Standard bezpieczeństwa online placówek oświatowych - II wydanie

Ze strony https://akademia.nask.pl

"Prezentujemy Państwu **II wydanie „Standardu bezpieczeństwa online placówek oświatowych”** - jest to rozszerzona edycja wydawnictwa z 2015 r. opracowanego na zlecenie Ministerstwa Administracji i Cyfryzacji w ramach projektu pt.: „Działania na rzecz bezpiecznego korzystania z internetu”. Publikacja została przygotowana przez zespół ekspertów NASK – Państwowego Instytutu Badawczego i Wyższej Szkoły Pedagogicznej im. Janusza Korczaka w Warszawie".

Wprowadzenie

W grudniu 2017 roku weszła w życie ustawa o Ogólnopolskiej Sieci Edukacyjnej. Na mocy jej zapisów do wszystkich placówek oświatowych w Polsce doprowadzony zostanie szerokopasmowy internet (symetryczny Internet o przepływności 100mb). Tak więc internet stanie się wkrótce trwałym elementem funkcjonowania wszystkich placówek oświatowych. Już dziś sieć funkcjonuje w większości polskich szkół, a praktycznie wszyscy uczniowie są jej użytkownikami. Także i dziś szkoły korzystają z internetu wykorzystując go przede wszystkim w procesie nauczania, ale coraz częściej także jako element działania i funkcjonowania organizacyjnego i administracyjnego placówki. Jeszcze do niedawna traktowany jako nowość dziś jawi się nie tylko jako stały, ale także niezbędny element funkcjonowania szkoły. Budowa sieci OSE, pozwoli na swobodne wykorzystywanie internetu w procesie dydaktycznym, w sferze organizacyjnej funkcjonowania placówek. Znikną istniejące do tej pory w wielu miejscach bariery techniczne.

Należy jednak zauważyć, iż gwałtowana ekspansja sieci, jej coraz większa obecność w edukacji i w procesach komunikowania, w naturalny sposób nie szły dotąd w parze z tworzeniem zasad, procedur i norm postępowania. Samemu zaś rozwojowi sieci towarzyszy pojawienie się w Internecie niebezpiecznych zjawisk i przestępczości. Możemy mówić zarówno o przenoszeniu się negatywnych zjawisk ze świata realnego do sieci jaki i o tworzeniu się całkiem nowych kategorii zjawisk niekorzystnych i przestępstw. Mamy do czynienia zarówno z zagrożeniami o charakterze technicznym jak i społecznym. Te pierwsze to między innymi wykradanie danych, blokowanie dostępu, wszelkiego rodzaju wirusy komputerowe niszczące zasoby i wiele innych. Zagrożenia o charakterze społecznym wiążą się przede wszystkim z pojawianiem się w sieci niebezpiecznych i nielegalnych treści. Mówimy tu między innymi o zachowaniach ryzykownych, cyberprzemocy, groomingu, sekstingu, hejtingu, pornografii dziecięcej, treściach rasistowskich, zachęcaniu do samobójstw. Warto dodać, iż opisywany tu katalog zjawisk nie jest katalogiem zamkniętym. Lista zagrożeń rozszerza się, co związane jest zarówno z coraz większym zasięgiem i jakością sieci, ale także z postrzeganiem internetu jako miejsca w którym można pozostać anonimowym, a co za tym idzie bezkarnym, nawet działając w złej wierze lub niezgodnie z prawem.

Na potrzeby tego standardu dokonano podziału zagrożeń online na dwie podstawowe

grupy: • zagrożenia o charakterze społeczno-wychowawczym • zagrożenia technologiczne.

Ze względu na trudność precyzyjnego rozgraniczenia obu grup, warto zapoznać się z całością materiału poświęconą zagrożeniom. Daje to pełny obraz skomplikowanego spectrum niebezpieczeństw występujących w cyberprzestrzeni.

Szczegółowo omówione zostały najczęściej występujące zagrożenia. To właśnie z tymi zagrożeniami muszą radzić sobie placówki oświatowe. Niezależnie od zaprezentowanej w dokumencie listy mogą pojawić się także inne niebezpieczeństwa, także takie, których nie ujęto w niniejszym opracowaniu. Procedura reagowania w takich sytuacjach winna być wzorowana na modelach zaprezentowanych w standardzie.