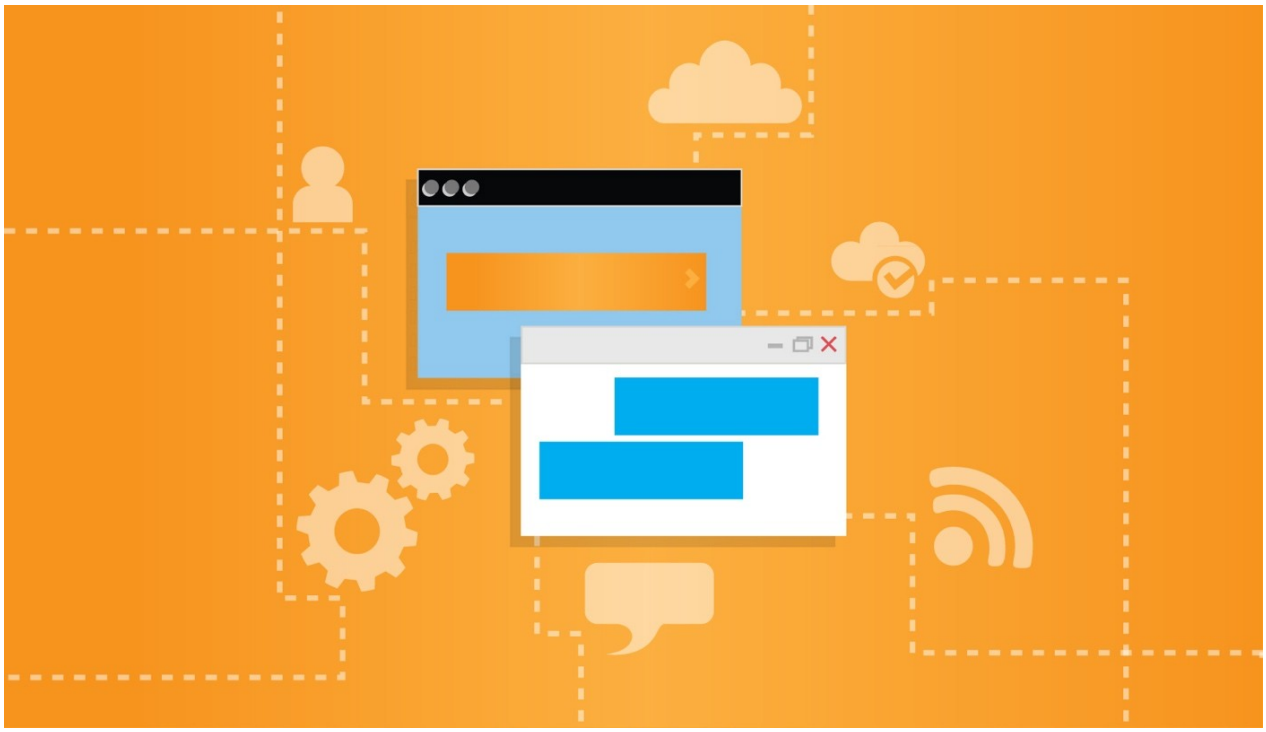
W przypadku sieci bezprzewodowych mających połączenie z siecią lokalną szkoły zalecane jest podłączanie ich przez zaporę sieciową (ang. *firewall*) oraz wykorzystanie indywidualnych danych do logowania (nazwa użytkownika i hasło) dla każdego użytkownika.

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 a wspólne dla wszystkich hasło można udostępniać uprawnionym osobom np. za pośrednictwem tablicy ogłoszeń, informacji na recepcji itp.

Spotykane jest również rozwiązanie typu Hotspot, w którym sama sieć bezprzewodowa jest całkowicie otwarta (dostępna bez hasła), ale dostęp do Internetu wymaga już zalogowania się na stronie internetowej. Rozwiązanie to jest niezalecane, ponieważ sieć taka jest pozbawiona szyfrowania, co z kolei naraża jej użytkowników na podsłuchiwanie i ataki typu MITM.

Pod żadnym pozorem nie należy udostępniać sieci pozbawionych całkowicie szyfrowania i kontroli dostępu. 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.


WiFi W SZKOLE - DOBRE PRAKTYKI
TAK
NIE
Mocne!
4A$ikoU#
hasło
admin1
WPA 2
WPA
WPS
LAN
guest
x
open hotspot



6. Szkolne zasoby w sieci

Praktycznie wszystkie szkoły mają własne strony internetowe, a połowa z nich umieszcza również swoje dane na stronach firm trzecich – na przykład w świadczonych jako usługi tzw. dziennikach internetowych. We wszystkich przypadkach istnieje realne ryzyko, że osoby z zewnątrz znajdą w serwisach 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, a w najgorszym kradzież danych osobowych lub inne ataki skutkujące wymiernymi stratami finansowymi.

6.1. Strona internetowa szkoły

Bezpieczeństwo stron internetowych szkoły należy planować od samego początku, przed podjęciem jakichkolwiek innych działań. Nie jest to szczególnie skomplikowane i większość osób, które potrafią programować bez problemu przyswoi opisane poniżej zasady. (Większość włamań na strony WWW ma miejsce w instytucjach, które nie znały przedstawionych zasad).

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 włamaniami to błędy oczywiste i łatwe do uniknięcia, pod warunkiem, że 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 oficjalnym uruchomieniem. Testy należy powtarzać

przynajmniej raz na kilka lat, ze względu na pojawiające się nowe ataki wymierzone w aplikacje WWW[16].

Zarządzanie bezpieczeństwem stron umieszczanych w Internecie przez szkołę nie musi być procesem kosztownym. Niezależnie od tego, czy jest ono realizowane siłami nauczycieli, uczniów, wyspecjalizowanej kadry, czy zlecane zewnętrznej firmie, przestrzeganie kilku prostych zasad pozwoli uniknąć problemów w przyszłości.

6.2. Zamawiać czy budować własnymi siłami?

Większość szkół ma strony WWW, a nawet kompletną infrastrukturę komputerową, zbudowaną siłami własnymi pracowników, uczniów i rodziców. Jest to rozwiązanie najtańsze i pozwalające maksymalnie wykorzystać dostępny sprzęt, często używany, odkupiony od firm i innych instytucji.

Samodzielna budowa strony internetowej przez szkolną wspólnotę jest doskonałą metodą budowania kompetencji technicznych, które później procentują w życiu zawodowym. Ponieważ do pracy biorą się jednak amatorzy, może to być proces długotrwały, a efekt niekoniecznie musi odpowiadać oczekiwaniom.

Zalety	**Wady**
● 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 funkcjonalnej i dobrze wyglądającej strony może zająć sporo czasu; ● strona może zawierać liczne błędy i podatności na zagrożenia; ● trudne określenie jednoznacznych wymagań funkcjonalnych i jakościowych.

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

[16] 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.

Zalety	Wady
• Funkcjonalna i dobrze wyglądająca wersja strony dostępna w ustalonym terminie; • możliwość egzekwowania wymagań jakościowych i funkcjonalnych.	• Konieczność wydatkowania od kilku do kilkudziesięciu tysięcy złotych na stworzenie strony; • konieczność jednorazowego, precyzyjnego opisania wymagań funkcjonalnych i jakościowych; • strona może nadal zawierać błędy i podatności na zagrożenia; • samo zamówienie witryny bez umowy na jej utrzymanie i przy braku kompetentnych osób wewnątrz instytucji gwarantuje, że po kilku latach strona będzie podatna na ataki.

Podsumowując, zatrudnienie zewnętrznej firmy zwiększa prawdopodobieństwo uzyskania produktu wysokiej jakości, 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 być w stanie poprawnie to nazwać oraz opisać. Jeśli takich umiejętności nie mamy, to możemy poszukać gotowego produktu, 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 dokumentów przetargowych (SIWZ).
- Na tej podstawie zamawiamy właściwy **system informatyczny**. Podmioty wykonujące oba zamówienia powinny być od siebie niezależne.
- Podmiot sporządzający dokumentację warto również poprosić o konsultacje i obecność przy odbiorze ukończonego produktu.

Dalej skupiamy się na typowych projektach informatycznych w edukacji – każdy z nich ma własną specyfikę.

6.2.1. Zagrożenia dla stron internetowych

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

Witryny tego typu od strony technicznej działają najczęściej w oparciu o oprogramowanie do zarządzania zawartością (ang. *Content Management System*, skr. CMS). Nazwą tą określa się aplikacje internetowe, których główną funkcją jest zarządzenie publikacją stron w różnej postaci. W edukacji dominują aplikacje, które są wolnym oprogramowaniem (ang. *free software*) lub takie,

dla których dostarczono kod źródłowy (ang. *open source*)[17]. Jeśli chodzi o języki programowania to dominuje 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 WWW, gdy już zostaną opublikowane w Internecie.

Żeby doszło do ingerencji w treść strony musi dojść do przejęcia kontroli nad panelem administracyjnym, aplikacją zarządzania treścią lub samym systemem operacyjnym serwera.

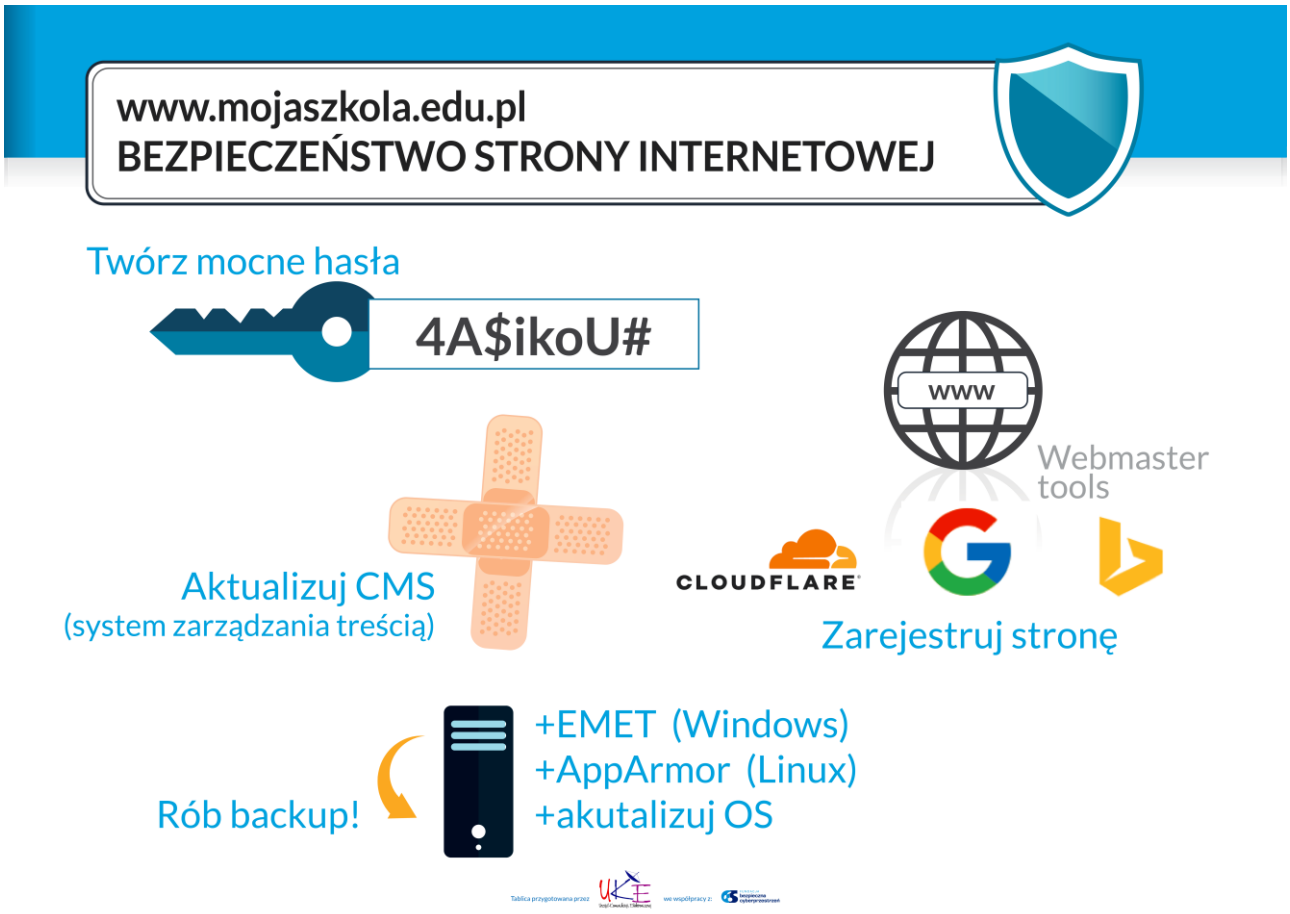
6.2.2. Porady

Poniższa tabela zawiera zalecenia dla administratorów stron WWW:

Ryzyko	**Przyczyna**	**Zabezpieczenia**
Przejęcie kontroli nad panelem administracyjnym.	Słabe hasła.	Stosuj silne hasła.
Przejęcie kontroli nad aplikacją CMS.	Nieznane wcześniej błędy w CMS, które nie zostały załatane na czas. Łatwe do znalezienia błędy w samodzielnie napisanej aplikacji	Regularnie czytaj aktualne ogłoszenia o nowych lukach w aplikacji CMS[18] i **poprawiaj błędy natychmiast po ich znalezieniu**.
Przejęcie kontroli nad systemem operacyjnym serwera.	Brak aktualizacji systemu operacyjnego.	Zawsze włączaj automatyczne aktualizacje w systemie operacyjnym serwera.

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

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


www.mojaszkola.edu.pl
BEZPIECZEŃSTWO STRONY INTERNETOWEJ
Twórz mocne hasła
4A$ikoU#
www
Webmaster tools
Aktualizuj CMS
(system zarządzania treścią)
CLOUDFLARE
Zarejestruj stronę
Rób backup!
+EMET (Windows)
+AppArmor (Linux)
+akutalizuj OS

6.3. Dziennik elektroniczny i inne internetowe serwisy transakcyjne

Z punktu widzenia świadczonych funkcji 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 będzie zawierać specjalny panel administracyjny, to ta część serwisu będzie przykładem części transakcyjnej. **Serwisem transakcyjnym będzie również osobny dziennik internetowy, system obiegu dokumentów czy serwis dostępu do skrzynek poczty elektronicznej.**

6.3.1. Zagrożenia

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, umowne 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 w stosunku do tych serwisów.

6.3.2. Porady – czego wymagać od dostawców

W przypadku stron zamawianych u zewnętrznych dostawców zamawiający musi wprost wskazać pewne wymagania związane z bezpieczeństwem. Poniżej prezentujemy najważniejsze i absolutnie konieczne – “serwis” oznacza całość stron składających się na daną witrynę internetową wraz z oprogramowaniem, a “strony” oznaczają jego pojedyncze podstrony.

- 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 oraz stosuje zabezpieczenia rekomendowane przez OWASP Application Security Verification Standard.
- 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[19].

- Odporność na ataki jest potwierdzona z użyciem testu penetracyjnego lub skanu bezpieczeństwa serwisu, przeglądu lub skanu kodu źródłowego oprogramowania wykonanego przez osoby inne niż zespół projektujący i tworzący dany serwis.
- Usługa pomocy technicznej 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.

W 2012 roku weszło w życie rozporządzenie w sprawie Krajowych Ram Interoperacyjności (Dz. U. 2012, poz. 526), które w rozdziale IV, zawiera wykaz wymagań wobec systemów teleinformatycznych instytucji publicznych. Są to wymagania zgodne z najlepszymi praktykami inżynierskimi, wymienionymi także w tym poradniku, licznie odwołujące się do krajowych i międzynarodowych standardów branżowych. Na szczególną uwagę zasługują wymagania dotyczące bezpieczeństwa oraz dostępności serwisów dla osób niepełnosprawnych[20].

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

- Serwer wirtualny (VPS) – maszyna wirtualna z wybranym przez zamawiającego systemem operacyjnym, działająca w ramach fizycznego serwera, współdzielona z wieloma innymi użytkownikami. Z punktu widzenia użytkownika VPS jest całkowicie autonomicznym systemem operacyjnym, jednak izolacja od innych maszyn wirtualnych ma charakter wyłącznie logiczny, a nie fizyczny.
- Serwer dedykowany – fizyczny komputer umieszczony w serwerowni dostawcy, przydzielony na wyłączność 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 (uruchomionych jednocześnie programów), 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.

---

[19] Kontrola właściciela strony nad wyszukiwarkami internetowymi często bywa lekceważona. Tymczasem to właśnie wyszukiwarki są najczęściej pierwszym narzędziem, przy pomocy którego intruzi wyszukują ofiary. Warto zaznaczyć, że wyszukiwarki przez jakiś czas utrzymują w pamięci podręcznej kopie zindeksowanych stron, nawet jeśli usunięto je z oryginalnego serwisu (GIODO przypomina jak zabezpieczać serwisy przed wyciekiem). Najprostszą metodą jest stworzenie pliku robots.txt; zalecane jest też zarejestrowanie strony w usługach Google Webmaster Tools i Bing Webmaster Tools.

[20] Wymagania są oparte o międzynarodowy standard Web Content Accessibility Guidelines (WCAG) 2.0, przystępnie podsumowany na stronie projektu DostepneStrony.pl.

Wybór odpowiednich metod ma istotne znaczenie z punktu widzenia bezpieczeństwa. W każdym przypadku ktoś – albo właściciel serwisu, albo platformy hostingowej – musi być odpowiedzialny za bezpieczeństwo usługi i przetwarzanych oraz magazynowanych z jej udziałem danych, ale zakres tej odpowiedzialności może być różny. W przypadku serwera lokalnego sprawa jest jasna – jego właścicielem i operatorem jest szkoła.

Gdy mamy do czynienia z utrzymywaniem serwisu na serwerze zewnętrznym, odpowiedzialność nie jest już tak jednoznaczna i jej konkretny zakres musi wynikać z umowy:

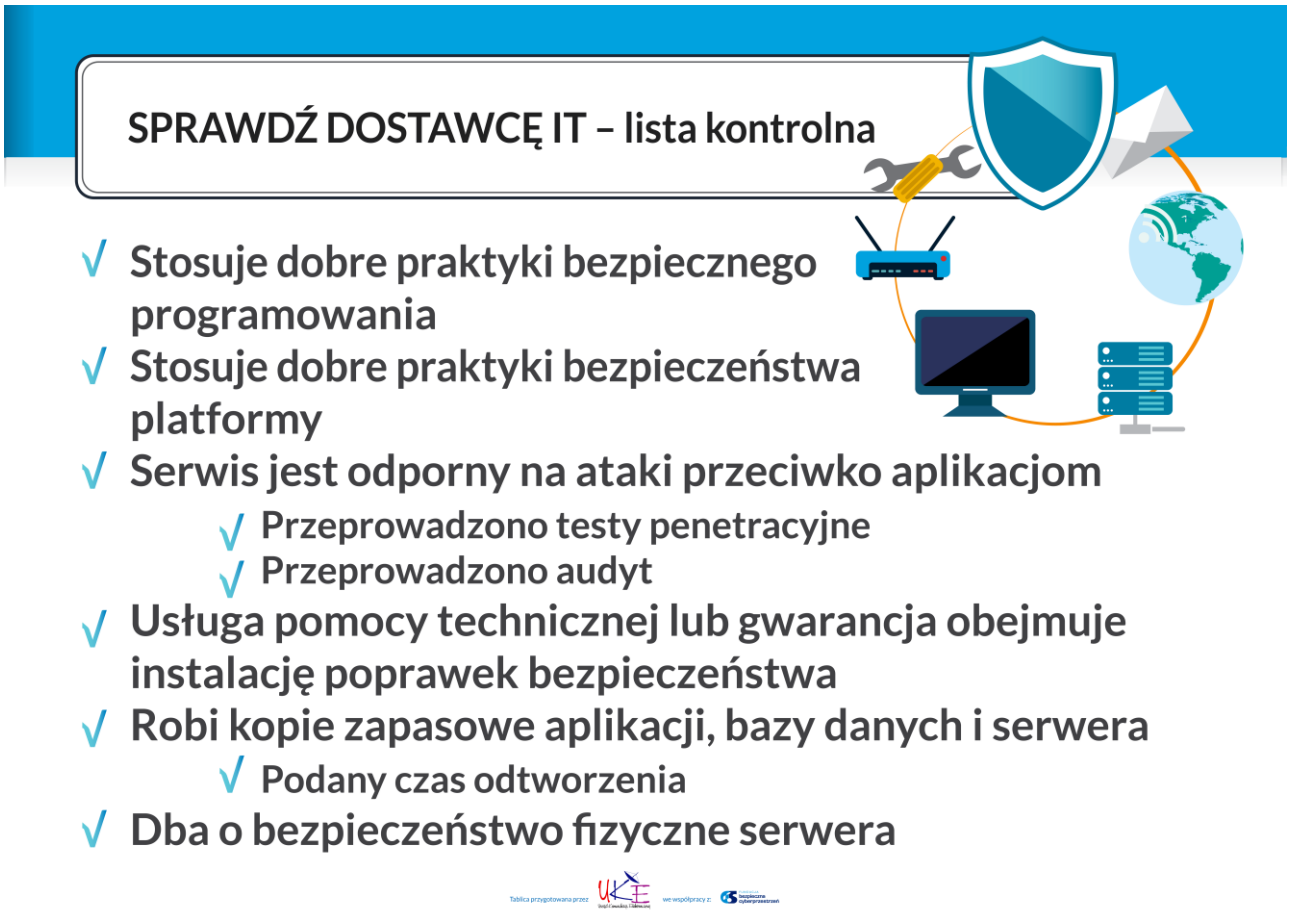
- Kto odpowiada za tworzenie kopii zapasowych oprogramowania serwera, aplikacji i bazy danych?
- Jaka jest częstotliwość ich tworzenia?
- Kto odpowiada za ich odtworzenie w razie awarii?
- Po jakim czasie od wystąpienia awarii dane zostaną odtworzone, a serwis przywrócony do stanu poprzedniego?
- Kto odpowiada za instalowanie aktualizacji systemu operacyjnego?
- Jak szybko po publikacji uaktualnień 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 w postaci jawnej, to musimy mieć możliwość określenia geograficznej lokalizacji danych. W przypadku chmur może to być utrudnione.

W praktyce dane wrażliwe utrzymywane są wyłącznie na serwerach fizycznych będących w wyłącznej dyspozycji właściciela, czyli w jego własnej serwerowni. Dane mniej wrażliwe można przechowywać i przetwarzać 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 w tzw. chmurach.

W 2016 Najwyższa Izba Kontroli opublikowała “Podręcznik kontroli systemów informatycznych”. Jest to obszerny dokument niezwykle przydatny dla osób nie tylko kontrolujących, ale także zamawiających i projektujących systemy informatyczne dla sektora publicznego.



6.4. Działania profilaktyczne

Testy bezpieczeństwa pozwalają na wykrycie i naprawienie usterek bezpieczeństwa zanim aplikacja zostanie udostępniona szerszej publiczności. Na tym jednak nie koniec – nowe błędy są często odkrywane już w trakcie eksploatacji usługi. Nie muszą to być luki w samej stronie WWW (które powinny być znalezione w testach), mogą to być usterki w systemie operacyjnym i komponentach używanych do budowy serwisu. Dlatego bezpieczeństwo usługi musi mieć charakter wielopoziomowy.

Warto zapamiętać kilka zasad, które minimalizują ryzyko występowania incydentów związanych z bezpieczeństwem:

- W przypadku systemów operacyjnych i innego oprogramowania działającego na serwerach stosujemy dokładnie te same zasady, o których pisaliśmy w rozdziale 4. Kluczowe są **częste aktualizacje** oraz dodatkowe zabezpieczenia na poziomie systemu operacyjnego, takie jak EMET dla Windows czy AppArmor dla GNU/Linuksa.
- Ustawmy silne hasła do paneli administracyjnych. W styczniu 2012, gdy doszło do włamania na stronę Kancelarii Prezesa Rady Ministrów, włamywacze ujawnili, że dostęp do panelu administracyjnego możliwy był dzięki nazwie użytkownika *admin* i hasłu *admin1* – nie powtórzmy tego błędu.
- Zarejestrujmy stronę w darmowych usługach związanych z bezpieczeństwem:
    - Google Webmaster Tools oraz Bing Webmaster Tools – panele administracyjne popularnych wyszukiwarek. Dają znacznie większą kontrolę nad wynikami wyszukiwania dla utrzymywanych stron. **Rejestracja strony pozwoli na przykład szybko usunąć z wyników wyszukiwania niefortunnie opublikowane danych.**

- CloudFlare – usługa ochrony stron przed przeciążeniem i atakami, zwłaszcza zagrożeniami **blokadą usług** (ang. *denial-of-service*, skr. DoS) i **rozproszoną blokadą usług** (ang. *distributed-denial-of-service*, skr. DDoS) również pozwala korzystać z darmowego wariantu. CloudFlare nie wymaga instalacji oprogramowania na serwerze, a wdrożenie polega na podmianie serwerów DNS przypisanych stronie WWW obejmowanej ochroną. Dla CloudFlare'a dostępnych jest wiele rozszerzeń zapewniających dodatkową ochronę, np. darmowa wersja Dome9.

- Skorzystajmy z darmowych narzędzi chroniących serwery WWW i działające na nich aplikacje:
  - ModSecurity – zaawansowana, bezpłatna zapora aplikacyjna przeznaczona dla serwisów webowych działających pod kontrolą serwera Apache;
  - URLScan – zapora aplikacyjna współpracująca z serwerem Microsoft IIS.

6.4.1. Kopie zapasowe zasobów

Awarie sprzętu komputerowego i nośników danych są zjawiskiem nieuniknionym. Dochodzi do nich w wyniku zdarzeń losowych (pożary, zalania, burze), zużycia sprzętu jak i wad powstałych w procesie produkcji[21].

Zachowanie elementarnych zasad bezpieczeństwa opracowanych w ramach badań nad ciągłością działania (ang. *business continuity*) pozwala na uniknięcie negatywnych konsekwencji awarii.

- **Kopie zapasowe tworzone na nośnikach lokalnych.** Zarówno systemy Windows jak i Mac OS X (Time Machine) umożliwiają automatyczne zapisywanie kopi zapasowych danych użytkownika na zewnętrznych nośnikach. Dobrym rozwiązaniem przy pracy zespołowej jest też korzystanie z foldera sieciowego fizycznie znajdującego się na serwerze plików. Oczywiście, serwer plików musi również być regularnie zapisywany do kopii zapasowych.
- **Kopie zapasowe w chmurze.** Bardzo popularne obecnie rozwiązania tego typu umożliwiają automatyczne kopiowania wszystkich plików ze wskazanego folderu do foldera sieciowego utrzymywanego w chmurze obliczeniowej. Folder ten można następnie powielać na dowolnej liczbie komputerów.

Najpopularniejszy serwis ostatniego typu, czyli Dropbox budzi jednak wątpliwości z punktu widzenia bezpieczeństwa i ochrony danych osobowych, ponieważ operator serwisu może uzyskać dostęp do przesyłanych tam danych.

Zasady tworzenia kopii zapasowych muszą być jasno opisane w polityce bezpieczeństwa. Jeszcze ważniejsze jest jednak cykliczne ich testowanie - czy nadal jesteśmy w stanie odtworzyć pliki z kopii zapasowej, czy też może przez kilka miesięcy nie były one poprawnie zapisywane np. z powodu awarii nośnika?

---

[21] Według badań przeprowadzonych przez Google w 2007 roku niemal 2% nowych dysków ulegała awarii po roku pracy, zaś po trzech latach przestawało działać już prawie 9%.

6.5. Obowiązki prawne

6.5.1. 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 z użyciem:

- 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 więc opisać procedury:
  - przyznawania dostępu,
  - odbierania dostępu (np. w razie zwolnienia lub przeniesienia do innego działu),
  - cyklicznego weryfikowania listy uprawnionych osób;
- uwierzytelnienie użytkowników mających dostęp do danych – na przykład z użyciem nazwy użytkownika i hasła, albo odpowiednich uprawnień dostępu w systemie operacyjnym;
- szyfrowania danych osobowych oraz haseł przesyłanych przez sieć, np. z użyciem 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.

6.5.2. 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 – ang. *cookies*[22]).

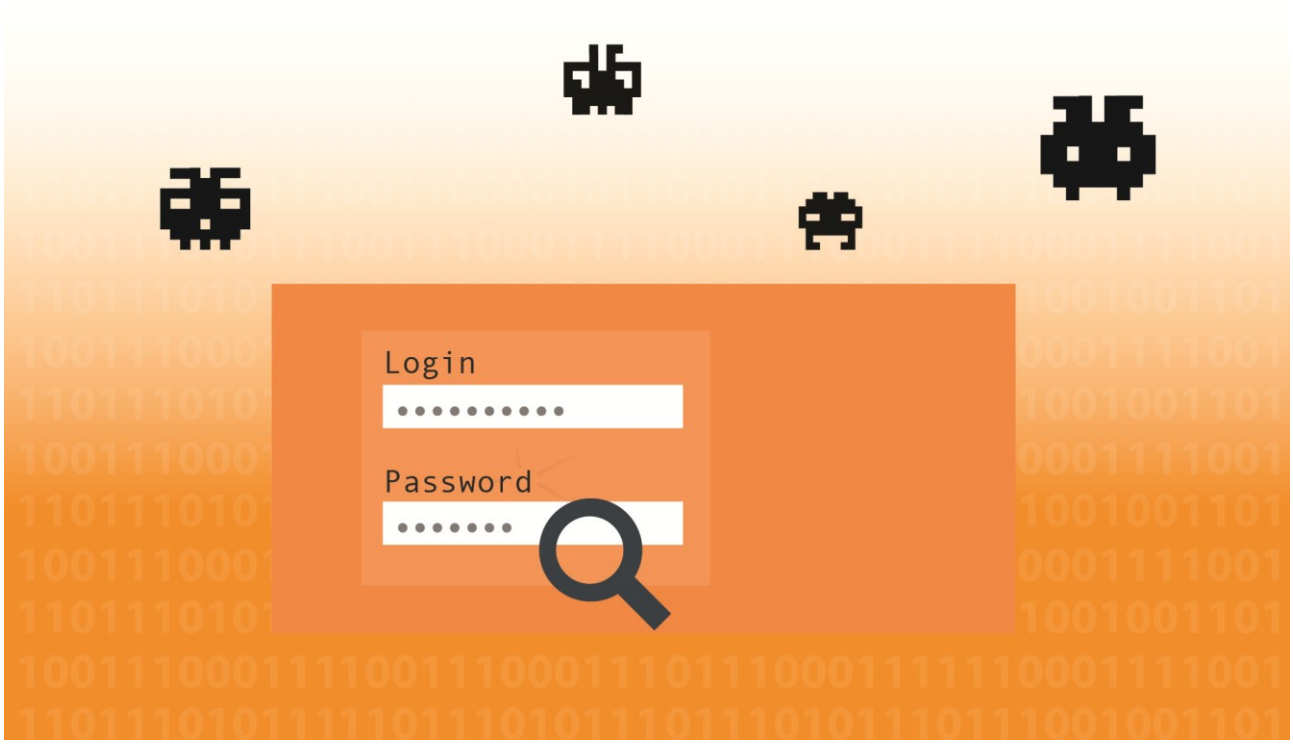
Konkretny sposób realizacji tego obowiązku jest różnie interpretowany. Większość stron komercyjnych dla uniknięcia ewentualnych sporów interpretacyjnych wyświetla wyraźne okno z informacjami o stosowaniu ciasteczek, zasłaniające część strony i wymagające kliknięcia. Z drugiej strony większość stron rządowych realizuje ten obowiązek przez umieszczenie dobrze

[22] Paweł Krawczyk, *“Cookies - niedźwiedzia przysługa”*, Computerworld, 27 kwietnia 2012.

widocznego (np. na górze strony) odnośnika do podstrony zawierającej szczegółowe informacje o stosowanych ciasteczkach[23].

Nie ma zatem powodu, aby stosować techniki dalej idące niż te stosowane np. na stronach GIODO.

[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.org.



7. Hasła

Przy pomocy szybkich programów, testujących hasła w tempie kilku milionów na sekundę (!), te najprostsze można odgadnąć już w kilkanaście minut, a dłuższe w kilka godzin lub dni. Jednak nie jest to żaden problem dla zdeterminowanego włamywacza – uruchamia program i zajmuje się czym innym, aż którekolwiek z haseł "padnie".

Tymczasem hasła mogą być i łatwe do zapamiętania, i trudne do odgadnięcia. Oto kilka zasad:

- **Hasła od dawna nie muszą już mieć ośmiu znaków**. Kiedyś bezpieczne hasło kojarzyło się z niezrozumiałą zbitką znaków bo ówczesne systemy musiały zmieścić się w ośmiu znakach. Obecnie hasła mogą zawierać odstępy i znaki przestankowe, a nawet polskie litery i mieć długość całych zdań (zwykle do 128 znaków).
- **Najbezpieczniejszym hasłem jest zatem po prostu grupa kilku słów lub całe zdanie.** Na przykład *"Litwo! ojczyzno! moja!"* jest praktycznie nie do złamania z użyciem słownika[24]. Użytkownicy tradycyjnie korzystają z prostych haseł (jak *"marysia"*) bo są łatwe do zapamiętania. Nauczmy ich, że kilka słów (np. *"marysia hestia kabanos"*) jest równie łatwe do zapamiętania, a o wiele bardziej bezpieczne.
- O ile polskich liter lepiej unikać, bo nie wiemy z jakiej klawiatury przyjdzie nam się logować, o tyle ze spacji i znaków specjalnych (+-,.=_{}[];:"\/?><!@#$%^&*) możemy korzystać do woli. **Każdy znak specjalny to znaczne utrudnienie dla włamywacza.**

O powyższych zasadach użytkownicy muszą wiedzieć – należy ich o nich poinformować, zachęcić do korzystania z takich "długich haseł" i przełamać nawyki wyniesione ze starych książek i regulaminów, mówiące o ośmioznakowych hasłach składających się z losowych liter oraz cyfr i przez lata bezrefleksyjnie powtarzanych. Trzeba mówić o tym wprost, pokazywać na przykładach

[24] 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".

i zdać się na erudycję użytkowników. Wymagania te powinny być opisane w polityce bezpieczeństwa (o niej w dalszej części poradnika).

Kolejnym problemem, z którym borykamy się dziś jest **zarządzanie hasłami do wielu serwisów**. Jedno do banku, drugie do poczty, trzecie do szkolnej strony i tak dalej. Łatwo się pogubić i wiele osób rozwiązuje ten problem używając wszędzie tego samego hasła. Jest to rozwiązanie fatalne - jeśli ktoś je pozna (jakkolwiek), będzie mógł uzyskać dostęp do wszystkich serwisów. **Do każdego serwisu należy zatem koniecznie stosować osobne hasła.** Tylko jak je zapamiętać?

7.1.1. Zarządzanie hasłami

Tutaj z pomocą przychodzą **programy do zarządzania hasłami** (ang. *password managers*)**,** które umożliwiają bezpieczne zapamiętywanie i przechowywanie nawet setek haseł. Muszą być one zawsze zabezpieczone jednym **hasłem głównym** (ang. *master password*), które chroni wszystkie pozostałe. Jeśli narzędzia tego typu wbudowane są w przeglądarki internetowe to tym lepiej, bo zapamiętają hasła po pierwszym wpisaniu na danej stronie, a przy kolejnym logowaniu wprowadzą w odpowiedni formularz, wyręczając użytkownika.

Wśród popularnych narzędzi do zarządzania hasłami 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 wykraść wszystkie hasła. Przeglądarki zapamiętują tylko hasła do aplikacji webowych, ale już nie do tych instalowanych na komputerze.
- LastPass oraz 1Password – usługi komercyjne zintegrowane z większością przeglądarek, o bardzo rozbudowanych funkcjach (np. generowanie haseł, wymiana haseł między użytkownikami) przechowujące dane w chmurze.
- KeePass – otwarte oprogramowanie pozwalające na edytowanie i bezpieczne przechowywanie listy haseł w zaszyfrowanym pliku. Może zapamiętywać dowolne hasła i notatki. Integracja z przeglądarkami za pomocą wtyczek.
- PwdHash – strona, która z podanego hasła oraz adresu URL generuje silne hasło, unikalne dla tej strony. Dzięki temu można pamiętać tylko jedno hasło “główne” dla wielu stron, a faktycznie na każdej z nich mieć ustawione inne hasło. *PwdHash* ma jedną ogromną zaletę - działa w każdej przeglądarce, nie wymaga instalacji czegokolwiek, więc można go używać w sytuacjach awaryjnych. Dostępne także w postaci wtyczek dla Chrome i Firefoksa, ale można go używać bez nich.

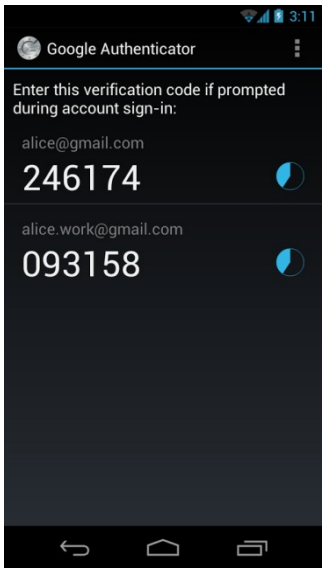
Programy do zarządzania hasłami zaakceptowane do stosowania w danej instytucji powinny być wymienione w polityce bezpieczeństwa.

7.1.2. Uwierzytelnianie wieloskładnikowe

Tradycyjne hasła mają jedną zasadniczą zaletę - można je podsłuchać, ukraść lub złamać bez wiedzy ofiary. W sieci regularnie publikowane są hasła wykradzione przez włamywaczy z różnych serwisów internetowych - oznacza to, że każde z kont może zostać praktycznie natychmiast przejęte, a oryginalny właściciel może się o tym nawet nie dowiedzieć.

Z tego powodu od dawna podejmowano próby wprowadzenia metod uwierzytelniania, które byłyby odporne na podsłuch - na przykład haseł jednorazowych czy uwierzytelniania opartego o różnego rodzaju moduły sprzętowe - generatory haseł i karty kryptograficzne. Zapewniają one wysoki poziom bezpieczeństwa, ale są niestety kosztowne we wdrożeniu i codziennej obsłudze.

Istnieje jednak co najmniej kilka rozwiązań, które można uruchomić stosunkowo niskim kosztem i stosować we własnych aplikacjach webowych. Jednym z nich jest Google Authenticator, który jest darmowym generatorem haseł jednorazowych. Oprogramowanie go po stronie aplikacji webowej jest stosunkowo proste, a klienta można zainstalować na większości urządzeń mobilnych (tablety, smartfony itd.).



Google Authenticator w systemie Android. Fot. Google

Rozwiązaniem czysto sprzętowym jest YubiKey, generator haseł jednorazowych, który, po wetknięciu do portu USB "udaje" klawiaturę. Po wciśnięciu przycisku "wpisuje" do wybranej aplikacji jednorazowe hasło, dzięki czemu nie wymaga po stronie klienta żadnego oprogramowania czy sterowników.

YubiKey. Fot. YubiCo

Również rządowy system ePUAP oferuje usługę bezpiecznego logowania (ang. *single sign-on*) dla aplikacji zewnętrznych[25].

[25] Przydatne informacje praktyczne z integracji serwisów WWW z ePUAP można znaleźć na stronie http://www.extern.pl/artykuly/

8. Edukacja i uświadamianie użytkowników

W minionych latach cyberprzestrzeń stała się miejscem, w którym możemy spotkać się z zagrożeniami różnego typu. Szkodliwe oprogramowanie na systemy tradycyjne i mobilne, aplikacje szyfrujące całe dyski twarde, fałszywa korespondencja, phishing itp., to ataki, na które szkoły są narażone każdego dnia i mogą spowodować znaczne straty nie tylko finansowe, ale i wizerunkowe.

Cyberprzestępcy większość ataków rozpoczynają wykorzystując **metody socjotechniczne**. Zwykle ich celem są najmniej świadomi pracownicy. Przestępca zakłada bowiem, że najłatwiej będzie mu skłonić ich do działań pozwalających na uzyskanie praw dostępu do zasobów informatycznych lub instalację złośliwego oprogramowania (wystarczy kliknąć w link z wiadomości e-mail, otworzyć zawirusowaną stronę lub rozpakować załącznik).

Zatem prowadzenie działań uświadamiających o zagrożeniach teleinformatycznych jest kluczowe dla całego systemu bezpieczeństwa szkoły i powinno dotyczyć każdego szczebla, ponieważ każdy z pracowników może się okazać najsłabszym ogniwem w systemie zabezpieczeń.

Z tego powodu, wzmacnianie warstwy ochronnej powinno zacząć się od odpowiedniego przeszkolenia osób wykorzystujących zasoby informatyczne. Wszystkich. Cały personel powinien poznać zasady bezpieczeństwa komputerowego oraz metody działań cyberprzestępców, podnosząc tym samym ochronę teleinformatyczną organizacji.

Głównym celem szkoleń powinno być zatem uświadomienie personelowi zagrożeń komputerowych poprzez pokazanie metod rozpoznawania najpopularniejszych ataków, sposobów przeciwdziałania, a także, a może i przede wszystkim, procedur reagowania na nie.

9. Studium przypadków

Większość dostępnych informacji o włamaniach do systemów szkolnych dotyczy bezpośrednio ich uczniów, którzy mieli jasną motywację – poprawić swoje oceny. Widać też, że reprezentują oni różne poziomy umiejętności, jednak w większości przypadków dostęp do dzienników był możliwy poprzez uzyskanie danych do logowania nauczycieli.

Na uwagę zasługuje przypadek z Poznania[26], w którym uczeń zastosował modus operandi znany z włamań na konta bankowe (bankowość internetowa). Stworzył on bowiem stronę internetową wyglądającą jak panel logowania do e-dziennika. Zaprogramował ją w ten sposób, aby wszystkie dane na niej wpisywane (login użytkownika i hasło) były utrwalane i przesyłane do niego. Wystarczyło więc jeszcze przekonać któregoś z nauczycieli do odwiedzenia spreparowanej strony i wpisania swoich danych uwierzytelniających. Nie jest do końca jasne w jaki sposób do tego doszło. Możemy domniemywać. Uczeń mógł wysłać mail z linkiem do swojej strony do nauczyciela z przekonującą prośbą o jego otworzenie. Mógł otworzyć ją na komputerze w pracowni szkolnej i czekać na logowanie nauczyciela. Mógł też podmienić link w zasobach, do których udało mu się uzyskać dostęp. Mógł również zainfekować komputer nauczyciela oprogramowaniem, którego jedynym zadaniem było przekierowanie przeglądarki internetowej na skompromitowaną witrynę.

Błędnie skonfigurowane szkolne WiFi, o którym pisaliśmy, mogło być przyczyną kradzieży hasła nauczyciela w Starogardzie Gdańskim[27]. Jeden z uczniów przez dwa lata penetrował system informatyczny swojej szkoły. Wg opinii pozostałych uczniów, zapewne dobrze poinformowanych, włamywał się on na różne konta i podrabiał wejście do pokoju nauczycielskiego. Podobno pisał o tym nawet na swoim blogu. Mógł mieć dostęp również do dziennika, konta dyrektora, do jego komputera.

Nie powinno pozostawać też bez komentarza, że zdarzają się przypadki, w których uczniowie w sposób przypadkowy mogą wejść w posiadanie danych uwierzytelniających[28]. Dlatego też warto zwracać uwagę czy uczniowie nie stoją za plecami logującego się nauczyciela, nie zapisują hasła na kartkach lub czy „wylogowują" się po zakończonych czynnościach.

Skutki włamań na strony internetowe szkół to przede wszystkim straty wizerunkowe[29]. Ten aspekt z kolei lubią wykorzystywać aktywiści i wszystkie inne ugrupowania polityczne, społeczne czy religijne by zaistnieć i przekazać swoje żądania.

10. Literatura przedmiotu

- *"Bezpieczeństwo informacyjne"*, Krzysztof Liderman, PWN, 2012
- *"OWASP Application Security Verification Standard Project"*, OWASP, 2009
- *"Podręcznik kontroli systemów informatycznych"*, Najwyższa Izba Kontroli, 2016
- *„Bezpieczeństwo informatyczne szkół i instytucji publicznych", Paweł Krawczyk*

---

[26] http://www.gloswielkopolski.pl/artykul/376527,poznan-mlody-haker-zmienial-szkolne-oceny,id,t.html

[27] http://m.radiogdansk.pl/index.php/wiadomosci/item/23891-mogl-zmieniac-oceny-jak-chcial-uczen-zhakowal-serwer-szkoly-w-starogardzie-gd/23891-mogl-zmieniac-oceny-jak-chcial-uczen-zhakowal-serwer-szkoly-w-starogardzie-gd.html

[28] http://newsbook.pl/2016/08/14/wlamanie-do-elektronicznego-dziennika-w-szkole-uczen-poprawial-oceny/

[29] http://www.dziennikbaltycki.pl/wiadomosci/nowy-dwor-gdanski/a/islamscy-hakerzy-zaatakowali-strone-szkoly-w-nowym-dworze-gdanskim,9984107/