

**Zagrożenia bezpieczeństwa technicznego sieci, komputerów i zasobów online
procedura reagowania**

–

	Zagrożenia bezpieczeństwa technicznego sieci, komputerów i zasobów online – procedura reagowania
Rodzaj zagrożenia objętego procedurą	Kategoria technicznych zagrożeń bezpieczeństwa cyfrowego obejmuje obecnie szerokie spectrum problemów: a) ataki przez wirusy, robaki i trojany, b) ataki na zasoby sieciowe (hakerstwo, spyware, crimeware, exploit, ataki słownikowe i back door, skanowanie portów, phishing, pharming, sniffing, spoofing, ataki Denial of service (DoS), rootkit) i ataki socjotechniczne. Na styku z zagadnieniami technicznymi lokalizują się zagrożenia wynikające z nieprawidłowych i szkodliwych zachowań użytkowników np. używanie łatwych do odgadnięcia haseł, pozostawianie komputerów włączonych bez opieki, czy brak zabezpieczeń na wypadek braku energii elektrycznej
SPOSÓB POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA ZAGROŻENIA	
Przyjęcie zgłoszenia i ustalenie okoliczności zdarzenia	W przypadku wystąpienia incydentów zagrożenia bezpieczeństwa cyfrowego pracownik szkoły zobowiązany jest do zgłoszenia go osobie odpowiedzialnej za infrastrukturę cyfrową szkoły oraz dyrekcji. Kluczowe znaczenie ma zebranie i zabezpieczenie przez specjalistę dowodów w formie elektronicznej.
Opis okoliczności, analiza, zabezpieczenie dowodów	Szczegółowy opis procedur reagowania na wystąpienie w szkole różnorodnych zagrożeń bezpieczeństwa cyfrowego powinien zostać zawarty w dokumencie „polityka bezpieczeństwa cyfrowego” danej szkoły stanowiącej element Szkolnego Planu Zapewnienia Bezpieczeństwa Cyfrowego. W części przypadków szkoła poradzi sobie we własnym zakresie, w niektórych konieczne będzie skorzystanie z zewnętrznego wsparcia wyspecjalizowanych firm
Identyfikacja sprawców	Identyfikację sprawców ataku należy pozostawić specjalistom – informatykom. W sytuacji, gdy incydent spowodował szkole

Zagrożenia bezpieczeństwa technicznego sieci, komputerów i zasobów online
procedura reagowania

–

	straty materialne lub wiązał się z utratą danych należy powiadomić Policję, aby podjęła działania na rzecz zidentyfikowania sprawcy
Aktywności wobec sprawców zdarzenia ze szkoły/ spoza szkoły	Jeśli sprawcami incydentu są uczniowie danej szkoły, o zaistniałej sytuacji należy powiadomić ich rodziców, zaś wobec nich podjąć działania wychowawcze. Jeżeli skutki ataku mają dotkliwy charakter, doprowadziły do zniszczenia mienia lub utraty istotnych danych (np. gromadzonych w e-dzienniku szkoły), należy taki przypadek zgłosić na Policję
Aktywności wobec świadków	O incydencie należy powiadomić społeczność szkolną (uczniów, nauczycieli, rodziców) i zaprezentować podjęte sprawnie działania, tak przywracające działanie aplikacji i sieci komputerowej w szkole, jak i wychowawczo-edukacyjne wobec dzieci
Współpraca z Policją i sądami rodzinnymi	W przypadku wystąpienia strat materialnych oraz utraty danych (szczególnie danych wrażliwych) należy zgłosić incydent na Policji.
Współpraca ze służbami społecznymi i placówkami specjalistycznymi	W przypadkach zaawansowanych awarii (np. wywołanych przez trojany) lub strat (np. utrata danych z e-dziennika) konieczne jest skorzystanie z zewnętrznego wsparcia eksperckiego, kontakt z serwisem twórcy oprogramowania lub zamówienie usługi w wyspecjalizowanej firmie