2018

Usługi Bezpieczeństwa sieci OSE

Ochrona użytkownika OSE

Spis treści

O projekcie Ogólnopolskiej Sieci Edukacyjnej

Ogólnopolska Sieć Edukacyjna (zwana dalej „OSE") jest projektem konstytuowanym na mocy ustawy z dnia 27 października 2017r. o Ogólnopolskiej Sieci Edukacyjnej (zwanej dalej „Ustawą").

Zgodnie z Ustawą, jest publiczną siecią telekomunikacyjną, dzięki której szkoły otrzymają nieodpłatny dostęp do szybkiego internetu wraz z usługami bezpieczeństwa sieciowego i teleinformatycznego oraz usługami ułatwiającymi dostęp do technologii cyfrowych.

Operatorem OSE jest Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (zwany dalej „NASK"), nadzorowany przez Ministra Cyfryzacji.

Uwarunkowania prawne funkcjonowania usługi bezpieczeństwa

Ustawa przewiduje świadczenie Szkole przez Operatora OSE usług bezpieczeństwa teleinformatycznego, obejmujących ochronę przed szkodliwym oprogramowaniem oraz monitorowanie zagrożeń i bezpieczeństwa sieciowego.

Ponadto zgodnie z art. 27 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe, szkoły i placówki zapewniające uczniom dostęp do Internetu są obowiązane podejmować działania zabezpieczające uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju, w szczególności zainstalować i aktualizować oprogramowanie zabezpieczające.

Mając powyższe na uwadze, NASK dostarcza usługę bezpieczeństwa OSE, która ma na celu zapewnienie ochrony szerokopasmowego dostępu do internetu przed szkodliwym oprogramowaniem oraz monitorowanie zagrożeń i bezpieczeństwa sieciowego. Ponadto NASK zapewnia wsparcie Szkole w podejmowaniu działań zabezpieczających uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju. Szczególnie ważne są zatem usługi i narzędzia, związane z potencjalnym dostępem użytkowników sieci OSE do treści szkodliwych, które mogą wywoływać negatywne emocje u odbiorcy. NASK w ramach projektu OSE udostępnia system/narzędzie do ochrony użytkownika w sieci. System chroni użytkownika w sieci poprzez automatyczną ochronę przed treściami nielegalnymi czyli treściami, których prezentacja i dystrybucja jest zabroniona i podlega karze, zgodnie z przepisami kodeksu karnego i ustaw właściwych, oraz innych treści szkodliwych dla dzieci.

Decyzja o włączeniu usługi ochrony użytkownika OSE należy do Dyrektora Szkoły. Do prawidłowego działania usługi wymagana jest inspekcja ruchu szyfrowanego SSL w celu umożliwienia analizy ruchu sieciowego przesyłanego w ramach komunikacji wymienianej z siecią internet. Wiąże się to z koniecznością instalacji dostarczonych przez NASK certyfikatów SSL na wszystkich komputerach oraz urządzeniach komputerowych (tablety, smartfony, laptopy) w szkole.

Opis usługi Ochrona Użytkownika OSE

Mając na uwadze dyrektywy zawarte w Europejskiej Strategii dla Lepszego Internetu dla Dzieci: European Strategy for a Better Internet for Children, z 2.05.2012 r., Operator OSE udostępnia system/narzędzie, dzięki któremu szkoła może zapewnić dzieciom bezpieczne korzystanie z internetu.

Wyniki wielu badań potwierdzają, że kontakt dzieci z treściami szkodliwymi w internecie często powoduje wystąpienie wysokiego poziomu negatywnych emocji oraz zaburza prawidłowy rozwój i obniża poczucie bezpieczeństwa. Może też mieć negatywny wpływ na psychikę dzieci i prowadzić do większej tolerancji na przemoc lub wręcz agresji wobec innych dzieci, zwierząt, a także do innych ryzykownych zachowań. W związku z tym, w ocenie specjalistów pedagogów i psychologów, treści szkodliwe nie powinny być dostępne dla najmłodszych użytkowników.

System ochrony zlokalizowany w węzłach centralnych w sieci OSE na podstawie zaawansowanych algorytmów automatycznie monitoruje, wykrywa i blokuje zagrożenia, związane z potencjalnym dostępem do treści nielegalnych i szkodliwych dla użytkowników sieci OSE, będących w szkołach, które zdecydowały się skorzystać z usługi bezpieczeństwa. W tych szkołach systemy OSE zapewniają odpowiedni dobór treści internetowych poprzez blokowanie stron www i aplikacji webowych, sklasyfikowanych jako nielegalne lub szkodliwe.

System bezpieczeństwa chroni przede wszystkim przed dostępem do treści nielegalnych, czyli treści których dystrybucja jest zabroniona i podlega karze, zgodnie z przepisami kodeksu karnego i ustaw właściwych, do których należą:

- treści pornograficzne z udziałem małoletnich określane jako materiały przedstawiające seksualne wykorzystywanie dziecka (z ang. CSAM-child sexual abuse materials),
- treści zawierające materiały o charakterze pedofilskim oraz propagowanie i pochwalanie tych treści,
- treści zawierające uwodzenie małoletnich w Internecie,
- treści zawierające publiczne propagowanie faszystowskiego lub innego totalitarnego ustroju państwa lub nawoływania do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość,
- treści zawierające publicznie rozpowszechniane i prezentowane informacje, które mogą ułatwić popełnienia przestępstwa terrorystycznego,
- treści zawierające publiczne znieważanie grupy ludności albo poszczególnej osoby z powodu jej przynależności narodowej, etnicznej, rasowej, wyznaniowej albo z powodu jej bezwyznaniowości,
- treści zawierające informacje o narkotykach, dopalaczach – witryny, które omawiają, zachęcają, promują, oferują, sprzedają, dostarczają lub w inny sposób promują użycie, hodowlę, produkcję lub dystrybucję narkotyków i dopalaczy, rozumianych jako między innymi: niefarmaceutyczne leki, rośliny odurzające, rozpuszczalniki, lub inne substancje chemiczne, oraz związanych z nimi akcesoriów,

- strony służące do oferowania gier hazardowych niezgodnie z ustawą o grach hazardowych.

Poza nielegalnymi treściami określanymi przez przepisy, system bezpieczeństwa automatycznie chroni przed treściami szkodliwymi, czyli treściami, które zawierają materiały jednoznacznie nieadresowane do młodych odbiorców oraz treściami drastycznymi, wywołującymi bardzo negatywne emocje u odbiorcy, w szczególności treści takie, jak:

- treści zawierające pornografię – witryny przedstawiające treści pornograficzne, takie jak tekst, obrazy lub wideo zawierające wizerunek osób lub przedmiotów o cechach jednoznacznie seksualnych,
- treści zawierające przemoc – witryny, których celem jest przedstawianie fizycznych lub innych szkód wyrządzanych ludziom, zwierzętom lub mieniu, lub które dostarczają instrukcji, jak spowodować takie szkody,
- treści zawierające materiały dla dorosłych – witryny przedstawiające materiały przeznaczone dla dorosłych odbiorców, ale nie zakwalifikowane w kategorii pornografia i przemoc. Witryny te zawierają często wulgarne, erotyczne, lub inne treści, które nie są odpowiednie dla dzieci,
- treści zawierające promowanie alkoholu i tytoniu – witryny i materiały promujące alkohol i tytoń, jego sprzedaż i spożywanie, w tym, ale nie wyłącznie, piwo, wino i inne wysokoprocentowe napoje alkoholowe,
- treści zawierające promowanie broni i materiałów wybuchowych – witryny i materiały promujące broń, jej produkcję, używanie i modyfikacje, w tym, ale nie wyłącznie, pistolety, karabiny oraz materiały wybuchowe,
- treści zawierające promowanie anoreksji i innych zaburzeń odżywiania – witryny i materiały promujące niezdrowy i niewłaściwy tryb życia, związany z zaburzeniami odżywiania,
- treści zawierające promowanie samookaleczeń – witryny i materiały promujące niebezpieczny, niezdrowy i niewłaściwy tryb życia, związany z umyślnym uszkodzeniem własnego ciała w wyniku autoagresji lub depresji,
- treści zawierające elementy psychomanipulacji, czyli sterowania cudzymi uczuciami, którego celem jest wyłudzenie korzyści materialnych lub zmuszenie do niewłaściwych, często ryzykownych zachowań.

Podsumowanie

Uruchomienie przez Dyrektora Szkoły usługi ochrony użytkownika OSE oznacza, że:

- Strony zawierające treści nielegalne oraz szkodliwe są zablokowane i nie będą dostępne dla użytkowników sieci OSE dzięki działaniu automatycznych zaawansowanych algorytmów.
- Strony o nierozpoznanej zawartości (Uncategorized), czyli strony o treściach, których system nie potrafił automatycznie sklasyfikować i przyporządkować do żadnej z kategorii

(zarówno dozwolonej jak i niedozwolonej) zostaną zablokowane aż do momentu podjęcia decyzji dotyczącej ich przyporządkowania przez dostawcę systemu lub/i Operatora OSE.

- NASK monitoruje zagrożenia i przypadki naruszeń bezpieczeństwa użytkowników sieci OSE wykryte przez system ochrony użytkownika OSE.
- NASK udostępnia Dyrektorowi Szkoły raporty, dotyczące monitorowania zagrożeń i przypadków naruszeń bezpieczeństwa użytkowników OSE zawierające dane o sposobie korzystania z internetu w szkole (Top N kategorii dozwolonych/niedozwolonych, Top N najpopularniejszych stron),
- System ochrony użytkowników w żadnym zakresie nie będzie obejmować witryn z obszarów: bankowość i finanse, opieka zdrowotna i poczta elektroniczna.
- Usługi bezpieczeństwa OSE nie obejmują działaniem sieci LAN w szkołach, a tylko komunikację sieci LAN z internetem.
- Systemy bezpieczeństwa OSE oparte są na zaawansowanych systemach technicznych, które wszystkie operacje monitoringu i kontroli treści wykonują w sposób automatyczny w monitorowanych procesach ruchu internetowego bez ingerencji osób obsługujących. Odpowiednie procedury i mechanizm działania systemów zapewniają pełną poufność i bezpieczeństwo przetwarzanych danych.
- Usługa ochrony użytkownika przed nielegalnymi i szkodliwymi treściami bazuje na narzędziach technicznych, które w czasie rzeczywistym, na bazie zaawansowanych algorytmów określają charakter treści danej strony bez ingerencji NASK. Ze względu na olbrzymią ilość treści w internecie systemy techniczne klasyfikujące kategorie stron mogą w niektórych przypadkach kategoryzować strony i treści, nieprawidłowo blokując treści dozwolone lub nie zablokować treści niedozwolonej. W razie zauważenia przez użytkownika w Szkole takiej sytuacji, Szkoła jest proszona o zgłoszenie takiego przypadku do operatora OSE.
- Zaawansowane funkcje bezpieczeństwa OSE wykonywane są na urządzeniach centralnych w sieci OSE. Do ich poprawnego działania wymagana jest inspekcja ruchu szyfrowanego SSL w celu umożliwienia analizy ruchu sieciowego przesyłanego w ramach komunikacji wymienianej z internetem. NASK udostępnia certyfikaty SSL, umożliwiające inspekcje ruchu szyfrowanego, które Szkoła, korzystająca z usługi bezpieczeństwa, jest zobowiązana zainstalować na wszystkich komputerach oraz urządzeniach komputerowych (tablety, smartfony, laptopy) w celu umożliwienia poprawnego działania usługi ochrony przed zagrożeniami technicznymi. Sposób instalacji certyfikatów SSL na urządzeniach komputerowych opisany jest w Procedurze wdrożenia usługi bezpieczeństwa w Szkole.
- Z powodów niezależnych od NASK i użytych przez niego w sieci OSE systemów bezpieczeństwa zapewniających zaawansowane funkcje bezpieczeństwa pewna część aplikacji sieciowych (głównie mobilnych, czyli instalowanych na urządzeniach, takich jak tablety i smartfony) może nie działać poprawnie, lub nie działać w ogóle.
- NASK na bazie posiadanych systemów zabezpieczeń oraz wdrożonych procedur organizacyjnych uniemożliwia dostęp jakimkolwiek osobom do treści podlegających monitorowaniu i kontroli.