cyfrowo bezpieczni.pl

BEZPIECZNA SZKOŁA CYFROWA

BEZPIECZNA SZKOŁA CYFROWA

Zalecenia i rekomendacje

dla samorządów - realizatorów projektów
w ramach unijnej perspektywy budżetowej 2014-2020

Dokument został opracowany przez Stowarzyszenie „Miasta w Internecie" - realizatora projektu *Cyfrowobezpieczni.pl – Bezpieczna Szkoła Cyfrowa*, finansowanego przez Ministerstwo Edukacji Narodowej w ramach rządowego programu wspomagania w latach 2015-2018 organów prowadzących szkoły w zapewnieniu bezpiecznych warunków nauki, wychowania i opieki w szkołach – „Bezpieczna+"

MINISTERSTWO
EDUKACJI
NARODOWEJ

Autorzy

Anna Borkowska , Ośrodek Rozwoju Edukacji
Krzysztof Głomb, Stowarzyszenie „Miasta w Internecie"
Andrzej Grzybowski, Intel Technology Poland
Michał Jaworski, Microsoft Polska
Barbara Kędzierska, Uniwersytet Pedagogiczny w Krakowie
Tomasz Kruk, Politechnika Warszawska
Tomasz Kuczyński, Poznańskie Centrum Superkomputerowo-Sieciowe
Michał Sołtan, IRS
Agnieszka Wrońska, NASK

Konsultacja

Krzysztof Silicki, NASK

Redakcja

Krzysztof Głomb, Stowarzyszenie „Miasta w Internecie"

Warszawa, grudzień 2016 r.

SPIS TREŚCI

WPROWADZENIE

1. Dokument zawiera pakiet zaleceń i rekomendacji dla samorządów wojewódzkich i lokalnych, które planują realizację w latach 2014-2020 projektów edukacyjnych oraz infrastrukturalnych, finansowanych ze środków Regionalnych Programów Operacyjnych, ukierunkowanych na podnoszenie kompetencji cyfrowych i informacyjnych nauczycieli oraz uczniów, a także zapewniających szkołom nowoczesne wyposażenie w sprzęt cyfrowy i szerokopasmowy dostęp do Internetu.

2. Zalecenia i rekomendacje odnoszą się wyłącznie do tematyki bezpieczeństwa cyfrowego w szkołach, a celem tej publikacji jest wsparcie twórców projektów w ich merytorycznym przygotowaniu i skutecznej realizacji.

3. Przedstawione zalecenia i rekomendacje pozwolą wdrożyć systemy i rozwiązania technologii informacyjno-komunikacyjnych (TIK) - w pełni funkcjonalne, bezpieczne i przystosowane do realizacji zadań dydaktycznych i administracyjnych.

4. Jeśli w projektach planowanych do realizacji w latach 2015-2020 wykorzystywane będą dotychczas eksploatowane urządzenia i oprogramowanie, to powinny one spełniać wymagania niniejszych zaleceń i rekomendacji. W przypadku niespełniania niniejszych zaleceń i rekomendacji należy dokonać analizy ryzyka i oceny zagrożeń wynikających z wykorzystania elementów niezgodnych z niniejszymi zaleceniami i rekomendacjami. Decyzja o pozostawieniu takich elementów - a tym samym potencjalnym obniżeniu poziomu bezpieczeństwa w szkole - powinna być podjęta z całą świadomością konsekwencji z nich wynikających.

5. Przedstawione w dokumencie zalecenia i wnioski zostały sformułowane w wyniku analizy doświadczeń zdobytych podczas realizacji rządowego programu rozwijania kompetencji uczniów i nauczycieli w zakresie stosowania technologii informacyjno-komunikacyjnych „Cyfrowa Szkoła" oraz w trakcie realizacji w latach 2010-2014 regionalnych projektów edukacyjnych.

I. REKOMENDACJA STRATEGICZNA

Projekty unijnej perspektywy finansowej 2014-2020 powinny uwzględniać problematykę zapewnienia bezpieczeństwa w szkole ery cyfrowej[1], w kontekście:

- zagrożeń online związanych z pozyskiwaniem, przetwarzaniem i publikowaniem informacji w sieci,
- technicznym - związanym z inwestycjami w nowoczesne urządzenia cyfrowe
- organizacyjnym - wdrożenie polityki bezpieczeństwa cyfrowego
- zapewnienia wysokiej jakości dostępu do Internetu.

Niezbędne jest także włączenie tematyki bezpieczeństwa cyfrowego do programu projektów edukacyjnych dla wszystkich użytkowników TIK w szkole.

II. REKOMENDACJE DLA PROJEKTÓW EDUKACYJNYCH

1. W projektach edukacyjnych należy zapewnić realizację komponentów szkoleniowych umożliwiających nabywanie przez uczniów, nauczycieli oraz kadry zarządzające szkolną infrastrukturą cyfrową umiejętności bezpiecznego i odpowiedzialnego korzystania z narzędzi i treści cyfrowych. W działaniach tych należy uwzględnić także elementy podnoszące poziom wiedzy rodziców na temat bezpiecznego korzystania przez dzieci z zasobów Internetu.

2. Działania edukacyjne i organizacyjne w projektach powinny obejmować tematykę kompetencji informacyjnych, a to:

    a. uwarunkowań przekazu medialnego (odbioru, interpretacji i publikowania)
    b. odpowiedzialnego i efektywnego poszukiwana wiarygodnych informacji
    c. krytycznej analizy treści
    d. ochrony danych wrażliwych (w szczególności danych osobowych)
    e. kształtowania własnego obrazu użytkownika w sieci

[1] W niniejszym dokumencie stosujemy także wymiennie określenia: bezpieczeństwo cyfrowe i cyberbezpieczeństwo

f. poszanowania praw autorskich i własności intelektualnej
g. stanowienia i utrzymywania polityki bezpieczeństwa cyfrowego
h. pomocy dla użytkowników systemów i narzędzi TIK w zakresie podanym powyżej.

3. W szczególności, w projektach edukacyjnych należy uwzględnić:

3.1 działania edukacyjne adresowane do uczniów:

a. zajęcia na temat bezpiecznego korzystania z TIK, obejmujące także aspekty prawne[2], ze szczególnym uwzględnieniem korzystania z Internetu w celach edukacyjnych
b. zajęcia warsztatowe ukierunkowane na: nabywanie kompetencji informacyjnych, bezpieczne korzystanie z technologii, świadomy i krytyczny odbiór przekazu medialnego oraz na kształtowanie i promowanie pozytywnych postaw i odpowiedzialnych decyzji odnoszących się do ryzykownych i niebezpiecznych zachowań w Internecie
c. zajęcia na temat zasad polityki bezpieczeństwa cyfrowego przyjętych w szkole, w tym procedur reagowania w sytuacjach zagrożenia, a także zajęcia upowszechniające wśród uczniów informacje o punktach pomocy, infoliniach, telefonach zaufania dla dzieci i młodzieży, w których można zgłaszać przypadki niebezpiecznych zdarzeń w Internecie
d. uczniowskie „projekty edukacyjne", uwzględniające - twórcze i odpowiedzialne wykorzystywanie Internetu jako źródła informacji oraz promujące zróżnicowane formy wykorzystywania Internetu i innych środków komunikacyjnych.

3.2 działania edukacyjne i organizacyjne adresowane do nauczycieli przedmiotów nie-informatycznych oraz kadry zarządzającej szkołami:

a. warsztaty z zakresu umiejętności obsługi sprzętu cyfrowego (w tym mobilnego), a zwłaszcza wykorzystania go w codziennej praktyce nauczania metodami dydaktycznymi inspirującymi i aktywizującymi ucznia[3], prowadzone w modelu pełnego dostępu uczestnika do sprzętu
b. zajęcia poświęcone edukacji medialnej i profilaktyce zagrożeń (m.in. wiedzy o zasadach bezpiecznego korzystania z TIK, zagrożeniach, czynnikach ryzyka, a także nabywaniu umiejętności rozpoznawania zagrożeń oraz podnoszące kompetencje nauczycieli w zakresie udzielania wsparcia uczniom w sytuacji doświadczenia zagrożeń)
c. zajęcia mające na celu przygotowanie nauczycieli wszystkich przedmiotów do (będącego konsekwencją hipertekstowego (cyfrowego) przekazu informacji) nowych metod i form prowadzenia zajęć; medialny (fragmentaryczny) sposób pozyskiwania i przetwarzania informacji modyfikuje proces poznawczy współczesnego człowieka. Metody uczenia się

[2] M.in. konsekwencje wykorzystania plików z nieznanych źródeł, udostępniania materiałów w sieci ze szczególnym uwzględnieniem korzystania z Internetu w celach edukacyjnych oraz radzenia sobie z zagrożeniami online takimi, jak: szkodliwe i nielegalne treści; niebezpieczne kontakty, anonimowe i zafałszowane dane osobowe, zachowania ryzykowne, seksting i aktywność seksualna; agresja elektroniczna i cyberprzestępczość (w tym oszustwa komputerowe, hacking, szpiegostwo komputerowe)

[3] M.in. odwrócona klasa, kształcenie hybrydowe, nauczanie problemowe, metoda projektowa, web quest i gamifikacja

bazujące jedynie na linearnej strukturze stały się nieefektywne i powinny być zastąpione metodami wielostronnie aktywizującymi

d. zajęcia na temat prawnych i organizacyjnych wymagań dotyczących bezpieczeństwa systemów TIK wykorzystywanych w szkole
e. zajęcia na temat zasad przygotowania i komunikowania wymagań bezpieczeństwa w szkole, w tym przygotowania i wdrożenia podstawowego zbioru zasad oraz procedur działania i reagowania w sytuacjach zidentyfikowanych jako niebezpieczne w cyberprzestrzeni placówki oświatowej, a także pojawiających się w związku z użytkowaniem sieci przez uczestników systemu (nauczycieli, innych pracowników szkoły, uczniów, rodziców).

3.3 szkolenia dla osób administrujących szkolną infrastrukturą o tematyce podstaw bezpieczeństwa cyfrowego w zakresie umożliwiającym uniknięcie błędów podczas bieżącej eksploatacji, obejmującej zagadnienia:

a. opracowywania i wdrażania polityk bezpieczeństwa cyfrowego w szkole
b. współczesnych zagrożeń systemów TIK oraz ogólnych zasad ochrony przed nimi
c. utwardzania (*hardening*) systemów i technologii (w tym konkretnych technologii używanych w chronionej infrastrukturze)
d. bezpiecznej konfiguracji sieci komputerowych
e. systemów bezpieczeństwa oraz zasad ich prawidłowej konfiguracji
f. bezpiecznego monitorowania działania sieci i systemów
g. bieżącej obsługi zabezpieczeń infrastruktury oraz metod postępowania w przypadku zaistnienia incydentu bezpieczeństwa TIK
h. stawiania wymagań techniczno-organizacyjnych dostawcom chmury obliczeniowej.

3.4 zajęcia edukacyjne dla rodziców – różnorodne zajęcia w formule spotkań informacyjnych, szkoleń lub wspólnych akcji z dziećmi na terenie szkoły, których celem będzie zwiększanie wiedzy prawnej, psychologicznej i technicznej rodziców na temat zagrożeń *online* oraz podnoszenie ich kompetencji wychowawczych w zakresie wprowadzania zasad bezpiecznego korzystania z sieci w domu.

4. Dla zapewnienia możliwie jak najwyższej jakości i efektywności podejmowanych działań niezbędne są: zrealizowanie na wstępnym etapie przygotowań do realizacji projektów - na poziomie samorządów lokalnych - badań sondażowo-diagnostycznych aktualnego poziomu kompetencji informacyjnych nauczycieli, uczniów i rodziców oraz dokonanie analizy zasobów infrastruktury i potrzeb szkoły.

III. REKOMENDACJE DLA PROJEKTÓW INWESTYCYJNYCH

1. Zapewnienie bezpieczeństwa cyfrowego winno być integralną częścią każdego projektu inwestycyjnego. Musi obejmować właściwe przygotowanie specyfikacji technicznych zamówień, przygotowanie do wdrożenia, uruchomienie (w tym niezależną startową ocenę bezpieczeństwa oraz przeszkolenie osób odpowiedzialnych za bieżącą obsługę systemu) i późniejszą eksploatację wdrożonych systemów (w tym podstawowe, niezależne i okresowe audyty bezpieczeństwa).

2. W ramach wszystkich projektów cyfrowej modernizacji szkół należy opracować i wdrożyć - jako obowiązujące wewnątrzszkolne przepisy prawne - politykę bezpieczeństwa cyfrowego w szkole (bezpiecznego korzystania z zasobów sieci oraz infrastruktury cyfrowej w szkole[4]). Polityka bezpieczeństwa uwzględniać musi wprowadzenie standardów i procedur zgłaszania incydentów oraz podejmowania interwencji w sytuacji wystąpienia zagrożenia (jak zgłaszać, do kogo, gdzie szukać pomocy, itp.). Wprowadzeniu takich regulacji towarzyszyć winny szkolenia dla uczniów, rodziców i nauczycieli przedmiotów nie-informatycznych oraz innych pracowników szkoły, a także działania uświadamiające adresowane do rodziców.

3. Projekty finansowane w perspektywie 2014-2020 powinny zapewnić bieżącą administrację szkolnej infrastruktury cyfrowej oraz utrzymanie odpowiedniego poziomu bezpieczeństwa. W zależności od przyjętego sposobu realizacji projektów może to oznaczać:

    a. zatrudnienie osoby odpowiedzialnej za lokalne zasoby infrastrukturalne
    b. wykorzystanie specjalistów obsługujących wiele jednostek (na poziomie organu prowadzącego szkoły), w tym poprzez zdalną administrację infrastrukturą w poszczególnych jednostkach
    c. postawienie odpowiednich wymogów dotyczących administracji i bezpieczeństwa dostawcom rozwiązań w chmurze obliczeniowej
    d. zlecenie opieki nad owymi zasobami zewnętrznej, wyspecjalizowanej instytucji
    e. realizację wszystkich tych działań jednocześnie na odpowiednim poziomie.

[4] Tak zdefiniowaną politykę bezpieczeństwa cyfrowego w szkole należy rozumieć jako zbiór zasad obejmujący procedury działania i reagowania w sytuacjach zidentyfikowanych i sklasyfikowanych jako występujące w cyberprzestrzeni szkoły oraz pojawiające się w związku z użytkowaniem sieci przez nauczycieli, uczniów i osób trzecich.

1. Sieci komputerowe

1.1 W ramach projektów planowanych do realizacji w latach 2014-2020 należy zapewnić elementarny **poziom bezpieczeństwa sieci komputerowych** wdrażanych w szkołach. W szczególności rozważyć należy odpowiednio skonfigurowany i poprawnie wdrożony system zapory sieciowej (*firewall*) nowej generacji (NGFW) o parametrach dopasowanych do aktualnych i przyszłych potrzeb szkoły. NGFW powinien:

a. posiadać funkcjonalność ssl-proxy umożliwiającą filtrowanie ruchu zaszyfrowanego
b. być wyposażony w regularnie aktualizowany system blokowania ruchu pod kątem filtrowania treści nieodpowiednich dla dzieci i młodzieży (*web-filtering*)
c. posiadać zainstalowany system IPS zapewniający zabezpieczenie sieci przed złośliwym oprogramowaniem (zarówno z wewnątrz sieci, jak i z zewnątrz (np. przez łącze internetowe).

1.2 Dla każdej sieci szkolnej konieczne jest opracowanie **osobnej architektury sieci**, która zapewni optymalne bezpieczeństwo zasobów. W szczególności konieczne jest wydzielenie w ramach sieci następujących podsieci:

a. podsieć dla **pracowni i laboratoriów**, w których działać będą komputery administrowane przez szkołę
b. podsieć dla **nauczycieli**, w której działać będą komputery będące w administracji szkoły, z których korzystać będą nauczyciele
c. podsieć dla **gości szkoły** - bezprzewodowa, w której działać będą wszelkie urządzenia przynoszone z zewnątrz (nie będące w administracji szkoły), w tym urządzenia należące do uczniów, wykorzystywane w modelu BYOD[5]
d. podsieć **administracyjna**, w której będą interfejsy administracyjne urządzeń i komputery administratorów (zalecane rozważenie podsieci dla księgowości i nauczycieli).

1.3 Okablowanie sieciowe powinno obejmować **wszystkie kluczowe pomieszczenia w szkole** i być wykonane przy użyciu kabla miedzianego, co najmniej kategorii 5e, co umożliwia przenoszenie danych z przepływnością do 1 Gbit/s.

1.4 Urządzenia sieciowe (przełączniki, *firewall*) muszą umożliwiać:

a. konfigurację wirtualnych sieci logicznych (VLAN) zgodnych z 802.1q, aby możliwe było odseparowanie podsieci, np. służącej do zarządzania, dla pracowników administracji szkoły lub uczniów, WiFi.
b. zdalną konfigurację i monitorowanie parametrów pracy. Funkcja *firewall* może być realizowana poprzez instalację dedykowanego sprzętu i/lub zakup odpowiedniej usługi. Poza filtrowaniem ruchu sieciowego, zapora sieciowa powinna mieć możliwość zapisywania

[5] Ang. Bring Your Own Device – przynieś swoje urządzenie

ruchu sieciowego do dziennika (log systemowy). Zapisy w logach mogą pomóc w ustaleniu źródeł ewentualnych ataków i prób naruszenia bezpieczeństwa. Ponadto dostarczają informacji o obciążeniu pasma internetowego.

1.5 Dla zapewnienia **bezpieczeństwa infrastruktury sieciowej** konieczne jest ponadto spełnienie następujących warunków **minimalnych**:

a. zainstalowanie centralnie zarządzanego systemu antywirusowego, dokonującego analizy przesyłanych treści pod kątem złośliwej zawartości lub – opcjonalnie – oprogramowania zabezpieczającego zasoby w chmurze
b. sprzęt sieciowy oraz pola krosowe okablowania miedzianego muszą być zainstalowane w dedykowanym chronionym pomieszczeniu lub, w przypadku braku takich możliwości, w pomieszczeniu o ograniczonym dostępie w zabezpieczonej szafie teletechnicznej. Urządzenia aktywne systemu powinny być przystosowane do montażu w szafie typu rack. Wskazane jest, aby terminal/modem łącza szkoły z Internetem został zainstalowany również w szafie typu rack. W miejscu, w którym będą instalowane aktywne urządzenia sieciowe, należy zapewnić odpowiednie zasilanie energetyczne oraz odpowiednią temperaturę (np. poprzez montaż klimatyzacji),
c. zapewnienie ochrony dostępu do sieci bezprzewodowej, opartej o dedykowaną bazę użytkowników oraz o standard 802.1x (możliwe jest wykorzystanie standardów i zaleceń wypracowanych w ramach standardu eduroam http://www.eduroam.pl/). Mniej restrykcyjne zapisy polityki w zakresie uwierzytelniania dopuszcza się jedynie w podsieci dla gości i to tylko przy założeniu minimalnych uprawnień dostępnych w owej podsieci.

1.6 Zaleca się spełnienie dodatkowych warunków: instalację systemu UPS umożliwiającego podtrzymanie zasilania dla urządzeń sieciowych oraz stworzenie dedykowanego systemu dostępu do zasobów szkoły poprzez zastosowanie technologii VPN (w celu ułatwienia korzystania z zasobów tak pracownikom, jak i uczniom). System taki można wykorzystać także na potrzeby zdalnego zarządzania elementami sieci. W przypadku udostępnienia zdalnego dostępu z zewnątrz przy pomocy technologii VPN mechanizm ten musi zostać poddany niezależnej ocenie bezpieczeństwa.

2. Urządzenia cyfrowe

2.1 Wobec różnorodności urządzeń cyfrowych dostępnych w szkołach[6] oraz rosnącego zakresu ich wykorzystania, zapewnienie bezpieczeństwa sprzętu oraz oprogramowania powinno być kluczowym elementem projektów realizowanych w latach 2015-2020. Dla zapewnienia **bezpieczeństwa korzystania ze sprzętu cyfrowego w szkole** oraz upowszechnienia TIK w codziennej dydaktyce należy zapewnić **dostępność**:

[6] Większość z nich stanowią obecnie tradycyjne, często wyeksploatowane komputery stacjonarne. Obecne są także urządzenia mobilne: laptopy, tablety, urządzenia typu „dwa w jednym" (tablet z dedykowaną klawiaturą i systemem Windows), a także smartfony. Sytuacja ta jednak będzie się wyraźnie zmieniać. W nadchodzących latach należy się spodziewać przede wszystkim inwestycji w cyfrowe urządzenia mobilne oraz zminiaturyzowane urządzenia o pełnych funkcjach komputera.

a. służbowego sprzętu komputerowego: **każdy nauczyciel powinien zostać wyposażony w służbowy komputer do użytku w szkole oraz w domu** np. dla przygotowywania zajęć lekcyjnych oraz w celu wprowadzania danych do e-dziennika[7]
b. mobilnych urządzeń cyfrowych dla uczniów, wykorzystywanych w procesach nauczania w szkole
c. legalnego oprogramowania[8].

2.2 Urządzenia cyfrowe, w tym sprzęt komputerowy powinny być:

a. zabezpieczone fizycznie przed dostępem osób niepowołanych
b. chronione przed zanikiem zasilania (który może skutkować ich awarią) poprzez podłączenie do zasilania awaryjnego UPS.

2.3 Konfiguracja sprzętu komputerowego powinna **uniemożliwiać wystartowanie systemu operacyjnego z nośników wymiennych**. Również BIOS komputerów powinien być zabezpieczony hasłem przed nieuprawnionym dostępem.

2.4 Dla zapewnienia bezpieczeństwa systemów TIK w szkole oraz obniżenia kosztów technicznego administrowania nimi konieczne jest zapewnienie we wdrożeniach TIK finansowanych w ramach projektów perspektywy 2014-2020 **odpowiednich standardów sprzętowych** pozwalających zdalnie zarządzać, konfigurować, diagnozować, izolować i naprawiać zainfekowane komputery[9].

2.5 Dla ochrony urządzeń wykorzystywanych w procesie dydaktycznym niezbędne są: **program antywirusowy, host *firewall* oraz host IPS.** Zaleca się stosowanie:

a. zabezpieczeń przed wyciekiem danych wrażliwych
b. odpowiednich polityk dla urządzeń podłączanych, wymuszających używanie tylko zaszyfrowanych nośników USB
c. szyfrowania całych urządzeń lub plików/folderów użytkowników.

2.6 Serwery powinny być **zabezpieczone przed uszkodzeniem i nieuprawnionym dostępem osób niepowołanych**. Aktywne urządzenia sieciowe oraz serwery powinny znajdować się w

[7] Będzie to wymagało wprowadzenia dedykowanych temu komponentowi zapisów w projektach inwestycyjnych.
[8] Należy zwrócić uwagę, iż użytkowanie programu, który jest bezpłatny do użytku domowego na prywatnym komputerze nauczyciela, a wykorzystywany w szkole w celach zawodowych może łamać postanowienia licencyjne np. oprogramowanie antywirusowe.
[9] Na przykład poprzez sprzętową funkcję zdalnego sterowania klawiaturą, monitorem i myszą technicy zyskują dostęp do graficznego interfejsu użytkownika i mogą zobaczyć komunikaty o błędach wyświetlane na ekranie i w ten sposób naprawiać komputery bezpośrednio zamiast przeprowadzać użytkowników telefonicznie przez poszczególne etapy tego procesu. Dzięki inteligentnym, wbudowanym funkcjom zdalnej pomocy technicznej, zabezpieczeń i zarządzania można w dowolnym momencie reagować na newralgiczne problemy informatyczne: a) zdalne monitorowanie komputerów przewodowych i bezprzewodowych (także bezczynnych i odłączonych od sieci), b) rozsyłanie aktualizacji zabezpieczeń do użytkowników w celu zapobiegania włamaniom, a także diagnozowanie, izolowanie i naprawianie zainfekowanych komputerów w przypadku naruszenia zabezpieczeń, c) identyfikowanie i korygowanie niezgodnych komputerów w celu skuteczniejszego zarządzania zgodnością oraz d) zapisywanie danych dotyczących zasobów w pamięci chronionej (w tym danych zasobów sprzętowych i wersji oprogramowania).

zamkniętych szafach serwerowych (typu rack), ulokowanych w pomieszczeniach klimatyzowanych i być zabezpieczone przez system awaryjnego zasilania UPS.

2.7 Stacje robocze powinny być zaopatrzone w system antywirusowy. W ramach projektów należy zapewnić możliwość bieżącej instalacji i aktualizacji definicji wirusów oraz szczepionek przez pobranie ich z Internetu lub przy zastosowaniu centralnie zarządzanego oprogramowania antywirusowego w sieci lokalnej. Poza skanowaniem w poszukiwaniu wirusów na żądanie (także skompresowanych archiwów np. ZIP, RAR) system powinien zapewniać możliwość skanowania plików pobranych z sieci w trybie online. Oprócz tego skanowanie systemu plików w poszukiwaniu złośliwej zawartości powinno odbywać się regularnie, według ustalonego harmonogramu. Przeglądarka internetowa powinna być aktualizowana do najnowszej wersji, ze wszystkimi dostępnymi poprawkami bezpieczeństwa (dotyczy to również powszechnie wykorzystywanych wtyczek do przeglądarki[10]).

3. System operacyjny

3.1 System operacyjny instalowany na urządzeniach użytkowników końcowych powinien posiadać stałe wsparcie producenta (szczególnie w zakresie poprawek bezpieczeństwa), a aktualizacja poprawek systemowych powinna odbywać się automatycznie.

3.2 System operacyjny instalowany w urządzeniach użytkowników (uczniów, nauczycieli, innych pracowników) w szkołach powinien posiadać:

a. wbudowaną zaporę internetową (*firewall*) dla ochrony połączeń internetowych
b. możliwość zainstalowania ochrony antywirusowej przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami, w szczególności w zakresie współpracy z centralnie zarządzanymi aplikacjami antywirusowymi
c. zabezpieczony hasłem hierarchiczny dostęp do systemu operacyjnego, konta oraz profile użytkowników zarządzane zdalnie. Praca systemu winna się odbywać w trybie ochrony kont użytkowników
d. możliwość uruchamiania systemu operacyjnego na maszynie wirtualnej
e. możliwość zapewnienia pełnej funkcjonalności systemu, w tym możliwość autonomicznego uruchamiania urządzenia i lokalnych aplikacji także przy braku połączenia z siecią
f. możliwość zarządzania urządzeniem wyposażonym w system operacyjny poprzez polityki grupowe, w tym możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu operacyjnego. Przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji
g. możliwość wsparcia systemu operacyjnego dla IPSEC opartego na politykach – możliwość wdrażania IPSEC opartą na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny

[10] Do wtyczek będących w powszechnym użyciu, często aktualizowanych m.in. z powodu konieczności załatania luk bezpieczeństwa należą – np. Adobe® Flash, Java, Adobe® Reader

h. mechanizmy logowania w oparciu o:
   - ✓ login i hasło
   - ✓ karty z certyfikatami (*smartcard*)
   - ✓ wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM)

i. wbudowane mechanizmy wieloelementowego (wieloskładnikowego) uwierzytelniania (*multi-factor authentication*)

j. wbudowany mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika

k. wbudowane narzędzie do szyfrowania dysków przenośnych lub - opcjonalnie: z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych[11]

l. wbudowany mechanizm pozwalający użytkownikowi urządzenia zarejestrowanego w systemie instytucji urządzenia na uprawniony dostęp do zasobów tego systemu

m. wbudowane oprogramowanie dla tworzenia kopii zapasowych (*backup*) - automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej

n. wbudowaną możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)

o. wbudowany w system operacyjny mechanizm wirtualizacji

p. możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.

3.3 System operacyjny powinien posiadać ponadto:

a. zintegrowany system bezpłatnych aktualizacji i poprawek, w tym poprawek bezpieczeństwa, dla określonej wersji systemu operacyjnego poprzez Internet[12]

b. możliwość dokonywania aktualizacji i poprawek systemu operacyjnego poprzez mechanizm zarządzany przez administratora systemu.

3.4 W przypadku korzystania z usług katalogowych należy unikać zakładania w systemie operacyjnym lokalnych kont użytkowników, z wyjątkiem uprzywilejowanego konta administratora, do którego dostęp powinien posiadać jedynie administrator.

3.5 System operacyjny działający na stacjach roboczych użytkowników końcowych (nauczycieli, uczniów, innych pracowników szkoły) powinien umożliwiać uwierzytelnianie użytkowników tak, aby otrzymywali dostęp jedynie do ściśle określonych danych i aplikacji.

[11] Wymaganie wobec urządzeń nauczyciela.

[12] Aktualizacja powinna być realizowana z wykorzystaniem mechanizmu udostępnianego przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne, przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim.

3.6 System operacyjny komputera uczniowskiego i nauczycielskiego powinien pozwalać na uruchomienie:

a. aplikacji pozwalających na skorzystanie z programu e-Podręczniki
b. aplikacji edukacyjnych dostępnych w języku polskim.

3.7 Konto użytkownika nie powinno posiadać uprawnień do instalowania oprogramowania. System operacyjny powinien wymuszać używanie haseł o wysokim stopniu skomplikowania, nie krótszych niż 8 znaków z użyciem dużych i małych liter, cyfr i znaków specjalnych, oraz powinien posiadać mechanizm zapisywania do dzienników systemowych działań użytkowników.

4. Chmura obliczeniowa

4.1 Rozwiązania chmury obliczeniowej[13] są coraz częściej stosowane w projektach umożliwiających zarządzanie zasobami edukacyjnymi oraz szkołą. Dostawca usługi chmury obliczeniowej winien spełnić następujące wymagania odnoszące się do bezpieczeństwa:

a. dane użytkownika - realizatora projektu winny być przechowywane na terenie Unii Europejskiej, co powinno być wyraźnie wskazane przy zamawianiu usługi. Pożądana jest możliwość zapewnienia precyzyjnej informacji o lokalizacji danych
b. usługa chmurowa winna spełniać co najmniej wymagania europejskich klauzul umownych (*EU Model clauses*)
c. użytkownik usługi chmurowej - realizator projektu winien być wyłącznym administratorem danych osobowych w chmurze. Dane użytkownika muszą pozostawać własnością użytkownika. Dostawca usługi chmurowej – nawet wówczas, gdy jest podmiotem publicznym - nie może wykorzystywać danych w innym celu, niż to określił użytkownik
d. wykorzystywanie tych danych przez dostarczyciela usługi chmurowej do celów reklamowych i marketingowych nie jest dozwolone. Uzależnienie uruchomienia usługi chmurowej przez dostawcę od wyrażenia zgody przez realizatora projektu na taki sposób wykorzystania danych osobowych jest zabronione. Potwierdzenie spełniania wymagań ISO 27018 (ochrona danych w chmurze) jest wypełnieniem tego wymagania.

4.2. Dostawca usługi chmurowej winien:

a. posiadać dostęp do informacji dotyczącej zasad bezpieczeństwa, w tym do posiadanych certyfikatów bezpieczeństwa. Posiadanie certyfikatu ISO 27001 (Zarządzanie bezpieczeństwem Internetu) jest wypełnieniem tego wymagania[14]

[13] http://pl.wikipedia.org/wiki/Chmura_obliczeniowa
[14] Wypełnienie kryteriów ISO 27001 jako zapewnienie warunków bezpiecznej eksploatacji systemów informatycznych zostało określone w Rozporządzeniu Rady Ministrów w sprawie Krajowych Ram Interoperacyjności z dn. 16 maja 2012 roku (par. 20 p.3), a także w projekcie Rozporządzenia Ministra Administracji i Cyfryzacji w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych z 18 grudnia 2014 (par. 20). Jednostki edukacyjne nie są

b. zachowywać transparentność w zakresie bezpieczeństwa, przedstawiając informacje o zastosowanych mechanizmach ochrony danych, takich jak ochrona antyspamowa, szyfrowanie przechowywanych danych i danych podczas przesyłania, a także metody uwierzytelniania użytkowników usługi, backup itd.

c. udostępnić realizatorom projektu wykaz podwykonawców i współpracujących instytucji, realizujących daną usługę chmurową. Podwykonawcy muszą być zobowiązani do zapewnienia takiego samego poziomu ochrony, jak dostawca usługi chmurowej

d. wskazać - w umowie o świadczenie usługi - zakres odpowiedzialności, jakim jest objęty w związku ze świadczeniem tej usługi.

e. stosować środki techniczne i organizacyjne w celu zabezpieczenia danych, w szczególności:
   - ✓ całodobowo monitorować fizyczne zabezpieczenia centrów danych
   - ✓ kontrolować i rejestrować dostęp do danych przez personel dostawcy usługi chmurowej
   - ✓ wdrożyć mechanizmy ochrony przed złośliwym oprogramowaniem oraz wykrywania włamań i ataków DDoS
   - ✓ umożliwić szyfrowanie danych oparte na Infrastrukturze Klucza Publicznego, w ramach którego administrator ma kontrolę nad kluczami kryptograficznymi
   - ✓ zapewnić dostępność usługi na poziomie co najmniej 99,9%

f. być zobowiązany do:
   - ✓ informowania użytkownika – realizatora projektu o wszelkich zobowiązaniach publicznych w stosunku do policji, organów ścigania oraz służb specjalnych w zakresie przekazywania im dostępu do danych zamieszczonych przez użytkownika w chmurze
   - ✓ zapewnienia realizatorowi projektu niezbędnych informacji, co do zasad retencji danych i ich usuwania. Opcjonalnie dostawca usługi chmurowej może zapewnić mu możliwość ustawienia własnych zasad retencji i usuwania danych
   - ✓ raportowania wszystkich incydentów bezpieczeństwa danych, ze szczególnym uwzględnieniem tych, które dotyczyć mogą danych osobowych przetwarzanych przez podmiot publiczny w chmurze.

4.3 Użytkownik usługi chmurowej powinien mieć możliwość szybkiego i prostego zgłoszenia incydentów naruszenia bezpieczeństwa do jej dostawcy.

4.4 Dostawca usługi chmurowej IaaS[15] oraz SaaS[16] powinien zapewnić możliwość wykorzystania standardowych formatów przechowywania danych zgodnie z rozporządzeniem o Krajowych Ramach Interoperacyjności. Dane te powinny być przenoszone bezpiecznie i bez przeszkód formalnych pomiędzy usługą chmurową dostarczyciela, a urządzeniami realizatora projektu.

---

objęte tymi aktami, gdyż nie obejmuje ich ustawa o informatyzacji w zakresie dotyczącym systemów dla dydaktyki, ale oba te dokumenty stanowią dobrą referencję do postawienia wymogów wobec dostawców usług chmurowych.

[15] IaaS – Infrastructure as a Service
[16] SaaS – Software as a Service

Dostawca usługi chmurowej PaaS powinien zapewnić możliwość uruchamiania popularnych serwerowych systemów operacyjnych na maszynach wirtualnych.

4.5 Umowy zawarte pomiędzy placówkami szkolnymi a organami prowadzącymi, powinny zawierać klauzule umożliwiające powierzenie przetwarzania organowi trzeciemu – dostawcy usługi chmurowej.[17]

5. Wytwarzane oprogramowanie

5.1. Aplikacje wytwarzane na potrzeby procesu edukacyjnego muszą być produkowane z uwzględnieniem bezpieczeństwa w cyklu życia oprogramowania (*Secure Development Life Cycle – SDLC*)

5.2. Otwarty kod źródłowy aplikacji wykorzystywanych w szkołach powinien podlegać niezależnej ocenie bezpieczeństwa przed wdrożeniem aplikacji. Dostawca aplikacji o zamkniętym kodzie źródłowym powinien wykazać, że kod źródłowy aplikacji został zbadany pod kątem bezpieczeństwa przez niezależnych audytorów.

[17] W świetle obowiązującego prawa dysponentem i podmiotem odpowiedzialnym za przetwarzanie danych osobowych jest podmiot, który takie dane zbiera i jest do tego upoważniony. Szczególnym przypadkiem jest sytuacja, w której upoważnienie do przetwarzania danych jest upoważnieniem ustawowym. Dotyczy to np. placówek szkolnych w relacji z uczniami i opiekunami oraz pracownikami. Mamy zatem do czynienia z sytuacją, w której szkoła ma uprawnienia do przetwarzania danych pracowników, uczniów oraz opiekunów, zaś organ prowadzący uprawnień takich nie posiada. Ustawodawca przewidział możliwość powierzenia przetwarzania danych podmiotowi trzeciemu. Placówka może podpisać umowę z innym podmiotem, któremu powierza przetwarzanie danych, samemu pozostaje nadal ich dysponentem. Podmiotem, któremu powierzono przetwarzanie danych może być firma komercyjna np. dostarczyciel usługi chmurowej, jak jednostka samorządu terytorialnego.

Zawarcie właściwych umów dotyczących przetwarzania danych jest szczególnie istotne w przypadku realizacji projektów informatycznych z zakresu informatyzacji placówek oświatowych obejmujących swoim zasięgiem wiele takich placówek położonych na terenie miasta, gminy, powiatu lub województwa. Brak umowy uniemożliwi zbudowanie systemu o architekturze scentralizowanej, a tym bardziej wykorzystanie rozwiązań chmury publicznej. W przypadku organów prowadzących, które zamierzają korzystać z usługi chmurowej, wskazane jest by w umowach partnerskich, jakie zawierają oni z uczestnikami projektu (placówkami), została wyrażona wprost zgoda placówki na przetwarzanie danych osobowych, jakimi ona dysponuje w chmurze. Najlepszym rozwiązaniem jest zaakceptowanie przez poszczególne placówki regulaminu działania chmury wraz z postanowieniami umowy o przetwarzaniu danych. Takie rozwiązania uchronią później beneficjenta projektu w przypadku kontroli GIODO od konsekwencji naruszenia przepisów ustawy o ochronie danych osobowych.