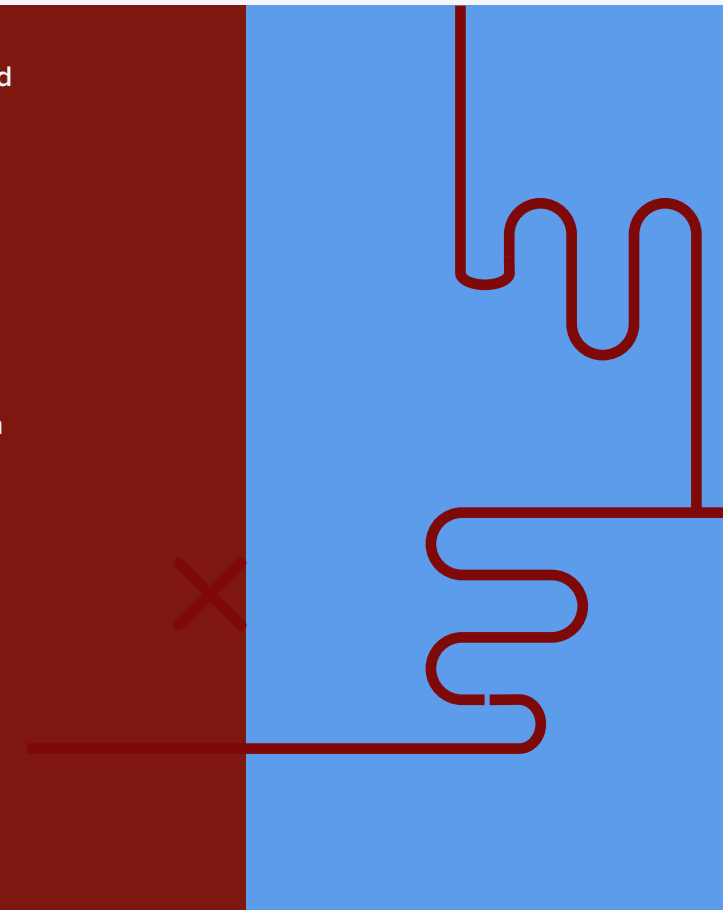
Beveiliging voor het onderwijs voor beginners

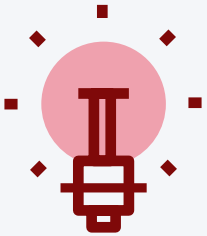
jamf

Er zijn maar weinig sectoren die de transformerende invloed van technologie zo voelen als het onderwijs.

De vooruitgang op het gebied van personal computing en de ontwikkeling van cloud-gebaseerde diensten hebben een revolutie teweeggebracht in een aantal basisprincipes van de manier waarop leren plaatsvindt, zoals:

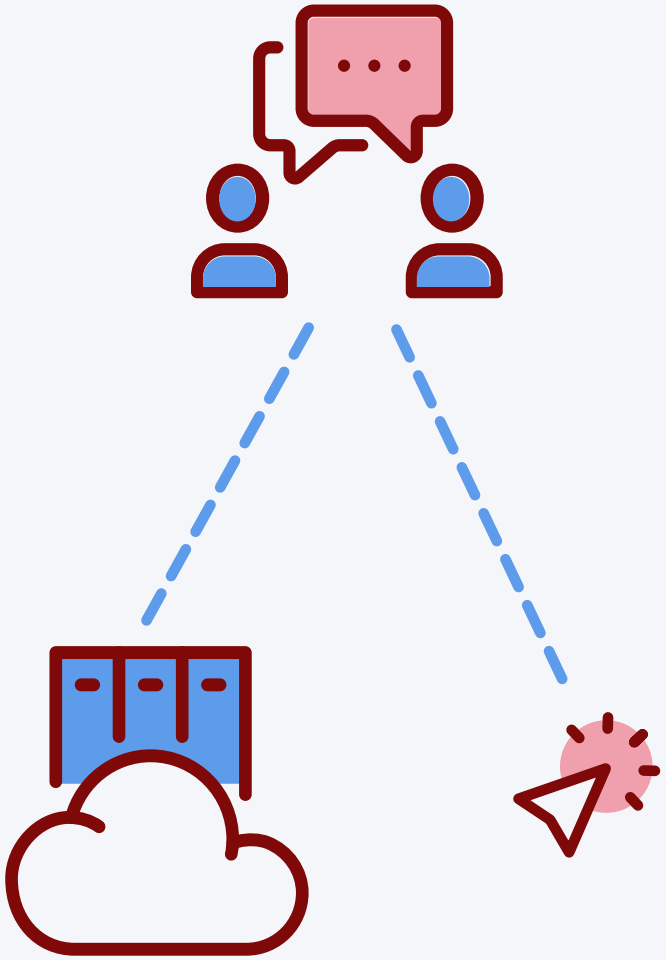
- De toegang tot boeken en bronnen is exponentieel gegroeid en overstijgt de fysieke beperkingen.
- Globale communicatielijnen tussen leerlingen, leerkrachten en ouders zijn onmiddellijk beschikbaar.
- Gestandaardiseerde tests zijn gestroomlijnd door over te stappen op computergebaseerde modellen.
- De uiteenlopende behoeften van leerlingen kunnen worden aangepakt via één gemeenschappelijk apparaat met gespecialiseerde apps.
- Convergentie tussen meerdere onderwijsmodaliteiten en onderwijsstijlen kan worden bereikt door meerdere technologische instrumenten te integreren.
- Afstandsonderwijs is een levensvatbare onderwijsmethode gebleken, ondanks een aanhoudende pandemie of een andere wereldwijde crisis.





Een visie creëren

Het is duidelijk dat technologie in haar geheel is omarmd door het basis- en middelbaar onderwijs vanaf het eerste moment, toen een van de eerste computers van Apple, de Apple IIe, jonge geesten in 1983 leerde optellen, lezen en typen. Die kinderen zijn nu volwassenen - en in sommige gevallen zelf leerkrachten – die deze praktijk voortzetten door de nieuwste MacBook Air en iPad te gebruiken, naast een groeiende catalogus van bijna 2 miljoen apps, om de leerlingen van nu onderwijs te geven.

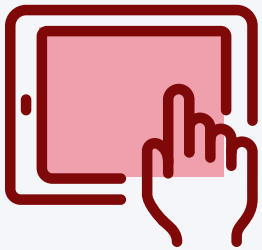


In tegenstelling tot veertig jaar geleden, toen cyberbeveiliging nog niet eens een term was om rekening mee te houden, is het moderne computerlandschap vandaag de dag totaal anders. Zelfs vijftien jaar geleden was het niet zoals nu, met talloze bedreigingen voor de beveiliging van je apparaten. Van het beperken van de toegang tot kritieke gegevens en diensten door deze te infecteren met ransomware, tot het in gevaar brengen van leerlingdossiers en gevoelige gegevens door datalekken – de huidige bedreigingen kunnen zelfs een aanzienlijk veiligheidsrisico vormen door het ongeoorloofd buitmaken van privacygegevens.

Dit e-book is niet bedoeld om angst aan te jagen, maar om mensen bewust te maken van de zeer reële en soms angstaanjagende beveiligingsproblemen in het onderwijs.

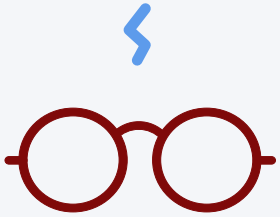
Een visie creëren

En daarnaast nemen we ook even afstand nemen van de engere elementen, want bedreigingen komen vaker tot uiting in het verlies van het gebruik van apparaten en/of beperkte toegang tot middelen. Al deze vertragingen verhinderen natuurlijk dat er geleerd wordt! Bovendien zijn de voorschriften die zijn ingevoerd om deze situaties te voorkomen, soms gekoppeld aan financieringsstructuren die rechtstreeks van invloed zijn op het vermogen van een school om het niveau van dienstverlening te bieden dat hun belanghebbenden en de gemeenschap vereisen, als een inbreuk op de voorschriften is vastgesteld.



In dit e-book gaan we in op de unieke cyberbeveiligingsbedreigingen die van invloed zijn op basis- en middelbaar onderwijs, benadrukken we waarom het zo belangrijk is om ze proactief aan te pakken.

- **Kijk naar de cruciale rol die cyberbeveiliging tegenwoordig speelt – en in de toekomst van het onderwijs.**
- **De externe en interne bedreigingen illustreren die de meerderheid van de kwaadaardige aanvallen op het onderwijs vormen.**
- **Ga na welke praktijken kunnen worden versterkt om apparaten, vertrouwelijke gegevens en leerlingen te beschermen.**
- **Pak voorkomende misvattingen over Apple en beveiliging aan.**
- **Bespreek hoe opleidingsprogramma's voor belanghebbenden bijdragen tot succesvolle cyberbeveiligingsprogramma's.**
- **Leg uit hoe de oplossingen van Jamf de risico's beperken en tegelijkertijd je eindpunten uitgebreid beveiligen.**

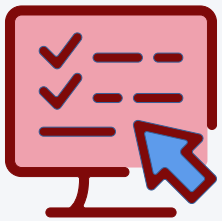


Welkom op Zweinstein

In de tovenaarswereld van Harry Potter gaat de hoofdpersoon, een leerling met een ongelooflijk potentieel, naar Zweinstein, waar hij en zijn medescholieren een opleiding krijgen in de verschillende aspecten van magie. Maar dat is niet het geheel van kennis die de leerkrachten overbrengen, toch?

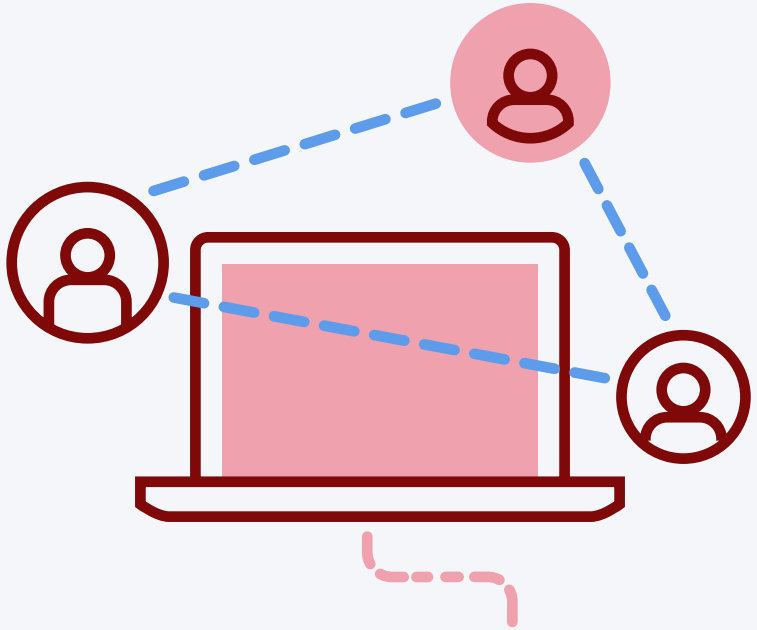
Nee, dat is het niet. In feite beginnen de leerlingen van Zweinstein, net als de echte tegenhangers op scholen, aan een reis van kennis in veel verschillende onderwerpen gedurende hun tijd op school. Sommige zijn academisch, andere extra-curriculair - maar alle vormen een hechte en samenhangende band die een alomvattende, evenwichtige opleiding vormt.

Welnu, cyberbeveiliging en de manier waarop die aansluit bij de unieke behoeften en vereisten van de onderwijssector, indien succesvol geïmplementeerd, werkt ongeveer hetzelfde. Er is immers niet één toverspreuk, zoals Lumos, die de geheimen van eindpuntbescherming belicht. In plaats daarvan werkt een verzameling hulpmiddelen, gecombineerd met best practices en opleiding van eindgebruikers, samen om de beveiliging van de infrastructuur van je school op peil te houden.



Waarom is cyberbeveiliging zo belangrijk?

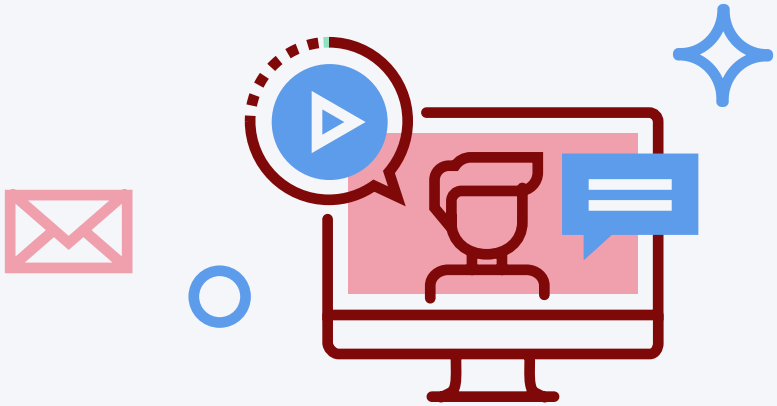
Afgezien van de eerdergenoemde redenen om de veiligheid, vertrouwelijkheid en integriteit van je eindpunten — leerlingen, gegevens en apparaten — te waarborgen, wordt het belang van cyberbeveiliging vergroot door enkele onderwijsspecifieke uitdagingen die organisaties er soms van weerhouden de juiste oplossingen te implementeren om kwaadaardige bedreigingen te beperken en aanvallen te bestrijden.



Budgettaire beperkingen

In een artikel van Forbes over hoe Amerikaanse scholen worstelen met de financiering van onze toekomst wordt opgemerkt dat 'staten die zowel billijkheid als toereikendheid hebben bereikt, sterkere prestaties en slagingspercentages zien...'. Als je een willekeurige vraagt die ooit op zoek is geweest naar een vervangende lamp voor zijn LCD-projector of een sterker access point om het aantal gebruikers dat verbinding maakt met wifi aan te kunnen, heeft hij meestal te horen gekregen dat een gebrek aan financiële middelen de boosdoener is waarom hij niet kreeg wat hij vroeg.

Budgettaire overwegingen liggen vaak aan de basis van infrastructuurupgrades om netwerkapparatuur te updaten voor snellere connectiviteit of om meer apparaten te ondersteunen naarmate een scholengroep een 1:1 apparaatmodel invoeren, evenals de aanschaf van beveiligingsdiensten die malware detecteren en voorkomen op schoolapparatuur.



Oude infrastructuur

In combinatie met budgettaire beperkingen worden scholen vaak gedwongen 'meer te doen met minder'. Dit betekent dat verouderde, achterhaalde apparatuur in gebruik blijft, lang nadat een leverancier de ondersteuning ervan heeft stopgezet. Hoewel deze verouderde apparaten technisch gezien nog steeds werken, beschikken ze vaak niet over de middelen die nodig zijn om te voldoen aan de minimumeisen van moderne apps en diensten, zoals computergestuurd testen (CBT).

Andere keren staan de apparaten zelf op het randje van de bruikbaarheid en veroorzaken ze allerlei problemen voor leerlingen en leerkrachten. Nog erger is het feit dat deze oudere apparaten en apps niet langer worden ondersteund, wat betekent dat beveiligingspatches die normaliter bugs in de software corrigeren en kwetsbaarheden dichten die door kwaadwillenden worden gebruikt om ongeoorloofde toegang tot gegevens te krijgen, niet worden gecorrigeerd. Dit laat een gapend gat in de beveiliging zonder een verdedigingsmiddel totdat nieuwe apparatuur en/of toepassingen worden aangeschaft.

Schaduw-IT

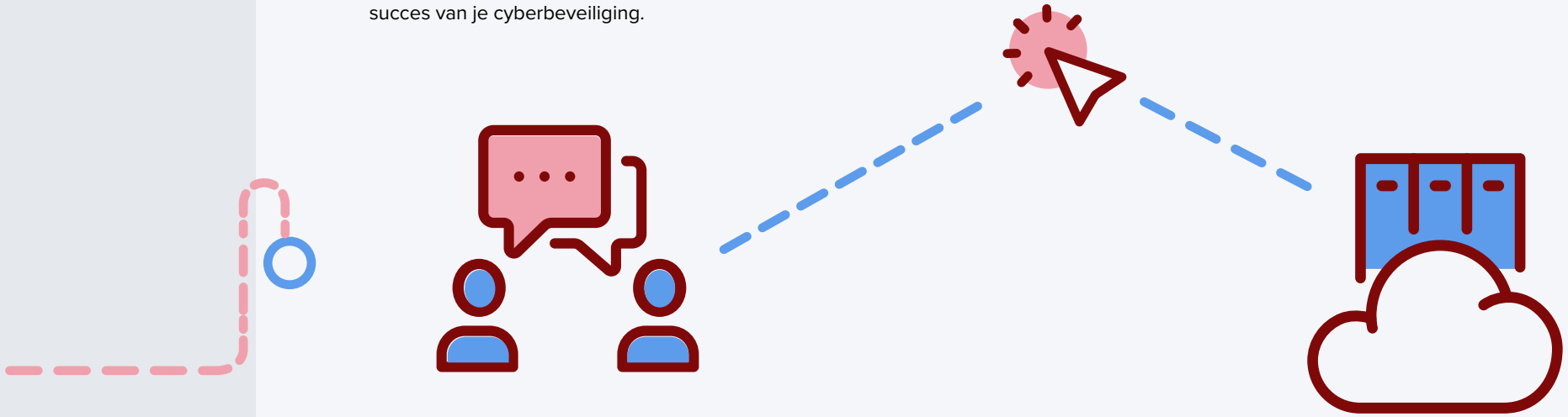
De definitie van schaduw-IT is het gebruik van elk type informatietechnologisch apparaat, app of dienst dat niet wordt beheerd of goedgekeurd door de IT-afdeling van de school. Dit kan en zal verwijzen naar het binnenbrengen van een persoonlijke computer die de strikte configuraties van door de school uitgegeven apparaten omzeilt, je eigen wifi-router van thuis om de draadloze bandbreedte in je klaslokaal of kantoor 'toe te voegen of uit te breiden' en elke toepassing of dienst die wordt gebruikt in combinatie met het werk als leerling of leerkracht die niet is goedgekeurd voor gebruik, zoals een persoonlijke Dropbox.

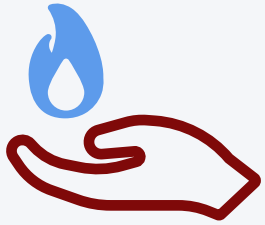
Dit lijkt onschuldig genoeg, vooral wanneer budgettaire overwegingen de toegang beperken tot technologie die het leven gemakkelijker maakt, maar het kan leiden tot een enorm probleem. Deze apps/diensten zijn niet goed doorgelicht om na te gaan of het gebruik ervan binnen het netwerk van de scholengroep problemen of risico's oplevert.

Gebrek aan beveiligingsbewustzijnstraining

Wie heeft de tijd om over beveiliging te leren, naast het voorbereiden van de klas, het oplossen van kleine (en minder kleine) problemen, de zorg voor leerlingen, het opstellen van lesplannen, het nakijken van toetsen en, weet je wel, lesgeven? We weten het, het is moeilijk!

Helaas weten bedreigers dit ook en maken zij hier niet alleen handig gebruik van, maar rekenen zij ook voortdurend op tijdgebrek en het gebrek aan beveiligingsbewustzijnstraining om de onderwijssector aan te vallen. Je personeel, leerlingen en ouders trainen in het actief herkennen van schadelijke content via e-mail of oplichting via sms, en het ontwikkelen van betere hygiënepraktijken op school en thuis, is essentieel voor het succes van je cyberbeveiliging.





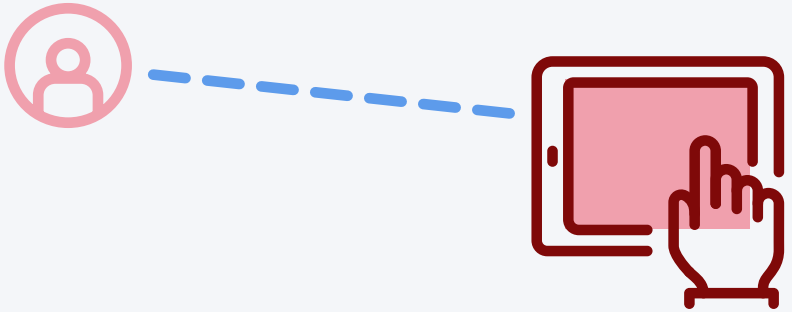
"Hij die niet genoemd mag worden"

De eerste stap die de tovenaars in de Harry Potter-serie namen om hun angsten onder ogen te zien, was het erkennen ervan en het personifiëren ervan bij naam: Voldemort. Pas toen dit gebeurd was, konden de hoofdpersonen zich verdedigen tegen het kwaad dat hen bedreigde.

Evenzo is een van de eerste dingen die je bij cyberbeveiliging moet doen een risicobeoordeling uitvoeren om te bepalen welke apparatuur, apps, diensten, enz. door scholen worden gebruikt, hoe vaak, in welke mate en hoe het scoort op basis van de kriticiteit ervan. Zodra dit is gebeurd, kun je vervolgens 'je angsten onder ogen zien' door te weten welke soorten bedreigingen van invloed zijn op de punten in je risicobeoordeling.

Hoewel deze lijsten kunnen, en zullen, veranderen afhankelijk van de infrastructuurbehoeften van je scholen, zijn er verschillende bedreigingen die algemeen worden aanvaard als zijnde gericht op het basis- en middelbaar onderwijs.

Externe bedreigingen



Van de verschillende soorten bedreigingen die van externe bronnen uitgaan, zijn sommige van de meest ontwrichtende afkomstig van bepaalde soorten malware en Denial of Service (DoS)-aanvallen. Deze laatste probeert de toegang tot toepassingen, diensten en websites te verhinderen door een stortvloed van verzoeken naar de beoogde dienst te sturen, waardoor deze in wezen niet meer kan reageren op — al dan niet legitieme — verzoeken. Tot overmaat van ramp kunnen dit soort aanvallen via meerdere computers worden versterkt tot een Distributed Denial of Service (DDoS), waardoor het veel moeilijker wordt zich ertegen te beschermen.

De eerste bedreiging is gebaseerd op een type malware genaamd ransomware dat zijn naam krijgt door veelgebruikte bestandstypen, zoals DOCX en PDF, te versleutelen met een willekeurig gegenereerde sleutel. Zodra dit is gebeurd, seint de malware terug naar een externe server waar een verzoek wordt gedaan om uw documenten te ontsleutelen of te ontgrendelen in ruil voor een geldelijke betaling. Deze kunnen variëren van duizenden euro's tot miljoenen euro's.

> **'57% van de gerapporteerde ransomware-incidenten betrof scholen in het basis- en middelbaar onderwijs - meer dan twee keer het aantal ransomware-aanvallen op scholen dat in de eerdere maanden van 2020 werd gerapporteerd.'**
>
> - Gezamenlijk advies inzake cyberbeveiliging, opgesteld door het Federal Bureau of Investigation (FBI), het Cybersecurity and Infrastructure Security Agency (CISA) en het Multi-State Information Sharing and Analysis Center (MS-ISAC)

Andere externe bedreigingen en aanvallen die vaak gericht zijn op onderwijsystemen zijn:

Malware: Een algemene classificatie voor alle stukken kwaadaardige code, zoals een virus dat op een apparaat draait met als doel ongeoorloofde toegang te verkrijgen tot het apparaat en/of gegevens, en degenen die ermee verbonden zijn binnen hetzelfde netwerk.

Spyware: Dit type malware werkt discreet terwijl het informatie over de gebruiker verzamelt. Het verkrijgt gegevens, zoals documenten, foto's en zoekt vaak naar persoonlijk identificeerbare informatie (PII) die later door aanvallers kan worden verkocht, zoals burgerservicenummers, leerlingdossiers, opnames van ingebouwde camera's en microfoons, locatiegegevens, kredietkaartgegevens en financiële gegevens.

Man-in-the-Middle (MitM): Wanneer je verbinding maakt met het wifi-netwerk van je school, weet je dan of het verbinding maakt met de juiste dienst? Het doel van MitM-aanvallen is gebruikers te verleiden om verbinding te maken met een website of dienst van een aanvaller die zich voordoet als een legitieme, om gegevens te verzamelen die later worden gebruikt om verdere toegang te krijgen tot bronnen in het district.

Phishing: Net als MitM hierboven, berust phishing ook op social engineering om een gebruiker voor de gek te houden, maar niet noodzakelijkerwijs via technologie. Vaak vinden deze aanvallen plaats via e-mail, sms en ouderwetse telefoongesprekken, waarbij gebruikers worden overgehaald (of bedreigd) met boetes, om hen zover te krijgen dat zij gevoelige informatie prijsgeven die later wordt gebruikt om systemen verder te compromitteren en gegevensinbreuken uit te voeren.

Scannen op kwetsbaarheid: Op basis van een legitiem IT-proces helpt het scannen op problemen teams om te bepalen welke problemen er bestaan, zodat ze kunnen worden opgelost voordat ze leiden tot een beveiligingsincident. Bedreigers hebben toegang tot dezelfde tools als de goedwillenden en gebruiken die om actief vast te stellen welke apparaten kwetsbaar zijn, om vervolgens die zwakte aan te vallen.

Communicatiekaping: Aanvallen op populaire video- en communicatiesoftware, zoals Teams en Zoom, doen zich voor wanneer ruimtes verkeerd geconfigureerd zijn, waardoor externe aanvallers de communicatie kunnen verstoren, gesprekken in gevaar kunnen brengen, het welzijn van scholieren in gevaar kunnen brengen en/of gevoelige informatie kunnen blootleggen.

Interne bedreigingen

Voor alle duidelijkheid: elk van de bovengenoemde externe bedreigingen kan worden gebruikt als een interne bedreiging. De twee sluiten elkaar niet uit, maar de beslissende factor is waar de dreiging vandaan komt: van de interne gebruiker of van een externe, onbekende entiteit. Dit gezegd zijnde, volgt hier een lijst van veel voorkomende interne bedreigingen voor het onderwijs:

Social Engineering: Hoewel dit al eerder in het gedeelte over phishing is aangestipt, verdient het een extra vermelding omdat het vaak de poort die bedreigingen laat slagen. Bijvoorbeeld de deur openhouden voor iemand die een beveiligde ingang binnengaat. Het is een vriendelijk gebaar, maar het kan ertoe leiden dat onbevoegden toegang krijgen tot gebieden waar zij niet mogen komen.

Zwakke wachtwoorden: Hoe makkelijker een wachtwoord te onthouden is, hoe makkelijker het te raden is. Dit, in combinatie met gestolen gegevens hieronder, zijn twee volledig vermijdbare bedreigingsscenario's.

Gestolen gegevens: De toegenomen complexiteit van wachtwoorden en het grote aantal wachtwoorden dat zowel privé als beroepsmatig wordt gebruikt, kan ertoe leiden dat de wachtwoorden worden opgeschreven, bijvoorbeeld op een post-it achter het toetsenbord of het beeldscherm. Het klinkt misschien lachwekkend, maar dit vormt een ernstig beveiligingsrisico voor de gebruiker en zijn gegevens.

Apparaten niet up-to-date: Alle apparaten en apps vereisen regelmatig updates om bugs en kwetsbaarheden te 'patchen". Zonder de laatste patches staan apparaten open voor interne en externe bedreigingen, waardoor het voor bedreigingen triviaal wordt om ingebouwde beveiligingen te omzeilen, gevoelige gegevens te verzamelen en verbonden bronnen verder te ontdekken.

Diefstal/exfiltratie van gegevens: Met iets alomvattends als een USB-stick kunnen gegevens worden opgeslagen en verplaatst tussen apparaten, en het is handig als je werk mee naar huis neemt. Het kan echter ook een kwaadaardiger doel dienen als middel om gegevens van een beveiligde locatie naar een mogelijk onbeveiligde locatie te verplaatsen of te helpen bij het verwijderen van vertrouwelijke gegevens.

Verkeerd geconfigureerde instellingen: Computerinstellingen lijken veel op voorkeuren, we hebben ze allemaal en ze kunnen van persoon tot persoon verschillen. Soms moeten instellingen echter op een bepaalde manier worden ingesteld om apparaten te beveiligen en mogelijke problemen te voorkomen, zoals het verwijderen van de mogelijkheid voor een webbrowser om gegevens op te slaan om te voorkomen dat iemand gewoon naar een apparaat loopt en toegang krijgt tot je gevoelige gegevens.

Eindpuntbescherming verwijderen: Hoewel dit in de loop der jaren moeilijker is geworden, is het nog steeds een mogelijkheid, waarbij gebruikers vaak een afname van de prestaties als belangrijkste reden aanvoeren, om dezelfde software te verwijderen die je apparaat beschermt tegen malwarebedreigingen.

Schaduw IT: Eerder besproken: schaduw-IT heeft als doel een probleem op te lossen, maar laat vaak een of meer beveiligingsproblemen na.

Je denkt misschien: waarom is dit cruciaal voor het succes van de leerlingen, hoe beïnvloedt dit de prestaties van de leerlingen? Cyberbeveiliging heeft zowel directe als indirecte gevolgen voor het leer- en werkvermogen van belanghebbenden.

Digitale kloof

Afhankelijk van de demografische gegevens kan het aantal leerlingen dat thuis geen toegang heeft tot betrouwbaar breedbandinternet variëren ten opzichte van het gemiddelde van 40%, zoals blijkt uit een onderzoek van het Public Policy Institute of California (PPIC). Hoewel er de laatste jaren in de VS bijvoorbeeld een aantal lokale, staats- en federale initiatieven zijn geweest om het aantal apparaten in de handen van leerkrachten en leerlingen op te voeren, is de digitale kloof nog steeds een zeer reële zorg voor veel schooldistricten, vooral wanneer je je bedenkt dat deze apparaten en mobiele hotspot internettoegang de enige middelen zijn die zij hebben om deel te nemen aan afstandsonderwijs of hun huiswerk uit te voeren.

Geen toegang tot apparaten of middelen

Eenvoudig gezegd, als een apparaat niet toegankelijk is door een technisch probleem, momenteel bij IT in triage is of wacht op service van een externe leverancier, dan zitten medewerkers of leerlingen in wezen zonder hun hulpmiddelen. Hetzelfde geldt voor software of diensten die niet beschikbaar zijn. Als ze niet toegankelijk zijn, betekent dat gemiste kansen voor onderwijs en leren.

Financiering gekoppeld aan vorderingen van leerlingen/testresultaten

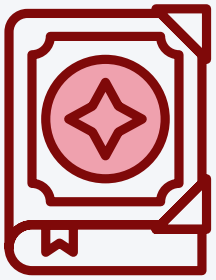
Net als de hierboven genoemde digitale kloof in de VS kan het onderwerp toetsresultaten en vorderingen van leerlingen die van invloed zijn op de hoogte van de ontvangen financiering, van schooldistrict tot schooldistrict verschillen en sterk afhankelijk zijn van de demografische situatie in een bepaald gebied.

- Prestatiebeloning of promoties voor leerkrachten en beheerders
- Eenmalige bonussen voor leerkrachten
- Meer financiering voor scholen of schoolprogramma's
- Toegang tot bepaalde subsidies of alternatieve vormen van financiering
- Slecht presterende scholen kunnen verplicht worden bijles aan te bieden
- Op slecht presterende scholen kunnen leerkrachten en beheerders worden vervangen

Onlineveiligheid voor leerlingen

Wij zijn het er allemaal over eens dat de veiligheid van leerlingen en personeel van het allergrootste belang is in het onderwijs. Door de toename van beveiligingsrisico's naarmate de technologie zich verder in ons dagelijks leven nestelt, en de groei van cyberbeveiligingsaanvallen gericht op de onderwijssector, zijn de dagen van het eenvoudigweg installeren van antivirussoftware op je apparaten allang voorbij.

Naast malwaredreigingen en aanvallen op apps en diensten, zijn er kwaadwillende dreigingsactoren die munt willen slaan uit het inbreken in netwerken omleerlinggegevens te bemachtigen endeze te verkopen op het dark web. Erger nog, het ontbreken van de juiste beveiligingscontroles kan het welzijn van belanghebbenden in gevaar brengen door hen onbewust te bespioneren via camera's of microfoons, hun locaties te volgen of door zich voor te doen als iemand die zij kennen om ernstigere misdrijven te plegen. Leerlingen voorlichten over het belang van onlineveiligheid en hen tegelijkertijd de vaardigheden bijbrengen om zelf bedreigingen te herkennen, is de sleutel tot een degelijk leerplan voor onlineveiligheid.



Vraag M.O.M.

In de tovenaarswereld van Harry Potter is het Ministerie van Toverkunst de poortwachter van informatie en alles wat met magie te maken heeft. In de onderwijssector heb je Jamf om door de verkeerde informatie heen te prikken en te bepalen welke beveiligingspraktijken het beste passen bij jouw unieke behoeften, en natuurlijk om met jou samen te werken bij de succesvolle implementatie ervan.

Laten we, voordat we op de zaken vooruitlopen, even stilstaan bij een aantal gangbare opvattingen en misvattingen over Apple beveiliging, waaronder opvattingen over de rol die cyberbeveiliging speelt in het onderwijs.

Apple krijgt geen virussen: dit was nooit helemaal waar, Mac waren gewoon niet zo populair. Daarom richtten kwaadwillenden zich op Windows, dat een groter marktaandeel had. De laatste jaren is dit drastisch veranderd en de explosieve groei van Apple is een aanzienlijk doelwit gebleken.

Onderwijs is zeer gericht: Waar. Uit een rapport van Bitdefender blijkt zelfs dat het onderewijs op de tweede plaats staat, net na retail, als hoogste doelwit voor ransomware. Hoewel malware slechts één soort bedreiging vormt, behoort het tot de belangrijkste bedreigingen.

Het onderwijs is zwak op het gebied van beveiliging: Dit is zeker hoe het wordt gezien volgens dreigingsanalyses en rapportages, zoals die van Security Scorecard, waaruit bleek dat 'van de 17 bedrijfstakken in de VS, het onderwijs op de laatste plaats staat wat betreft totale cyberbeveiliging' In het rapport werd met name opgemerkt dat de patchcadans en de beveiliging van apps en netwerken tot de belangrijkste pijnpunten behoren.

Beveiliging is moeilijk en duur: er is een tekort aan cyberbeveiligingsprofessionals, zoveel is bekend. Dat komt deels doordat het geen gemakkelijk werk is. Daarom is het voor een succesvol cyberbeveiligingsprogramma van het grootste belang dat je je omgeving kent, je behoeften beoordeelt en samenwerkt met betrouwbare partners om deze problemen aan te pakken. Vertrouwen op de 'hype' zonder de oplossingen te verifiëren is een recept voor een ramp. In diezelfde geest kan het omhoog gooien van de handen in de lucht je district blootstellen aan bedreigingen, waarbij het opruimen van een datalek en het aanpakken van nalevingsboetes hoge kosten met zich meebrengen.

Vraag M.O.M.

'Hackers hoeven het maar één keer goed te doen; wij moeten het elke keer goed doen.'

- Chris Triolo, een beveiligingsprofessional bij HP

One size fits all oplossingen: Hand in hand met de moeilijkheid versus de kosten hierboven, is de mythe van de 'one size fits all' oplossing. Een leverancier kan meerdere oplossingen ontwikkelen die samenwerken om vele bedreigingen aan te pakken, zeker, maar dit verwijst specifiek naar één enkel product dat beweert alle bedreigingsaspecten aan te pakken. Historisch gezien hebben dergelijke producten tekortgeschoten in verschillende doelstellingen, en op het gebied van de cyberbeveiliging zal dat niet volstaan.

Het is een IT-probleem: dit is meer een algemene opvatting, maar belangrijk voor de discussie over onderwijs. In het kader van budget- en tijdzorgen kan een belanghebbende gemakkelijk het gevoel krijgen dat er een grens in het zand is waar zijn functie eindigt en een andere rol begint. De waarheid is dat beveiliging – net als zwerfvuil – een probleem is van iedereen en dat het de inspanning van alle betrokkenen vergt om het te handhaven. Denk aan de analogie dat een ketting zo sterk is als zijn zwakste schakel.

Maak je geen zorgen over beveiliging, tenzij je gehackt wordt: De 'kop in het zand steken'-benadering, maar niets is minder waar. Feit is dat op een gegeven moment alle instellingen niet werden getroffen door een beveiligingslek... totdat dat wel het geval was. Proactief zijn in plaats van reactief biedt scholen de mogelijkheid om te controleren op bedreigingen, punten van zorg op te sporen en deze te verhelpen om te voorkomen dat bedreigingen zich ontwikkelen tot iets veel ernstigers.

Jamf + Apple

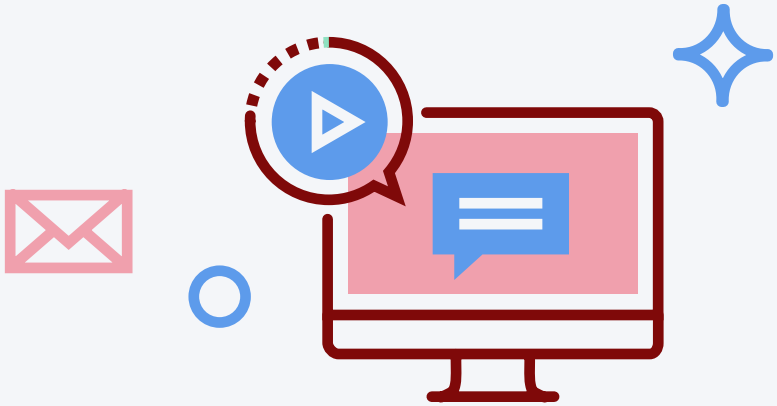
In nauwe samenwerking met Apple is elke oplossing speciaal ontwikkeld om niet alleen je apparaten, gebruikers en gegevens te beschermen, maar dit ook te doen met zo min mogelijk middelen, zodat deze naadloos aansluit op de gebruikerservaring waar Apple producten om bekend staan.

Samen voegen ze de diensten en apparatuur van Apple samen met oplossingen van Jamf die tegemoetkomen aan de unieke behoeften van het onderwijs. Leerlingen en leerkrachten kunnen zich gesterkt voelen en prioriteit geven aan het gebruik van technologie op nieuwe en vindingrijke manieren, terwijl IT- en beveiligingsteams er zeker van kunnen zijn dat risico's worden beperkt en bedreigingen geminimaliseerd door oplossingen die zich richten op apparaatbeheer, identiteitsbepaling en -verificatie en eindpuntbescherming op de achtergrond.

Apple School Manager (ASM)

Start het eindpuntbeheerproces met de gecentraliseerde, cloudgebaseerde console die even krachtig als gebruiksvriendelijk is. De dienst, die gratis door Apple wordt aangeboden, synchroniseert aankopen met de online console en biedt IT een middel om een verbinding tot stand te brengen met de MDM-software (Mobile Device Management) van de scholengroep, zodat apparaten automatisch kunnen worden geregistreerd voor beheer.

Jamf School



De toonaangevende oplossing voor het onderwijs voor het beheer van alle apparaten in het Apple ecosysteem, maar exclusief afgestemd op leerkrachten, instructietechnologen en Mac-beheerders in het onderwijs. De Jamf School MDM-oplossing stelt meer dan 36 miljoen scholieren wereldwijd in staat om eenvoudig gebruik te maken van de functionaliteit voor klaslokaalbeheer, apps, lesmateriaal en beperkingen samen te stellen en gemakkelijk beheerde Apple ID's uit te rollen, zonder dat je een — al dan niet technische — expert hoeft te zijn. Bovendien helpt het ingebouwde incidentbeheersysteem bij het bijhouden van gemelde problemen, zoals apparaten die niet meer onder de garantie vallen, wat uiteindelijk allemaal bijdraagt aan een succesvolle cyberbeveiligingsstrategie.

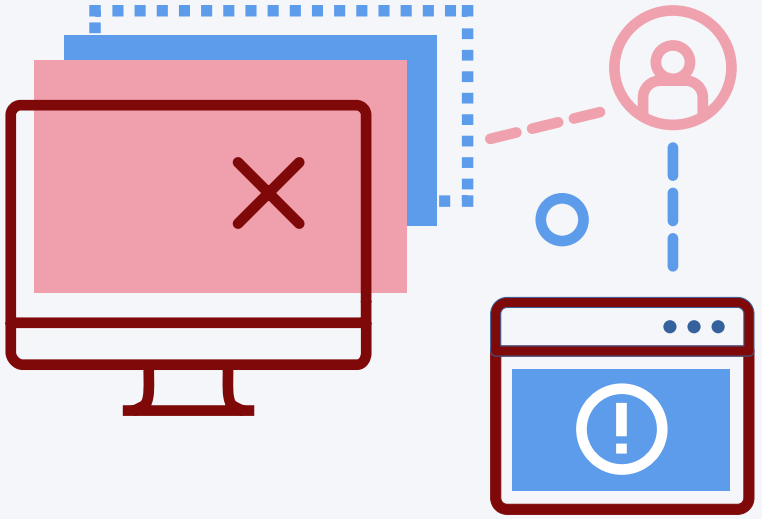
Meer informatie

Jamf Pro

De toonaangevende MDM-oplossing voor organisaties die een MDM-platform met geavanceerde functionaliteit en ondersteuningsmodellen nodig hebben. Jamf Pro bevat dezelfde functies als Jamf School, maar voegt automatisering en robuuste integratie toe met andere producten in je netwerk- en systeembeheerstack, zoals API-toegang (Application Programming Interface) voor beveiligde communicatie tussen apps en diensten of zeer technische functies die toegewijde IT-teams de extra kracht bieden die nodig is om meerdere scholen of een hele groep te beheren.

Meer informatie

Jamf Connect



Jamf Connect maakt gebruik van gecentraliseerd, cloudgebaseerd accountbeheer en is de spil waarmee accounts kunnen worden aangemaakt voor gebruikers om zich op hun Mac te verifiëren. Meer nog, ze kunnen dit doen met slechts één account - niet meerdere wachtwoorden onthouden - met echte Single Sign-On (SSO) voor toegang tot alle toegewezen apps en diensten, inclusief Multifactor Authentication (MFA) die een tweede laag van toegangsbeveiliging toevoegt.

Meer informatie

Jamf Protect

Jamf Protect richt zich uitsluitend op de beveiliging van Apple door beveiligingsteams te helpen bekende malware te voorkomen, bedreigingen te detecteren en gedragsanalyses te gebruiken om potentiële risico's voor de gezondheid van je apparaten te identificeren. Bovendien beschikt het over realtime waarschuwingen en logging, die granulair inzicht bieden in eindpunten om niet alleen je doelstellingen op het gebied van compliance van regelgeving te bereiken, maar IT ook de mogelijkheid bieden om problemen te verhelpen en gebruikers te helpen zonder ze in de weg te lopen.

Meer informatie

Breng je onderwijstechnologie naar een hoger niveau

jamf

Wil je meer details over wat Jamf biedt of heb je vragen over het implementeren van deze tools in je eigen school? Start een gratis proefperiode om er meteen in te springen.

Proefversie aanvragen

Of neem contact op met de reseller van Apple hardware van jouw keuze.