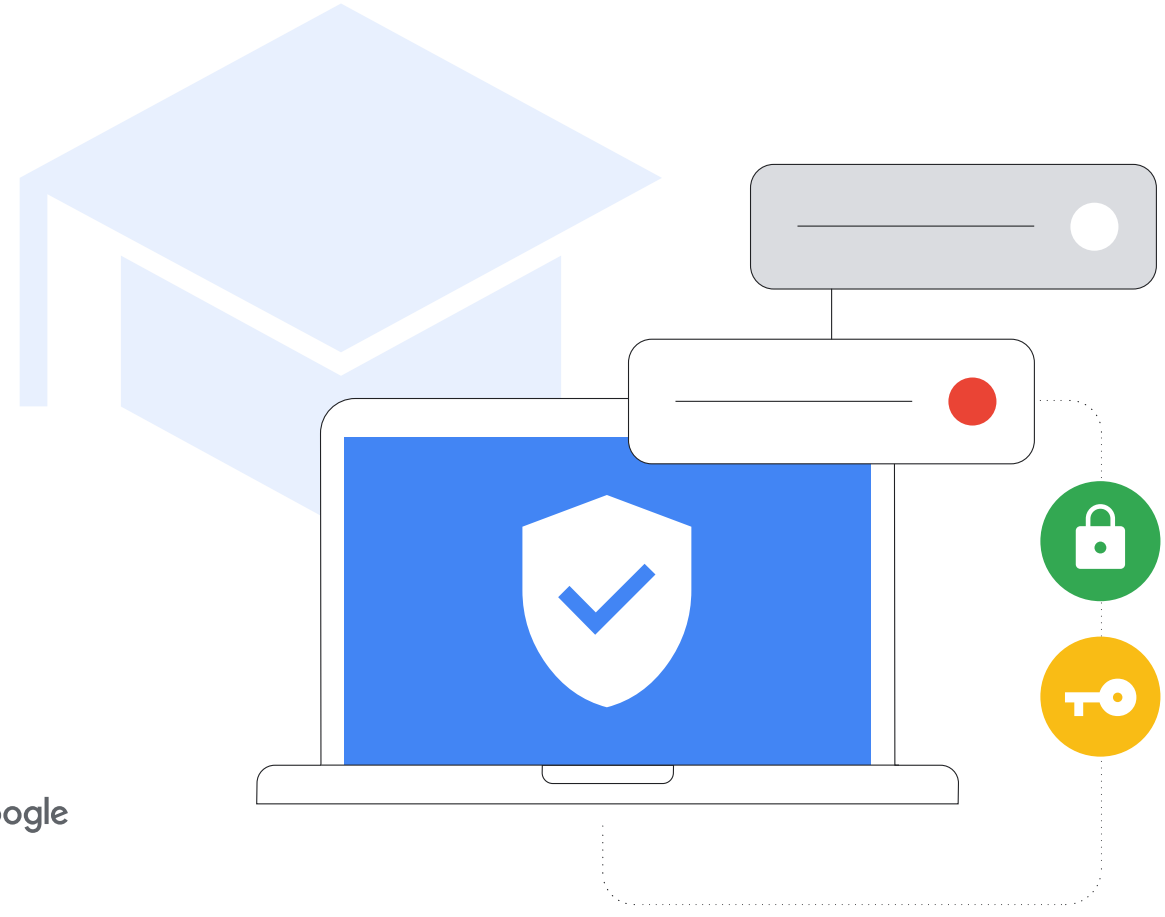
Google for Education

Cybersikkerhedsguide til grundskole og ungdomsuddannelser

Opdateret august 2023



Safer with Google

Resumé

Som fremhævet i CISA's rapport "*Protecting Our Future*"[1], er det afgørende, at grundskoler og ungdomsuddannelser investerer i online sikkerhed for at beskytte elever, deres familier, undervisere, medarbejdere og lokalsamfundet. I dette dokument får du vejledning i og bedste praksis til it-administratorer i forbindelse med opsætning og konfiguration af hardware og software, som kan forbedre online sikkerheden for grundskoler og ungdomsud dannelser. Det indeholder både generel bedste praksis samt specifikke retningslinjer for Googles produkter og tjenester. Googles mission er at organisere verdens oplysninger og gøre dem almindeligt tilgængelige og brugbare. Dette spiller en væsentlig rolle i Google for Education-teamets arbejde: Vi udvikler værktøjer, der er designet til undervisning og læring. I denne vejledning deler vi vores erfaringer fra vores arbejde.

Vi giver dig de mest optimale sikkerhedsløsninger efter emne. Under hvert emne får du en mere dybdegående gennemgang af konfiguration, opsætning og strategier til risikostyring. Vi forklarer også, hvordan Google håndterer online i forhold til vores tjenester – særligt for vores uddannelsesværktøje. Selvom vi i dette dokument giver detaljeret vejledning uafhængigt af produkter eller tjenester, mener vi, at vores produkter byder på overlegen og installationsklar beskyttelse mod almindelige angreb.

Risiko

Uddannelsesinstitutioner er primære mål for cyberangreb, når ondsindede aktører forsøger at udnytte skolernes store mængder af data til deres egen vinding. 46 % af de skoler, som endnu ikke har været udsat for et cyberangreb, mener, at de vil blive ramt før eller siden, fordi ransomwareangrebene bliver mere sofistikerede — og vanskeligere at stoppe. 42 % af disse skoler mener desuden, at ransomware er så almindeligt, at et angreb vil være uundgåeligt. Da skolerne i 2020 var nødt til hurtigt at gå over til fjernundervisning, var dette medvirkende til, at der opstod huller i onlinesikkerheden, så skolerne blev sårbare over for angreb.

Forsvar

Disse angreb kan begrænses. Selvom der ikke findes en teknologi, der helt fjerner risikoen, kan uddannelsessektoren og leverandører af uddannelsesteknologi samarbejde om at fastslå og implementere bedste praksis for at skabe en sikker, tryg og omfattende tilgang, som markant vil reducere risikoen. Med de rigtige sikkerhedsforanstaltninger og politikker til at beskytte brugere og enheder og til at sikre databeskyttelsen kan uddannelsesinstitutionerne bedre håndtere risiciene og begrænse angreb.

De vigtigste anbefalinger

- **BRUG SIKKER GODKENDELSE** til at beskytte følsomme oplysninger, mails, filer og andet indhold samt forhindre, at uautoriserede brugere får adgang til uddannelsesinstitutionens systemer. Anvend bedste praksis til brugergodkendelse, herunder stærke adgangskoder og totrinsverificering (2SV), adgangsnøgler og adgangskodeadministratorer, hvor dette er muligt, særligt for it-administratorer og medarbejdere, der håndterer følsomme oplysninger.
- **ANVEND PASSENDE SIKKERHEDSINDSTILLINGER** til at beskytte dine brugere, dine data og dit miljø. Googles produkter er som standard sikre, men det er vigtigt, at administratorerne også anvender og konfigurerer netværk og systemer korrekt for at opretholde sikkerheden. Du skal anvende principperne om nultillid og minimumsrettigheder: Brugerne bør kun have adgang til den software og de data, apps og systemer, som de har behov for til at kunne udføre deres arbejde effektivt.
- **OPDATER OG OPGRADER DINE SYSTEMER** for at sikre, at brugerne er beskyttet mod de nyeste trusler. Brug moderne operativsystemer (OS) og browsere, og sørg for, at brugerne har de nyeste softwareversioner på alle enheder (eller godkendte og stabile versioner med langtidsunderstøttelse), og at de opdateres automatisk. Opgradering til en mere sikker løsning, f.eks. Chromebooks, kan øge sikkerheden. Der er aldrig blevet registreret ransomware på en ChromeOS-enhed.
- **ANVEND SYSTEMER TIL ADVARSEL OG KONTROL I REALTID**, så du kan være på forkant med sikkerheden og begrænse eventuelle problemer hurtigt. Du kan bruge de funktioner, der er integreret i din primære samarbejds- og kommunikationssoftware, f.eks. Google Workspace for Education, eller implementere separate løsninger til sikkerhedslogning og -kontrol. Sørg for, at der implementeres omfattende sporing af aktiviteter på tværs skolens netværk, enheder, programmer, brugere og data. Kontrollér login på konti, fildeling, mailvolumen (særligt forsøg på phishing og malware), enhedsaktivitet og ændringer i konfigurationsændringe. Hold dine advarsels- og kontrolløsninger opdaterede for at få notifikationer om trusler, kritiske hændelser og systemændringer.
- **UNDERVIS UNDERVISERE, MEDARBEJDERE OG ELEVER** i sikker brug af enheder og software og i, hvordan man identificerer og rapporterer potentielle trusler samt deler data forsvarligt, da dette hjælper med at beskytte od nogle af de mest almindelige angreb. SSkoler eller distrikter kan oprette brandede undervisningsmaterialer og bruge dem sammen med offentligt tilgængelige materialer, hvilket giver skolerne omfattende værktøjer.

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

Specifikke anbefalinger til brugere af Googles produkter: Googles produkter, f.eks. Google Workspace for Education og Chromebooks, kan forbedre skolens onlinesikkerhed og gøre det let at implementere hver af disse anbefalinger. Sammen udgør anbefalingerne en omfattende løsning, der er med til at beskytte brugernes privatliv og give optimal sikkerhed til din uddannelsesinstitution.

Disse strategier danner, sammen med den supplerende vejledning, et solidt grundlag for sikkerheden på grundskoler og ungdomsuddannelser.

Googles tilgang til uddannelse

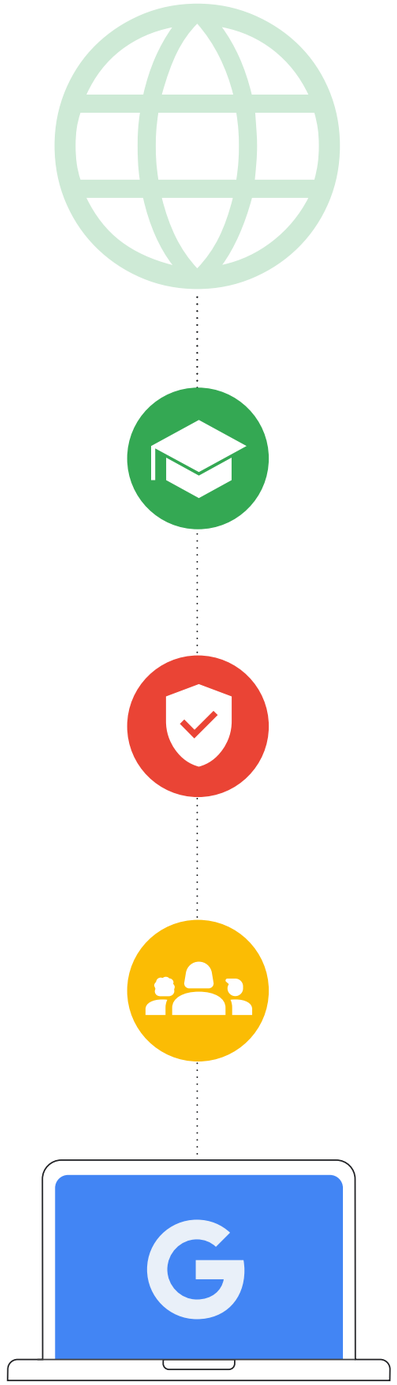
Googles mission er at organisere verdens oplysninger og gøre dem almindeligt tilgængelige og brugbare, hvilket også uddannelsessektoren. På Google for Education-teamet arbejder vi hen mod dette ved at udvikle værktøjer som Chromebooks og Google Classroom, der gør det nemt og sikkert for elever og undervisere at skabe, dele og organisere deres eget indhold samt tilgå og anvende uddannelsesressourcer og onlineværktøjer.

Skolerne fortjener teknologier, der som standard er sikre og designet med henblik på privatlivsbeskyttelse, som sikrer, at du bevarer kontrollen, og med pålideligt indhold og information. Med produkter som Chromebooks og Google Workspace for Education får skolerne optimal sikkerhed i høj kvalitet, som lever op til de højeste, globale uddannelsesstandarder. It-administratorer får fuld synlighed og problemfri styring af deres data- og sikkerhedspolitikker, og eleverne kan koncentrere sig fuldt ud om læringen i et mere sikkert digitalt miljø, der understøtter aldersbaseret indhold og begrænser spam og cybertrusler.

Vi har prioriteret indbyggede sikkerhedsfunktioner og indbygget sikkerhedsstyring, de højeste privatlivsstandarder og muligheder for at anvende mere proaktive sikkerhedsværktøjer for at garantere en sikker læring or alle. ChromeOS-enheder hjælper med at begrænse de trusler, skolerne oplever, og udgør det bedste forsvar mod den primære trussel mod skoler, nemlig ransomware, da der aldrig er blevet gennemført et ransomware-angreb mod Chromebooks.

Google Workspace for Education er én af verdens mest populære og sikre skybaserede kommunikations- og samarbejdspakker. Du kan få flere oplysninger i den sidste del om, hvordan de hver især beskytter onlinesikkerheden i henhold til disse anbefalinger.

Denne vejledning består af to dele: I den første del får du en praktiske og generelle sikkerhedsvejledning til grundskoler og ungdomsuddannelser uafhængigt af produkter. Den anden del indeholder specifik vejledning til de uddannelsesinstitutioner, der anvender Google for Education-produkter, f.eks. Google Workspace for Education og Chromebooks. Begge dele indeholder oplysninger om, hvordan du opretholder onlinesikkerheden for dig og dine elever.



Indledning

Grundskoler og ungdomsuddannelser er i højrisikogruppen for cyberangreb, og det gælder både deres enheder og netværk. Det er afgørende, at de implementerer den bedst mulige sikkerhed for at beskytte eleverne og forhindre ab af data, tjenester, ressourcer, tid og penge, som kan være konsekvensen af sådanne angreb (Kilde).

Denne vejledning er et værktøj, som har til formål at give dig indblik i bedste praksis nden for online sikkerhed, som skoleadministratorer og skolesystemer kan implementere med henblik på en bedre sikkerhed i deres miljøer. Når denne bedste praksis implementeres, kan grundskoler og ungdomsuddannelser begrænse eller forhindre alvorlige og dyre cyberangreb på uddannelsessystemer og beskytte elever, familier, undervisere og medarbejdere.

Cyberangreb, der er målrettet skoler, sker oftere de bliver løbende mere alvorlige. I henhold til K-12 Cybersecurity Resource Center blev der mellem 2016 og 2021 offentliggjort mere end 1.300 cyberhændelser, som har involveret uddannelsesorganisationer på tværs af alle USA's 50 stater. Uddannelseslederne i dag skal beskytte data og personlige oplysninger om elever, undervisere og medarbejdere samt deres uddannelsesinstitutions systemer og information. Det er en stor opgave, især i betragtning af at uddannelsessektoren traditionelt har haft sværere ved at holde trit med onlinesikkerheden sammenlignet med andre sektorer.

Et vellykket cyberangreb, herunder ransomware, phishing, malware m.m., kan medføre omfattende databrud i forbindelse med personhenførbare oplysninger (PII), udbetalinger af store pengesummer (den gennemsnitlige udbetaling i forbindelse med ransomware er femdoblet siden 2020 til 812.260 USD), ligesom det kan forårsage længerevarende forstyrrelser i forhold til undervisningen og andre skolerelaterede aktiviteter. For nyligt var et vellykket ransomwareangreb skyld i nedlukningen af et helt skolesystem, hvilket påvirkede hele lokalsamfundet, fordi eleverne ikke kunne komme i skole i mange dage. Med begrænsede ressourcer og midler vil grundskoler og ungdomsuddannelser fortsat være et oplagt mål for cyberangreb, medmindre der investeres i forbedret onlinesikkerhed.

Onlinesikkerheden understøttes altid bedst af kommunikation, samarbejde og partnerskab. Dette dokument er udarbejdet på baggrund af Googles tips om sikkerhed, Cybersecurity Framework fra National Institute for Standards and Technology (NIST) samt CISA's K-12 Cybersecurity Toolkit and Recommendations fra 2023, som alle er almindeligt anerkendte kilder for praksis i forhold til onlinesikkerhed. Dette dokument gennemgår generelle skridt, som it-administratorer bør tage eller overveje, nogle af Googles egne bedste praksisser og vejledning i vores produkter. Der henvisesogså til sikkerhedstips og -tjenester fra andre virksomheder. Administratorerne bør gennemgå al sikkerhedsvejledning fra de relevante virksomheder og implementere deres seneste vejledning, da det er den ansvarlige virksomhed, der er bedst i stand til at beskrive sine egne produkter og eventuelle ændringer, der måtte være sket.

Inden du implementerer tiltag på baggrund af anbefalingerne nedenfor, bør du også overveje følgende faktorer:

Overvejelser

1. **Beskyttelse af dine elever.**
Alle skoler har forskellige behov, og for nogle elevgrupper kræves der muligvis yderligere tiltag for at opretholde sikkerheden og beskytte deres privatliv. Mange uddannelsesteknologiske værktøjer har funktioner, der medvirker til aldersbaseret adgang, f.eks. ved at begrænse upassende indhold eller sikre, at elevernes lokation og kontaktoplysninger er private.

2. **Den type data, du opbevarer.**
Hvis du opbevarer følsomme oplysninger, skal du måske kryptere dataene eller opbevare dem på en anden lokation.

3. **Den type enheder, du anvender, og din implementeringsmodel.**
Enheder og programmer på enhederne bør køre automatiske opdateringer for at maksimere sikkerheden, kryptere data og isolere konti for at sikre, at brugerne kun har adgang til deres egne oplysninger.

4. **Politikker for din skole, dit distrikt eller din region.**
Din skole kan have specifikke politikker vedrørende anvendelse af teknologi. Du skal sikre dig, at alle sikkerhedsforanstaltninger er i overensstemmelse med disse politikker.

Hver dag blokeres
100 millioner
phishingforsøg af Gmail.

Hver uge identificerer Google
300,000
usikre websites.

Hver dag får
74 millioner
brugere hjælp fra Googles Adgangskodeadministrator.

Hvert år øger
700 millioner
personer deres sikkerhed takket være Sikkerhedstjek.

Brug sikker godkendelse

Sikker godkendelse bør være den højeste prioritet på skoler og andre uddannelsesinstitutioner. I fjerde kvartal af 2022 udgjorde konti med dårlig beskyttelse eller uden login 48 % af årsagerne til sikkerhedsbrud. Implementering af de vigtigste anbefalinger kan være med til at verificere, at brugerne er dem, de siger, de er, og begrænse adgangen til oplysninger i forhold til den enkelte brugers rolle.

It-administratorerne bør håndhæve anvendelsen af totrinsverificering (også kendt som totrinsgodkendelse), og gå over til godkendelse uden adgangskode (dvs. adgangsnøgler), når dette er muligt, hvilket gælder særligt i tilfælde, hvor brugerne har fjernadgang til uddannelsesinstitutionens systemer. Totrinsverificering giver dine onlinekonti et ekstra sikkerhedslag og gør det meget sværere for hackerne at få adgang til dem.

Skolerne anvender i dag mange enhedstyper og implementeringsmodeller , og de tekniske færdigheder arierer meget inden for ddannelsesmiljøet på grundskoler og ungdomsuddannelser. Konto- og enhedssikkerheden varierer på tværs af brugerroller og -typer med definerede bedste praksisser: It-administratorer, undervisere og medarbejdere samt ældre elever, som anvender de tildelte enheder, og yngre elever, som bruger delte enheder. Vi gennemgår pecifikke anbefalinger for hver gruppe nedenfor. Der er flere godkendelsesmetoder, som kan ses som bedste praksis i de fleste miljøer:

Der er flere godkendelsesmetoder, der kan ses som bedste praksis i de fleste miljøer:

- **Stærke adgangskoder:**
  Bed brugerne om at oprette deres egen adgangskode ved første login. Sæt tekniske krav om, at koden skal have en minimumslængde og en vis kompleksitet. Længere adgangssætninger giver et ekstra sikkerhedslag på grund af længden og anvendelsen af komplekse tegn. Det bør ikke være påkrævet, at brugerne regelmæssigt ændrer deres adgangskoder, da det tilskynder dem til at anvende mere enkle adgangskoder eller foretage meget små ændringer (f.eks. opdatering af et enkelt tegn).
- **Totrinsverificering (2SV):**
  Totrinsverificering beskytter konti med et ekstra trin – ofte gennem noget, som en bruger har med sig, f.eks. en sikkerhedsnøgle eller en app på mobiltelefonen, der opretter en engangsverificeringskode. Selvom enhver form for totrinsverificering tilføjer kontosikkerhed, bør administratorerne undgå anvendelsen af verificeringskoder, der sendes via besked eller opkald, som kan være sårbare over for telefonnummerbaserede angreb.
- **Godkendelse uden adgangskode:**
  Adgangsnøgler er mere sikre, og de kan være nemmere at bruge end adgangskoder. Brugerne kan logge ind på apps og websites med en pinkode, et mønster, en biometrisk sensor (f.eks. fingeraftryk eller ansigtsgenkendelse) eller et tryk på en sikkerhedsnøgle, så de slipper for at skulle huske og holde styr på adgangskoder. Selvom disse måske ikke passer til alle uddannelsesmæssige omstændigheder, erstatter de i stigende grad traditionelle former for godkendelse og giver sikrere og hurtigere login. Adgangsnøgler beskytter brugerne mod phishingangreb, da de kun virker på de websites og i de apps, de er registreret til.
- **Single Sign-On (SSO:**
  Single Sign-On iver brugerne adgang til flere programmer og websites med ét enkelt login Når brugerne kun skal huske ét login , er det mindre sandsynligt, at de skriver detm ned. Når skolerne ikke behøver at administrere flere brugerlogin kan de desuden spare penge på it-support og helpdeskomkostninger. Google Workspace for Education understøtter som standard Single Sign-On , så brugerne kan anvende deres Google-kontologin til at logge ind på tredjepartsprogrammer. De kan også bruge en anden udbyders login til at logge ind på deres Google-konti.
- **Adgangskodeadministratorer:**
  Adgangskodeadministratorerne kan hjælpe brugerne med at oprette stærke og unikke adgangskoder til konti og tjenester, som de bruger i skolen eller på deres arbejde (når de ikke anvender Single Sign-On). De hjælper ikke med at logge ind på en enheds operativsystem, men de kan administrere adgangskoder, når brugeren er logget på. Google-brugere kan anvende Adgangskodeadministratoren i Chrome på alle platforme, herunder ChromeOS og Android.

Hver gruppe har unikke behov, som imødekommes gennem specialiserede undergrupper eller kombinationer af disse typer godkendelse, alt efter deres rolle i en uddannelsesinstitution, typen af systemer, data, de har adgang til, samt deres alder.

Skoleadministratorer

Administratorerne styrer systemerne og størstedelen af de data, der er forbundet med en grundskole eller ungdomsuddannelse. Beskyttelsen af deres konti er vigtig for hele systemets sikkerhed: Fra infrastruktur til kontodata og enheder, der administreres af uddannelsesinstitutionen. Derfor bør de anvende den højeste standard inden for godkendelse, herunder anvendelsen af stærke adgangskoder, en god adgangskodeadministrator og totrinsverificering. Hver af disse tilføjer et beskyttelseslag, der, når de anvendes sammen, giver den stærkeste sikkerhed for administratorkontoen og de tjenester, der bruges.

- Administratorerne bør anvende en fysisk sikkerhedsnøgle eller en kryptografisk sikker metode til totrinsverificering, som kræver en godkendt enhed og prompter. Dette kan omfatte en tjeneste som f.eks. Google Authenticator eller en anden app, der genererer engangsverificeringkoder. Chromebooks, der er udgivet efter 2019, og som har en TPM-chip, har en afbryderknap, som kan benyttes til totrinsverificering.
- Administratorerne bør anvende en pålidelig adgangskodeadministrator, der understøtter totrinsverificering til at gemme deres adgangskoder til forskellige tjenester.

Undervisere og medarbejdere, der anvender tildelte enheder

Ligesom administratorerne har undervisere og medarbejdere adgang til følsomme oplysninger, men de styrer ikke den digitale infrastruktur, og deres tekniske færdigheder varierer mere.

- Undervisere og medarbejdere, som anvender Chromebooks, bør have mulighed for at logge ind med biometrisk verificering, f.eks. fingeraftryk, når dette er lovligt.
- Administratorerne bør kræve brug af totrinsverificering og anvende godkendelse uden adgangskode, når dette er muligt, og i de tilfælde, hvor medarbejderne har fjernadgang til uddannelsesinstitutionens systemer.

Ældre elever, der anvender tildelte enheder

(typisk fra 4. klasse)

Ældre elever er bedre uddannet i, hvordan de beskytter sig selv, og de er normalt bedre til at anvende godkendelsesmetoder, der beskytter mere, som er passende til den type tjenester, de sandsynligvis vil bruge. De bør kun have adgang til deres egen konto og den information, der er blevet delt med dem.

- Elever, som anvender Chromebooks, bør have mulighed for at oprette en enhedsspecifik pinkode for hurtigere at kunne logge ind på den pågældende enhed. Det kan være, at de biometriske metoder hverken er passende eller en mulighed i mange skolemiljøer.
- Hver elev bør støttes i at oprette en unik adgangskode, der ikke indeholder personlige oplysninger (f.eks. navn, klasselokale eller fødselsdato). Eleverne bør undervises i, hvordan anvendelsen af adgangssætninger kan give kompleksitet og samtidig gøre adgangskoden let at huske.

Yngre elever, der anvender elte enheder

(typisk indskolingen)

De yngste elever er stadig ved at lære at bruge uddannelsesteknologi en og får mere ud af simpel godkendelse – som er velegnet til at anvende ammen med begrænsede tjenester og data.

- Skoler, der bruger adgangskodealternativer fra tredjeparter, f.eks. QR-koder eller billedlogin, til de yngste elever, og dem, der ikke kan logge ind med adgangskoder, bør implementere sikkerhedsforanstaltninger, da disse alternativer er mindre sikre. Administratorerne bør ændre eller opdatere en elevs adgangskode, hvis eleven mister sin kode, eller hvis koden er blevet vist til andre.
- Skolerne bør oplyse både elever og forældre om vigtigheden af at holde adgangskoderne hemmelige, og om hvordan man opbevarer alternative loginoplysninger, f.eks. QR-koder, sikkert.
- For tildelte enheder som tablets kan en enhedsspecifik pinkode anvendes som en alternativ sikker godkendelsesmetode.

Anvend passende sikkerhedsindstillinger

Skolernes enheder og netværk er et mål med høj synlighed og værdi for hackere over hele verden, så det er afgørende at anvende den bedst mulige sikkerhed for at forhindre tab af tjenester, ressourcer, tid og penge. Systemadministratorerne bør implementere effektive og passende sikkerhedsfunktioner, der er tilgængelige i de produkter, deres uddannelsesinstitutioner anvende, men de skal også sørge for, at disse systemer stadig er nemme at bruge for undervisere, medarbejdere og elever. Der bør konfigureres vigtige sikkerheds- og privatlivsindstillinger, som individuelle brugere ikke har mulighed for at deaktivere eller ændre, og der bør være beskyttelses standarder for andre indstillinger, som er konfigureret af administratoren. Det er afgørende at anvende den bedst mulige sikkerhed for at forhindre tab af tjenester, ressourcer, tid og penge. Hvis du bruger Chromebooks, kan du se vores forslag til konfiguration af enhedspolitikker i den sidste del.

Sørg for at integrere "dataminimering" i din fremgangsmåde ved at begrænse formålene og midlerne til indsamling, anvendelse og videregivelse af personlige oplysninger for enkeltpersoner til, hvad der med rimelighed er nødvendigt og proportionalt for at levere tjenesten eller på anden måde er i overensstemmelse med sammenhængen i forholdet.

Programmer og opdateringer

Begræns og minimer de apps, dine brugere kan installere, da enhver app på en enhed er en potentiel angrebsvektor, der kan udnyttes. Brug kun apps fra pålidelige kilder, i det omfang dette er muligt. Anbefal f.eks. brugerne at se efter et verificeringsbadge i Google Play Butikken for at sikre, at de downloader de officielle apps, der har været igennem en sikkerhedsgennemgang. Alle OS- eller hardwareændringer (jailbreaking eller rooting) udgør betydelige sikkerhedsrisici og bør undgås.

Adgang og synlighed

Administratorerne bør sikre, at brugerne kun har adgang til de data, den software samt de tjenester og systemer, som de har brug for til at udføre deres opgaver eller lære effektivt. Dette hjælper med at begrænse utilsigtet adgang og spore, hvem der har adgang til hvilke ressourcer. Vær særligt opmærksom på meget følsomme oplysninger, f.eks. personhenførbare brugeroplysninger, og systemer (f.eks. til HR, løn, karaktergivning, sikkerhed og konfiguration) ved at styre, hvilke brugere der har adgang til dataene og under hvilke omstændigheder, ved at begrænse adgangen til skoleejede enheder, og sikre, at det kun er bestemte medarbejdere, der har adgang.

Gennemgå dine datadelingspolitikker for samarbejdsværktøjer for at forhindre upassende deling eller overdeling og uautoriseret adgang. Begræns eller bloker deling uden for dit miljø (især for elever), og aktivér politikker i forbindelse med kontrol med deling af følsomt indhold.

Tab eller tyveri af enheder

En mistet enhed betyder ikke nødvendigvis, at du mister dine data . Administratorerne bør standardisere en plan for at sikre adgangen til oplysninger og dokumenter i tilfælde af tab eller tyveri af en enhed, f.eks. lagring af dokumenter i et skybaseret miljø. Download og udskriv sikkerhedskopier af koder til dine processer for totrinsverificering or at forhindre en afbrydelse af kontoadgangen.

Når en enhed rapporteres som mistet eller stjålet, skal du sørge for, at enheden fjernlåses, hvis det er muligt, og at tilknyttede konti låses eller rapporteres for at sikre, at de ikke bruges til at få uautoriseret adgang. Chromebooks kan fjernryddes, hvis de mistes, og Google Workspace for Education-konti kan kontrolleres for mistænkelig aktivitet eller suspenderes (låses), hvis det er nødvendigt.

Avanceret beskyttelse for højrisikobrugere

For brugere med høj synlighed og følsomme oplysninger (herunder Google Workspace for Education-administratorer) tilbyder Google programmet Avanceret beskyttelse (APP). Programmet giver brugerne yderligere beskyttelse mod målrettede angreb som phishingforsøg, skadelige downloads og brud på adgangskodesikkerheden. Programmet Avanceret beskyttelse er specialdesignet til at forhindre målrettede onlineangreb på Google-konti og anvender automatisk stærk godkendelse og sikkerhedsnøgler samt begrænser tredjepartsadgang til kontooplysningerne. Andre onlinekontoudbydere giver også stærk kontobeskyttelse til højrisikobrugere, og administratorer og medarbejdere bør altid anvende den, hvis de har adgang til personlige oplysninger eller teknologisystemer.

Opdater og opgrader dine systemer

Én af de vigtigste ting, man kan gøre for at beskytte sig selv, er at holde sin enheds operativsystem og programmer opdaterede. Dette er endnu vigtigere for grundskoler og ungdomsuddannelser, da de udgør så igtig en del af et barns uddannelse og daglige liv. De fleste malwareangreb, der finder sted både i uddannelsesmæssig sammenhæng og i andre sammenhænge , hvor der er en høj risiko, har været Windows-baserede. Det gælder både SolarWinds, ransomwareangrebet på Los Angeles' samlede skoledistrikt, hackingangrebet på Little Rock-skoledistriktet, bruddet på datasikkerheden hos Microsoft Exchange Server, ransomwareangrebet på Albuquerque-skoledistrikt samt det nylige sikkerhedsbrud på Microsoft Federal. Dette er endnu et tilfælde, hvor anvendelsen af skybaserede produkter og tjenester kan gøre en administrators opgave lettere ved at reducere angrebsfladen og sikre, at deres systemer og programmer automatisk forbliver opdaterede.

Opgrader til et moderne operativsystem, og hold det opdateret

Den nyeste version af ethvert operativsystem (OS) indeholder normalt nye sikkerhedsfunktioner, der hjælper med at forhindre kendte angrebsvektorer. Du bør aktivere funktionen til automatisk opdatering i enhedens operativsystem. Hvis det ikke er muligt at aktivere de automatiske opdateringer, bør du downloade og installere programrettelser og opdateringer fra en pålidelig leverandør hver måned som minimum.

Chromebooks kører på ChromeOS, så de har hyppige, automatiske opdateringer med de nyeste sikkerhedsprogramrettelser for at muliggøre hurtig implementering af de seneste sikkerhedsinnovationer, og de verificerer integriteten af det skrivebeskyttede operativsystem før opstart. De krypterer også alle data, der er gemt på enheden, beskytter den mod uautoriseret adgang og kører alle websider og programmer i separate sandboxes. Det betyder, at hvis et website eller en app bliver inficeret med malware, kan den ikke sprede sig til andre dele af enheden.

Hvis din skole ikke er klar til at gå over til Chromebooks, findes der ChromeOS Flex, som er en version af ChromeOS, der er lavet til at modernisere din skoles enheder. ChromeOS Flex giver alle en samlet, moderne undervisnings- og læringsoplevelse, der har proaktiv ndbygget sikkerhed og skybaserede administrationsmuligheder. ChromeOS Flex kan give automatiseret beskyttelse og blokere skadelige eksekverbare filer og apps, uden at den eksisterende hardware skal skiftes ud.

Opgrader til en moderne browser, og hold den opdateret

Det er vigtigt at sørge for, at browseren også er opdateret og sikker. Moderne browsere tilbyder mere avancerede sikkerhedsfunktioner, som browserne kan bede brugerne om at aktivere. Sikkerhedsfunktionerne kan også konfigureres af administratorerne for at aktivere dem som standard på uddannelsesinstitutioners computere. Dette giver mulighed for at beskytte fortroligheden af følsomme oplysninger under overførsel via internettet. Browseren skal altid være opdateret. Uanset om du arbejder, studerer eller laver andre aktiviteter online, vil en opdateret, moderne browser:

- **Anvende robust sikkerhed**, herunder isolering af websites og sikker browsingbeskyttelse for at forhindre, at brugerne går ind på farlige websites ved et uheld
- **Muliggøre automatiske opdateringer** for at sikre, at din browser bliver sikkerhedsopdateret hurtigt
- **Sørge for, at forbindelsen er sikker.** Moderne browsere bør anvende Transport Layer Security, og brugerne kan klikke ud for webadressen og tjekke, om forbindelsen er markeret som sikker

Chrome er udviklet med henblik på sikkerheden og med sikkerhedsfunktioner som browsingbeskyttelse aktiveret som standard. Der er derudover en integreret adgangskodeadministrator, som kan udfylde adgangskoder automatisk, når du browser på nettet, så du nemt kan anvende stærke adgangskoder.

Anvend systemer til advarsel og kontrol i realtid

Systemerne til advarsel og kontrol i realtid kan hjælpe skoler med at identificere og reagere hurtigt på trusler, før de forårsager skade. Det er vigtigt at sikre, at der kører sikkerhedsværktøjer i baggrunden, som indsamler og logger sikkerhedshændelser på tværs af dine systemer. AI-værktøjer er særligt velegnede til at gennemsøge de store mængder af indsamlede data og finde afvigelser og mønstre, som kan anvendes til hurtigere og nemmere at opdage trusler og til at behandle og afhjælpe sårbarheder. Dette giver mulighed for prioritering af, hvilke aktiviteter der skal gennemgås af it-administratoren eller medarbejderne.

Skolerne kan anvende advarsels- og styringsfunktioner, der er indbygget i deres primære samarbejds- og kommunikationssoftware, f.eks. Google Workspace for Education, eller implementere separate løsninger til sikkerhedsinformation og hændelsesstyring (SIEM).

Systemerne til advarsel og kontrol realtid kan spore en række aktiviteter på tværs af en skoles netværk, enheder, apps, brugere og data, f.eks. brugerlogin, adgang til filer, potentiel indtrængen, tyveri eller forsøg på tyveri af data og administratoraktiviteter.

Hvis systemet registrerer nogen form for mistænkelig aktivitet, kan det sende en advarsel til skolens it-medarbejdere. Dette giver administratorerne mulighed for at undersøge problemet og igangsætte handlinger, der kan modvirke truslen.

Derudover kan advarsels- og kontrolværktøjer bruges til at opnå en dybere forståelse af de trusler, som skolerne står over for. Ved at analysere data fra disse realtidssystemer kan skolerne identificere tendenser og mønstre, der kan hjælpe dem til bedre at beskytte sig selv.

Her kan du se nogle af de bedste praksisser for anvendelsen af advarsels- og kontrol systemer (inkl. sikkerhedsinformation og hændelsesstyring):

1. **Definer dine sikkerhedsmål**
   Identificer, hvilke oplysninger og systemer der er mest kritiske for skolen, samt hvilke typer trusler der udgør den største risiko for dem. Arbejd derefter på at identificere de data, du skal indsamle for at kontrollere disse trusler.
2. **Find de rigtige data, og konfigurer programmerne korrekt**
   Det er vigtigt at indsamle de rigtige data og konfigurere programmerne, så de understøtter dine mest relevante sikkerhedsmål. Dette kan omfatte data fra firewalls, indholdsfiltre, systemer til registrering af indtrængen, webservere og andre sikkerhedsenheder samt kommunikations- og samarbejdssoftware, skoleinformationssystemer og undervisningssystemer.
3. **Undersøg og reager på advarsler**
   Når dit kontrolsystem genererer en advarsel, er det vigtigt at undersøge problemet og igangsætte passende foranstaltninger. Dette kan betyde, at man bringer flere teams sammen for at undersøge advarselskilden, så man kan afgøre, om det er en falsk positiv, eller om man skal træffe foranstaltninger or at modvirke truslen, f.eks. suspendering af konti, nulstilling af brugeradgangskoder, karantæne eller sletning af mails, ændring af filtilladelser eller rydning af enheder.

Undervis undervisere, medarbejdere og elever

Grundskoler og ungdomsuddannelser bør øge bevidstheden og vanerne omkring sikkerhed i skolefællesskaberne ved at anvende kampagner og partnerskaber til at styrke brugerne. Uddannelse af undervisere, medarbejdere og elever i vigtigheden af sikkerhed er afgørende for at hjælpe dem med at beskytte sig selv online og forhindre alvorlige onlinesikkerhedstrusler. Lær dem, hvordan de anvender de produkter og tjenester, der er implementeret på tværs af uddannelsesinstitutionen, hvordan de genkender og rapporterer trusler som phishingmails og vigtigst af alt, hvordan de skal handle for at forhindre disse angreb. Skoler og distrikter bør øge brugernes bevidsthed og vaner omkring sikkerheden i skolefællesskaberne ved at bruge kampagner og partnerskaber til at styrke deres brugere.

Sådan bruger du enheder og software sikkert

Administratorerne kan samarbejde med undervisere og eksperter om at udvikle et pensum om alderssvarende onlinesikkerhed, som kan hjælpe eleverne med at forstå, hvordan de bruger enheder, software, og systemer sikkert. Udarbejdelsen af undervisningsmaterialer hjælper dine undervisere og elever med at kontekstualisere anbefalingerne, men du kan også med fordel anvende materiale, der allerede er tilgængeligt, f.eks. Be Internet Awesome, der er tilgængelig på Safety.Google og Khan Academy, og tilpasse det efter dine behov. Disse programmer kan hjælpe dine brugere med at opretholde sikkerheden, uanset hvor de er – i skolen eller inden for deres fællesskab.

Trusselsgenkendelse

Uddannelse af undervisere, medarbejdere og elever i at identificere trusler er en vigtig del af at opretholde sikkerheden for dem. Det er vigtigt at lære børn, hvordan de kan afgøre, om noget er en trussel eller ej, da de måske ikke ved, hvordan man kan se, om noget er legitimt. Der er nogle få typer trusler, som de bør kunne identificere. De skal vide, hvordan de rapporterer dem, og administratorerne bør fokusere på de emner, som de mener, vil give det største udbytte. Det er vigtigt, at brugerne ikke kun lærer at identificere truslen, men at de også lærer, hvordan man skal forholde til sig den. Almindelige trusler, som brugerne bør genkende, omfatter ransomware, phishing, social manipulation, malware og svindel. Hvis bestemte trusler er mere udbredte inden for en given uddannelsesinstitution, er det værd at sikre, at skolens brugere orienteres om de specifikke trusler.

Sikker deling af filer og data

Undervisere og medarbejdere bør undervises i passende deling af filer og data, og om hvordan man genkender upassende anmodninger via mail. Det er vigtigt, at de sikrer, at følsomme personlige oplysninger kun deles eller behandles, når det er nødvendigt, og med yderligere datbeskyttelseslag, så de f.eks. aldrig bliver delt via mail eller med eksterne parter. De bør anvende unktioner til forebyggelse af datatab (inkluderet i ChromeOS og Workspace for Education) til at advare og forhindre slutbrugerne i at dele filer med følsomme oplysninger (f.eks. personnumre) eller kopiere og indsætte følsomt indhold uden for domænet.

Googles tilgang i praksis: e nheder og tjenester til uddannelsessektoren

Anskaffelse af software er et af de mest kraftfulde værktøjer, et skoledistrikt har til at beskytte sig selv. Software bør være robust udviklet og designet til at minimere sårbarhedsrisikoen – med indbygget sikkerhed på hvert lag. Ved at kræve, at skolerne køber sikker software eller software fra virksomheder med dokumenterede kompetencer inden for sikkerhed, kan den overordnede cyberrisiko reduceres betydeligt. Hos Google har vi f.eks. styrket vores ChromeOS, mens vi løbende implementerer mere proaktive, intelligente løsninger, der udnytter styrken af vores ekspertise inden for maskinlæring, skyen og identitet.

Google har forpligtet sig til at udvikler produkter, der hjælper med at beskytte privatlivet for elever og undervisere, og leverer sikkerhed i topklasse til din uddannelsesinstitution. Du kan være sikker på, at Google for Education-produkter og -tjenester altid beskytter brugere, enheder og data mod mere komplekse trusler. Denne del gennemgår sikkerhedsanbefalingerne ved brug af Google for Education-produkter over for skolernes it-administratorer.

Google Workspace for Education

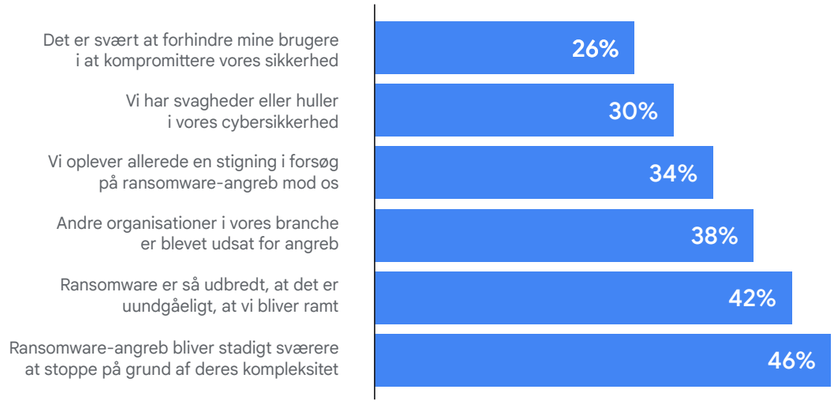
Google Workspace for Education er en pakke med Google-værktøjer og -tjenester, der er skræddersyet til skoler, så de kan samarbejde, strømline undervisningen og gøre det trygt at lære. Google for Education-produkter og -tjenester beskytter løbende brugere, enheder og data mod stadigt mere komplekse trusler og leverer værktøjer som advarsels- og sikkerhedscentre, en vault til eDiscovery, Identity and Access Management samt forebyggelse af datatab.

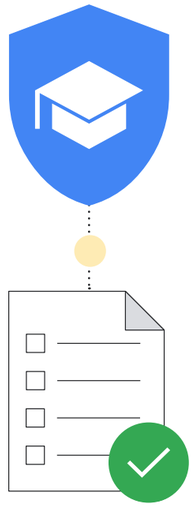
Vi har samlet nyttige materialer, hvis du lige er startet med Google Workspace for Education, og mange af dem kan hjælpe dig med at konfigurere efter anbefalingerne i denne vejledning. Hvis du har brug for hjælp til at komme i gang med Google Workspace for Education, kan du se denne lynvejledning til it-konfiguration.

Sikkerhedstjeklister

Gennemgå sikkerhedstjeklisterne ffor at få flere oplysninger om, hvordan du styrker sikkerheden og privatlivsbeskyttelsenet for din uddannelses institution. De skoler, der anvender Google Workspace for Education Standard og Plus kan også bruge siden Sikkerhedstilstand til at kontrollere konfigurationen af indstillingerne for din Administrationskonsol. Du kan f.eks. tjekke indstillingsstatus som automatisk videresendelse af mail, enhedskryptering, delingsindstillinger for Drev og meget mere. Hvis det er nødvendigt, kan du ændre dit domænes indstillinger på baggrund af de generelle retningslinjer og bedste praksis for sikkerhed, samtidig med at du justerer disse retningslinjer i forhold til din organisation behov og politikker for risikostyring.

Derfor forventer uddannelsessektoren at blive ramt





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

Her er nogle flere nyttige tips til, hvordan du kan optimere den beskyttelse, der er indbygget i Google Workspace for Education:

Opret organisationsenheder

Det giver ikke mening, at alle på din Google Workspace for Education-konto har de samme indstillinger. Organisationsenheder er brugergrupper, som gør det muligt for dig at give forskellige tjenester, indstillinger og tilladelser til forskellige brugere: For eksempel kan du anvende totrinsverificering til undervisere og medarbejdere og alderssvarende godkendelse til yngre elever. Opret separate organisationsenheder til medarbejdere, undervisere og elever, så du kan anvende de relevante politikker for hver af disse brugergrupper. En veldesignet struktur er afgørende for at kunne administrere din Google Workspace for Education-konto effektivt og fleksibelt.

Konfigurer adgangskodepolitikker og beskyttelse for administratorkonti

Som nævnt er brugergodkendelse en afgørende del af at opretholde sikkerheden for din uddannelsesinstitution. Derfor har vi udviklet fleksible måder, administratorerne kan styre godkendelsen, som giver dig mulighed for at sikre, at brugerne har en passende og sikker kontobeskyttelse. Konfigurer adgangskodepolitikker for at sikre, at brugerne opretterlaver stærke adgangskoder, og overvej at kræve anvendelse af totrinsverificering, hvor dette er relevant baseret på de anbefalede grupperinger under afsnittet Secure Sign-On. Du kan håndhæve anvendelsen af totrinsverificering for en undergruppe af brugere (brugerne får tid til at konfigurere dette) og implementere totrinsverificering2SV via en række forskellige metoder, herunder sikkerhedsnøgler (mest sikre), en Google-loginbesked (ved hjælp af Googles apps på Android og iOS), apps, der kan generere sikkerhedskoder til verificering (f.eks. Google Authenticator), og beskeder eller telefonopkald (selvom disse er metoder, der er mindst sikre).

Hvis din organisation bruger en anden identitetsudbyder (IdP) end Google, kan du konfigurere Single Sign-On (SSO) via en tredjepartsidentitetsudbyder. Du kan stadig bruge totrinsverificerin med Single Sign-On til administratorkonti, der ikke er superadministratorkonti, hvis du foretrækker det.

Slå tjenester til eller fra

Administratorerne kan styre, hvilke Google-tjenester brugerne kan tilgå via deres Google Workspace for Education-konto, gennem Google Administrationskonsollen. Du kan styre adgangen til Google-tjenester som Kalender, Drev og Meet ved at slå tjenester til eller fra efter organisationsenhed (du kan også slå tjenester til, når du anvender grupperne). Du kan ligeledes gennemgå forskellene mellem Workspace-kernetjenester og yderligere tjenester, inden du slår tjenester som YouTube, Google Maps og Blogger til. Administratorerne opfordres til at konfigurere adgangen til Googles tjenester baseret på alder. Husk, at de brugere, der er under 18 år, automatisk har begrænsninger på nogle af Googles tjenester, når de er logget ind på deres Google Workspace for Education-konto.

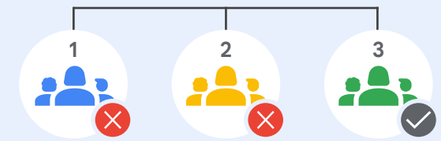
Du kan også bruge Kontekstbevidst adgang (tilgængelig i Workspace for Education Standard og Plus) til at tillade eller blokere adgang til Googles apps som f.eks. Gmail, Drev og Kalender baseret på en enheds IP-adresse, geografiske oprindelse, sikkerhedspolitikker eller operativsystem. Du kan f.eks. give tilladelse, så Drev til computer kun anvendes på virksomhedsejede enheder i bestemte lande/regioner.

Metoder til at give brugerne adgang til tjenester

I Google Administrationskonsol kan du deaktivere en organisationsenheds adgang til en Google-tjeneste som for eksempel Google Drev. Hvis bestemte brugere i denne organisationsenhed har behov for at bruge Drev, har du 2 muligheder:

1. Flyt brugerne til en organisationsenhed, hvor Drev er aktiveret.
2. Føj brugerne til en adgangsgruppe, og aktivér Drev for denne gruppe. Alle gruppemedlemmer kan bruge tjenesten, selvom deres organisationsenhed har slået tjenesten fra.

Organisationsenheder



Google Drev er slået fra for organisationsenhed 1 og 2.

I en adgangsgruppe

Men en **brugergruppe** i organisationsenhed 1 og 2 kan bruge Google Drev

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

Indstil politikker for datadeling og regler for opbevaring

Som administrator kan du styre, om brugerne kan dele Google Drev-filer og -mapper med personer uden for din organisation. Dette kan være med til at forhindre utilsigtet eller for omfattende deling af data og filer, hvilket forhindrer datalæk. Adskillelse af filer og drev, oprettelse af organisatoriske enheder og anvendelse af princippet om minimumsrettigheder er vigtigt for at forhindre hackerne i at bevæge sig på tværs af netværk, hvis de infiltrerer én konto. Jo færre data og jo mindre dele af netværket en potentiel hacker kan tilgå, jo mindre skade kan det forårsage.

Slå ekstern fildeling fra for eleverne (eller begræns ekstern deling til tilladte domæner), og indstil "Adgangstjek" til "Kun modtagere". Hvis du tillader nogle eller alle brugere at dele filer uden for dit domæne, så indstil en advarsel, når en bruger gør dette. Du bør også deaktivere offentliggørelse af filer på nettet og bede eksterne samarbejdspartnere om at logge ind med en Google-konto.

Brugere af Workspace for Education Standard og Plus kan derudover anvende målgrupper og tillidsregler til at angive anbefalinger og begrænsninger for deling på et mere detaljeret niveau. Med målgrupper indstiller du f.eks. standardmålgruppen for linkdeling for underviserne til "undervisere og medarbejdere" i stedet for alle på din uddannelsesinstitution. Med tillidsreglerne kan du blokere eleverne i grundskolen, så de ikke kan dele filer med de ældre elever.

Gennemgå politikkerne for fællesdrev for at sikre, at det kun er de relevante brugere, som kan oprette fællesdrev, og sørg for at forhindre eksterne brugere i at få adgang til fællesdrev. Det anbefales, at du kun giver administratorer (eller medarbejdere og undervisere) tilladelse til at oprette fællesdrev, og at du administrerer adgangen til fællesdrev omhyggeligt.

Tænk over at begrænse synligheden af Indekset og deling af kontakter, når dette er muligt, ved enten at deaktivere delingen af kontakter for nogle eller alle brugere, eller ved at oprette tilpassede indekser for at begrænse, hvilke brugere andre brugere kan se. Konfigurer politikker for forebyggelse af datatabdata (DLP) i Drev og Gmail for at registrere og blokere følsomme oplysninger. Der er integrerede politikker, der kan bruges til at beskytte almindelige følsomme oplysninger (såsom bankoplysninger eller kreditkortnumre). Du kan også oprette tilpassede politikker baseret på søgeord, ordlister og regulære udtryk (regex).

Administrer Gmail-indstillingerne

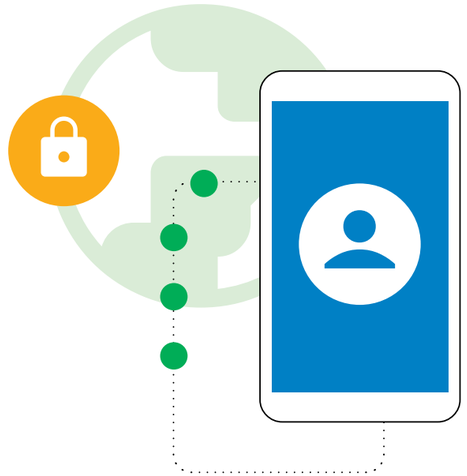
Gmail er én af kernetjenesterne i Google Workspace for Education, og der er mange indstillinger, som administratorerne kan anvende til at beskytte deres uddannelsesinstitution og deres brugere. Undgå spam, spoofing og phishing med Gmail-godkendelse. Tilpas spamfilterindstillingerne, herunder krav om afsendergodkendelse for alle godkendte afsendere og deaktivering af omgåelse af spamfiltre for interne afsendere.

Deaktiver POP/IMAP-adgangen når det er muligt, og aktivér forbedret scanning af meddelelser inden levering og avanceret beskyttelse mod phishing og malware. Hvis du tillader eksterne mails for nogle eller alle brugere, kan du aktivere advarsler om eksterne modtagere.

Brugere af Google Workspace for Education Standard og Plus kan også hjælpe med at beskytte mod malware og ransomware ved at oprette regler til at opdage skadelige vedhæftede filer med Sikkerhedssandbox.

Tredjepartsapps

Brug indbyggede godkendelsesarbejdsgange til at godkende tredjepartsapps, der får adgang til kontodata via API'er. Dette hjælper med at forhindre uautoriserede data i at blive delt med tredjepartsapps, der ikke er godkendt til skolebrug.



Rapporter og kontrol

Som administrator kan du se rapporter og hændelseslogger i Google Administrationskonsol for at gennemgå aktiviteten i din organisation, f.eks. potentielle sikkerhedsrisici, se, hvem der logger ind og hvornår, og forstå, hvordan brugerne opretter og deler indhold. Du kan se data på domæneniveau sammen med detaljer på brugerniveau gennem grafer og tabeller. Se rapporter og auditlogger (herunder Underretningscenter) for at identificere sikkerhedsrisici, analysere anvendelsen af tjenester, diagnosticere konfigurationsproblemer, spore brugeraktivitet og meget mere.

Administratorer af Google Workspace for Education Standard og Plus kan anvende sikkerhedskontrolpanelet til at få en oversigt over forskellige sikkerhedsrapporter, identificere tendenser og sammenligne nuværende og historiske data, ff.eks. fildeling i Drev, spam-, phishing- og malwareaktivitet i Gmail, mistænkelige brugerkontologin og mistænkelige enhedsaktiviteter. De fleste logger for brug og aktivitet samt auditlogger – herunder hændelseslogger for Administrator, Drev, Meet og Chat – og sikkerhedsrapporter er tilgængelige i seks måneder.

Brug sikkerhedscenteret

Administratorer i Google Workspace for Education Plus og Standard kan bruge sikkerhedscenteret, hvor de kan få avancerede sikkerhedsoplysninger og analyser, og som giver yderligere synlighed og kontrol i forbindelse med sikkerhedsproblemer, som påvirker dit domæne.

Sikkerhedscenteret har et værktøj til sikkerhedsundersøgelse, der kan hjælpe administratorerne med at identificere, prioritere og handle på problemer i forbindelse med sikkerhed og privatlivsbeskyttelse, f.eks. phishingangreb, upassende fildeling, mistænkelig bruger- eller enhedsaktivitet og meget mere.

Google Workspace er verdens mest sikre skybaserede kommunikations- og samarbejdspakke

0

aktivt udnyttede softwaresårbarheder i Workspace siden november 2021*

50%

potentielle besparelser på forsikringspræmier i forbindelse med cybersikkerhed ved brug af Workspace

2x

så mange sikkerhedshændelser for de organisationer, der bruger Workspace, i forhold til dem, der bruger Microsoft 365

2.5x

færre sikkerhedshændelser for de organisationer, der bruger Workspace, i forhold til dem, der bruger Microsoft Exchange

*Ifølge CISA er dette markant mindre end andre produktivitetsleverandører på dette område.

Google Chromebooks for Education

Chromebooks er computere til elever og undervisere, der er yderst sikre, skalerbare og brugervenlige, takket være Chromebooks indbyggede sikkerhedsfunktioner, der er klar til brug. Der har aldrig været rapporteret et ransomwareangreb på en ChromeOS-enhed fra virksomheder, skoler eller forbrugere. Chromebooks hjælper med at beskytte skolerne mod nye trusler med opdaterede funktioner, og opdateringerne sker automatisk i baggrunden, så brugerne kan komme tilbage til arbejdet på få sekunder.

Automatiske opdateringer af operativsysteme og apps med indbygget malwarebeskyttelse

Hackerne forsøger konstant at udnytte fejl og smuthuller i operativsystemer, browsere og populære apps til at installere malware og stjæle brugeroplysninger. For at beskytte dig og dine brugere holder Chromebook dit operativsystem og dine apps opdateret, fordi den er udviklet sikkert som standard med sikkerhedsopdateringer – og apps i skyen behøver aldrig softwareopdateringer, som lokale apps gør. Den Google-designede sikkerhedschip på Chromebooks hjælper med at holde enhederne sikre, beskytte brugeridentiteten og sikre systemets integritet

Chromebooks i din flåde kører automatisk de nyeste opdateringer til malwarebeskyttelse. Elever og undervisere er beskyttet mod cybertrusler med indbyggede sikkerhedsfunktioner som datakryptering, verificeret opstart, sandbox og automatiske opdateringer.

Sikre brugeroplysninger

Når du logger ind på en Chromebook med din Google-konto, gemmes alle dine data i krypterede filer, hvilket sikrer, at ingen andre på enheden kan se dine data eller logge ind på apps via din konto. Dette gør det meget nemt og sikkert for eleverne at dele enheder i et klasseværelse, og for skolerne at reducere deres samlede omkostninger til computere. For mere avancerede sikkerhedsfunktioner byder enhedsadministrationslicensen Chrome Education Upgrade på forbedret synlighed.

Fjernkonfiguration af sikkerhedspolitikker på brugeradministrerede enheder

Skoleadministratorerne kan konfigurere ChromeOS-politikker og installere/opdatere apps på afstand med Google Administrationskonsol. Med et klik på en knap kan é enkelt it-administrator opdatere politikker og konfigurationer affor hundredtusindvis af Chromebooks på et øjeblik.

Dette sikrer at:

- Eleverne kun har adgang til indhold og apps, som er godkendt af skolen
- Alle apps og udvidelser er opdateret med de nyeste sikkerhedsrettelser
- Brugerne ikke kan kopiere, overføre eller dele skolerelaterede data uden for enheden
- Man kan træffe databaserede beslutninger med tilpassede sikkerhedsanbefalinger fra Google for at modvirke sikkerhedstrusler
- Man kan administrere sikkerhed og identitet centralt og tilgå administrationspolitikkerne for alle brugere i Administrationskonsollen

Nogle fremhævede politikker, som administratorerne bør overveje at konfigurere, er:

Enhedspolitikker

- **Gæstetilstand**
  Det anbefales, at du deaktiverer dine enheders gæstetilstand, så elever og undervisere skal logge ind med deres egne loginoplysninger i stedet for at bruge enheden anonymt.
- **Begrænsninger for login**
  Du vil måske ikke have, at dine elever og undervisere logger ind på din skoles Chromebooks med deres personlige Gmail-konti. Håndhæv loginbegrænsninger til kun at omfatte dit Workspace-domæne for de enheder, der udelukkende bruges af elever.
- **Bruger- og enhedsrapportering**
  Administratorerne bør overveje at aktivere bruger- og enhedsrapporteringen, så de kan indsamle metrics om, hvor ofte deres Chromebooks bliver brugt, hvem der bruger dem, og tilstanden af deres hardware.
- **Tvungen gentilmelding**
  Det er afgørende, at en Chromebook, der tilhører en skole, bliver på skolen, medmindre en administrator deprovisionerer den. Administratorerne bør overveje at aktivere tvungen gentilmelding af Chromebooks, så en Chromebook altid vil gentilmelde sig selv, hvis den skulle gå hen og blive slettet eller forsøgt stjålet.

Brugerpolitikker

- **Inkognitotilstand**
  Eleverne skal have de bedste muligheder for at få succes, når de bruger Chromebooks til skoler. Dette indebærer, at de begrænses til deres godkendte browser, så webindholdsfiltre kan holde dem væk fra upassende websites. Administratorerne bør deaktivere inkognitotilstanden, så eleverne ikke kan omgå webfiltrene.
- **Proxytilstand**
  Nogle skoler kan bruge proxyer til webfiltrering, og her er det vigtigt at deaktivere mulighederne for, at dine brugere selv kan ændre proxyindstillingerne.
- **Samlet login fra flere konti**
  Hvis brugerne har tilladelse til at logge ind på en sekundær konto, mens de bruger din skoles Chromebooks og Workspace-konti, kan det give en bruger mulighed for nemt at flytte følsomme elev- eller skoledata/-oplysninger til den sekundære konto. Administratorerne bør overveje at blokere samlet login fra flere konti.
- **Browserhistorik**
  For eleverne kan det være nyttigt at deaktivere funktionen til at rydde browserhistorikken. Hvis der forekommer en sikkerhedshændelse på internettet, kan disse logfiler med internethistorik være nyttige under en undersøgelse.

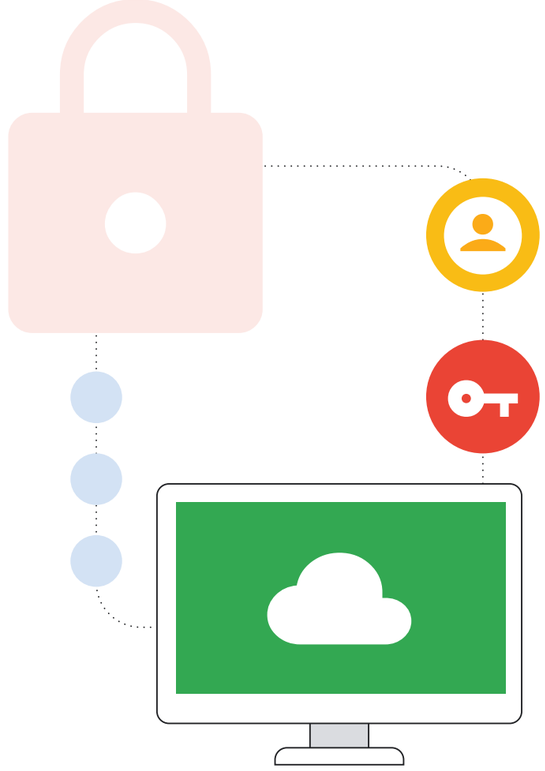
Denne liste er et godt udgangspunkt, når du vil sikre, at dine netværk er beskyttet mod de mest almindelige typer fejl, der kan føre til alvorlige cyberhændelser. Du kan finde flere anbefalede sikkerhedspolitikker på vores Sikkerhedstjekliste.

Slutpunktsadministration for sikker anvendelse når som helst og hvor som helst

Systemet til fjernadministration af politikker i ChromeOS gør det muligt for skoleadministratorerne at anvende sikkerhedsindstillinger og køre sikkerhedsværktøjer, f.eks. indholdsfiltreringssystemer, på enheden i stedet for på skolens netværksservere. Dette sikrer, at eleverne får de samme sikkerhedsfordele på skolens Chromebooks derhjemme, som de gør i klasseværelset. Efterhånden som skolerne migrerer mod digitale lærebøger og onlinelæringsværktøjer, bliver dette vigtigere, fordi eleverne skal have computeren med hjem for at kunne lave deres lektier.

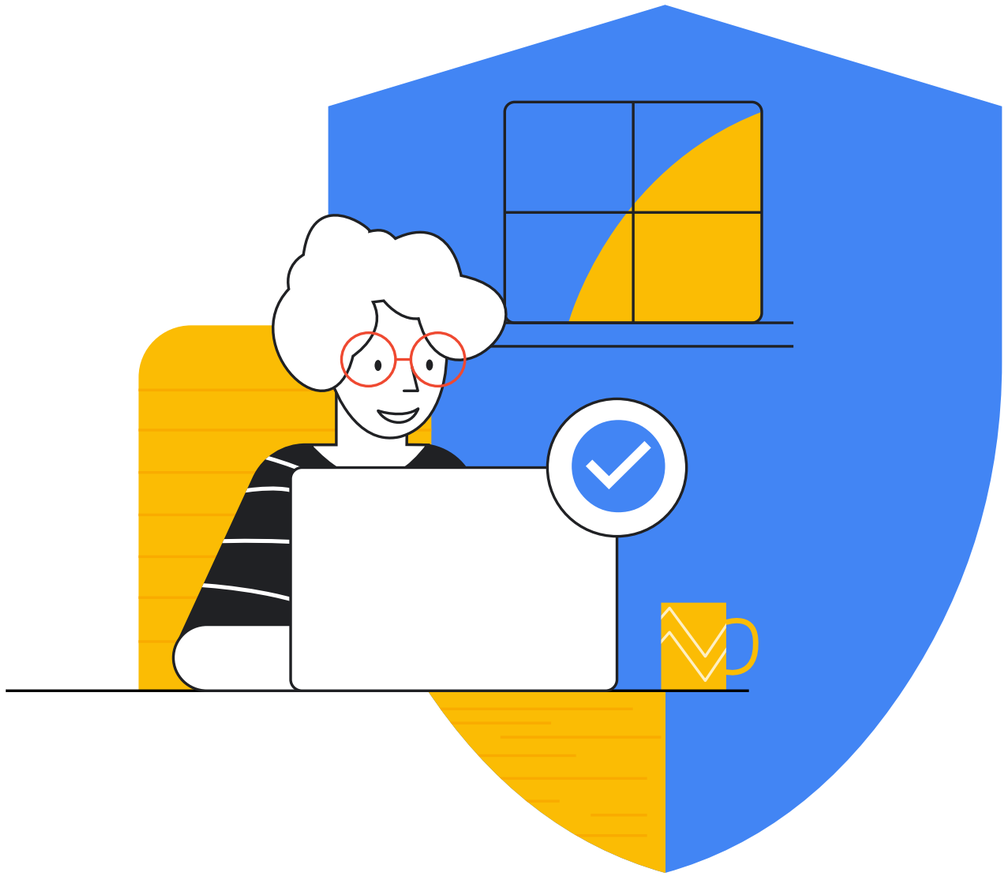
Konklusion

Udfordringerne med at sikre grundskoler og ungdomsuddannelser mod cyberhændelser er en kompleks opgave, men det er værd at investere i at beskytte sig selv, elever, undervisere, medarbejdere og det bredere onlineøkosystem. De punkter, der er gennemgået i dette dokument, er en god start, men hver enkelt skole er nødt til at tilpasse anbefalingerne til deres unikke behov og fortsætte med at holde sig opdateret i forhold til et voksende trusselslandskab og de nye teknologier. Denne ressource danner et godt grundlag for et sikkerhedsprogram til enhver grundskole og ungdomsuddannelse. Den kan fungere som et udgangspunkt for eventuelle næste skridt og implementerbare handlingspunkter. Google har også en række ressourcer, kurser og dygtige onlinesikkerhedsprofessionelle til rådighed, som kan hjælpe skoler og organisationer med at følge denne vejledning og med nye teknologier som f.eks. AI. Googles produkter er skræddersyet til uddannelsessektoren og leverer færdige løsninger til mange af de faldgruber, der er relateret til onlinesikkerhed, som er beskrevet i dette dokument. Vi glæder os til at samarbejde med dig, når du designer og implementerer dine sikkerhedsprogrammer.



Liste over ressourcer

- Google. "Værktøjer og tips til sikkerhed online." Google Sikkerhedscenter, https://safety.google/security/security-tips/. Tilgået den 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. Tilgået den 6. oktober 2022.
- Microsoft. "Microsoft AccountGuard." Microsoft AccountGuard, https://www.microsoftaccountguard.com/en-us/. Tilgået den 6. oktober 2022.
- Google. "Programmet Avanceret beskyttelse." Googles stærkeste sikkerhedsfunktion er med til at beskytte dine private oplysninger., https://landing.google.com/advancedprotection. Tilgået den 6. oktober 2022.
- Google. "Google Sikkerhedscenter." En sikrere måde at søge, https://safety.google. Tilgået den 6. oktober 2022.
- Meta. "Meta Basics: Help Secure Your Account." Meta Basics: Secure Your Account, https://www.facebook.com/gpa/resources/basics/security. Tilgået den 6. oktober 2022.
- Meta. "Facebook Protect." Facebook, https://www.facebook.com/gpa/facebook-protect. Tilgået den 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. Tilgået den 6. oktober 2022.
- Passwordless login with passkeys: https://developers.google.com/identity/passkeys
- CISA's rapport "Protecting Our Future" om onlinesikkerhed i grundskoler og på ungdomsuddannelser https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- GAO-rapport https://www.gao.gov/products/gao-20-644
- Du kan få flere oplysninger om, hvordan Google for Education kan hjælpe dig med at beskytte din uddannelsesinstitution, i Google for Educations Privatlivs- og sikkerhedscenter.
- Zcalers rapport vedrørende phishing



Google for Education