ZAGROŻENIA BEZPIECZEŃSTWA TECHNICZNEGO SIECI, KOMPUTERÓW I ZASOBÓW ONLINE

PRZYJĘCIE ZGŁOSZENIA I USTALENIE OKOLICZNOŚCI ZDARZENIA

Zgłoś incydent 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

W części przypadków szkoła poradzi sobie we własnym zakresie, w niektórych konieczne będzie skorzystanie z zewnętrznego wsparcia wyspecjalizowanych firm.

IDENTYFIKACJA SPRAWCY

Pozostaw specjalistom identyfikację sprawców ataku

AKTYWNOŚCI WOBEC SPRAWCÓW

Powiadom Policję

W sytuacji, gdy incydent spowodował szkole straty materialne lub wiązał się z utratą danych.

A także jeśli skutki ataku doprowadziły do zniszczenia mienia lub utraty istotnych danych (np. gromadzonych w e-dzienniku szkoły).

Podejmij działania wychowawcze i powiadom rodziców

Jeśli sprawcami incydentu są uczniowie danej szkoły.

AKTYWNOŚCI WOBEC ŚWIADKÓW

Powiadom społeczność szkolną

Zaprezentuj podjęte sprawnie działania, tak przywracające działanie aplikacji i sieci komputerowej w szkole, jak i wychowawczo-edukacyjne wobec dzieci (np. akademia w tej sprawie).

WSPÓŁPRACA Z POLICJĄ I SĄDAMI

Zgłoś incydent na Policję

W przypadku wystąpienia strat materialnych oraz utraty danych (szczególnie danych wrażliwych).

WSPÓŁPRACA ZE SPECJALISTYCZNYMI PLACÓWKAMI

Skorzystaj z zewnętrznego wsparcia eksperckiego

W przypadkach zaawansowanych awarii (np. wywołanych przez trojany) lub strat (np. utrata danych z e-dziennika).

Skontaktuj się z serwisem twórcy oprogramowania lub zamów usługi w wyspecjalizowanej firmie.

§ **PODSTAWY PRAWNE: Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe, Statut szkoły, Regulamin szkoły**