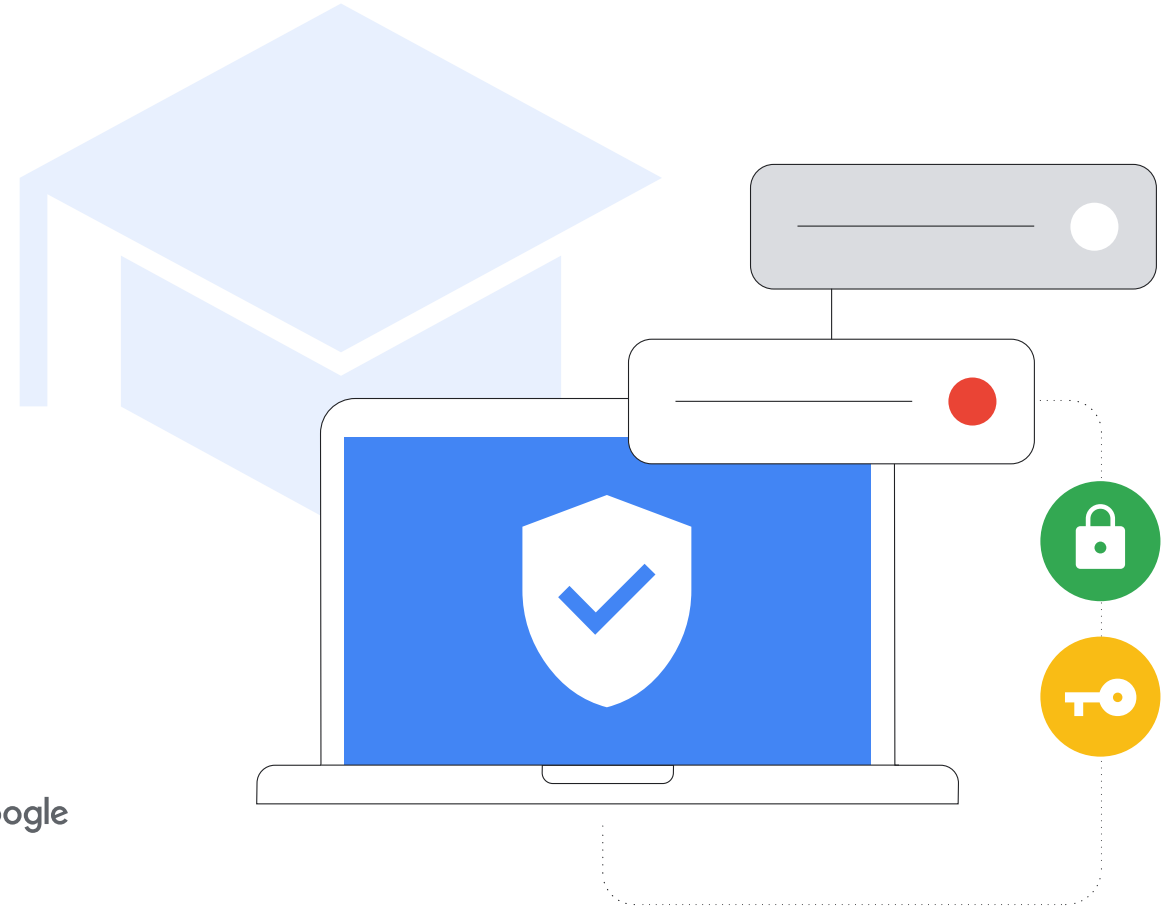
Google for Education

Handleiding cyberbeveiliging in het basis- en middelbaar onderwij

Update augustus 2023



Safer with Google

Managementsamenvatting

Zoals blijkt uit het rapport *Protecting Our Future*[1] van CISA is het belangrijk dat instellingen voor het basis- en middelbaar onderwijs investeren in cyberbeveiliging om hun leerlingen, de gezinnen van hun leerlingen, hun docenten, hun medewerkers en de school als geheel te beschermen. Dit document biedt IT-beheerders van instellingen voor het basis- en middelbaar onderwijs richtlijnen en best practices om hardware en software in te stellen en cyberbeveiliging te verbeteren. Het bevat algemene best practices en richtlijnen specifiek voor Google-producten en -services. De missie van Google is alle informatie ter wereld te ordenen en universeel toegankelijk en bruikbaar maken. Dit is een cruciale factor in het werk dat we in het Team Google for Education doen: tools maken speciaal voor lesgeven en leren. In deze handleiding delen we de lessen die we daaruit hebben geleerd.

We geven best practices voor begeleiding ingedeeld op onderwerp, waarmee we dieper ingaan op instellingen en strategieën voor risicobeperking. We leggen ook uit hoe Google cyberbeveiliging aanpakt in onze services, met name onze tools voor het onderwijs. We geven uitgebreide richtlijnen in dit document die niet specifiek zijn voor producten of services, maar we gaan ervan uit dat onze producten al superieure bescherming bieden tegen veelvoorkomende aanvallen.

Het risico

Onderwijsinstellingen zijn populaire doelen voor cyberaanvallen. Kwaadwillenden krijgen maar wat graag toegang tot de gegevensrijke omgevingen van scholen. 46% van de scholen die nog niet het slachtoffer zijn geworden van een cyberaanval denkt dat dit uiteindelijk wel gaat gebeuren, omdat ransomware-aanvallen steeds beter en moeilijker te stoppen worden. En 42% van die scholen denkt dat ransomware zo alom aanwezig is dat een aanval onvermijdelijk is. De nood voor scholen om in 2020 snel over te stappen op onderwijs op afstand droeg sterk bij aan de achterstand op het gebied van cybersecurity, waardoor scholen kwetsbaar worden voor aanvallen.

De verdediging

Je kunt deze aanvallen verminderen. Geen enkele technologie neemt het risico helemaal weg, maar het onderwijs en edtech-leveranciers kunnen samenwerken om best practices te ontwikkelen en te implementeren voor een beveiligde, allesomvattende aanpak die het risico sterk vermindert. Met de juiste voorzorgsmaatregelen en beleidsregels om gebruikers en apparaten te beveiligen en de privacy van gegevens te waarborgen, kunnen onderwijsinstellingen risico's beter beheren en aanvallen tegenhouden.

Belangrijke aanbevelingen

- **GEBRUIK BEVEILIGDE VERIFICATIEMETHODEN** om gevoelige informatie te beveiligen, e-mails, bestanden en andere content te beschermen en te voorkomen dat ongeautoriseerde gebruikers toegang hebben tot onderwijssystemen. Gebruik waar mogelijk best practices voor gebruikersverificatie, zoals sterke wachtwoorden, verificatie in 2 stappen, toegangssleutels en wachtwoordmanagers, vooral voor IT-beheerders en andere medewerkers die werken met gevoelige informatie.
- **PAS DE JUISTE BEVEILIGINGSINSTELLINGEN TOE** om je gebruikers, gegevens en omgeving te beveiligen. Google-producten zijn standaard beveiligd ontworpen, maar het is belangrijk dat beheerders hun netwerken en systemen ook goed uitrusten en instellen om ze te beveiligen. Houd scholen veilig door de principes van Zero Trust en minimale rechten. Geef gebruikers alleen toegang tot de software, gegevens, apps en systemen die ze nodig hebben om hun werk goed te kunnen uitvoeren.
- **UPDATE EN UPGRADE JE SYSTEMEN,** zodat gebruikers beveiligd zijn tegen de nieuwste bedreigingen. Gebruik moderne besturingssystemen (OS) en browsers, zorg dat gebruikers de nieuwste softwareversie (of goedgekeurde langdurige stabiele versie) hebben op al hun apparaten en stel in dat die automatisch worden geüpdatet. Je zorgt voor nog betere beveiliging door te upgraden naar een meer beveiligde oplossing, zoals Chromebooks. Er is nog nooit ransomware gevonden op een ChromeOS-apparaat.
- **GEBRUIK REALTIME MELDINGS- EN CONTROLESYSTEMEN** voor meer beveiliging en om mogelijke problemen snel te kunnen aanpakken. Je kunt de functies gebruiken die zijn ingebouwd in je primaire software voor samenwerking en communicatie, zoals Google Workspace for Education, of aparte logboek- en controlefuncties voor beveiliging implementeren. Zorg dat je een overzicht hebt van de activiteiten die worden uitgevoerd in en op de netwerken, apparaten, apps, gebruikers en gegevens van je school. Controleer inlogpogingen op accounts, gedeelde bestanden, het aantal e-mails (met name phishing- en malwarepogingen), apparaatactiviteit en veranderingen in de configuratie. Houd je meldings- en controleoplossing up-to-date om meldingen te krijgen over bedreigingen, kritieke gebeurtenissen en systeemwijzigingen.
- **TRAIN DOCENTEN, MEDEWERKERS EN LEERLINGEN,** zodat ze apparaten en software op een veilige manier gebruiken, mogelijke bedreigingen herkennen en melden en gegevens op de juiste manier delen. Zo bescherm je ze tegen enkele van de meest voorkomende aanvallen. Scholen kunnen trainingsmateriaal met hun merk maken of algemeen beschikbaar, kant- en-klaar materiaal gebruiken. Zo kunnen ze een uitgebreid pakket maken speciaal voor scholen.

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

Belangrijke opmerking: Dit document biedt richtlijnen om instellingen voor het basis- en middelbaar onderwijs beter te beveiligen, maar geen enkele richtlijn kan volledige bescherming garanderen tegen slechte actoren. Google is niet verantwoordelijk voor de implementatie of effectiviteit van de stappen die in deze richtlijn worden vermeld. Daarnaast mag niets in dit document worden gevolgd als het niet in overeenstemming is met de richtlijnen van de overheid.

Aanbevelingen specifiek voor gebruikers van Google-producten: met Google-producten als Google Workspace for Education en Chromebooks kun je de cyberbeveiliging van je school verbeteren en al deze aanbevelingen makkelijk implementeren. Samen vormen ze een allesomvattende oplossing om de privacy van gebruikers te waarborgen en je onderwijsinstelling zo goed mogelijk te beveiligen.

Deze strategieën, samen met de aanvullende richtlijnen in het volgende artikel, vormen een goede basis voor de beveiliging van instellingen voor het basis- en middelbaar onderwijs.

De aanpak van Google voor het onderwijs

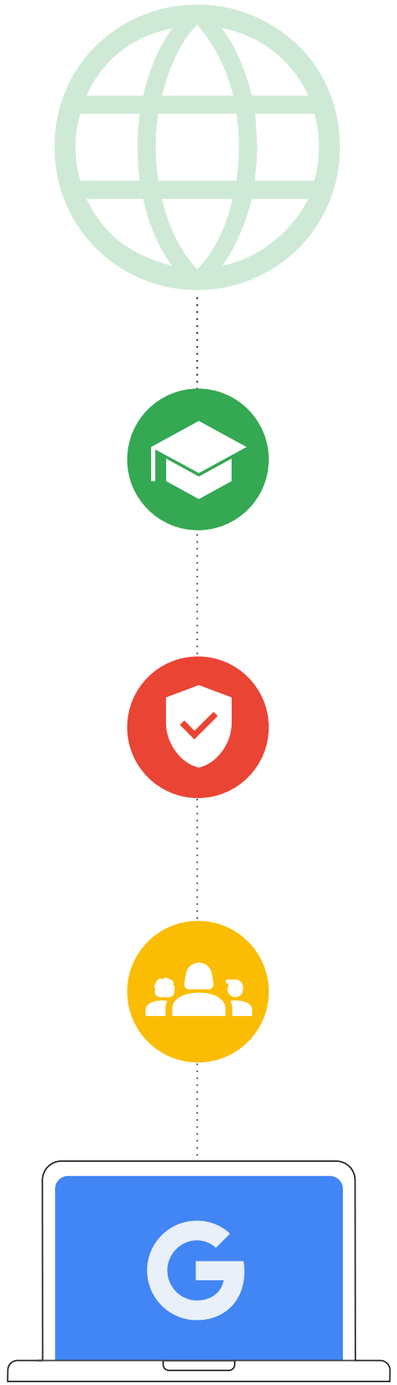
De missie van Google is alle informatie ter wereld te ordenen en universeel toegankelijk en bruikbaar maken. Dat geldt ook voor het onderwijs. Bij Team Google for Education doen we dit door tools te maken zoals Chromebooks en Google Classroom, waarmee leerlingen en docenten makkelijk en beveiligd hun eigen content kunnen maken, delen en ordenen, en toegang krijgen tot onderwijsbronnen en online tools.

Scholen verdienen het om technologie te gebruiken die beveiligd en privé is ontworpen, waar je zelf de controle over hebt en die betrouwbare content en informatie bevat. Met producten als Chromebooks en Google Workspace for Education krijgen scholen toonaangevende beveiligingsmaatregelen die de hoogste wereldwijde onderwijsstandaarden naleven. IT-beheerders krijgen volledige zichtbaarheid en makkelijke controle over hun gegevens en beveiligingsbeleid. Leerlingen kunnen zich helemaal richten op het leerproces in een beveiligde digitale omgeving met content die geschikt is voor hun leeftijd en minder spam en cyberdreigingen.

We geven prioriteit aan ingebouwde beveiligingsfuncties, de hoogste privacystandaarden en opties om proactievere beveiligingstools te gebruiken, zodat iedereen kan leren. Met ChromeOS-apparaten zorgen we dat scholen minder cyberdreigingen tegenkomen. Ze zijn de beste verdediging tegen de meestgebruikte aanval op scholen: ransomware. Er is nog nooit een ransomware-aanval geslaagd op een Chromebook.

Daarnaast is Google Workspace for Education één van de populairste en best beveiligde cloudpakketten voor communicatie en samenwerking ter wereld. Ga naar het laatste gedeelte voor meer informatie over hoe elke aanbeveling hier zorgt voor betere cyberbeveiliging.

Dit artikel bestaat uit twee gedeelten. Het eerste gedeelte bevat praktische en algemene beveiligingsrichtlijnen voor instellingen voor het basis- en middelbaar onderwijs, ongeacht de gebruikte producten. Het tweede gedeelte bevat specifieke configuratierichtlijnen voor onderwijsinstellingen die Google for Education-producten gebruiken, zoals Google Workspace for Education en Chromebooks. Beide gedeelten bevatten informatie om jou en je leerlingen online veilig te houden.



Inleiding

Instellingen voor het basis- en middelbaar onderwijs (zowel hun apparaten als netwerken) lopen veel risico op cyberaanvallen. Het is erg belangrijk dat deze onderwijsinstellingen de beste beveiligingsmaatregelen implementeren om leerlingen te beschermen en verlies van gegevens, services, resources, tijd en geld te voorkomen als resultaat van dit soort aanvallen. (Bron)

Deze handleiding is een tool om best practices voor cyberbeveiliging onder de aandacht te brengen bij schoolbeheerders en ze te vertellen welke schoolsystemen ze kunnen implementeren om hun omgeving beter te beveiligen. Door deze best practices in gebruik te nemen, kunnen instellingen voor het basis- en middelbaar onderwijs ernstige, dure cyberaanvallen op onderwijssystemen verminderen of voorkomen en leerlingen, hun gezinnen, docenten en andere medewerkers beschermen.

Cyberaanvallen op scholen komen steeds vaker voor, met steeds grotere gevolgen. Volgens het K-12 Cybersecurity Resource Center waren er tussen 2016 en 2021 in alle 50 staten van de VS meer dan 1300 openbaar bekendgemaakte cyberincidenten op onderwijsinstellingen. Onderwijsleiders moeten de gegevens en persoonlijke informatie van leerlingen, docenten en andere medewerkers, en de systemen en informatie van hun onderwijsinstelling beschermen. Dit is een uitdaging, vooral om het onderwijs altijd al moeite heeft gehad om up-to-date te blijven met cyberbeveiliging, vergeleken met andere sectoren.

Als een cyberaanval (inclusief ransomware, phishing en malware) slaagt, kan dit leiden tot grootschalige gegevenslekken van persoonlijk identificeerbare informatie (PII), dure uitbetalingen (de gemiddelde uitbetaling bij ransomware is sinds 2020 5 keer zoveel geworden, namelijk $ 812.260) en langdurige verstoringen van lessen en andere taken op school. Onlangs slaagde een ransomware-aanval erin een heel schoolsysteem te blokkeren. Dit leidde tot problemen in de hele onderwijscommunity, omdat leerlingen dagenlang niet naar school toe konden. Instellingen voor het basis- en middelbaar onderwijs hebben vaak beperkte (financiële) middelen. Ze blijven dus het doelwit van dit soort aanvallen, tenzij ze investeren in verbeterde cyberbeveiliging.

Cyberbeveiliging werkt het best door communicatie, samenwerking en partnerschap. Dit document is gemaakt aan de hand van de beveiligingstips van Google, het Cybersecurity Framework van de National Institute for Standards and Technology (NIST) en de toolkit en aanbevelingen voor cyberbeveiliging op instellingen voor het basis- en middelbaar onderwijs van CISA uit 2023, allemaal bekende bronnen van richtlijnen voor cyberbeveiliging. In dit document vind je algemene stappen die IT-beheerders kunnen uitvoeren, enkele best practices die we bij Google zelf gebruiken en begeleiding voor het gebruik van onze producten. We verwijzen ook naar de beveiligingstips en -services van andere bedrijven. We raden beheerders aan alle beveiligingsrichtlijnen van de relevante bedrijven door te nemen en de nieuwste richtlijnen in gebruik te nemen, omdat bedrijven zelf hun producten het beste kunnen omschrijven en kunnen laten weten welke wijzigingen ze daarin hebben aangebracht.

Voordat je de aanbevelingen hieronder uitvoert, raden we je aan ook na te denken over het volgende:

Overwegingen

1. **Leerlingen beschermen.**
De behoeften van scholen verschillen. Op sommige scholen zijn misschien meer stappen nodig om leerlingen en medewerkers te beveiligen. Veel edtech-tools bevatten functies om leerlingen op leeftijd gebaseerde toegang te geven, zoals ongepaste content blokkeren of zorgen dat hun locatie en contactgegevens privé blijven.

2. **De soorten gegevens die je opslaat.**
Als je gevoelige gegevens opslaat, raden we je aan die te versleutelen of op te slaan op een aparte locatie.

3. **Welke soorten apparaten je gebruikt en je implementatiemodel.**
Zorg dat apparaten en de apps daarop automatisch worden geüpdatet om ze zo goed mogelijk te beveiligen. Versleutel ook de gegevens en isoleer accounts, zodat gebruikers alleen toegang hebben tot hun eigen informatie.

4. **Wat het beleid is van je school, district of regio.**
Misschien heeft je school een beleid specifiek voor het gebruik van technologie. Zorg dat alles wat je doet op het gebied van beveiliging in overeenstemming is met dit beleid.

Elke dag houdt Gmail
100 miljoen
phishingpogingen tegen.

Elke week identificeert Google
300,000
onveilige websites.

Elke dag krijgen
74 miljoen
gebruikers hulp van Google Wachtwoordmanager.

Elk jaar verbeteren
700 miljoen
mensen hun beveiliging met de Beveiligingscheck.

Gebruik beveiligde verificatie

Beveiligde verificatie moet de hoogste prioriteit hebben op scholen en andere onderwijsinstellingen. In het 4e kwartaal van 2022 bestond 48% van de gehackte accounts uit accounts met zwakke of helemaal geen inloggegevens. Door een paar belangrijke aanbevelingen op te volgen, weet je zeker dat gebruikers zijn wie ze zeggen te zijn en zorg je dat gebruikers alleen toegang hebben tot informatie die past bij hun rol.

We raden IT-beheerders aan het gebruik van verificatie in 2 stappen af te dwingen en waar mogelijk wachtwoordloze verificatie (zoals toegangssleutels) te gebruiken, vooral als iemand op afstand toegang heeft tot de systemen van de onderwijsinstelling. Met verificatie in 2 stappen voeg je een extra beveiligingslaag toe aan je online accounts, zodat hackers er veel minder makkelijk toegang toe krijgen.

Scholen in het basis- en middelbaar onderwijs gebruiken veel verschillende soorten apparaten en implementatiemodellen en niet iedereen is even goed met technologie. Account- en apparaatbeveiliging verschilt per gebruikersrol en -type aan de hand van bepaalde best practices: IT-beheerders, docenten en andere medewerkers, oudere leerlingen die ieder een eigen apparaat krijgen en jongere leerlingen die gedeelde apparaten gebruiken. Hieronder geven we specifieke aanbevelingen voor elke groep.

Er zijn verschillende verificatiemethoden die je kunt gebruiken in de meeste situaties:

- **Sterke wachtwoorden:**
  Stel in dat gebruikers bij de eerste keer inloggen een wachtwoord moeten instellen en dwing een minimumlengte en vereisten voor complexiteit af. Wachtwoordzinnen zijn nog beter, omdat ze langer zijn en meer en complexere tekens gebruiken. Vraag gebruikers niet om regelmatig hun wachtwoord te wijzigen, omdat ze dan makkelijkere wachtwoorden gebruiken of slechts kleine wijzigingen aanbrengen (zoals één teken veranderen).
- **Verificatie in 2 stappen:**
  Met verificatie in 2 stappen bescherm je accounts met een tweede stap. Dit is vaak iets wat de gebruiker bij zich heeft, zoals een beveiligingssleutel of een app op een mobiele telefoon die een eenmalige verificatiecode maakt. Alle vormen van verificatie in 2 stappen maken accounts veiliger, maar we raden beheerders af verificatiecodes via tekstbericht of telefoon toe te staan. Deze manier is namelijk kwetsbaarder voor op telefoonnummers gebaseerde aanvallen.
- **Wachtwoordloze verificatie:**
  Toegangssleutels zijn een veiliger en makkelijker alternatief voor wachtwoorden. Gebruikers kunnen inloggen bij apps en websites met een pincode, patroon, biometrische sensor (zoals een vingerafdruk of gezichtsherkenning) of door te tikken op een beveiligingssleutel. Zo hoeven ze geen wachtwoorden te onthouden en te beheren. Wachtwoordsleutels zijn niet geschikt voor elke situatie op scholen, maar ze worden steeds vaker gebruikt in plaats van traditionele verificatievormen en ze zorgen dat gebruikers veiliger en sneller kunnen inloggen. Ze beschermen gebruikers tegen phishing-aanvallen, omdat ze alleen werken voor hun geregistreerde websites en apps.
- **Single Sign-On (SSO):**
  Met SSO hebben gebruikers na één keer inloggen toegang tot meerdere apps en websites. Als gebruikers maar één set inloggegevens hoeven te onthouden, schrijven ze die minder snel op. En als scholen niet meerdere sets inloggegevens hoeven te beheren voor gebruikers, besparen ze geld aan IT-support en helpdesks. SSO-ondersteuning is ingebouwd in Google Workspace for Education. Gebruikers kunnen dus met de inloggegevens van hun Google-account inloggen bij apps van derden of met de inloggegevens van een andere provider inloggen op hun Google-account.
- **Wachtwoordmanagers:**
  M et wachtwoordmanagers kunnen gebruikers sterke, unieke wachtwoorden maken voor alle accounts en services die ze op school en op het werk gebruiken (als ze geen SSO gebruiken). Je kunt er niet mee inloggen op het besturingssysteem van een apparaat, maar je kunt er wachtwoorden mee beheren nadat je bent ingelogd. Google-gebruikers kunnen Wachtwoordmanager gebruiken in Chrome op elk platform, inclusief ChromeOS en Android.

Verschillende groepen hebben baat bij bepaalde subsets of combinaties van deze verificatiemethoden, afhankelijk van hun rol in de onderwijsinstelling, tot welke systemen en gegevens ze toegang hebben en hun leeftijd.

IT-beheerders op school

IT-Beheerders beheren de systemen en veel van de gegevens van scholen in het basis- en middelbaar onderwijs. Het belangrijkste in dit hele systeem (van infrastructuur tot accountgegevens tot apparaten die worden beheerd door de onderwijsinstelling) is het beveiligen van de accounts. Daarom raden we IT-beheerders aan de beste verificatiemethoden te gebruiken, zoals sterke wachtwoorden, een krachtige wachtwoordmanager en verificatie in 2 stappen. Met al deze methoden voeg je een beveiligingslaag toe. Als je ze allemaal samen gebruikt, heb je de beste beveiliging voor je beheerdersaccount en zakelijke services.

- Beheerders moeten een fysieke beveiligingssleutel of een cryptografisch beveiligde methode voor verificatie in 2 stappen gebruiken waarvoor een veilig apparaat en prompts nodig zijn. Hiervoor kan bijvoorbeeld een service als Google Authenticator worden gebruikt of een andere app die eenmalige verificatiecodes maakt. Chromebooks van na 2019 met een TPM-chip hebben een aan/uit-knop die kan worden gebruikt voor verificatie in 2 stappen.
- We raden IT-beheerders ook aan een vertrouwde wachtwoordmanager te gebruiken die verificatie in 2 stappen ondersteunt om hun wachtwoord op te slaan voor verschillende services.

Docenten en andere medewerkers die een apparaat van de school gebruiken

Net als IT-beheerders hebben docenten en andere medewerkers toegang tot gevoelige gegevens. Maar ze hebben geen controle over de digitale infrastructuur en zijn niet altijd even goed met technologie.

- Geef docenten en andere medewerkers met Chromebooks de optie om (waar dit juridisch is toegestaan) in te loggen met biometrische verificatie, zoals hun vingerafdruk.
- We raden IT-beheerders aan het gebruik van verificatie in 2 stappen af te dwingen en waar mogelijk wachtwoordloze verificatie te gebruiken, vooral als iemand op afstand toegang heeft tot de systemen van de onderwijsinstelling.

Oudere leerlingen die een apparaat van de school gebruiken (meestal vanaf groep 7)

Oudere leerlingen weten meestal al redelijk goed hoe ze zichzelf moeten beschermen en kunnen betere verificatiemethoden gebruiken die passen bij de soorten services die ze veelal gebruiken. Geef ze alleen toegang tot hun eigen account en informatie die met ze is gedeeld.

- Geef leerlingen met een Chromebook de optie een apparaatspecifieke pincode in te stellen om sneller te kunnen inloggen op dat apparaat. Biometrische opties zijn in veel schoolomgevingen niet geschikt of haalbaar.
- Help leerlingen een uniek wachtwoord te maken dat geen persoonlijke informatie bevat (zoals hun naam, klas of geboortedatum). Leer leerlingen hoe ze met wachtwoordzinnen een complexer wachtwoord kunnen maken dat ze zelf makkelijker kunnen onthouden.

Jongere leerlingen die gedeelde apparaten gebruiken (meestal groep 1-6)

De jongste leerlingen moeten nog leren hoe ze technologie gebruiken in het onderwijs. Voor deze leerlingen zijn makkelijke verificatiemethoden het beste, waarmee ze toegang hebben tot beperkte services en gegevens.

- Scholen die voor de jongste leerlingen alternatieven van derden gebruiken voor een wachtwoord, zoals inloggen met een QR-code of afbeelding, en scholen die helemaal geen wachtwoorden gebruiken, moeten beveiligingsmaatregelen instellen, omdat ze meer risico lopen. We raden beheerders aan het wachtwoord van leerlingen te wijzigen en de code te updaten als leerlingen die vergeten zijn of als anderen er toegang toe hebben gekregen.
- We raden scholen aan zowel leerlingen als ouders te leren dat het belangrijk is hun wachtwoord geheim te houden en alternatieve inloggegevens, zoals QR-codes, veilig op te slaan.
- Voor schoolapparaten zoals tablets kun je een apparaatspecifieke pincode gebruiken als alternatieve en veilige verificatiemethode.

Pas de juiste beveiligingsinstellingen toe

Schoolapparaten en -netwerken zijn een goed zichtbaar, waardevol doelwit voor aanvallers over de hele wereld. Ze moeten dus de beste beveiligingsmaatregelen implementeren om verlies van services, resources, tijd en geld te voorkomen. Systeembeheerders moeten effectieve en geschikte beveiligingsfuncties implementeren die beschikbaar zijn in de producten die hun onderwijsinstelling gebruikt, maar ze moeten er ook voor zorgen dat de systemen gebruiksvriendelijk blijven voor docenten, andere medewerkers en leerlingen. Beheerders moeten belangrijke beveiligings- en privacyopties zo instellen dat individuele gebruikers die niet kunnen uitzetten of aanpassen. Voor andere instellingen moeten ze beschermende standaardwaarden opgeven.

Scholen moeten de beste beveiligingsmaatregelen implementeren om verlies van services, resources, tijd en geld te voorkomen. In het laatste gedeelte vind je onze suggesties voor apparaatbeleid voor Chromebooks.

Zorg als laatste voor minimale gegevensverwerking door de persoonlijke informatie van individuele gebruikers alleen waar absoluut nodig te verzamelen, te gebruiken en vrij te geven. Doe dit alleen als het nodig is om de service te leveren of in andere situaties waar dit noodzakelijk is.

Apps en updates

Zorg dat je gebruikers zo min mogelijk apps kunnen installeren, omdat elke app op een apparaat een mogelijke aanvalsmethode is. Gebruik waar mogelijk apps van vertrouwde bronnen. Vraag gebruikers bijvoorbeeld te checken of een app in de Google Play Store een verificatiebadge heeft, zodat ze zeker de officiële apps downloaden die zijn beoordeeld op hun veiligheid. Aanpassingen aan de OS of hardware (jailbreaking of rooting) leiden tot grote beveiligingsrisico's. Dit raden we dus af.

Toegang en zichtbaarheid

Beheerders moeten zorgen dat gebruikers alleen toegang hebben tot de gegevens, software, services en systemen die ze nodig hebben om hun taken te kunnen uitvoeren of goed kunnen leren. Zo voorkom je dat ze onbedoeld toegang krijgen tot de verkeerde items en kun je volgen wie toegang heeft tot welke resources. Wees extra voorzichtig met gevoelige gegevens, zoals PII van gebruikers en systemen (zoals voor HR, salaris, beoordelingen, beveiliging en configuratie) door te controleren welke gebruikers toegang hebben tot de gegevens en in welke situaties. Beperk de toegang tot apparaten die eigendom zijn van de school en stel in dat alleen specifieke medewerkers toegang hebben.

Check het beleid voor gegevens delen in samenwerkingstools om te voorkomen dat onbevoegden toegang hebben en dat bestanden met te veel mensen worden gedeeld. Beperk of blokkeer delen buiten je omgeving (vooral voor leerlingen) en stel beleid in waarmee je het delen van gevoelige content kunt controleren.

Verlies of diefstal van apparaten

Als je een apparaat kwijtraakt, betekent dat niet dat de gegevens ook verloren zijn. We raden beheerders aan een standaardplan te maken om ervoor te zorgen dat ze toegang blijven houden tot informatie en documenten voor als een apparaat wordt verloren of gestolen. Ze kunnen bijvoorbeeld instellen dat gebruikers documenten opslaan in de cloud. Download en print back-upcodes voor processen voor verificatie in 2 stappen om te zorgen dat gebruikers toegang blijven houden tot hun account.

Als een gebruiker meldt dat een apparaat is verloren of gestolen, moet je het indien mogelijk op afstand vergrendelen en zorgen dat gekoppelde accounts worden vergrendeld of gemarkeerd, zodat mensen er geen ongeautoriseerde toegang mee krijgen. Als gebruikers een Chromebook verliezen, kun je die wissen op afstand. Google Workspace for Education-accounts kun je controleren op verdachte activiteit of die opschorten (vergrendelen) als dit nodig is.

Geavanceerde beveiliging voor gebruikers die veel risico lopen

Voor gebruikers die toegang hebben tot veel gegevens en gevoelige informatie (zoals Google Workspace for Education-beheerders) heeft Google het programma Geavanceerde beveiliging (Advanced Protection Program, APP) ontwikkeld. Met het APP krijgen gebruikers extra bescherming tegen gerichte aanvallen, zoals phishingpogingen, schadelijke downloads en wachtwoordlekken. Het APP is speciaal gemaakt om gerichte online aanvallen op Google-accounts tegen te houden. Het gebruikt automatisch sterke verificatie en beveiligingssleutels en voorkomt dat externen toegang hebben tot accountgegevens. Andere aanbieders van online accounts bieden ook sterke accountbeveiliging voor gebruikers die veel risico lopen. We raden beheerders en andere medewerkers aan die altijd te gebruiken als ze toegang hebben tot persoonlijke informatie of technologiesystemen.

Update en upgrade je systemen

Eén van de belangrijkste dingen die je kunt doen om jezelf te beschermen is het besturingssysteem en de apps op je apparaat geüpdatet houden. Dit is nog belangrijker voor instellingen voor het basis- en middelbaar onderwijs, omdat die zo'n groot onderdeel zijn van het onderwijs en het dagelijks leven van kinderen. De meeste malwareaanvallen in het onderwijs en andere branches die veel risico lopen, vinden plaats in Windows. Enkele voorbeelden zijn SolarWinds, de ransomware-aanval op het Los Angeles Unified School District, de hack van het Little Rock School District, het gegevenslek van Microsoft Exchange Server, de ransomware-aanval op het Albuquerque School District en de recente inbreuk bij overheidsinstellingen via Microsoft. Ook hier kunnen cloudproducten en -services het beheerders makkelijker maken door het risico op aanvallen te verkleinen en te zorgen dat systemen en apps automatisch up-to-date blijven.

Upgrade naar een modern besturingssysteem en houd het up-to-date

De nieuwste versie van besturingssystemen (OS) heeft meestal nieuwe beveiligingsfuncties om je te beschermen tegen bekende aanvalsmethoden. Zet de functie voor automatisch updaten aan in het OS van het apparaat. Als dat niet mogelijk is, download je minstens één keer per maand patches en updates van een betrouwbare leverancier. Chromebooks draaien op ChromeOS en krijgen dus regelmatig automatische updates met de nieuwste beveiligingspatches. Zo krijg je snel de nieuwste beveiligingsinnovaties.

Chromebooks verifiëren de integriteit van het alleen-lezen besturingssysteem voordat het apparaat wordt opgestart. Ze versleutelen ook alle gegevens die je opslaat op het apparaat, waardoor onbevoegden er geen toegang toe hebben. Ook voeren ze elke webpagina en app in een aparte sandbox uit, dus als een website of app is geïnfecteerd met malware, kan die zich niet verspreiden naar de rest van het apparaat.

Als je school niet wil overstappen op Chromebooks, kun je ChromeOS Flex gebruiken, een versie van ChromeOS waarmee je de apparaten van je school kunt moderniseren. ChromeOS Flex geeft iedereen een uniforme, moderne omgeving voor lesgeven en leren met proactieve, ingebouwde beveiliging en beheermogelijkheden in de cloud. Flex biedt geautomatiseerde bescherming en blokkeert schadelijke uitvoerbare bestanden en apps zonder dat je je bestaande hardware hoeft te vervangen.

Upgrade naar een moderne browser en houd die up-to-date

Het is belangrijk dat je browser ook geüpdatet en beveiligd is. Moderne browsers bevatten geavanceerdere beveiligingsfuncties. Beheerders kunnen instellen dat gebruikers worden gevraagd die aan te zetten, of instellen dat de functies standaard aanstaan op de computers van de onderwijsinstelling. Zo houd je gevoelige informatie privé als die wordt verstuurd over het internet. Houd de browser up-to-date. Of je nu werkt, leert of andere online activiteiten uitvoert, een geüpdatete, moderne browser zorgt voor het volgende:

- **Krachtige beveiliging,** zoals site-isolatie en Safe Browsing, om te voorkomen dat gebruikers per ongeluk naar gevaarlijke websites gaan.
- **Automatische updates,** zodat de browser snel beveiligingsupdates krijgt.
- **Een veilige verbinding.** Moderne browsers gebruiken meestal Transport Layer Security (TLS). Gebruikers kunnen naast de URL klikken om te checken of de verbinding is gemarkeerd als veilig.

Chrome is gemaakt met beveiliging als uitgangspunt en beveiligingsfuncties als Safe Browsing staan standaard aan. Chrome heeft ook een geïntegreerde Wachtwoordmanager die wachtwoorden automatisch kan invullen als je browset op het web. Zo kun je makkelijk sterke wachtwoorden gebruiken.

Gebruik realtime meldings- en controlesystemen

Met realtime meldings- en controlesystemen kunnen scholen bedreigingen snel herkennen en aanpakken, voordat die schade veroorzaken. Zorg dat je op de achtergrond beveiligingstools uitvoert die beveiligingsgebeurtenissen vanuit je hele systeem verzamelen en vastleggen. AI-tools zijn heel goed in het doorspitten van de grote hoeveelheid verzamelde gegevens en daarin afwijkingen en patronen vinden. Zo kun je bedreigingen sneller en makkelijker vinden en kwetsbaarheden aanpakken. Hiermee kun je verschillende prioriteitsniveaus geven aan de activiteiten die de IT-beheerders of andere medewerkers moeten controleren.

Scholen kunnen de meldings- en controlefuncties gebruiken die zijn ingebouwd in hun primaire samenwerkings- en communicatiesoftware, zoals Google Workspace for Education, of aparte Security Information and Event Management-oplossingen (SIEM) implementeren.

Met realtime meldings- en controlesystemen kun je verschillende activiteiten volgen voor de netwerken, apparaten, apps, gebruikers en gegevens van de school, zoals inlogpogingen van gebruikers, toegang tot bestanden, mogelijke hackpogingen, pogingen tot diefstal van gegevens (en of die geslaagd zijn) en beheerdersactiviteiten.

Als het systeem verdachte activiteit vindt, kan het een melding sturen naar de IT-medewerkers van de school. Die kunnen het probleem dan onderzoeken en oplossen.

Met meldings- en controletools krijg je ook meer inzicht in de bedreigingen waarmee je school wordt geconfronteerd. Door de gegevens uit deze realtime systemen te analyseren, kunnen beheerders trends en patronen in kaart brengen waarmee ze hun school beter kunnen beschermen.

Dit zijn enkele best practices voor het gebruik van meldings- en controlesystemen (inclusief SIEM).

1. **Bepaal je beveiligingsdoelen**
   Breng in kaart welke informatie en systemen het meest kritiek zijn op de school en welke bedreigingen daarin de meeste schade aanrichten. Bepaal dan welke gegevens je moet verzamelen om te controleren op die bedreigingen.

2. **Verzamel de juiste gegevens en zorg voor de juiste configuraties**
   Zorg dat je de juiste gegevens verzamelt en apps zo instelt dat de meest relevante beveiligingsdoelen worden gehaald. Denk aan gegevens van firewalls, contentfilters, intrusion detection systems, webservers en andere beveiligingsapparaten, naast communicatie- en samenwerkingssoftware, leerlinginformatiesystemen en leerbeheersystemen.

3. **Onderzoek meldingen en kom in actie**
   Als je een melding krijgt van je controlesysteem, moet je het probleem onderzoeken en de juiste actie uitvoeren. Hiervoor moet je misschien meerdere teams samenbrengen om de bron van de melding te onderzoeken, bepalen of het vals positief is of stappen uitvoeren om het probleem op te lossen. Denk aan accounts opschorten, gebruikerswachtwoorden resetten, e-mails in quarantaine plaatsen of verwijderen, bestandsrechten wijzigen of apparaten wissen.

Train leerlingen, docenten en andere medewerkers

We raden instellingen voor het basis- en middelbaar onderwijs aan te zorgen dat de mensen op hun school zich bewust zijn van de beveiligingsmaatregelen en ze bepaalde gewoontes aan te leren. Dit kan door middel van campagnes en partnerschappen. Als je leerlingen, docenten en andere medewerkers leert hoe belangrijk beveiliging is, beschermen ze zichzelf online en voorkom je ernstige problemen met de cyberbeveiliging. Leer ze hoe ze de producten en services op school moeten gebruiken, hoe ze bedreigingen zoals phishingmails kunnen herkennen en melden, en (het belangrijkste) wat ze kunnen doen om aanvallen te voorkomen. We raden scholen aan te zorgen dat de mensen op hun school zich bewust zijn van de beveiligingsmaatregelen en ze bepaalde gewoontes aan te leren. Dit kan door middel van campagnes en partnerschappen.

Apparaten en software veilig gebruiken

Beheerders kunnen samenwerken met docenten en experts om lesprogramma's over cyberbeveiliging te ontwikkelen voor alle leeftijden. Zo leren leerlingen hoe ze apparaten, software en systemen veilig gebruiken. Als je trainingsmateriaal maakt met het logo van de school erop kun je de aanbevelingen in context plaatsen voor docenten en leerlingen. Je kunt ook kant-en-klaar materiaal gebruiken en aanpassen aan je behoeften, zoals van De InternetHelden, het materiaal dat beschikbaar is op Safety.Google en de Khan Academy. Met deze programma's leren je gebruikers het internet overal veilig te gebruiken, of ze nu op school zijn of ergens anders.

Bedreigingen herkennen

Leerlingen, docenten en andere medewerkers leren hoe ze bedreigingen kunnen herkennen, is een belangrijk onderdeel om ze veilig te houden. Het is belangrijk dat je kinderen leert hoe ze kunnen herkennen of iets een bedreiging is, omdat kinderen meestal niet weten hoe ze kunnen bepalen of iets legitiem is. Er zijn verschillende soorten bedreigingen die ze moeten kunnen herkennen. Ook moeten ze weten hoe ze bedreigingen kunnen melden. Beheerders moeten zich richten op de onderwerpen waarmee ze denken het meeste rendement op investering te kunnen behalen. Trainingen moeten gebruikers niet alleen leren om bedreigingen te herkennen, maar ook om actie te ondernemen. Enkele veelvoorkomende bedreigingen die gebruikers moeten herkennen zijn ransomware, phishing, social engineering, malware en scams. Maar als bepaalde bedreigingen vaker voorkomen op jouw school, is het belangrijk dat je je gebruikers daarover leert.

Gegevens en bestanden veilig delen

Train docenten en andere medewerkers hoe ze bestanden en gegevens op de juiste manier delen en hoe ze ongepaste verzoeken om gegevens via e-mail kunnen herkennen. Ze moeten vooral zorgen dat ze gevoelige persoonlijke informatie alleen delen als dat echt nodig is en gegevens extra beschermen, bijvoorbeeld door ze nooit te delen via e-mail of met externen. We raden je aan functies voor gegevensverlies voorkomen te gebruiken (ingebouwd in ChromeOS en Workspace for Education), waarmee je kunt instellen dat eindgebruikers een waarschuwing krijgen als ze bestanden met gevoelige gegevens (zoals burgerservicenummers) delen of gevoelige content kopiëren en plakken buiten het domein. Je kunt ook instellen dat dit helemaal niet mogelijk is voor gebruikers.

De aanpak van Google in actie: apparaten en services voor het onderwijs

Softwareprocurement is één van de beste manieren waarmee scholen zichzelf kunnen beschermen. Software moet goed gemaakt en zo ontworpen zijn dat er zo min mogelijk risico is op kwetsbaarheden, met beveiliging ingebouwd in elke laag. Door te vereisen dat scholen beveiligde software kopen of software van bedrijven die bewezen goed beveiligd zijn, kun je het risico op cyberdreigingen significant verminderen. Bij Google hebben we bijvoorbeeld ChromeOS beter bestand gemaakt tegen bedreigingen. Ook blijven we proactievere, intelligentere oplossingen implementeren die de kracht van onze machine learning, cloud en identiteitsexpertise benutten.

Google ontwikkelt producten die de privacy van leerlingen en docenten beschermen en onderwijsinstellingen de beste beveiliging in de branche bieden. Je kunt erop vertrouwen dat Google for Education-producten en -services gebruikers, apparaten en gegevens continu beschermen tegen steeds complexere dreigingen. In dit gedeelte vinden IT-beheerders van scholen informatie over beveiligingsaanbevelingen bij het gebruik van Google for Education-producten.

Google Workspace for Education

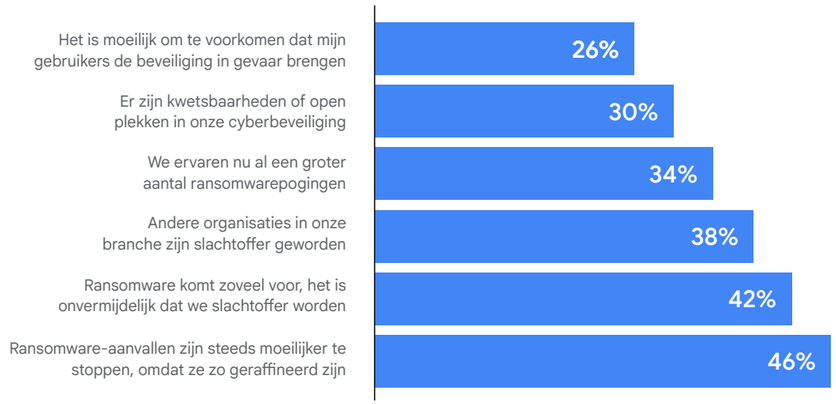
Google Workspace for Education is een reeks Google-tools en -services die speciaal zijn gemaakt voor scholen. Ze zorgen dat mensen kunnen samenwerken, dat docenten goed kunnen lesgeven en dat leren veilig blijft. Google for Education-producten en -services beschermen gebruikers, apparaten en gegevens continu tegen steeds complexere dreigingen. Ze hebben tools als meldings- en beveiligingscentrums, een vault voor eDiscovery, identiteits- en toegangsbeheer en Gegevensverlies voorkomen.

We hebben nuttig materiaal verzameld voor als je net aan de slag gaat met Google Workspace for Education. Met veel van dit materiaal kun je Google Workspace instellen volgens de aanbevelingen in deze handleiding. Ga voor hulp om aan de slag te gaan met Google Workspace for Education naar de Snelstartgids voor IT-installatie.

Beveiligingschecklists

Check de beveiligingschecklists voor instructies om de beveiliging en privacy van je onderwijsinstelling te verbeteren. Scholen met Google Workspace for Education Standard en Plus kunnen ook de configuratie van hun instellingen in de Beheerdersconsole checken op de pagina Beveiligingsstatus. Hier staat bijvoorbeeld de status van instellingen als automatisch doorsturen van e-mails, apparaatversleuteling en instellingen voor delen in Drive. Indien nodig kun je de instellingen van je domein aanpassen op basis van algemene beveiligingsrichtlijnen en praktische tips, terwijl je ook zorgt dat deze voldoen aan de zakelijke behoeften en het beleid voor risicobeheer van je organisatie.

Waarom het onderwijs verwacht slachtoffer te worden



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

Dit zijn een paar andere nuttige tips waarmee je alles haalt uit de beschermingsmaatregelen die zijn ingebouwd in Google Workspace for Education:

Stel organisatie-eenheden (OE's) in

NNiet alle gebruikers in je Google Workspace for Education-account moeten dezelfde instellingen hebben. Organisatie-eenheden zijn groepen gebruikers die je andere services, instellingen en rechten kunt geven. Je kunt bijvoorbeeld instellen dat docenten en andere medewerkers verificatie in 2 stappen gebruiken en dat jongere leerlingen een andere verificatiemethode gebruiken. Stel aparte organisatie-eenheden in voor docenten, andere medewerkers en leerlingen om beleid apart toe te passen op elke groep gebruikers. Een goed ontworpen structuur is essentieel om je Google Workspace for Education-account efficiënt en flexibel te beheren.

Stel wachtwoordbeleid en beschermingen voor beheerdersaccounts in

Zoals we al eerder hebben aangegeven, is gebruikersverificatie erg belangrijk om je onderwijsinstelling te beveiligen. Daarom hebben we flexibele manieren ingesteld om verificatie te beheren, zodat beheerders kunnen zorgen dat gebruikers gebruiksvriendelijke, goed beveiligde beschermingsmaatregelen hebben voor hun account. Stel wachtwoordbeleid in om te zorgen dat gebruikers sterke wachtwoorden maken. We raden je ook aan waar mogelijk verificatie in 2 stappen te gebruiken, gebaseerd op de aanbevolen groeperingen in het gedeelte over beveiligd inloggen. Je kunt het gebruik van verificatie in 2 stappen afdwingen voor een deel van de gebruikers (geef ze daarbij tijd om dit in te stellen) en verificatie in 2 stappen implementeren met verschillende methoden, zoals beveiligingssleutels (het veiligst), een Google-prompt (via de apps van Google op Android en iOS), apps die verificatiecodes maken (zoals Google Authenticator) en tekstberichten of telefoongesprekken (de minst veilige methode).

Als je organisatie een andere identiteitsprovider (IdP) dan Google gebruikt, kun je Single sign-on (SSO) instellen via die identiteitsprovider van derden. Je kunt als je wilt nog steeds verificatie in 2 stappen gebruiken met SSO voor gebruikers die geen hoofdbeheerder zijn.

Zet services aan of uit

In de Google Beheerdersconsole kunnen beheerders bepalen tot welke Google-services gebruikers toegang hebben met hun Google Workspace for Education-account. Je bepaalt wie toegang heeft tot Google-services als Agenda, Drive en Meet door services aan of uit te zetten per organisatie-eenheid (OE) (je kunt services ook aanzetten als je groepen gebruikt). Check ook het verschil tussen kernservices van Workspace en aanvullende services voordat je aanvullende services aanzet, zoals YouTube, Google Maps en Blogger. We raden beheerders aan om de toegang tot Google-services in te stellen gebaseerd op leeftijd. Bovendien gelden er voor gebruikers voor wie je instelt dat ze onder de 18 zijn automatisch beperkingen in sommige Google-services als ze zijn ingelogd op hun Google Workspace for Education-account.

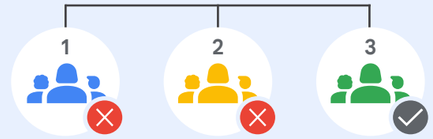
Je kunt ook contextbewuste toegang gebruiken (beschikbaar in Workspace for Education Standard en Plus) om de toegang toe te staan of te blokkeren tot Google-apps als Gmail, Drive en Agenda, gebaseerd op het IP-adres, de geografische oorsprong, het beveiligingsbeleid of het OS van een apparaat. Je kunt bijvoorbeeld instellen dat gebruikers alleen toegang hebben tot Drive voor desktop op apparaten die eigendom zijn van de school in specifieke landen of regio's..

Methoden om gebruikers toegang te geven tot services

In de Google Beheerdersconsole kun je de toegang van een organisatie-eenheid tot een Google-service, zoals Google Drive, uitzetten. Als bepaalde gebruikers in die organisatie-eenheid Drive wel moeten kunnen gebruiken, heeft u 2 opties:

1. De gebruikers verplaatsen naar een organisatie-eenheid waarvoor Drive aanstaat.
2. De gebruikers toevoegen aan een toegangsgroep en Drive aanzetten voor de groep. Elk lid van de groep heeft toegang tot de service, zelfs als de service uitstaat voor hun organisatie-eenheid.

Organisatie-eenheden



Google Drive staat uit voor organisatie-eenheid 1 en 2

Met een toegangsgroep

Maar een **groep gebruikers** in organisatie-eenheid 1 en 2 heeft wel toegang tot Google Drive

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

Stel bewaarregels en beleid voor het delen van gegevens in

Als beheerder kun je bepalen of gebruikers Google Drive-bestanden en -mappen kunnen delen met mensen buiten je organisatie. Zo kunnen mensen gegevens en bestanden niet per ongeluk of met de verkeerde mensen delen en voorkom je datalekken. Door bestanden en schijven te scheiden, organisatie-eenheden te maken en het principe van minimale rechten na te leven, voorkom je dat aanvallers toegang krijgen tot andere netwerken als ze één account weten te hacken. Hoe minder gegevens en netwerken een aanvaller kan bereiken, hoe minder schade die kan aanrichten.

Zet de optie om bestanden extern te delen uit voor leerlingen (of beperk externe delen tot alleen toegestane domeinen) en stel Toegangscontrole in op Alleen ontvangers. Als je een deel van of alle gebruikers toestaat bestanden te delen buiten je domein, stel je in dat de gebruiker een waarschuwing krijgt als dit gebeurt. Stel ook in dat gebruikers bestanden niet kunnen publiceren op het web en vereis dat externe bijdragers inloggen met een Google-account.

Klanten met Workspace for Education Standard en Plus kunnen bovendien doelgroepen en vertrouwensregels gebruiken om gedetailleerdere aanbevelingen en beperkingen voor delen in te stellen. Met doelgroepen kun je bijvoorbeeld instellen dat de standaard doelgroep voor het delen van links voor docenten 'docenten en andere medewerkers' is, in plaats van iedereen in je onderwijsinstelling. Met vertrouwensregels kun je instellen dat leerlingen in lagere leerjaren geen bestanden kunnen delen met oudere leerlingen.

Controleer beleid voor gedeelde Drives om te zorgen dat alleen bepaalde gebruikers gedeelde Drives kunnen maken en ervoor te zorgen dat externe gebruikers geen toegang hebben tot gedeelde Drives. We raden je aan alleen beheerders (of alleen docenten en andere medewerkers) toe te staan gedeelde Drives te maken en de toegang tot gedeelde Drives zorgvuldig te beheren.

We raden je aan de zichtbaarheid van de directory en de mogelijkheid contacten te delen waar mogelijk te beperken door het delen van contacten uit te zetten voor een deel van of alle gebruikers of door aangepaste directory's te maken om te beperken wie welke gebruikers kan zien.

Stel beleid voor Gegevensverlies voorkomen (Data Loss Prevention, DLP) in Drive en Gmail in om gevoelige informatie te detecteren en te blokkeren. Er zijn vooraf ingestelde beleidsregels waarmee je veelvoorkomende gevoelige informatie (zoals bank- of creditcardnummers) kunt beschermen. Je kunt ook aangepast beleid maken gebaseerd op zoekwoorden, woordenlijsten en reguliere expressies (regex).

Beheer de Gmail-instellingen

Gmail is één van de kernservices van Google Workspace for Education. Er zijn veel verschillende instellingen waarmee beheerders hun onderwijsinstelling en gebruikers kunnen beschermen.

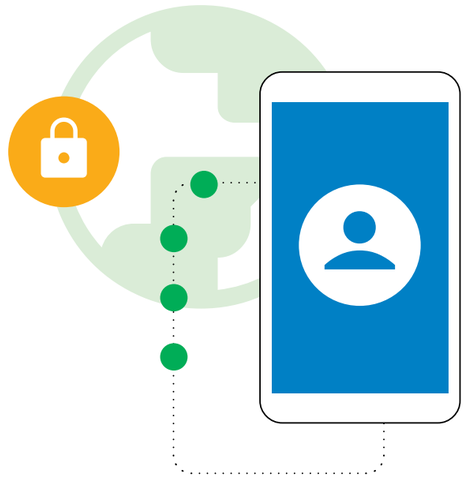
Voorkom spam, spoofing en phishing met Gmail-verificatie. Pas de instellingen voor de spamfilters aan, bijvoorbeeld door afzenderverificatie te vereisen voor alle goedgekeurde afzenders en in te stellen dat interne afzenders de spamfilters niet kunnen overslaan.

Zet POP/IMAP-toegang uit waar mogelijk en zet verbeterde scans voordat berichten worden bezorgd en geavanceerde beveiliging tegen phishing en malware aan. Als je een deel van of alle gebruikers toestaat externe e-mails te sturen, kun je waarschuwingen voor externe ontvangers aanzetten.

Klanten met Google Workspace for Education Standard en Plus kunnen hun onderwijsinstelling ook beschermen tegen malware en ransomware door regels in te stellen om schadelijke bijlagen te detecteren met Beveiligingssandbox.

Apps van derden

Gebruik ingebouwde goedkeuringsworkflows om apps van derden goed te keuren die via API's toegang hebben tot accountgegevens. Zo voorkom je dat gegevens worden gedeeld met apps van derden die je niet hebt goedgekeurd voor gebruik op school.



Rapporten en controles

Als beheerder kun je rapporten en logboekgebeurtenissen bekijken in de Google Beheerdersconsole om de activiteiten in je organisatie in kaart te brengen, zoals mogelijke beveiligingsrisico's, wie wanneer inlogt en hoe gebruikers content maken en delen. In diagrammen en tabellen zie je gegevens op domeinniveau naast gedetailleerde gegevens op gebruikersniveau. Bekijk rapporten en controlelogboeken (inclusief het meldingencentrum) om onder andere beveiligingsrisico's te herkennen, servicegebruik te analyseren, configuratieproblemen in kaart te brengen en gebruikersactiviteit te controleren.

Beheerders met Google Workspace for Education Standard en Plus kunnen het beveiligingsdashboard gebruiken om een overzicht van verschillende beveiligingsrapporten te bekijken, trends in kaart te brengen en huidige en historische gegevens te vergelijken, zoals bestanden delen in Drive, spam-, phishing- en malwareactiviteit in Gmail, verdachte inlogpogingen op gebruikersaccounts en verdachte apparaatactiviteiten. De meeste gebruiks-, activiteiten- en controlelogboeken (inclusief gebeurtenissen in het beheerderslogboek en de logboeken Drive, Meet en Chat) en beveiligingsrapporten zijn 6 maanden beschikbaar.

Gebruik het beveiligingscentrum

Beheerders met Google Workspace for Education Plus en Standard kunnen het beveiligingscentrum gebruiken. Hierin vinden ze geavanceerde beveiligingsinformatie en -analyse, en meer zichtbaarheid en controle over de beveiligingsproblemen in hun domein.

Het beveiligingscentrum bevat de tool voor beveiligingsonderzoek, waarmee beheerders beveiligings- en privacyproblemen kunnen herkennen, beoordelen en verhelpen, zoals phishing-aanvallen, ongepast delen van bestanden en verdachte gebruikers- en apparaatactiviteit.

Google Workspace is 's werelds best beveiligde pakket voor communicatie en samenwerking in de cloud.

0

actief uitgebuite softwarekwetsbaarheden in Workspace sinds november 2021*

50%

mogelijke besparing op verzekeringen voor cyberbeveiliging door Workspace te gebruiken

2x minder

beveiligingsincidenten voor organisaties die Workspace gebruiken in plaats van Microsoft 365

2.5x minder

beveiligingsincidenten voor organisaties die Workspace gebruiken in plaats van Microsoft Exchange

*Volgens de CISA is dit aanzienlijk minder dan in productiviteitstools van andere aanbieders.

Google Chromebooks voor onderwijs

Chromebooks zijn streng beveiligde, schaalbare en gebruiksvriendelijke computers voor leerlingen en docenten. Ze bevatten speciale ingebouwde beveiligingsfuncties. Er is nog nooit een ransomware-aanval gemeld op een zakelijk, educatief of persoonlijk ChromeOS-apparaat. Met Chromebooks zijn scholen beschermd tegen steeds veranderende bedreigingen, doordat functies automatisch op de achtergrond worden geüpdatet. Zo kunnen gebruikers binnen een paar seconden weer aan het werk.

Automatische updates van het OS en apps, met ingebouwde bescherming tegen malware

Aanvallers proberen steeds bugs en kwetsbaarheden te vinden in besturingssystemen, browsers en populaire apps om malware te installeren en gebruikersgegevens te delen. Chromebooks beschermen jou en je gebruikers door het OS en de apps up-to-date te houden. Chromebooks zijn standaard beveiligd met beveiligingsupdates en je hoeft de software van cloud-apps niet te updaten zoals met lokaal geïnstalleerde apps. De door Google ontworpen beveiligingschip in Chromebooks beveiligt het apparaat en de identiteit van de gebruiker en beschermt de systeemintegriteit.

Je Chromebooks krijgen automatisch de nieuwste updates voor bescherming tegen malware. Leerlingen en docenten zijn beschermd tegen cyberdreigingen dankzij ingebouwde beveiligingsfuncties zoals gegevensversleuteling, Verified Boot, sandboxen en automatische updates.

Beveiligde gebruikersgegevens

Als je met je Google-account inlogt op een Chromebook, worden al je gegevens opgeslagen in versleutelde bestanden. Zo heeft niemand anders op het apparaat toegang tot je gegevens en kan niemand met jouw account inloggen bij apps. Zo kunnen leerlingen makkelijk en beveiligd op school apparaten delen en zijn scholen minder geld kwijt aan computers. Als je geavanceerdere beveiligingsfuncties wilt, krijg je met de Chrome Education Upgrade, de licentie voor apparaatbeheer, meer zichtbaarheid.

Beveiligingsbeleid op afstand voor door beheerde apparaten van gebruikers

Schoolbeheerders kunnen op afstand ChromeOS-beleid instellen en apps installeren/updaten via de Google Beheerdersconsole. Met een simpele muisklik kan één IT-beheerder het beleid en de configuraties van honderdduizenden Chromebooks tegelijk updaten.

Zo zorg je voor het volgende:

- Leerlingen hebben alleen toegang tot content en apps die zijn goedgekeurd door de school.
- Alle apps en extensies worden geüpdatet met de nieuwste beveiligingsfixes.
- Gebruikers kunnen schoolgegevens niet kopiëren, overzetten of delen buiten het apparaat.
- Neem gegevensgestuurde beslissingen met aangepaste beveiligingsaanbevelingen van Google om beveiligingsbedreigingen aan te pakken.
- Beheer beleid voor beveiliging en identiteits- en toegangsbeheer voor alle gebruikers, rechtstreeks vanuit de Beheerdersconsole.

Dit zijn enkele belangrijke beleidsregels die we beheerders aanraden in te stellen:

Apparaatbeleid

- **Gastmodus**
  We raden je aan de gastmodus uit te zetten op je apparaten, zodat leerlingen en docenten moeten inloggen met hun eigen inloggegevens in plaats van het apparaat anoniem te gebruiken.
- **Inlogbeperkingen**
  Je wilt misschien niet dat leerlingen en docenten kunnen inloggen op Chromebooks van de school met hun persoonlijke Gmail-account. Dwing inlogbeperkingen af, zodat gebruikers alleen kunnen inloggen met een account in je Workspace-domein op apparaten die alleen worden gebruikt door leerlingen.
- **Gebruikers- en apparaatrapporten**
  We raden beheerders aan gebruikers- en apparaatrapporten aan te zetten, zodat ze statistische gegevens kunnen verzamelen over hoe vaak Chromebooks worden gebruikt, door wie en wat de staat van de hardware is.
- **Afgedwongen opnieuw inschrijven**
  Het is belangrijk dat een Chromebook die eigendom is van de school op school blijft, tenzij een beheerder deze uitschrijft. We raden beheerders aan in te stellen dat Chromebooks afgedwongen opnieuw worden ingeschreven, zodat Chromebooks zichzelf altijd opnieuw inschrijven als ze worden gewist of als iemand ze probeert te stelen.

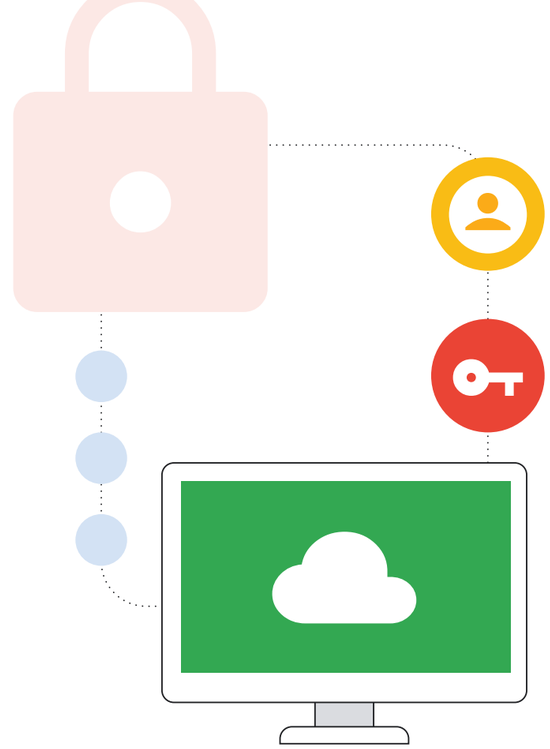
Gebruikersbeleid

- **Incognitomodus**
  Leerlingen moeten de Chromebooks van de school op de juiste manier gebruiken. Je kunt ze bijvoorbeeld beperken tot een geverifieerde browser, zodat filters voor webcontent kunnen zorgen dat ze niet naar ongepaste websites gaan. We raden beheerders aan de incognitomodus uit te zetten, zodat leerlingen deze webfilters niet kunnen omzeilen.
- **Proxymodus**
  Sommige scholen gebruiken proxy's voor webfiltering. Het is daarbij belangrijk dat je instelt dat gebruikers geen proxyinstellingen kunnen wijzigen.
- **Toegang tot meerdere accounts**
  Als gebruikers kunnen inloggen op een secundair account terwijl ze de Chromebooks en Workspace-accounts van je school gebruiken, kunnen ze makkelijk gevoelige gegevens en informatie van leerlingen en de school overzetten naar dat secundaire account. We raden beheerders aan toegang tot meerdere accounts uit te zetten.
- **Browsergeschiedenis**
  Het kan nuttig zijn voor leerlingen om in te stellen dat ze hun browsegeschiedenis niet kunnen wissen. Als zich een beveiligingsincident voordoet, kun je die geschiedenislogboeken gebruiken om onderzoek te doen.

Deze lijst is een goed begin om te zorgen dat je netwerken zijn beveiligd tegen de meest voorkomende fouten die gebruikers maken, die leiden tot grote cyberincidenten. Je vindt ander aanbevolen beveiligingsbeleid in de Beveiligingschecklist.

Eindpuntbeheer voor overal en altijd de beste beveiliging

Met het systeem voor beleidsbeheer op afstand van ChromeOS kunnen schoolbeheerders beveiligingsinstellingen toepassen en beveiligingstools (zoals systemen voor contentfilters) uitvoeren op apparaten in plaats van op de netwerkservers van de school. Zo hebben leerlingen thuis dezelfde beveiligingsvoordelen op hun school-Chromebooks als in de klas. Dit wordt steeds belangrijker, omdat scholen vaker digitaal lesmateriaal en online leertools gebruiken, waardoor leerlingen hun computer mee naar huis moeten nemen om hun huiswerk te kunnen doen.

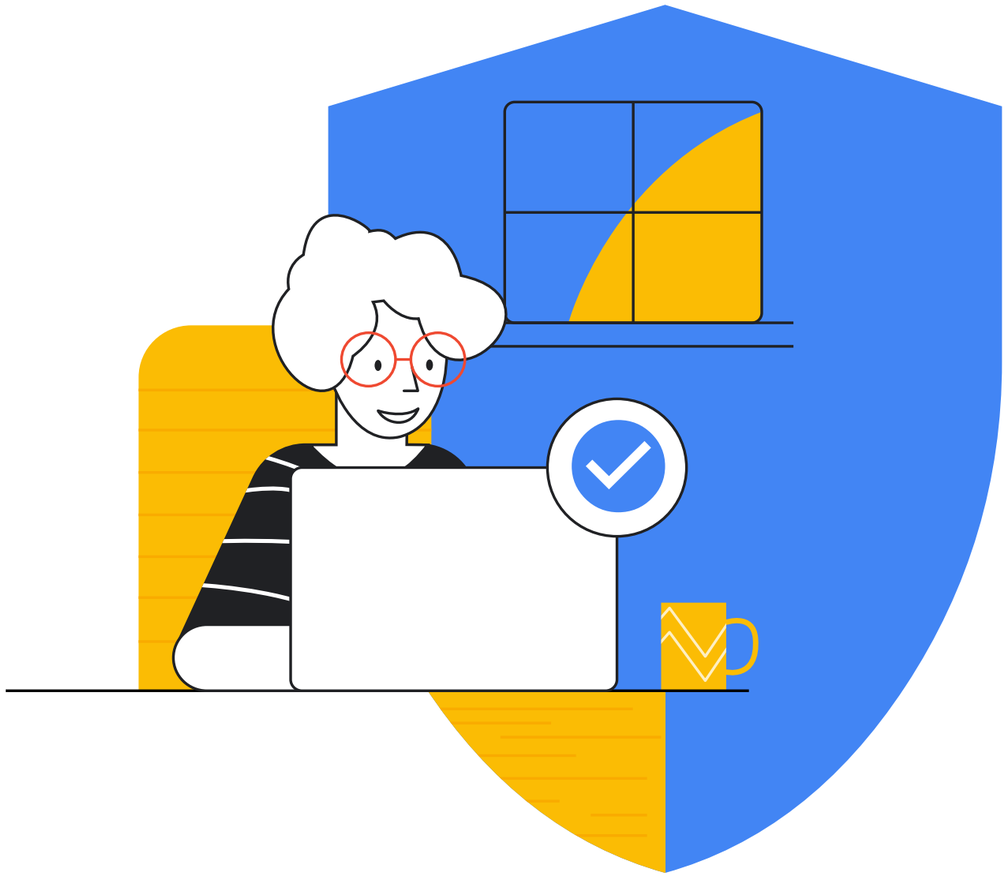


Conclusie

Het is een complexe uitdaging om instellingen voor het basis- en middelbaar onderwijs te beschermen tegen cyberincidenten, maar het is het de investering meer dan waard om jezelf, je leerlingen, je docenten, je andere medewerkers en het bredere online ecosysteem te beschermen. Wat we hebben besproken in dit document is een goed begin, maar alle scholen moeten de aanbevelingen aanpassen aan hun unieke behoeften en up-to-date blijven met steeds veranderende bedreigingen en nieuwe technologieën. Deze bron is een goede basis voor een beveiligingsprogramma voor scholen in het basis- en middelbaar onderwijs en bevat mogelijke vervolgstappen en actiepunten die je meteen kunt toepassen. Google heeft ook verschillende bronnen, trainingen en professionals op het gebied van cyberbeveiliging die scholen en organisaties kunnen helpen met de stappen in deze handleiding en met nieuwe technologieën, zoals AI. De producten van Google zijn speciaal gemaakt voor het onderwijs en geven je kant-en-klare oplossingen voor veel van de valkuilen op het gebied van cyberbeveiliging die we hebben besproken in dit document. We helpen je graag om je beveiligingsprogramma's te maken en te implementeren.

Bronnenlijst

- Google. Tips om online veilig en beveiligd te blijven. Google Veiligheidscentrum, https://safety.google/security/security-tips/. Geopend op 6 oktober 2022.
- NIST. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. NIST Technical Series Publications, 16 april 2018, https://doi.org/10.6028/NIST.CSWP.04162018. Geopend op 6 oktober 2022.
- Microsoft. Microsoft AccountGuard-programma. Microsoft AccountGuard-programma, https://accountguard.microsoft.com/nl-NL/. Geopend op 6 oktober 2022.
- Google. Het programma Geavanceerde beveiliging. Het programma Geavanceerde beveiliging, https://landing.google.com/advancedprotection. Geopend op 6 oktober 2022.
- Google. Google Veiligheidscentrum. Google Veiligheidscentrum: veiliger online, https://safety.google. Geopend op 6 oktober 2022.
- Meta. Basics: Help Secure Your Account. Help Secure Your Account, https://www.facebook.com/gpa/resources/basics/security. Geopend op 6 oktober 2022.
- Meta. Facebook Protect. Facebook, https://www.facebook.com/gpa/facebook-protect. Geopend op 6 oktober 2022.
- NIST. SP 800-124 Rev. 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise. NIST Technical Series Publications, https://doi.org/10.6028/NIST.SP.800-124r1. Geopend op 6 oktober 2022.
- Toegangssleutels: https://developers.google.com/identity/passkeys
- CISA-rapport over beveiliging in het basis- en middelbaar onderwijs, Protecting Our Future https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- GAO-rapport https://www.gao.gov/products/gao-20-644
- Ga voor meer informatie over hoe je je onderwijsinstelling beveiligt met Google for Education naar het Privacy- en beveiligingscentrum van Google for Education.
- Zscaler-rapport over phishing



Google for Education