Bitdefender

Cyberbezpieczeństwo w edukacji

17.05.2023

Szkoły były tradycyjnie postrzegane jako bezpieczne schronienie dla uczniów; miejsce, w którym dzieci mogą się uczyć i rozwijać w chronionym środowisku. Jednak wraz z nadejściem ery cyfrowej zarówno uczniowie, jak i pracownicy szkół podstawowych, średnich, branżowych i wyższych stają w obliczu rosnących zagrożeń dla swoich wrażliwych danych. Szkoły mają do czynienia z wieloma krytycznymi danymi, takimi jak akta uczniów (w tym daty urodzenia i adresy), informacje medyczne, dane finansowe oraz akta zatrudnienia nauczycieli i personelu administracyjnego. Hakerzy i cyberprzestępcy coraz częściej atakują instytucje edukacyjne, aby przetrzymywać wrażliwe dane w celu uzyskania okupu finansowego lub kraść je i sprzedawać w ciemnej sieci. Bardziej istotne niż kiedykolwiek wcześniej stało się wdrożenie przez instytucje edukacyjne solidnych programów cyberbezpieczeństwa, aby chronić szkołę, uczniów i personel.

Wzrost zagrożeń ransomware

Podobnie jak dla wielu innych branży, dla sektora edukacji jednym z najpoważniejszych zagrożeń jest obecnie rozwój oprogramowania ransomware. Zgodnie z raportem Data Breach Investigation Report z 2022 r. przeprowadzonym przez firmę Verizon, w którym przeanalizowano ponad 5200 potwierdzonych naruszeń danych, liczba ataków ransomware wzrosła o 13% względem poprzedniego roku. W sektorze edukacyjnym ponad 30% zbadanych naruszeń danych było wynikiem ataku ransomware.

Ataki ransomware na szkoły mogą być szczególnie niszczycielskie, ponieważ szkoły często mają ograniczone budżety przeznaczone na systemy antywirusowe i personel zajmujący się cyberbezpieczeństwem i nie dysponują zasobami, aby odbudować system informatyczny po ataku. W ankiecie przeprowadzonej przez firmę Bitdefender w 2022 r. obejmującej prawie 1700 organizacji odkryto, że wśród respondentów z branży edukacyjnej tylko 19% ma dedykowany personel ds. cyberbezpieczeństwa. Większość (81%) stwierdziła, że dbanie o cyberbezpieczeństwo to tylko jeden z wielu obowiązków spoczywających na (często już przepracowanym) zespole IT.

Czynnik ludzki w cyberbezpieczeństwie

Kolejnym zagrożeniem dla cyberbezpieczeństwa w szkołach jest „czynnik ludzki”. Pracownicy i użytkownicy o dobrych intencjach są w dużej mierze uznawani za najsłabsze ogniwo w każdej strukturze cyberbezpieczeństwa, a szkoły nie są wyjątkiem. Cyberprzestępcy wykorzystują techniki inżynierii społecznej, aby nakłonić użytkowników

do ujawnienia poufnych informacji, takich jak dane logowania lub dane osobowe. Ataki typu phishing, czyli fałszywe wiadomości e-mail, które wydają się pochodzić z zaufanego źródła, to powszechna taktyka socjotechniczna wykorzystywana do atakowania uczniów, studentów i pracowników szkół. W badaniu dotyczącym naruszeń bezpieczeństwa cybernetycznego z 2022 r. przeprowadzonym w ramach brytyjskiej Narodowej Strategii Cybernetycznej phishing stanowił najczęstszy rodzaj ataku, przy czym 88% szkół podstawowych i 97% szkół wyższych zgłosiło, że doświadczyło ataków phishingowych w ciągu ostatnich 12 miesięcy.

Oprócz ludzkiej skłonności do ulegania taktyce socjotechnicznej faktem jest również, że po prostu popełniamy błędy. W cytowanym wcześniej raporcie Verizon Data Breach Investigations Report 34% analizowanych naruszeń w sektorze edukacyjnym pochodziło z wiadomości e-mail wysłanej do niewłaściwej osoby lub z niewłaściwym załącznikiem. Błędne konfiguracje punktów końcowych szkoły (w tym komputerów i urządzeń mobilnych), chmur lub systemów informatycznych mogą również tworzyć luki w zabezpieczeniach, które hakerzy często wykorzystują jako punkt wejścia do sieci.

Cyberbezpieczeństwo w edukacji — jak zapobiegać zagrożeniom i w jaki sposób reagować w razie ataku?

Skuteczne zapobieganie zagrożeniom, wykrywanie ich i reagowanie na nie stanowi podstawę każdego solidnego programu cyberbezpieczeństwa i może pomóc chronić szkoły przed zagrożeniami

cybernetycznymi. Zapobieganie obejmuje środki podejmowane w celu zmniejszenia powierzchni ataku, takie jak eliminowanie błędnych konfiguracji i luk w zabezpieczeniach, zabezpieczanie poczty e-mail i urządzeń końcowych oraz zarządzanie ryzykiem, w tym ludzkim zachowaniem. Ochrona obejmuje wykorzystanie rozwiązań i usług w zakresie cyberbezpieczeństwa, które pomagają szkołom wykrywać incydenty, szybko na nie reagować i odzyskiwać siły po atakach.

Odpowiednie oprogramowanie antywirusowe umożliwia szkołom i instytucjom szkolnictwa wyższego wzmocnienie poziomu cyberbezpieczeństwa poprzez wykorzystanie ulepszonych technik zapobiegania i wielu warstw proaktywnej ochrony. Nowoczesne antywirusy mogą pomóc organizacjom zmniejszyć ryzyko poprzez eliminację błędnych konfiguracji i luk w zabezpieczeniach oraz utrzymywanie aktualności systemów operacyjnych i aplikacji. Antywirus może także wzmocnić obronę szkół przed atakami ransomware i zapewnia proaktywną ochronę danych poprzez monitorowanie udziałów sieciowych, zapobieganie szyfrowaniu plików i tworzenie automatycznych kopii zapasowych. Monitorowanie w czasie rzeczywistym identyfikuje podejrzane zachowania, blokuje uruchamianie złośliwego oprogramowania i złośliwych procesów oraz ułatwia szybką i dokładną reakcję na cyberincydenty, a także skraca czas przebywania atakującego i umożliwia szybkie odzyskiwanie danych po infekcji.

Szkoły borykające się z brakami personalnymi w dziale ochrony przed cyberniebezpieczeństwami mogą skorzystać z ochrony MDR, EDR lub XDR, które zapewniają całodobowe monitorowanie i reagowanie w razie zagrożenia. Dzięki tym rozwiązaniom pracownicy szkół mogą

wzmacniać środowiska sieciowe swoich placówek, aby zapobiegać naruszeniom, a następnie stale monitorować i eliminować zagrożenia, takie jak oprogramowanie ransomware, ataki typu zero-day i próby phishingu w punktach końcowych, sieciach i środowiskach chmurowych. Wdrażanie tych rozwiązań jest tak łatwe, że większość szkół może je uruchomić w ciągu jednego dnia.

„Cyberzagrożenia, takie jak oprogramowanie ransomware, phishing i naruszenia bezpieczeństwa danych, stanowią coraz większy problem dla szkół podstawowych i ponadpodstawowych, a także uczelni wyższych. Zapobieganie, wykrywanie i reagowanie to podstawa silnego programu cyberbezpieczeństwa, który może chronić szkoły, uczniów i personel. Dzięki platformie Bitdefender GravityZone lub usługom Bitdefender Extended Detection and Response (XDR) szkoły mogą przyjąć proaktywne podejście do silnego cyberbezpieczeństwa i zapewnić uczniom bezpieczne środowisko” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło: https://bitdefender.pl/cyberbezpieczenstwo-w-edukacji/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 17.05.2023
Z pozdrowieniami Piotr Rozmiarek
E-mail: piotr.r@marken.com.pl | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender

Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.