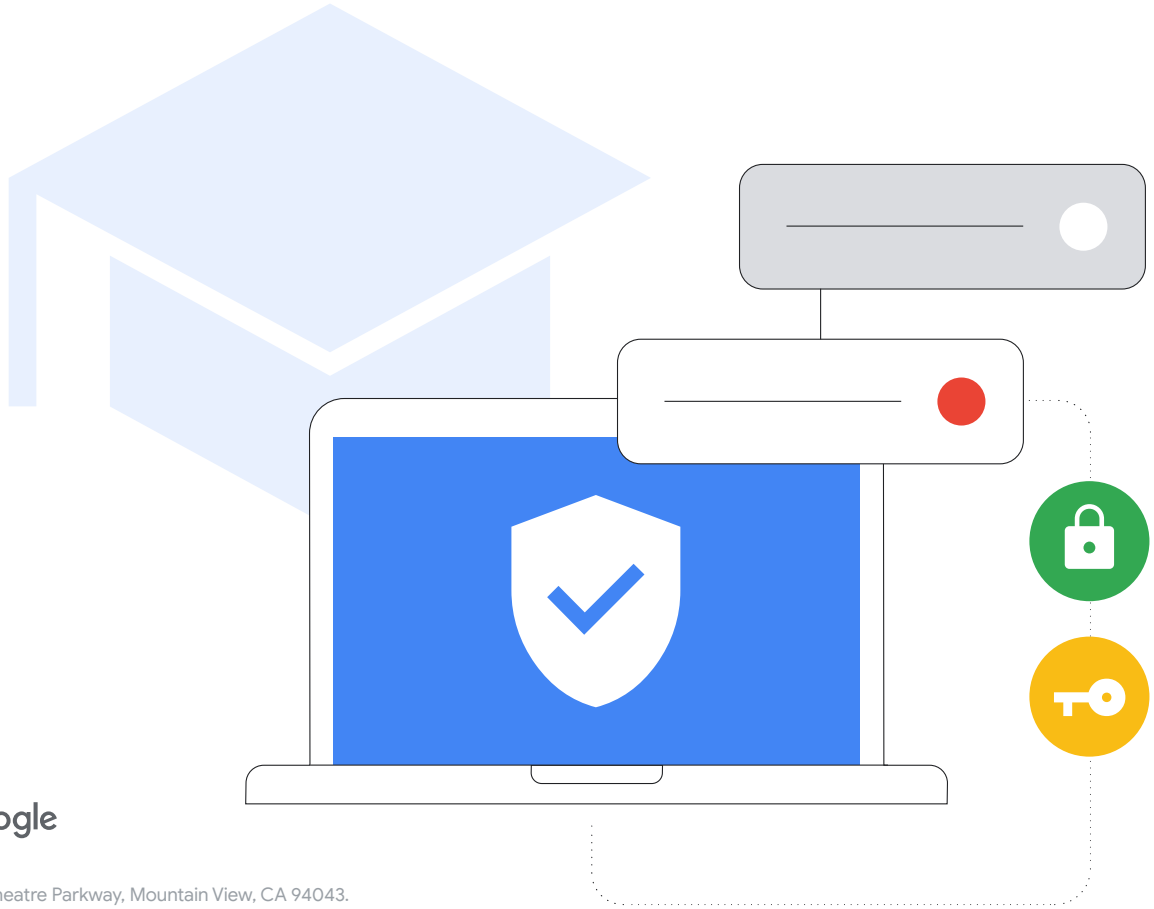
Google for Education

Przewodnik po cyberbezpieczeństwie dla szkół podstawowych i średnich



Safer with Google

Streszczenie

Jak wynika z raportu *Protecting Our Future*[1] da CISA, opracowanego przez amerykańską Agencję ds. Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (CISA), szkoły podstawowe i średnie muszą zainwestować w cyberbezpieczeństwo, aby chronić całą społeczność szkolną: swoich uczniów i ich rodziny, nauczycieli oraz innych pracowników szkoły. Ten dokument zawiera wskazówki dla szkolnych administratorów IT dotyczące konfigurowania sprzętu i oprogramowania w szkołach z myślą o wzmocnieniu cyberbezpieczeństwa. Obejmuje zarówno ogólne sprawdzone metody, jak i konkretne wytyczne dotyczące produktów i usług Google. Misją Google jest porządkowanie światowych zasobów informacji oraz zapewnianie ich powszechnej dostępności i użyteczności. Misja ta jest zarazem motorem do działania całego zespołu Google for Education, w którym tworzymy narzędzia przeznaczone do nauczania i zdobywania wiedzy. W tym przewodniku przedstawimy wnioski, do których doszliśmy w ramach naszej pracy.

Szczegółowo omówimy sprawdzone metody zapewniania bezpieczeństwa z podziałem na różne zagadnienia, takie jak konfiguracja, wdrożenie i strategie ograniczania ryzyka. Wyjaśnimy również, jak Google podchodzi do cyberbezpieczeństwa swoich usług, a zwłaszcza narzędzi edukacyjnych. W tym dokumencie zestawiamy szczegółowe wskazówki, nie odnosząc się przy tym do konkretnych produktów lub usług. Jesteśmy jednak przekonani, że nasze rozwiązania w standardzie zapewniają najlepszą ochronę przed najczęściej występującymi atakami.

Ryzyko

Instytucje edukacyjne należą do najczęstszych celów cyberataków, a przestępcy szukają sposobów na wykorzystanie bogatych zasobów szkolnych danych dla swoich korzyści. 46% szkół, które jeszcze nie zostały zaatakowane, sądzi, że koniec końców padnie ofiarą cyberprzestępców, ponieważ ataki typu ransomware stają się coraz bardziej zaawansowane i coraz trudniejsze do powstrzymania. 42% z tych szkół uważa, że z powodu powszechności ataków typu ransomware są one po prostu nie do uniknięcia. Konieczność szybkiego przejścia na naukę zdalną w 2020 r. mocno przyczyniła się do powstania luk w cyberzabezpieczeniach, przez co szkoły stały się podatne na ataki.

Obrona

Ataki te można minimalizować. Żadna technologia nie eliminuje ryzyka całkowicie, ale sektor edukacyjny i dostawcy rozwiązań z zakresu technologii w edukacji mogą wspólnie pracować nad wdrażaniem sprawdzonych metod, a w efekcie tworzyć bezpieczne i kompleksowe rozwiązania, które pozwalają znacznie zmniejszyć zagrożenie. Dzięki odpowiednim środkom ostrożności i zasadom, które chronią użytkowników i urządzenia oraz zapewniają prywatność danych, instytucje edukacyjne mogą lepiej zarządzać ryzykiem i łagodzić skutki ataków.

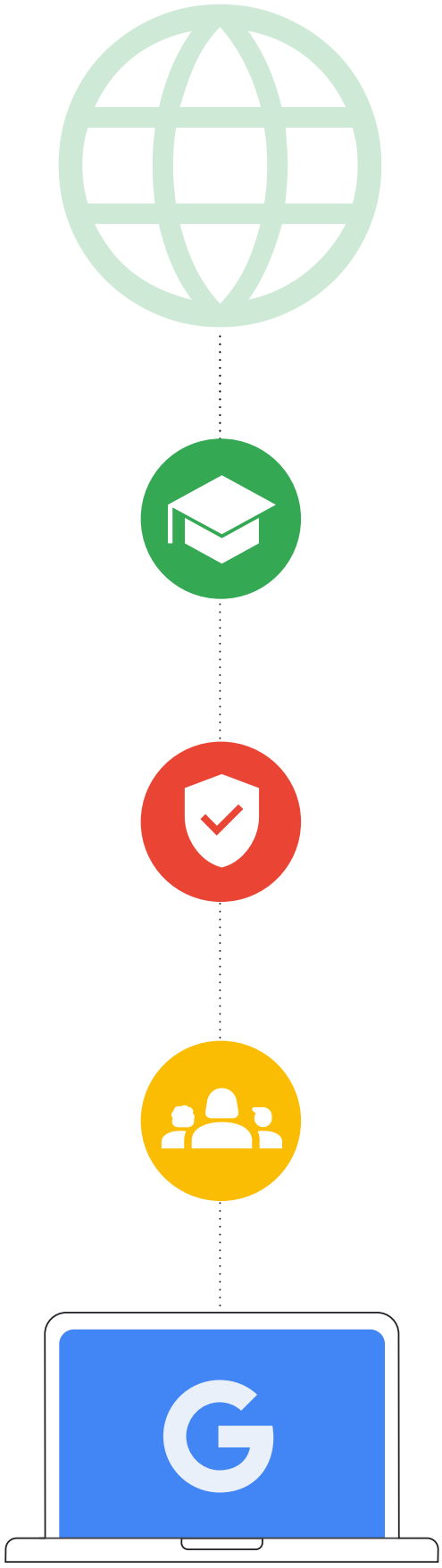
Principais recomendações

- **STOSUJ BEZPIECZNE UWIERZYTELNIANIE,** aby zapewnić ochronę informacji poufnych, e-maili, plików i innych treści oraz zapobiegać dostępowi nieautoryzowanych użytkowników do systemów edukacyjnych. Wszędzie tam, gdzie to możliwe, a zwłaszcza w przypadku administratorów IT i personelu, który ma w swojej pracy dostęp do danych wrażliwych, stosuj sprawdzone metody uwierzytelniania użytkowników, w tym silne hasła, weryfikację dwuetapową, klucze dostępu i menedżery haseł.
- **STOSUJ ODPOWIEDNIE USTAWIENIA ZABEZPIECZEŃ,** aby zapewnić bezpieczeństwo użytkowników, danych i środowiska. Usługi Google oferują bezpieczeństwo w standardzie, administratorzy muszą jednak właściwie wykorzystywać i konfigurować sieci oraz systemy pod kątem bezpieczeństwa. Aby chronić szkoły, należy stosować zasadę zero zaufania i zasadę jak najmniejszych uprawnień. Oznacza to, że użytkownicy powinni mieć dostęp tylko do tych programów, danych, aplikacji i systemów, które są im potrzebne do efektywnego wykonywania ich zadań.
- **AKTUALIZUJ I MODERNIZUJ SYSTEMY,** aby zapewnić użytkownikom ochronę przed najnowszymi zagrożeniami. Używaj nowoczesnych systemów operacyjnych i przeglądarek. Dbaj też o to, aby użytkownicy na wszystkich urządzeniach korzystali z najnowszych wersji oprogramowania (lub zatwierdzonych wersji stabilnych objętych długoterminowym wsparciem) i mieli włączone automatyczne aktualizacje. W zwiększeniu bezpieczeństwa może pomóc przejście na bezpieczniejsze rozwiązania, takie jak Chromebooki. Na żadnym urządzeniu z ChromeOS nie odnotowano dotychczas ataku ransomware.
- **STOSUJ SYSTEMY GENEROWANIA ALERTÓW I MONITOROWANIA W CZASIE RZECZYWISTYM,** aby ulepszać stan zabezpieczeń i szybciej eliminować potencjalne problemy. Możesz korzystać z funkcji wbudowanych w podstawowe oprogramowanie do współpracy i komunikacji, takie jak Google Workspace for Education, lub wdrożyć osobne rozwiązania do rejestrowania i monitorowania zdarzeń związanych z bezpieczeństwem. Zadbaj o całościowe śledzenie aktywności z uwzględnieniem wszystkich szkolnych sieci, urządzeń, aplikacji, użytkowników i danych. Monitoruj logowanie się użytkowników na konta, udostępnianie plików, e-maile (w szczególności pod kątem prób wyłudzenia informacji i przesyłania złośliwego oprogramowania), aktywność na urządzeniach oraz zmiany w konfiguracji. Aktualizuj stosowane rozwiązanie do generowania alertów i monitorowania, aby otrzymywać powiadomienia o zagrożeniach, newralgicznych zdarzeniach i zmianach w konfiguracji systemu.
- **PRZEPROWADZAJ SZKOLENIA DLA NAUCZYCIELI I INNYCH PRACOWNIKÓW ORAZ UCZNIÓW** w zakresie bezpiecznego używania urządzeń i oprogramowania, rozpoznawania i zgłaszania potencjalnych zagrożeń oraz prawidłowego udostępniania danych, co pomoże w ochronie przed najpowszechniejszymi atakami. Szkoły lub okręgi szkolne mogą tworzyć własne materiały szkoleniowe i korzystać z już dostępnych treści, uzyskując w ten sposób kompleksowe pakiety informacyjne dla swoich użytkowników.

1 https://www.cisa.gov/protecting-our-future-cybersecurity-k-12

Zalecenia dla użytkowników produktów i usług Google: produkty i usługi Google, takie jak Google Workspace for Education i Chromebooki, mogą zwiększać cyberbezpieczeństwo w szkole i ułatwiać wdrożenie każdego z przedstawionych zaleceń. Dzięki nim można stworzyć kompleksowe rozwiązanie, które chroni prywatność użytkowników i zapewnia instytucji najlepsze w swojej klasie zabezpieczenia.

Te strategie wraz z dodatkowymi wskazówkami przedstawionymi w tym dokumencie stwarzają znakomite podstawy dla bezpieczeństwa szkół podstawowych i średnich.



Podejście Google do edukacji

Misją Google jest porządkowanie światowych zasobów informacji oraz zapewnianie ich powszechnej dostępności i użyteczności. Dotyczy to również sektora edukacji. W zespole Google for Education realizujemy tę misję, tworząc takie narzędzia jak Chromebooki i Google Classroom, dzięki którym uczniowie i nauczyciele mogą łatwiej i bezpieczniej tworzyć, udostępniać i organizować swoje treści, uzyskiwać dostęp do zasobów edukacyjnych i narzędzi online oraz z nich korzystać.

Szkoły zasługują na technologie, które są z założenia bezpieczne i zaprojektowane z myślą o ochronie prywatności, umożliwiają im kontrolę i zawierają wiarygodne treści i informacje. Dzięki rozwiązaniom takim jak Chromebooki i Google Workspace for Education szkoły mają do dyspozycji najlepsze w swojej klasie zabezpieczenia, które są zgodne z najwyższymi światowymi standardami edukacyjnymi. Administratorom IT narzędzia te gwarantują pełną widoczność i bezproblemową kontrolę nad danymi i zasadami zabezpieczeń, a uczniom pozwalają zająć się nauką w bezpieczniejszym środowisku cyfrowym, które dostarcza im treści dostosowane do ich wieku oraz ogranicza spam i cyberzagrożenia.

Kładziemy nacisk na wbudowane funkcje i ustawienia zabezpieczeń, najwyższy poziom standardów ochrony prywatności i dostęp do bardziej proaktywnych narzędzi zabezpieczających, które pozwalają stworzyć bezpieczne środowisko edukacyjne dla każdego. Urządzenia z ChromeOS pomagają eliminować zagrożenia dla szkół i zapewniają najlepszą obronę przed najpoważniejszym z nich, czyli atakami typu ransomware, ponieważ Chromebooki jeszcze nigdy nie zostały skutecznie zaatakowane tą metodą.

Google Workspace for Education należy do najpopularniejszych i najbezpieczniejszych na świecie pakietów narzędzi do komunikacji i współpracy działających w chmurze. Więcej informacji o tym, jak każde z tych rozwiązań wspiera cyberbezpieczeństwo w związku z przedstawionymi tu zaleceniami, można znaleźć w drugiej części dokumentu.

Ten dokument jest podzielony na 2 części. W pierwszej z nich zajmiemy się praktycznymi, ogólnymi wskazówkami dla szkół podstawowych i średnich dotyczącymi bezpieczeństwa, nie odnosząc się przy tym do konkretnych produktów i usług. Druga część jest poświęcona konkretnym wskazówkom dotyczącym konfiguracji w instytucjach korzystających z oferty Google for Education, w tym Google Workspace for Education i Chromebooków. Obie części zawierają informacje pomocne w zapewnianiu pracownikom i uczniom bezpieczeństwa online.

Wprowadzenie

Urządzenia i sieci szkół podstawowych i średnich są w dużym stopniu narażone na cyberataki. Dlatego instytucje te muszą stosować najlepsze zabezpieczenia, które będą chronić uczniów i zapobiegać skutkom ataków, takim jak utrata danych, zasobów, czasu i pieniędzy oraz wyłączenia usług (źródło).

Ten przewodnik promuje sprawdzone metody zapewniania cyberbezpieczeństwa, które administratorzy szkół powinni wdrożyć w swoich systemach, aby lepiej je zabezpieczyć. Wprowadzając te rozwiązania, szkoły podstawowe i średnie mogą ograniczyć poważne i kosztowne cyberataki na systemy edukacyjne lub im zapobiegać, a także chronić uczniów, ich rodziny, nauczycieli i innych pracowników szkoły.

Cyberataki wymierzone w szkoły są coraz częstsze i przybierają na sile. Z danych K-12 Cybersecurity Resource Center wynika, że w latach 2016–2021 we wszystkich 50 stanach USA miało miejsce ponad 1300 ujawnionych publicznie cyberincydentów dotyczących instytucji edukacyjnych. Osoby odpowiedzialne za edukację muszą chronić zasoby informacji i dane osobowe uczniów, nauczycieli i innych pracowników, a także systemy i informacje instytucji. To niełatwe zadanie zwłaszcza z uwagi na fakt, że dotrzymywanie kroku wymaganiom w zakresie cyberbezpieczeństwa jest zwykle w edukacji trudniejsze niż w innych sektorach.

Skuteczne cyberataki, w tym ataki typu ransomware, wyłudzanie informacji, ataki z użyciem złośliwego oprogramowania itp., mogą spowodować rozległe naruszenia bezpieczeństwa informacji umożliwiających identyfikację osób, poważne obciążenia finansowe (średni okup zwiększył się od 2020 r. pięciokrotnie, sięgając 812 260 USD) oraz długotrwałe zakłócenia w nauczaniu i innej szkolnej działalności. Pewien skuteczny atak typu ransomware uniemożliwił niedawno działanie całego systemu szkolnego, co z kolei pociągnęło za sobą konsekwencje dla całej społeczności, ponieważ uczniowie przez jakiś czas nie mogli uczestniczyć w zajęciach. Szkoły podstawowe i średnie mają ograniczone zasoby i środki finansowe, a bez inwestycji w cyberzabezpieczenia instytucje te w dalszym ciągu będą celem chętnie wybieranym przez przestępców.

Cyberbezpieczeństwo działa najlepiej, gdy obejmuje komunikację, współpracę i partnerstwo. Ten dokument łączy wskazówki dotyczące bezpieczeństwa przygotowane przez Google, najlepsze praktyki dotyczące cyberbezpieczeństwa (Cybersecurity Framework) opracowane przez amerykański Narodowy Instytut Norm i Techniki (NIST) oraz narzędzia i zalecenia zebrane w 2023 r. w raporcie K-12 Cybersecurity przez organizację CISA. Wszystkie te materiały stanowią powszechnie uznane źródła informacji na temat metod pomagających zwiększać cyberbezpieczeństwo. Omawiamy tu ogólne działania, które powinni podjąć lub rozważyć administratorzy IT, oraz stosowane przez Google sprawdzone metody i wskazówki dotyczące naszych produktów i usług, a także wskazówki dotyczące bezpieczeństwa i usługi zabezpieczające oferowane przez inne firmy. Administratorzy powinni przejrzeć wszystkie wytyczne dotyczące bezpieczeństwa przygotowane przez producentów używanych rozwiązań i wdrażać ich najnowsze zalecenia, ponieważ producent najlepiej potrafi opisać własne produkty i wszelkie związane z nimi zmiany.

Przed realizacją wymienionych niżej zaleceń należy również wziąć pod uwagę następujące czynniki.

Kwestie do uwzględnienia

1. **Ochrona uczniów.**
   Każda szkoła ma inne potrzeby, a niektóre społeczności mogą wymagać dodatkowych kroków zapewniających bezpieczeństwo i prywatność. Wiele technologii używanych w edukacji jest wyposażonych w funkcje, które pomagają skonfigurować dostęp zależny od wieku, w tym ograniczać nieodpowiednie treści lub chronić prywatność lokalizacji i danych kontaktowych.
2. **Typy przechowywanych danych.**
   Jeśli przechowujesz dane wrażliwe, warto je zaszyfrować lub przechowywać w osobnej lokalizacji.
3. **Typy używanych urządzeń i model wdrożenia.**
   Urządzenia i zainstalowane na nich aplikacje powinny automatycznie się aktualizować (z myślą o maksymalnym bezpieczeństwie), szyfrować dane i izolować konta, ponieważ pozwoli to mieć pewność, że użytkownicy mają dostęp tylko do własnych informacji.
4. **Zasady szkolne, okręgowe lub regionalne.**
   Twoja szkoła może być objęta określonymi zasadami w zakresie korzystania z technologii. Zadbaj o to, aby wszystkie zabezpieczenia były skonfigurowane zgodnie z nimi.

Każdego dnia Gmail blokuje

100 mln

prób phishingu.

Każdego tygodnia Google identyfikuje

300 tys

niebezpiecznych stron internetowych.

Każdego dnia

74 mln

użytkowników korzystają z Menedżera haseł Google.

Każdego roku

700 mln

osób podnosi poziom swojego bezpieczeństwa dzięki stronie Sprawdzanie zabezpieczeń.

Use a autenticação segura

Bezpieczne uwierzytelnianie to jeden z głównych priorytetów szkół i innych instytucji. W IV kwartale 2022 r. słabo zabezpieczone lub pozbawione uwierzytelniania konta stanowiły 48% wszystkich ścieżek wykorzystanych w naruszeniach zabezpieczeń. Wdrożenie kilku kluczowych zaleceń może pomóc sprawdzić, czy użytkownicy są tymi, za kogo się podają, i ograniczyć ich dostęp do tych informacji, które są potrzebne w przypadku określonej roli użytkownika.

Administratorzy IT powinni wymusić stosowanie weryfikacji dwuetapowej (nazywanej również uwierzytelnianiem dwuskładnikowym) i wszędzie tam, gdzie to możliwe, przejść na uwierzytelnianie bez hasła (przy użyciu kluczy dostępu) – zwłaszcza wtedy, gdy użytkownik uzyskuje dostęp do systemów danej instytucji edukacyjnej zdalnie. Weryfikacja dwuetapowa wprowadza dodatkową warstwę zabezpieczeń, która znacznie utrudnia osobom przeprowadzającym atak uzyskanie dostępu.

Szkoły podstawowe i średnie stosują obecnie wiele typów urządzeń i modeli wdrożenia, a użytkownicy w środowiskach szkolnych dysponują różnymi umiejętnościami technicznymi. Zgodnie ze sprawdzonymi metodami wykorzystywane zabezpieczenia kont i urządzeń różnią się zależnie od ról i typów użytkowników: administratorzy IT, nauczyciele i inni pracownicy oraz starsi uczniowie korzystają z przypisanych do nich urządzeń, a młodsi uczniowie używają urządzeń współdzielonych. Poniżej omawiamy konkretne zalecenia dotyczące każdej z tych grup.

Istnieje kilka metod uwierzytelniania, które są zalecane przez sprawdzone metody w większości sytuacji.

- **Silne hasła:**
  Wymagaj od użytkowników ustawienia własnego hasła przy pierwszym logowaniu i za pomocą narzędzi technicznych egzekwuj wymagania dotyczące minimalnej długości i złożoności haseł. Dłuższe hasła zawierające znaki specjalne zapewniają dodatkowe bezpieczeństwo. Użytkownicy nie powinni być zmuszani do regularnych zmian haseł, ponieważ w efekcie często stosują prostsze hasła lub wprowadzają w nich jedynie nieistotne zmiany (na przykład modyfikują pojedynczy znak).
- **Weryfikacja dwuetapowa:**
  Chroni konta dzięki drugiemu etapowi weryfikacji, który często wykorzystuje coś, co użytkownik ma przy sobie, na przykład klucz bezpieczeństwa lub aplikację generującą jednorazowy kod weryfikacyjny na telefonie komórkowym. Każda forma weryfikacji dwuetapowej zwiększa bezpieczeństwo, jednak administratorzy powinni unikać stosowania kodów weryfikacyjnych wysyłanych w wiadomościach SMS lub przekazywanych telefonicznie, ponieważ są one narażone na ataki wykorzystujące numery telefonów.
- **Uwierzytelnianie bez hasła:**
  Klucze dostępu to bezpieczniejsza i łatwiejsza w obsłudze alternatywa dla haseł. Użytkownicy mogą logować się w aplikacjach i na stronach internetowych za pomocą kodu PIN, wzoru, czujnika biometrycznego (na przykład przy użyciu odcisku palca lub funkcji rozpoznawania twarzy) bądź dotknięcia klucza bezpieczeństwa, dzięki czemu nie muszą zapamiętywać haseł ani nimi zarządzać. Rozwiązania te nie zawsze są najbardziej odpowiednie w środowisku edukacyjnym, w coraz większym stopniu zastępują jednak tradycyjne formy uwierzytelniania, zapewniając bezpieczniejsze i szybsze logowanie na konta. Klucze dostępu chronią użytkowników przed atakami phishingowymi, ponieważ działają tylko z powiązanymi z nimi stronami internetowymi i aplikacjami.
- **Logowanie jednokrotne (SSO):**
  Umożliwia użytkownikom dostęp do wielu aplikacji i stron za pomocą jednego zestawu danych logowania. Gdy użytkownicy muszą zapamiętać tylko jeden taki zestaw danych, rzadziej je zapisują. Co więcej, gdy szkoły nie muszą zarządzać wieloma zestawami danych logowania użytkownika, mogą zaoszczędzić na kosztach wsparcia IT i zespołu pomocy. Google Workspace for Education natywnie obsługuje SSO, użytkownicy mogą więc korzystać ze swoich danych logowania na konto Google, aby logować się w zewnętrznych aplikacjach, lub wykorzystywać dane logowania z innej usługi do logowania się na swoje konta Google.
- **Menedżery haseł:**
  Mogą pomóc użytkownikom tworzyć silne, unikalne hasła do różnych kont i usług, których używają w szkole i w pracy (gdy nie korzystają z logowania jednokrotnego). Narzędzia te nie ułatwiają logowania się w systemie operacyjnym, ale mogą zarządzać hasłami, które użytkownik wykorzystuje już po zalogowaniu się na urządzeniu. Użytkownicy Google mogą korzystać z Menedżera haseł w Chrome na wszystkich platformach, w tym w ChromeOS i Androidzie.

Różne grupy mające unikalne potrzeby skorzystają na wprowadzeniu określonych elementów lub kombinacji tych metod uwierzytelniania zależnie od swojej roli w instytucji edukacyjnej, rodzaju systemów i danych, do których mają dostęp, oraz wieku.

Szkolni administratorzy

Administratorzy kontrolują systemy i znaczną część szkolnych danych. Ochrona ich kont jest kluczem do bezpieczeństwa całego systemu – od infrastruktury przez dane kont po urządzenia, którymi zarządza instytucja. Dlatego administratorzy powinni stosować złoty standard w zakresie uwierzytelniania, w tym silne hasła, sprawdzonego menedżera haseł i weryfikację dwuetapową. Każde z tych narzędzi zapewnia własną warstwę ochrony, a ich połączenie pozwala uzyskać najsilniejsze zabezpieczenia konta administratora i usług w instytucji.

- Administratorzy powinni stosować fizyczny klucz bezpieczeństwa lub szyfrowaną metodę weryfikacji dwuetapowej, która wymaga zaufanego urządzenia i potwierdzeń. Może to obejmować usługę taką jak Google Authenticator lub inną aplikację, która generuje jednorazowe kody weryfikacyjne. Chromebooki wydane po 2019 roku i wyposażone w chip TPM mają przycisk zasilania, którego można używać do uwierzytelniania dwuskładnikowego.
- Do przechowywania swoich haseł do różnych usług administratorzy powinni używać zaufanego menedżera haseł obsługującego weryfikację dwuetapową.

Nauczyciele i inni pracownicy szkoły używający przypisanych do nich urządzeń

Nauczyciele i inni pracownicy szkoły mają dostęp do danych wrażliwych tak jak administratorzy, ale nie kontrolują infrastruktury cyfrowej, a ich umiejętności techniczne są zróżnicowane.

- Tam, gdzie to dopuszczalne na mocy przepisów, nauczyciele i inni pracownicy szkoły korzystający z Chromebooków powinni mieć możliwość logowania się z użyciem weryfikacji biometrycznej, na przykład za pomocą odcisku palca.
- Administratorzy powinni wdrożyć stosowanie weryfikacji dwuetapowej i w miarę możliwości wprowadzić uwierzytelnianie bez hasła. Drugie z tych rozwiązań powinno być stosowane zawsze w przypadku zdalnego uzyskiwania dostępu do systemów instytucji edukacyjnej.

Starsi uczniowie korzystający z przypisanych do nich urządzeń (zwykle od 4 klasy w górę)

Starsi uczniowie lepiej wiedzą, jak się chronić, i zwykle potrafią korzystać z liczniejszych zabezpieczających mechanizmów uwierzytelniania dostosowanych do typów usług, których będą prawdopodobnie używać. Powinni mieć dostęp tylko do własnego konta i do informacji, które zostały im udostępnione.

- Uczniowie używający Chromebooków powinni mieć możliwość utworzenia kodu PIN, który przyspieszy logowanie się na danym urządzeniu. W wielu środowiskach szkolnych może nie być możliwości korzystania z opcji uwierzytelniania biometrycznego lub mogą one nie być odpowiednie.
- Każdemu uczniowi należy pomóc w utworzeniu unikalnego hasła, które nie zawiera danych osobowych (takich jak imię, nazwisko, klasa czy data urodzenia). Trzeba też pokazać uczniom, jak zwiększyć złożoność haseł, a jednocześnie łatwo je zapamiętać.

Młodsi uczniowie korzystający ze współdzielonych urządzeń (zwykle klasy 1–3)

Najmłodsi uczniowie wciąż jeszcze uczą się korzystać z technologii edukacyjnych i mogą używać prostego uwierzytelniania, które jest odpowiednie w przypadku ograniczonego dostępu do usług i danych.

- Szkoły, które stosują zewnętrzne alternatywy dla haseł, takie jak logowanie za pomocą kodu QR lub obrazków dla najmłodszych uczniów i tych, którzy nie są w stanie logować się przy użyciu hasła, powinny wdrożyć środki ostrożności, ponieważ metody te zapewniają mniejsze bezpieczeństwo. Administratorzy powinni modyfikować hasło ucznia i aktualizować kod za każdym razem, gdy uczeń go utraci lub gdy kod trafi w ręce kogoś innego.
- Szkoły powinny uczulić zarówno uczniów, jak i rodziców, jak ważne jest zachowywanie haseł w tajemnicy i bezpieczne przechowywanie alternatywnych danych logowania, takich jak kody QR.
- W przypadku urządzeń przypisanych do uczniów, na przykład tabletów, jako alternatywną bezpieczną metodę uwierzytelniania można zastosować powiązany z urządzeniem kod PIN.

Stosowanie odpowiednich ustawień zabezpieczeń

Szkolne urządzenia i sieci to dobrze widoczne, a zarazem atrakcyjne cele dla przestępców na całym świecie, dlatego tak ważne jest stosowanie jak najlepszych zabezpieczeń, które pomogą zapobiegać wyłączeniom usług oraz utracie zasobów, czasu i pieniędzy. Administratorzy systemów powinni wdrożyć skuteczne i odpowiednie funkcje zabezpieczeń dostępne w rozwiązaniach używanych przez ich instytucje. Muszą też jednak zadbać o to, aby systemy te były w dalszym ciągu łatwe w obsłudze dla nauczycieli i innych pracowników szkoły oraz uczniów. Ważne ustawienia zabezpieczeń i prywatności należy skonfigurować tak, aby poszczególni użytkownicy nie mogli ich wyłączyć lub zmienić. W przypadku innych ustawień administratorzy powinni skonfigurować dla bezpieczeństwa wartości domyślne. Niezwykle ważne jest stosowanie jak najlepszych zabezpieczeń, które pomogą zapobiegać wyłączeniom usług oraz stratom zasobów, czasu i pieniędzy. Jeśli używasz Chromebooków, w drugiej części tego dokumentu znajdziesz nasze sugestie na temat konfiguracji zasad dotyczących urządzeń.

Zadbaj też o uwzględnienie w swoich procedurach zasady minimalizacji danych, ograniczając cele i sposoby zbierania, używania i ujawniania danych osobowych poszczególnych osób do zakresu, który jest uzasadniony i adekwatny dla świadczonej usługi lub w inny sposób dostosowany do kontekstu danej relacji.

Aplikacje i aktualizacje

Ogranicz do minimum aplikacje, które mogą instalować użytkownicy, ponieważ każda aplikacja zainstalowana na urządzeniu to potencjalny wektor ataku. W miarę możliwości używaj aplikacji z zaufanych źródeł, np. zalecając użytkownikom sprawdzanie plakietki weryfikacyjnej w Sklepie Google Play, aby mieć pewność, że obierają oficjalne aplikacje, które przeszły kontrolę bezpieczeństwa. Każda modyfikacja systemu operacyjnego lub sprzętu (jailbreaking lub rootowanie) oznacza znaczne obniżenie poziomu bezpieczeństwa i należy tego unikać.

Dostęp i widoczność

Administratorzy powinni zadbać o to, aby użytkownicy mieli dostęp tylko do tych danych, programów, usług i systemów, które są im potrzebne do efektywnego uczenia się lub wykonywania obowiązków. Pomaga to ograniczyć przypadki niezamierzonego dostępu i śledzić, kto uzyskuje dostęp do określonych zasobów. Zwracaj szczególną uwagę na bardzo wrażliwe dane (takie jak informacje umożliwiające identyfikację użytkowników) i systemy (takie jak kadry, płace, oceny, bezpieczeństwo i konfiguracja). Kontroluj, którzy użytkownicy i w jakich okolicznościach mogą uzyskiwać dostęp do danych, ograniczając dostęp do szkolnych urządzeń i umożliwiając go tylko określonym pracownikom.

Przejrzyj zasady udostępniania danych w narzędziach do współpracy, aby zapobiec nieodpowiedniemu lub nadmiernemu udostępnianiu danych oraz nieautoryzowanemu dostępowi. Ogranicz lub zablokuj udostępnianie poza środowiskiem (zwłaszcza w przypadku uczniów) i włącz zasady, które odpowiadają za monitorowanie udostępniania poufnych treści.

Utrata lub kradzież urządzenia

Utrata urządzenia nie musi oznaczać utraty danych. Administratorzy powinni opracować standardowy plan obejmujący na przykład zapisywanie dokumentów w chmurze, który zapewni dostęp do informacji i dokumentów w przypadku utraty lub kradzieży urządzenia. Pobierz i wydrukuj kody zapasowe na potrzeby procesów weryfikacji dwuetapowej, aby zapobiec utracie dostępu do konta.

W przypadku utraty lub kradzieży urządzenia zadbaj o jego zdalne zablokowanie i o zablokowanie lub oznaczenie powiązanych z nim kont. Dzięki temu nie będą one używane do uzyskiwania nieautoryzowanego dostępu. Utracone Chromebooki można wyczyścić zdalnie, a konta Google Workspace for Education można monitorować pod kątem podejrzanej aktywności lub w razie potrzeby zawiesić (zablokować).

Proteção avançada para usuários de alto risco

Para os usuários com alta visibilidade e informações sensíveis, incluindo os administradores do Google Workspace for Education, o Google oferece o Programa Proteção Avançada (PPA). O PPA fornece aos usuários mais proteção contra ataques direcionados, como phishing, downloads nocivos e vazamento de senha. O programa foi especificamente criado para impedir ataques on-line direcionados às Contas do Google. Ele usa automaticamente um método de autenticação forte e chaves de segurança, além de restringir o acesso de terceiros aos dados da conta. Outros provedores de contas on-line também oferecem recursos de proteção robustos para usuários de alto risco. Os administradores e funcionários precisam sempre usar esse tipo de recurso caso tenham acesso a informações pessoais ou sistemas de tecnologia.

Aktualizowanie i modernizowanie systemów

Jednym z najważniejszych i dostępnych dla każdego sposobów ochrony jest aktualizowanie systemu operacyjnego urządzenia i zainstalowanych na nim aplikacji. W przypadku szkół podstawowych i średnich jest to szczególnie ważne, ponieważ stanowią one istotną część edukacji i codziennego życia dzieci. Większość ataków z użyciem złośliwego oprogramowania w kontekstach edukacyjnych i innych obszarach szczególnie narażonych ma miejsce w środowiskach opartych na systemie Windows. Tak było w przypadku ataków wykorzystujących oprogramowanie SolarWinds, ataku typu ransomware na okręg szkolny w Los Angeles, ataku hakerów na okręg szkolny Little Rock, naruszenia bezpieczeństwa danych w rozwiązaniu Microsoft Exchange Server, ataku typu ransomware na okręg szkolny w Albuquerque oraz niedawnych ataków na rozwiązania firmy Microsoft w amerykańskiej agencji federalnej. Tutaj również używanie działających w chmurze produktów i usług powinno ułatwić administratorom zadanie przez ograniczenie powierzchni ataku i automatyczne zapewnienie aktualności systemów i aplikacji.

Przejście na nowoczesny system operacyjny i dbanie o jego aktualność

Najnowsza wersja każdego systemu operacyjnego zawiera zwykle nowe funkcje zabezpieczeń, które pomagają w ochronie przed znanymi wektorami ataku. Włącz automatyczne aktualizacje w systemie operacyjnym urządzenia lub – jeśli to niemożliwe – pobieraj i instaluj łatki i aktualizacje od zaufanego dostawcy co najmniej raz w miesiącu.

Chromebooki działają na systemie operacyjnym ChromeOS, otrzymują więc częste, automatyczne aktualizacje z najnowszymi poprawkami zabezpieczeń, co umożliwia szybkie wdrażanie innowacyjnych rozwiązań w tym zakresie. Sprawdzają też integralność plików systemu operacyjnego oznaczonych jako tylko do odczytu jeszcze przed jego uruchomieniem. Szyfrują wszystkie dane zapisywane na urządzeniu, chronią je przed nieautoryzowanym dostępem i uruchamiają każdą stronę i aplikację w osobnej piaskownicy, dzięki czemu strony i aplikacje zainfekowane złośliwym oprogramowaniem nie mogą rozprzestrzenić go na inne części urządzenia.

Jeśli Twoja szkoła nie jest gotowa na przejście na Chromebooki, może skorzystać z systemu ChromeOS Flex – wersji ChromeOS, która powstała z myślą o modernizacji szkolnych urządzeń. ChromeOS Flex zapewnia wszystkim użytkownikom ujednolicone, nowoczesne środowisko do nauczania i zdobywania wiedzy, które jest wyposażone w proaktywne, wbudowane zabezpieczenia i działające w chmurze funkcje zarządzania. Oferuje również zautomatyzowaną ochronę i blokuje złośliwe pliki wykonywalne oraz aplikacje bez konieczności wymiany szkolnego sprzętu.

Zainstalowanie nowoczesnej przeglądarki i dbanie o jej aktualizację

Trzeba również zadbać o aktualizację i bezpieczeństwo przeglądarki internetowej. Nowoczesne przeglądarki oferują bardziej zaawansowane funkcje zabezpieczeń i mogą przypominać użytkownikom o ich łatwym włączeniu. Funkcje te mogą też skonfigurować administratorzy, aby były domyślnie włączone na szkolnych komputerach, co pomaga chronić informacje poufne przesyłane przez internet. Przeglądarka powinna być na bieżąco aktualizowana. Podczas pracy, nauki i innych aktywności online zaktualizowana, nowoczesna przeglądarka:

- **stosuje niezawodne zabezpieczenia**, w tym izolację witryn i funkcję bezpiecznego przeglądania, aby uniemożliwiać użytkownikom przypadkowe wejście na niebezpieczne strony;
- **Włącza automatyczne aktualizacje**, aby zapewnić szybkie instalowanie aktualizacji swoich zabezpieczeń;
- **Dba o bezpieczeństwo połączenia –** nowoczesne przeglądarki powinny stosować protokół TLS (Transport Layer Security), a użytkownicy mogą kliknąć obok adresu URL i sprawdzić, czy połączenie jest oznaczone jako bezpieczne.

Przeglądarka Chrome powstała z myślą o bezpieczeństwie, a funkcje zabezpieczeń takie jak Bezpieczne przeglądanie są w niej domyślnie włączone. Jest też wyposażona w zintegrowany menedżer haseł, który może automatycznie je uzupełniać podczas przeglądania stron internetowych, co ułatwia stosowanie silnych haseł.

Stosowanie systemów generowania alertów i monitorowania w czasie rzeczywistym

Działające w czasie rzeczywistym systemy generowania alertów i monitorowania mogą pomóc szkołom identyfikować zagrożenia i szybko na nie reagować, zanim wyrządzą szkody. Narzędzia zabezpieczające muszą działać w tle, zbierając i logując zdarzenia związane z bezpieczeństwem z całego systemu. Do przeszukiwania dużych ilości zebranych danych i wyszukiwania w nich anomalii i wzorców szczególnie dobrze nadają się narzędzia AI, które pozwalają szybciej i łatwiej wykrywać zagrożenia oraz przetwarzać i eliminować luki w zabezpieczeniach. Dzięki temu można określić, która aktywność wymaga priorytetowego sprawdzenia przez administratora lub zespół IT.

Szkoły mogą używać funkcji generowania alertów i monitorowania wbudowanych w swoje główne oprogramowanie do współpracy i komunikacji, takie jak Google Workspace for Education. Mogą też wdrożyć osobne rozwiązania do zarządzania informacjami i zdarzeniami bezpieczeństwa (SIEM).

Systemy generowania alertów i monitorowania w czasie rzeczywistym mogą śledzić zróżnicowaną aktywność, obejmując przy tym szkolną sieć oraz urządzenia, aplikacje, użytkowników i dane. Mogą na przykład uwzględniać logowanie się przez użytkowników, dostęp do plików, potencjalne włamania, udane lub nieudane przypadki kradzieży danych oraz czynności wykonywane przez administratora.

Jeśli system wykryje jakąkolwiek podejrzaną aktywność, może wysłać alert do szkolnego zespołu IT. Dzięki temu administratorzy są w stanie zbadać problem i podjąć działania, aby zniwelować zagrożenie.

Narzędzia do generowania alertów i monitorowania mogą też pomóc w lepszym zrozumieniu zagrożeń, z którymi mają do czynienia szkoły. Analizując dane z tych działających w czasie rzeczywistym systemów, szkoły mogą znajdować trendy i wzorce pomocne w skuteczniejszej ochronie ich środowisk. .

Oto niektóre ze sprawdzonych metod używania systemów generowania alertów i monitorowania (w tym systemów SIEM):

1. **Określ cele w zakresie bezpieczeństwa**
   Ustal, które informacje i systemy są dla szkoły najbardziej newralgiczne i jakie typy zagrożeń stanowią dla nich największe ryzyko. Następnie określ dane, które musisz zbierać, aby monitorować środowisko pod kątem tych zagrożeń.

2. **Zbieraj odpowiednie dane i zadbaj o poprawną konfigurację**
   Musisz zbierać odpowiednie dane i konfigurować aplikacje pod kątem najistotniejszych celów w zakresie bezpieczeństwa. Mogą to być dane z zapór sieciowych, filtrów treści, systemów wykrywania włamań, serwerów WWW i innych urządzeń zabezpieczających, a także z oprogramowania do komunikacji i współpracy, szkolnych systemów informacji i systemów zarządzania uczeniem.

3. **Analizuj alerty i reaguj na nie**
   Gdy system monitorowania wygeneruje alert, trzeba zbadać problem i podjąć odpowiednie działania. Może to wymagać wspólnej pracy kilku zespołów nad analizą źródła alertu, określenia, czy alert nie jest fałszywy, lub podejmowania działań pozwalających wyeliminować zagrożenie, na przykład przez zawieszenie konta, zresetowanie haseł użytkowników, poddanie e-maili kwarantannie lub ich usunięcie, zmianę uprawnień do plików czy wyczyszczenie pamięci urządzeń.

Szkolenie nauczycieli i innych pracowników szkoły oraz uczniów

Szkoły podstawowe i średnie oraz całe okręgi szkolne powinny pracować nad zwiększaniem w szkolnych społecznościach świadomości w zakresie bezpieczeństwa i wyrabianiem w nich odpowiednich nawyków poprzez różnego rodzaju kampanie i partnerstwa. Pokazywanie nauczycielom i innym pracownikom szkoły oraz uczniom, jak ważne jest bezpieczeństwo, ma kluczowe znaczenie, ponieważ pomaga im samym chronić się online i zapobiegać poważnym cyberzagrożeniom. Naucz użytkowników korzystać z produktów i usług wdrożonych w całej instytucji, dostrzegać i zgłaszać zagrożenia (na przykład e-maile wyłudzające informacje), a przede wszystkim działać w celu zapobiegania atakom.

Bezpieczne używanie urządzeń i oprogramowania

Aby pomóc uczniom zrozumieć, jak bezpiecznie używać urządzeń, oprogramowania i systemów, administratorzy mogą nawiązać współpracę z nauczycielami i ekspertami, którzy specjalizują się w opracowywaniu dostosowanych do wieku odbiorców programów nauczania poświęconych cyberbezpieczeństwu. Tworzenie materiałów szkoleniowych oznaczonych logo szkoły lub okręgu szkolnego pomaga umieścić zalecenia dla nauczycieli i uczniów w kontekście, możesz też jednak wykorzystać gotowe materiały dostępne na przykład w programie Asy Internetu, na stronie safety.google i na platformie Khan Academy oraz dostosować je do indywidualnych potrzeb. Programy te mogą pomóc użytkownikom zadbać o swoje bezpieczeństwo niezależnie od tego, gdzie się znajdują – w szkole czy poza nią.

Dostrzeganie zagrożeń

Pokazanie nauczycielom i innym pracownikom szkoły oraz uczniom, jak wykrywać zagrożenia, to ważna część zapewniania im bezpieczeństwa. Trzeba uczyć dzieci rozpoznawania, czy coś jest zagrożeniem czy nie, ponieważ mogą one jeszcze nie wiedzieć, jak sprawdzić wiarygodność treści. Istnieje kilka typów zagrożeń, które dzieci powinny umieć rozpoznawać i zgłaszać, dlatego dobrze by było, gdyby administratorzy skupiali się na tych zagadnieniach, które ich zdaniem przyniosą największy zysk z tej inwestycji w edukację. Co ważne, szkolenia powinny uczyć użytkowników nie tylko dostrzegać zagrożenia, lecz także podejmować odpowiednie działania. Do powszechnie spotykanych niebezpieczeństw, które użytkownicy powinni rozpoznawać, należą ransomware, wyłudzanie informacji, inżynieria społeczna, złośliwe oprogramowanie i oszustwa, ale w edukacji warto położyć nacisk na te, które w tej konkretnej sytuacji występują najczęściej.

Bezpieczne udostępnianie danych i plików

Nauczycielom i innym pracownikom szkoły należy organizować szkolenia, aby wiedzieli, jak poprawnie udostępniać pliki i dane oraz jak rozpoznawać nieodpowiednie prośby przesyłane w e-mailach. Poufne dane osobowe powinny być udostępniane lub przetwarzane tylko wtedy, gdy jest to konieczne, a także objęte dodatkowymi warstwami zabezpieczeń, aby nigdy nie przekazywano ich w e-mailach lub osobom spoza szkoły. Nauczyciele i inni pracownicy szkoły powinni używać funkcji zapobiegania utracie danych (dostępnych w ChromeOS i Workspace for Education), które ostrzegają użytkowników i uniemożliwiają im udostępnianie plików z danymi wrażliwymi (takimi jak numery PESEL) lub kopiowanie i wklejanie informacji poufnych poza domeną.

Podejście Google w praktyce: urządzenia i usługi w edukacji

Zakup oprogramowania to jedno z najskuteczniejszych działań, jakie mogą podjąć okręgi szkolne w celu zabezpieczenia swoich użytkowników i danych. Takie oprogramowanie powinno być niezawodne, zaprojektowane z myślą o minimalizowaniu ryzyka związanego z lukami w zabezpieczeniach oraz wyposażone w zabezpieczenia wbudowane na każdym poziomie. Gdy szkoła ma obowiązek zakupu bezpiecznego oprogramowania lub rozwiązania firm oferujących sprawdzone zabezpieczenia, można znacznie ograniczyć zagrożenia cybernetyczne. Na przykład firma Google wzmocniła zabezpieczenia systemu ChromeOS, a jednocześnie nieprzerwanie wdraża bardziej proaktywne, inteligentne rozwiązania, które wykorzystują możliwości naszych systemów uczących się i chmury oraz wiedzę w zakresie tożsamości.

Chcemy tworzyć usługi, które pomagają chronić prywatność uczniów i nauczycieli oraz zapewniają instytucji najlepsze zabezpieczenia w swojej klasie. Możesz mieć pewność, że produkty i usługi Google for Education nieustannie chronią użytkowników, urządzenia i dane przed coraz bardziej złożonymi zagrożeniami. W tej części przedstawiamy zalecenia dla szkolnych administratorów IT dotyczące bezpieczeństwa przy korzystaniu z rozwiązań Google for Education.

Google Workspace for Education

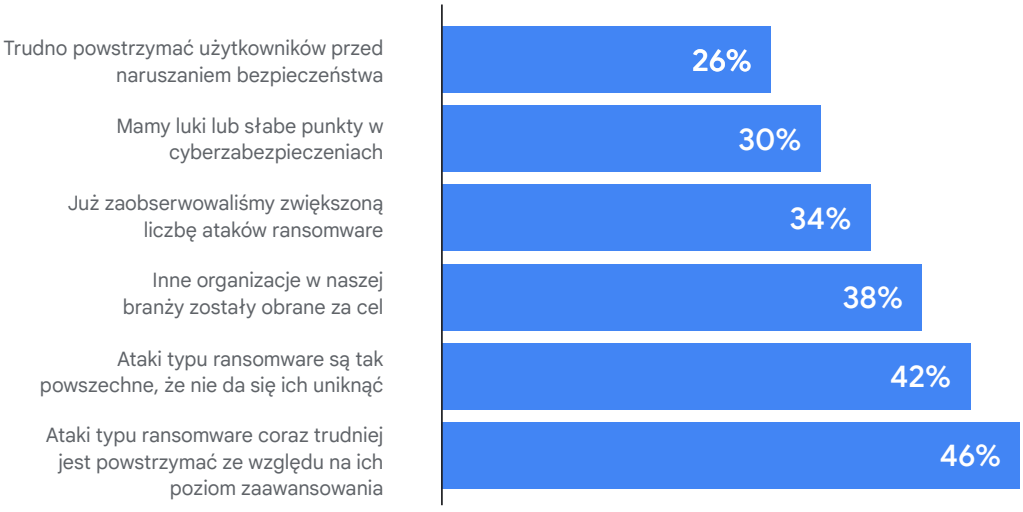
Google Workspace for Education to pakiet narzędzi i usług Google opracowanych z myślą o edukacji szkolnej, które ułatwiają pracę zespołową i przekazywanie wiedzy, a także pomagają zapewnić bezpieczną naukę. Produkty i usługi Google for Education nieustannie chronią użytkowników, urządzenia i dane przed coraz bardziej złożonymi zagrożeniami. Udostępniają takie narzędzia jak centrum alertów i bezpieczeństwa, sejf na potrzeby pozyskiwania danych elektronicznych, zarządzanie tożsamościami i dostępem oraz zapobieganie utracie danych (DLP).

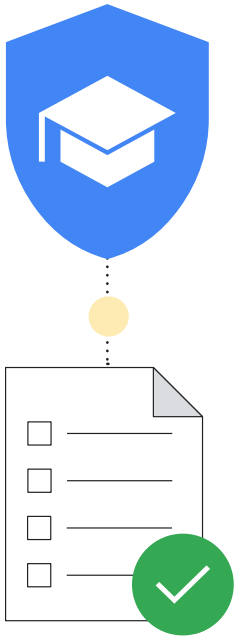
Zebraliśmy przydatne materiały, które przydadzą Ci się, jeśli dopiero zaczynasz korzystać z Google Workspace for Education. Wiele z nich pomoże Ci skonfigurować ustawienia zgodnie z zaleceniami z tego przewodnika. Aby dowiedzieć się, jak rozpocząć pracę z Google Workspace for Education, zajrzyj do tego krótkiego przewodnika po konfiguracji dla działu IT.

Listy kontrolne zabezpieczeń

Przejrzyj listy kontrolne zabezpieczeń, aby dowiedzieć się więcej o tym, jak zwiększyć bezpieczeństwo i prywatność w Twojej instytucji. Szkoły używające Google Workspace for Education w wersjach Standard i Plus mogą też skorzystać ze strony Stan zabezpieczeń, aby monitorować konfigurację ustawień konsoli administracyjnej. Możesz na niej sprawdzić stan ustawień, takich jak Automatyczne przekazywanie e-maili dalej, Szyfrowanie urządzenia czy Ustawienia udostępniania na Dysku. W razie potrzeby możesz zmieniać ustawienia domeny zgodnie z ogólnymi wskazówkami dotyczącymi bezpieczeństwa i sprawdzonymi metodami, biorąc pod uwagę potrzeby biznesowe oraz zasady zarządzania ryzykiem w organizacji..

Dlaczego sektor edukacyjny spodziewa się ataku





Źródło: https://assets.sophos.com/X24WTUEQ/at/g523b3nmgcfk5r5hc5sns6q/sophos-state-of-ransomware-in-education-2021-wp.pdf

Oto kilka innych przydatnych wskazówek, które pozwolą Ci maksymalnie wykorzystać zabezpieczenia wbudowane w Google Workspace for Education::

Skonfiguruj jednostki organizacyjne (OU)

Nikt nie twierdzi, że wszyscy użytkownicy powinni mieć takie same ustawienia na Twoim koncie Google Workspace for Education. Jednostki organizacyjne to grupy użytkowników, dla których można skonfigurować różne usługi, ustawienia i uprawnienia. Może to być na przykład weryfikacja dwuetapowa w przypadku nauczycieli i innych pracowników szkoły oraz uwierzytelnianie dostosowane do wieku odbiorcy w przypadku młodszych uczniów. Skonfiguruj osobne jednostki organizacyjne dla pracowników szkoły, nauczycieli i uczniów, aby do każdej z tych grup użytkowników stosować osobne zasady. Dobrze zaprojektowana struktura jest podstawą efektywnego i elastycznego zarządzania kontem Google Workspace for Education.

Skonfiguruj zasady dotyczące haseł i zabezpieczenia konta administratora

Joak wspominaliśmy, newralgicznym elementem ochrony instytucji jest uwierzytelnianie użytkowników. Dlatego przygotowaliśmy dla administratorów elastyczne sposoby zarządzania uwierzytelnianiem, które pozwolą Ci odpowiednio zabezpieczyć konta użytkowników. Skonfiguruj zasady dotyczące haseł, aby wymusić na użytkownikach tworzenie silnych haseł. W stosownych przypadkach rozważ wprowadzenie obowiązkowej weryfikacji dwuetapowej, wykorzystując przy tym zalecane grupowanie w sekcji bezpiecznego logowania się. Możesz wymusić stosowanie weryfikacji dwuetapowej dla pewnej podgrupy użytkowników (dając im czas na konfigurację tej funkcji) i wdrożyć to zabezpieczenie przy użyciu różnych metod, w tym kluczy bezpieczeństwa (to najbezpieczniejsze rozwiązanie), potwierdzeń od Google (za pomocą aplikacji Google na Androida i iOS), aplikacji do generowania kodów weryfikacyjnych (takich jak Google Authenticator) i wiadomości tekstowych lub połączeń telefonicznych (choć są to najmniej bezpieczne sposoby).

Jeśli Twoja organizacja korzysta z usług dostawcy tożsamości innego niż Google, możesz skonfigurować logowanie jednokrotne za pomocą tego dostawcy tożsamości. Jeśli wolisz, na kontach innych niż konto superadministratora w dalszym ciągu możesz używać weryfikacji dwuetapowej z logowaniem jednokrotnym.

Włącz lub wyłącz usługi

Za pomocą konsoli administracyjnej Google administratorzy mogą określać, do których usług Google mają dostęp użytkownicy na swoich kontach Google Workspace for Education. Możesz kontrolować dostęp do takich usług Google jak Kalendarz, Dysk i Meet, wyłączając lub włączając usługi dla poszczególnych jednostek organizacyjnych (usługi możesz również włączać, gdy korzystasz z grup). Przed włączeniem usług dodatkowych, na przykład YouTube, Map Google czy Bloggera, możesz także przejrzeć różnice między usługami podstawowymi i dodatkowymi w Workspace. Zachęcamy administratorów do skonfigurowania dostępu do usług Google na podstawie wieku użytkownika. Warto pamiętać, że użytkownicy oznaczeni jako osoby poniżej 18 roku życia automatycznie mają ograniczony dostęp do niektórych usług Google, gdy są zalogowani na swoje konto Google Workspace for Education.

Możesz również korzystać z dostępu zależnego od kontekstu (dostępnego w Workspace for Education Standard i Plus), aby umożliwiać lub blokować dostęp do aplikacji Google, takich jak Gmail, Dysk i Kalendarz, na podstawie adresu IP urządzenia, lokalizacji geograficznej, zasad zabezpieczeń lub systemu operacyjnego. Możesz na przykład zezwolić na używanie Dysku na komputer tylko na urządzeniach należących do instytucji w określonych krajach lub regionach.

Sposoby przyznawania użytkownikom dostępu do usług

W konsoli administracyjnej Google możesz wyłączyć dostęp jednostki organizacyjnej do usług Google, na przykład do Dysku Google. Jeśli niektórzy użytkownicy w tej jednostce organizacyjnej muszą korzystać z Dysku, masz 2 możliwości:

1. Przenieś tych użytkowników do jednostki organizacyjnej, która ma włączony dostęp do Dysku.
2. Dodaj tych użytkowników do grupy dostępu i włącz dla niej Dysk. Każdy członek tej grupy będzie miał dostęp do usługi, nawet jeśli jest ona wyłączona w jego jednostce organizacyjnej.

Dysk Google jest wyłączony w jednostkach organizacyjnych 1 i 2.

Jednak **grupa użytkowników** w jednostkach organizacyjnych 1 i 2 może korzystać z Dysku Google.

Źródło: https://support.google.com/a/answer/9050643?sjid=4805599982673626852-NA

Skonfiguruj zasady udostępniania i reguły przechowywania danych

Jako administrator określasz, czy użytkownicy mogą udostępniać pliki i foldery na Dysku Google osobom spoza organizacji. Może to zapobiec niezamierzonemu lub nadmiernemu udostępnianiu danych i plików, a przez to wyciekom danych. Oddzielenie plików i dysków, tworzenie jednostek organizacyjnych i działanie zgodnie z zasadą jak najmniejszych uprawnień utrudni przestępcom poruszanie się między sieciami, nawet jeśli uzyskają dostęp do pojedynczego konta. Im mniejsze możliwości dostępu do danych i sieci ma osoba przeprowadzająca atak, tym mniejsze szkody może spowodować.

Wyłącz możliwość udostępniania plików osobom spoza organizacji dla uczniów (lub ogranicz udostępnianie tylko do zatwierdzonych domen) i ustaw opcję Narzędzie do sprawdzania dostępu na wartość „Tylko adresaci". Jeśli zezwolisz niektórym lub wszystkim użytkownikom na udostępnianie plików poza Twoją domeną, włącz ostrzeżenie w przypadku takiego udostępniania. Wyłącz też publikowanie plików w internecie i wymagaj od współpracowników zewnętrznych logowania się za pomocą konta Google.

Dodatkowo administratorzy Workspace for Education Standard i Plus mogą używać grup odbiorców i reguł zaufania, aby bardziej szczegółowo ustawiać zalecenia i ograniczenia dotyczące udostępniania. Grupy odbiorców pozwalają ustawiać domyślnych adresatów, aby nauczyciele mogli udostępniać linki np. tylko nauczycielom i innym pracownikom, a nie wszystkim użytkownikom w instytucji. Za pomocą reguł zaufania można z kolei blokować możliwość udostępniania plików starszym uczniom przez ich młodszych kolegów.

Przejrzyj zasady dotyczące dysków współdzielonych, żeby aby mieć pewność, że tylko odpowiedni użytkownicy mogą tworzyć dyski współdzielone i że użytkownicy zewnętrzni nie mają dostępu do tych dysków. Zalecamy, aby tylko administratorzy (lub pracownicy i nauczyciele) mogli tworzyć dyski współdzielone. Pamiętaj też o rygorystycznym zarządzaniu dostępem do dysków tego typu.

W miarę możliwości rozważ ograniczenie widoczności katalogu i udostępniania kontaktów. Można to zrobić przez wyłączenie udostępniania kontaktów w przypadku niektórych lub wszystkich użytkowników albo przez utworzenie katalogów niestandardowych w celu ograniczenia ich widoczności dla określonych użytkowników. Skonfiguruj zasady zapobiegania utracie danych (DLP) na Dysku i w Gmailu, aby wykrywać i blokować poufne informacje. Do ochrony typowych informacji poufnych (takich jak numer konta bankowego lub karty kredytowej) możesz wykorzystać gotowe zasady. Możesz również tworzyć własne zasady bazujące na słowach kluczowych, listach słów i wyrażeniach regularnych.

Zarządzaj ustawieniami Gmaila

Gmail należy do usług podstawowych w Google Workspace for Education, a administratorzy mają do dyspozycji wiele ustawień, które zapewniają ochronę ich instytucji i użytkowników.

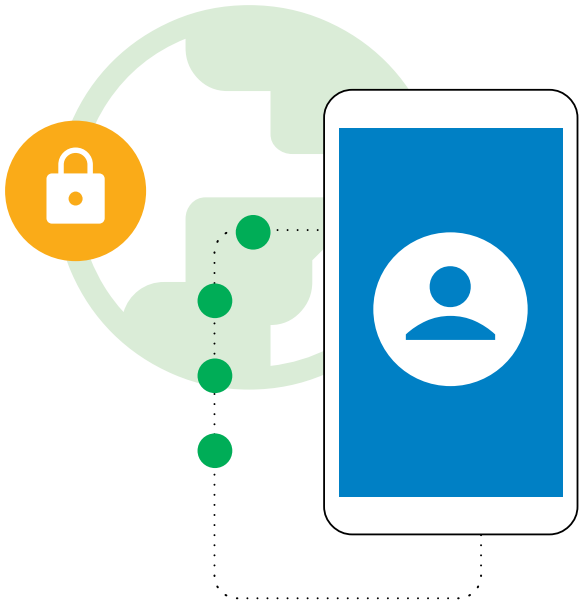
Uwierzytelnianie w Gmailu pomoże Ci zadbać o ochronę przed spamem, podszywaniem się i wyłudzaniem informacji. Dostosuj ustawienia filtrowania spamu, w tym wymaganie uwierzytelniania nadawcy dla wszystkich zatwierdzonych nadawców i wyłączenie możliwości ominięcia filtrów spamu przez nadawców wewnętrznych.

Tam, gdzie to możliwe, wyłącz dostęp POP/IMAP i włącz ulepszone skanowanie wiadomości przed dostarczeniem oraz zaawansowaną ochronę przed phishingiem i złośliwym oprogramowaniem. Jeśli zezwolisz niektórym lub wszystkim użytkownikom na wysyłanie e-maili poza domenę, możesz włączyć ostrzeżenie o odbiorcach spoza organizacji.

Użytkowników Google Workspace for Education w wersjach Standard i Plus można także chronić przed złośliwym oprogramowaniem i ransomware przez ustawienie reguł wykrywania szkodliwych załączników z wykorzystaniem bezpiecznej piaskownicy..

Aplikacje innych firm

Wykorzystaj wbudowane przepływy pracy do zatwierdzania aplikacji zewnętrznych, które uzyskują dostęp do danych na koncie przez interfejsy API. Zapobiega to nieautoryzowanemu udostępnianiu danych aplikacjom zewnętrznym, które nie są zatwierdzone do użytku szkolnego.



Raporty i monitorowanie

Jako administrator możesz wyświetlać raporty i zdarzenia z dziennika w konsoli administracyjnej Google, aby przeglądać aktywność w Twojej organizacji, w tym potencjalne zagrożenia, to, kto i kiedy loguje się w środowisku, oraz sposoby tworzenia i udostępniania treści przez użytkowników. Dzięki wykresom i tabelom możesz wyświetlać dane na poziomie domeny oraz szczegółowe dane na poziomie użytkownika. Wyświetlaj raporty i dzienniki kontrolne (w tym Centrum alertów), aby m.in. identyfikować zagrożenia, analizować wykorzystanie usług, diagnozować problemy z konfiguracją i śledzić aktywność użytkowników.

Administratorzy Google Workspace for Education Standard i Plus mają do dyspozycji **panel bezpieczeństwa**, w którym mogą wyświetlać zestawienie różnych raportów zabezpieczeń, znajdować trendy oraz porównywać dane bieżące i historyczne dotyczące na przykład udostępniania plików na Dysku, spamu, wyłudzania danych i aktywności złośliwego oprogramowania w Gmailu, podejrzanych logowań na konta użytkowników czy podejrzanej aktywności na urządzeniach. Większość dzienników dotyczących wykorzystania i aktywności oraz dzienników kontrolnych – obejmujących zdarzenia z dziennika administratora, dziennika Dysku, Meet i Google Chat – oraz raporty zabezpieczeń są dostępne przez 6 miesięcy.

Aproveite a central de segurança

Administratorzy Google Workspace for Education Plus i Standard mogą korzystać z Centrum bezpieczeństwa, które zawiera zaawansowane informacje o zabezpieczeniach i analizy, a przy tym zapewnia lepszy wgląd w problemy związane z bezpieczeństwem w domenie i pozwala je kontrolować.

Centrum bezpieczeństwa obejmuje narzędzie do analizy zagrożeń, które może pomóc administratorom identyfikować, klasyfikować i rozwiązywać problemy związane z bezpieczeństwem i prywatnością, takie jak ataki phishingowe, niewłaściwe udostępnianie plików, podejrzana aktywność użytkowników i aktywność na urządzeniach.

Google Workspace to najbezpieczniejszy na świecie chmurowy pakiet narzędzi do komunikacji i współpracy

0

aktywnie wykorzystanych luk w zabezpieczeniach oprogramowania Workspace od listopada 2021 roku*

50%

potencjalnych oszczędności na składkach ubezpieczeniowych w zakresie cyberbezpieczeństwa w przypadku korzystania z Workspace

2x mniej

Organizacje korzystające z Workspace odnotowały 2 razy mniej incydentów związanych z bezpieczeństwem niż te używające Microsoft 365

2.5x mniej

Organizacje korzystające z Workspace odnotowały prawie 2,5 raza mniej incydentów związanych z bezpieczeństwem niż te używające Microsoft Exchange

* Według danych agencji CISA to znacznie mniej niż w przypadku jakiegokolwiek innego dostawcy narzędzi biurowych na tym rynku.

Chromebooki Google dla szkół

Dzięki wbudowanym funkcjom zabezpieczeń Chromebooki to bardzo bezpieczne, skalowalne i łatwe w obsłudze komputery dla uczniów i nauczycieli. Dotychczas nie odnotowano żadnego ataku typu ransomware na żadne urządzenie z ChromeOS działające w firmach, instytucjach edukacyjnych i u klientów indywidualnych. Chromebooki pomagają chronić szkoły przed ewoluującymi zagrożeniami dzięki aktualizowanym na bieżąco funkcjom. Same aktualizacje odbywają się automatycznie w tle, użytkownicy mogą więc wrócić do pracy w ciągu kilku sekund.

Automatyczne aktualizacje systemu operacyjnego i aplikacji z wbudowaną ochroną przed złośliwym oprogramowaniem

Przestępcy nieustannie próbują wykorzystać błędy i luki w systemach operacyjnych, przeglądarkach i popularnych aplikacjach, aby instalować złośliwe oprogramowanie i kraść dane użytkowników. Z myślą o ochronie administratora i użytkowników Chromebooki domyślnie dbają o aktualność swojego systemu operacyjnego i aplikacji. Aplikacje działające w chmurze nie wymagają aktualizacji oprogramowania tak jak aplikacje lokalne, a zaprojektowany przez Google układ zabezpieczający w Chromebookach pomaga utrzymać bezpieczeństwo urządzeń i integralność systemu oraz chronić tożsamość użytkowników.

Chromebooki w instytucji będą automatycznie korzystać z najnowszych aktualizacji zabezpieczeń przed złośliwym oprogramowaniem. Uczniowie i nauczyciele są chronieni przed cyberzagrożeniami przez wbudowane funkcje zabezpieczeń, takie jak szyfrowanie danych, weryfikacja podczas uruchamiania, piaskownica i automatyczne aktualizacje.

Bezpieczne dane użytkowników

Gdy logujesz się na Chromebooku za pomocą konta Google, wszystkie Twoje dane są zapisywane w szyfrowanych plikach, dzięki czemu żaden inny użytkownik urządzenia nie może ich wyświetlić ani zalogować się w aplikacjach za pomocą Twojego konta. W ten sposób uczniowie mogą bardzo łatwo i bezpiecznie współdzielić urządzenia w klasie, a szkoły obniżyć całkowite koszty związane z zakupem i obsługą komputerów. Jeśli potrzebne są bardziej zaawansowane funkcje zabezpieczeń, licencja na Chrome Education do zarządzania urządzeniami zapewnia lepszą widoczność w tym zakresie.

Zdalne konfigurowanie zasad zabezpieczeń dla zarządzanych urządzeń użytkowników

Szkolni administratorzy mogą zdalnie konfigurować zasady dla systemu ChromeOS oraz instalować i aktualizować aplikacje za pomocą konsoli administracyjnej Google. Administrator IT potrzebuje zaledwie kliknięcia, aby zaktualizować zasady i konfiguracje setek tysięcy Chromebooków w jednej chwili.

Dzięki temu:

- uczniowie mają dostęp tylko do treści i aplikacji zatwierdzonych przez szkołę;
- wszystkie aplikacje i rozszerzenia są aktualizowane za pomocą najnowszych łatek bezpieczeństwa;
- użytkownicy nie mogą udostępniać, kopiować ani przesyłać szkolnych danych na inne urządzenia;
- możesz podejmować decyzje oparte na danych, wykorzystując przy tym spersonalizowane zalecenia Google dotyczące bezpieczeństwa, aby eliminować zagrożenia;
- w konsoli administracyjnej możesz centralnie zarządzać zasadami zabezpieczeń i zarządzania tożsamościami i dostępem, uwzględniając przy tym wszystkich użytkowników.

Oto niektóre ważne zasady, które powinni skonfigurować administratorzy.

Zasady dotyczące urządzeń

- **Tryb gościa**
  Zalecamy wyłączenie trybu gościa na urządzeniach używanych w szkole, aby uczniowie i nauczyciele musieli się logować za pomocą własnych danych logowania i nie korzystali z urządzeń anonimowo.
- **Ograniczenia logowania**
  Mmożesz uniemożliwić uczniom i nauczycielom logowanie się na szkolnych Chromebookach przy użyciu osobistych kont Gmail. Wprowadź ograniczenia, aby logowanie się na urządzeniach używanych wyłącznie przez uczniów było możliwe tylko za pomocą Twojej domeny Workspace.
- **R elatórios de usuários e dispositivos**
  Administratorzy powinni rozważyć włączenie raportów o urządzeniach i użytkownikach, co pozwoli im zbierać różne dane, na przykład na temat tego, jak często są używane Chromebooki, kto ich używa i w jakim stanie są te urządzenia.
- **Wymuszona ponowna rejestracja**
  Chromebook należący do szkoły musi pozostawać w szkole, chyba że administrator go wyrejestruje. Administratorzy powinni rozważyć włączenie wymuszonej ponownej rejestracji Chromebooków, aby urządzenie zawsze samo rejestrowało się ponownie, nawet jeśli zostanie wyczyszczone lub skradzione.

Zasady dotyczące użytkowników

- **Tryb incognito**
  Aby uczniowie mogli korzystać ze szkolnych Chromebooków, trzeba skonfigurować ich konta. Obejmuje to ograniczenie dostępnych dla nich możliwości do uwierzytelnionej przeglądarki, w której filtry treści z internetu uniemożliwią im wchodzenie na nieodpowiednie strony. Administratorzy powinni wyłączyć tryb incognito, dzięki czemu uczniowie nie będą mogli obejść filtrów treści.
- **Tryb proxy**
  Choć niektóre szkoły używają serwerów proxy do filtrowania treści z internetu, należy uniemożliwić użytkownikom samodzielne zmienianie ustawień serwera proxy.
- **Możliwość wielokrotnego logowania**
  Jeśli użytkownicy będą mogli zalogować się na dodatkowym koncie podczas używania szkolnych Chromebooków i kont Workspace, może to im umożliwić łatwe przesyłanie poufnych danych uczniów i szkoły na dodatkowe konto. Dlatego warto rozważyć zablokowanie możliwości wielokrotnego logowania.
- **Historia przeglądarki**
  W przypadku uczniów korzystne może być wyłączenie możliwości czyszczenia historii przeglądarki. Jeśli wystąpi incydent związany z bezpieczeństwem, takie logi historii przeglądania internetu mogą przydać się podczas śledztwa.

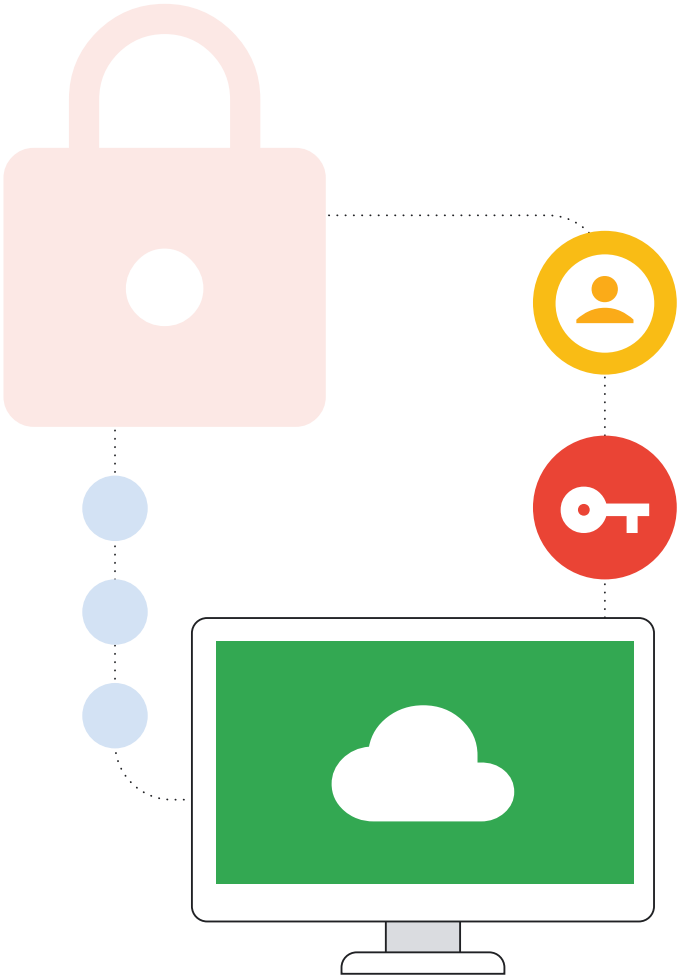
Przedstawiona lista jest dobrym punktem wyjścia pomagającym zapewnić ochronę szkolnych sieci przed najczęstszymi typami błędów, które narażają szkołę na poważne cyberincydenty. Dodatkowe zalecane zasady zabezpieczeń można znaleźć na naszej liście kontrolnej zabezpieczeń.

Zarządzanie punktami końcowymi z myślą o ich bezpiecznym używaniu w dowolnym miejscu i czasie

System zdalnego zarządzania zasadami w ChromeOS pozwala szkolnym administratorom stosować ustawienia zabezpieczeń i uruchamiać narzędzia zabezpieczające, takie jak filtrowanie treści, na urządzeniach, a nie na szkolnych serwerach sieciowych. Dzięki temu uczniowie mają do dyspozycji jednakowe zabezpieczenia podczas korzystania z Chromebooków zarówno w domu, jak i w klasie. To coraz ważniejsze, ponieważ szkoły przechodzą w stronę cyfrowych podręczników i internetowych narzędzi edukacyjnych, a uczniowie muszą zabierać komputery do domu, aby zrobić zadania domowe.

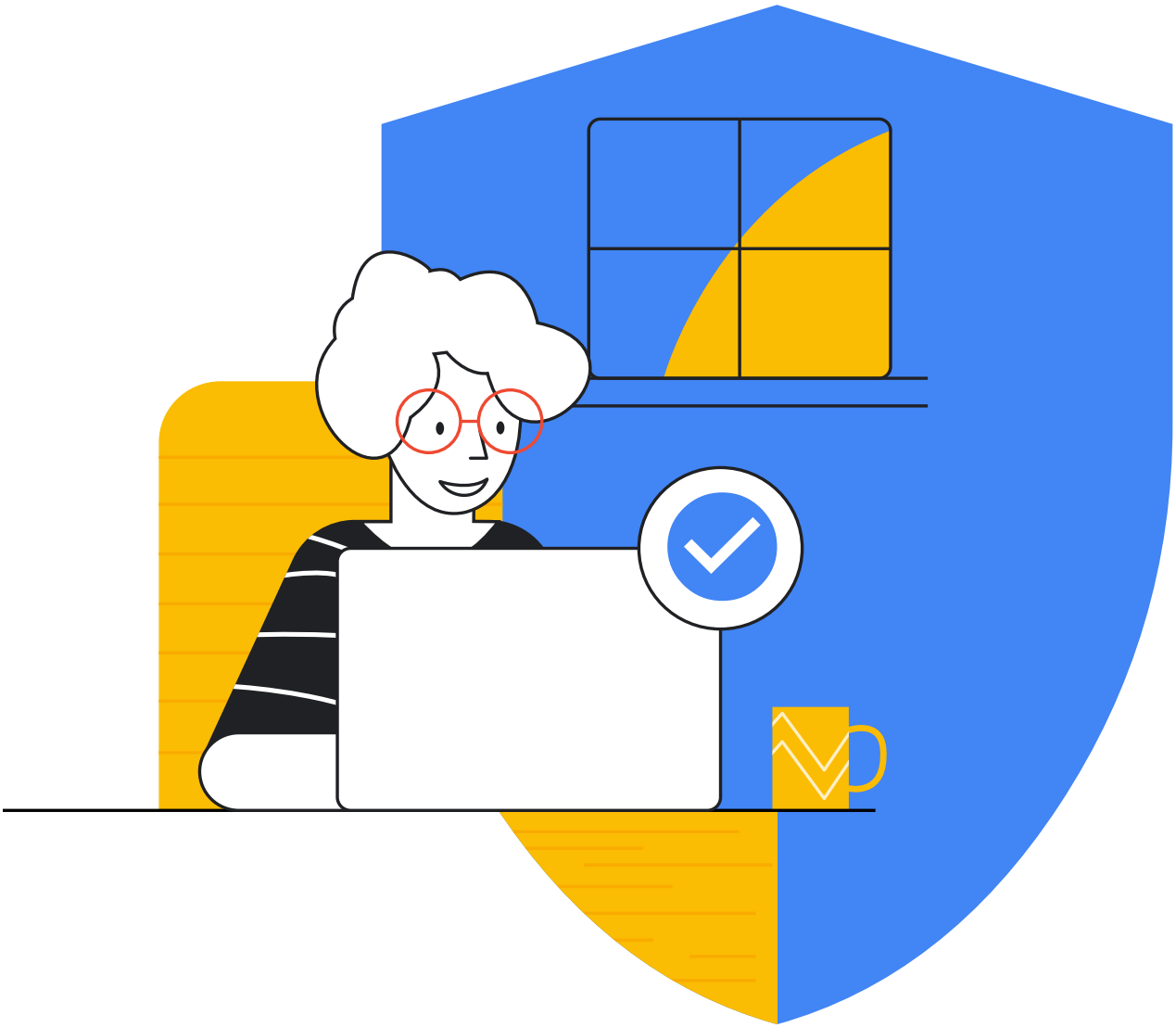
Podsumowanie

Wyzwania związane z ochroną szkół podstawowych i średnich przed cyberincydentami są złożone, warto jednak zainwestować w ochronę administratora, uczniów, nauczycieli, innych pracowników i szerszego ekosystemu online. Zagadnienia omówione w tym dokumencie to dobry początek, ale każda szkoła musi dopasować przedstawione zalecenia do swoich unikalnych potrzeb oraz zadbać o ochronę przed zmieniającymi się zagrożeniami oraz o to, aby być na bieżąco z nowymi technologiami. Ten materiał zapewnia solidne podstawy do stworzenia systemu zabezpieczeń w szkołach podstawowych i średnich. Może też być punktem wyjścia dla potencjalnych dalszych kroków i działań do wykonania. Google udostępnia też zróżnicowane materiały i szkolenia oraz oferuje wsparcie wykwalifikowanych specjalistów ds. cyberbezpieczeństwa, którzy mogą pomagać szkołom i organizacjom w realizacji zaleceń z tego przewodnika i korzystaniu z nowych technologii, takich jak sztuczna inteligencja. Produkty i usługi Google stworzone z myślą o edukacji to gotowe rozwiązania, które eliminują wiele pułapek związanych z cyberbezpieczeństwem opisanych w tym dokumencie. Z przyjemnością wesprzemy Cię w projektowaniu i wdrażaniu własnych systemów w tym zakresie.



Lista materiałów

- Google. „Narzędzia i wskazówki, które pomogą Ci zachować bezpieczeństwo w internecie". Centrum bezpieczeństwa Google, https://safety.google/security/security-tips/. Dostęp: 6 października 2022 r.
- NIST. „Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1" (Najlepsze praktyki pozwalające zwiększyć cyberbezpieczeństwo infrastruktury krytycznej, wersja 1.1). Publikacje techniczne NIST, 16 kwietnia 2018 r., https://doi.org/10.6028/NIST.CSWP.04162018. Dostęp: 6 października 2022 r.
- Microsoft. „Microsoft AccountGuard". Microsoft AccountGuard, https://www.microsoftaccountguard.com/pl-pl/. Dostęp: 6 października 2022 r.
- Google. „Program ochrony zaawansowanej". Program ochrony zaawansowanej Google, https://landing.google.com/advancedprotection. Dostęp: 6 października 2022 r.
- Google. „Centrum bezpieczeństwa Google". Centrum bezpieczeństwa Google – bezpieczeństwo w internecie, https://safety.google. Dostęp: 6 października 2022 r.
- Meta. „Meta od podstaw: Zabezpieczanie swojego konta". Zabezpieczanie swojego konta, https://www.facebook.com/gpa/resources/basics/security. Dostęp: 6 października 2022 r.
- Meta. „Facebook Protect". Facebook, https://www.facebook.com/gpa/facebook-protect. Dostęp: 6 października 2022 r.
- NIST. „SP 800-124 Rev. 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise" (SP 800-124 wersja 1: wytyczne dotyczące zarządzania bezpieczeństwem urządzeń mobilnych w firmie). Publikacje techniczne NIST, https://doi.org/10.6028/NIST.SP.800-124r1. Dostęp: 6 października 2022 r.
- Klucze: https://developers.google.com/identity/passkeys
- Raport CISA „Protecting Our Future" dotyczący cyberbezpieczeństwa w szkołach podstawowych i średnich: https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- Raport GAO: https://www.gao.gov/products/gao-20-644
- Więcej informacji o tym, jak Google for Education może pomóc Ci chronić Twoją instytucję, znajdziesz w Centrum prywatności i bezpieczeństwa Google for Education.
- Raport Zscaler na temat wyłudzania informacji



Google for Education