**Jak chronić się przed cyberatakami w szkole**

Data publikacji: 28 lutego 2022 r.

18



Agresja Rosji na Ukrainę wiąże się z coraz większą liczbą cyberataków na polskie strony internetowe. Dlatego premier zdecydował o ogłoszeniu trzeciego stopnia alarmowego dotyczącego zagrożeń w cyberprzestrzeni (CHARLIE-CRP). Potencjalne cyberataki mogą dotknąć także szkolnych stron internetowych i baz danych. Sprawdź, jakie rozwiązania zastosować, aby przeciwdziałać takim cyberatakom.

Cyberatak to działanie mające na celu **zmianę, zniszczenie lub kradzież danych** ewentualnie **wykorzystanie lub uszkodzenie sieci**. Jest ono ukierunkowane na komputer lub jakikolwiek element komputerowego systemu informatycznego. Atak taki może przebiegać na różne sposoby. Najbardziej znane z nich, które mogą mieć miejsce w szkole lub organie prowadzącym, są przedstawione w tabeli.

**6 rodzajów cyberataków w szkole**

|  |  |
| --- | --- |
| **Malware** | Jest to rodzaj złośliwego oprogramowania, które infekuje komputer. Jednocześnie zmienia sposób jego działania w sposób zaplanowany przez atakującego. Najczęściej niszczy dane lub szpieguje użytkownika. Złośliwe oprogramowanie może rozprzestrzeniać się z jednego urządzenia na drugie. Może też pozostawać na swoim miejscu, wpływając tylko na urządzenie gospodarza. |
| **DoS i DDoS** | Cyberatak typu denial-of-service (DoS) prowadzi do przeciążenia zasobów systemu. Przeciążenie następuje do tego stopnia, że system nie jest w stanie odpowiadać na uzasadnione żądania usług. Z kolei cyberatak DDoS (distributed denial-of-service) również ma na celu wyczerpanie zasobów systemu. Cyberatak DDoS jest inicjowany przez ogromną liczbę zainfekowanych złośliwym oprogramowaniem maszyn kontrolowanych przez atakującego. |
| **MiTM** | Cyberataki typu man-in-the-middle umożliwiają atakującemu podsłuchiwanie danych przesyłanych tam i z powrotem między dwiema osobami, sieciami lub komputerami. Nazwa cyberataku wzięła się stąd, że atakujący znajduje się „w środku” lub pomiędzy dwiema stronami próbującymi się komunikować. W efekcie atakujący szpieguje interakcję pomiędzy nimi. |
| **Phishing** | Atakujący wysyła wiadomości (e-mail, czat), które wydają się pochodzić z zaufanych, legalnych źródeł, próbując w ten sposób wyłudzić poufne informacje od swojego celu. Innymi słowy, atakujący wysyła link, który przeniesie użytkownika na stronę internetową. Następnie ma miejsce pobranie złośliwego oprogramowania albo przekazania atakującemu informacji o ofierze. |
| **Ransomware** | System ofiary jest przetrzymywany niejako w roli zakładnika, dopóki nie zostanie zapłacony okup atakującemu. Sam cyberatak pozbawia czasowo administratora dostępu do jego danych. W przypadku niezapłacenia okupu może dojść do trwałej utraty danych. Zmanipulowana ofiara pobiera oprogramowanie szyfrujące z witryny internetowej lub z załącznika do wiadomości e-mail. Wykorzystując luki na poszczególnych systemach, potrafi się ono zainstalować na wielu maszynach w danej sieci. Następnie, gdy atakujący zainicjuje szyfrowanie, wystąpi ono na wszystkich zainfekowanych systemach jednocześnie. |
| **Oszustwo nigeryjskie** | Nadawca prosi o pomoc, zazwyczaj w formie wiadomości e-mail, w ułatwieniu przekazania pewnej sumy pieniędzy. W zamian nadawca oferuje prowizję ‒ dużą kwotę, czasami nawet do kilku milionów dolarów. Następnie oszuści proszą o przesłanie pieniędzy w celu pokrycia części kosztów związanych z przelewem. Jeśli pieniądze zostaną wysłane do oszustów, to oni znikają. Ewentualnie oszuści próbują zdobyć więcej pieniędzy, twierdząc, że ciągle występują problemy z przelewem. |