Bescherming van IT-infrastructuren op scholen, hogescholen en universiteiten.

Barracuda®
Your journey, secured.

Netwerkbeveiliging is een les waar onderwijsinstellingen zich op kunnen voorbereiden

Als het om netwerkbeveiliging gaat, kunnen (en moeten) organisaties lering trekken uit de ervaringen van andere partijen. De echte uitdaging ligt in het bepalen welke lessen relevant zijn en hoe deze worden toegepast zodat de meest doeltreffende bescherming wordt geboden. Degelijke netwerkbeveiliging is een van de grootste uitdagingen voor een beveiligingsteam, maar er is veel kennis die kan worden overgedragen.

Netwerkbeveiliging is een term die verwijst naar tal van verschillende technologieën en beginselen. Het is niet simpelweg een kwestie van het juiste product kopen. Hieronder vallen geavanceerde firewalls, maar netwerkbeveiliging gaat verder dan het beveiligen van de perimeter; het omvat ook het controleren van het netwerkverkeer, het beheren van het bandbreedtegebruik, en het detecteren en in quarantaine plaatsen van internetbedreigingen. De huidige snelle IT-omgeving wordt aangejaagd door digitalisering en het invoeren van de cloud. Hierbij hebben organisaties oplossingen nodig die de beveiliging kunnen optimaliseren en tegelijk de prestaties voor gebruikers op een gedistribueerd netwerk kunnen verbeteren.

Werken op afstand (op verspreide locaties of campussen, of vanuit huis) was al in opmars en is door de COVID-19-pandemie in een stroomversnelling gekomen. Organisaties moeten een veel groter aanvalsoppervlak beveiligen, waarbij vaak apparaten en netwerken worden aangesloten die niet onder hun directe beheer staan. In de onderwijssector vormt netwerkbeveiliging een bijzondere uitdaging.

Barracuda.

De uitdaging voor onderwijsinstellingen en hoe deze aan te gaan

Het klinkt misschien gek, maar de onderwijssector loopt het grootste risico op cyberaanvallen – Microsoft bericht dat deze sector goed is voor viervijfde (82,6%) van alle malwaregevallen in de afgelopen 30 dagen, maar het onderwijs staat al jaren aan of in de buurt van de top van de lijst. Uit onze analyse van 3,5 miljoen spear-phishingaanvallen gedurende een periode van vier maanden, bleek dat meer dan duizend onderwijsinstellingen doelwit waren. Vergeleken met het gemiddelde liepen onderwijsinstellingen een meer dan twee keer zo grote kans om door een BEC-aanval te worden getroffen, waarbij slechte actoren zich voordoen als een personeelslid of een faculteit in een poging anderen over te halen informatie te delen of financiële transacties goed te keuren. Het aantal DDoS-aanvallen (Distributed denial of service) gericht tegen onderwijsinstellingen, waarbij netwerken worden overspoeld met een overweldigende hoeveelheid verkeer, is ook toegenomen. Deze DDoS-aanvallen kunnen niet alleen het online onderwijs verstoren, maar zij kunnen ook als dekmantel dienen voor pogingen om door de netwerkverdediging te dringen en malware in het systeem te injecteren.

Onderwijsinstellingen variëren sterk, van kleine scholen en hogescholen tot grote universiteiten met meerdere campussen. Ze hebben echter een aantal zaken gemeen die deze instellingen tot een aantrekkelijk doelwit maken. De sleutel tot risicobeperking is dat men zich bewust moet zijn van de risico's. Deze risico's omvatten:

- **Elk jaar een nieuwe lichting doelwitten:** Onderwijsinstellingen krijgen elk jaar een nieuwe lichting studenten binnen die wellicht enige training nodig hebben om met de aan hen ter beschikking gestelde IT-apparatuur om te gaan, ondersteuning nodig hebben om vertrouwd te raken met de verplichte authenticatieroutines, en de best practices moeten leren kennen om toegang te krijgen tot de middelen die zij nodig hebben om hun studie effectief te laten verlopen.

- **Toename in e-learning:** E-learning en leren op afstand maakten al een groei door toen de COVID-19-pandemie uitbrak, en dit heeft een exponentiële toename van netwerkverkeer tot gevolg gehad, waardoor het eenvoudiger wordt voor aanvallers om

zich te kunnen verbergen. De drastische toename van studenten die van huis uit leren, maakt een naadloze beschikbaarheid van gegevens en toepassingen onontbeerlijk, net als de schaalbaarheid van mechanismen voor toegang op afstand.

- **Meerdere locaties:** Of het nu een grote universiteit betreft met campussen verspreid over een stad of regio, een onderwijsraad of een academieketen – meerdere locaties betekent een grotere beveiligingsuitdaging. Studenten, de faculteit en personeel hebben vanaf tal van locaties legitiem toegang tot het netwerk, waardoor het moeilijker wordt aanvallers eruit te pikken.

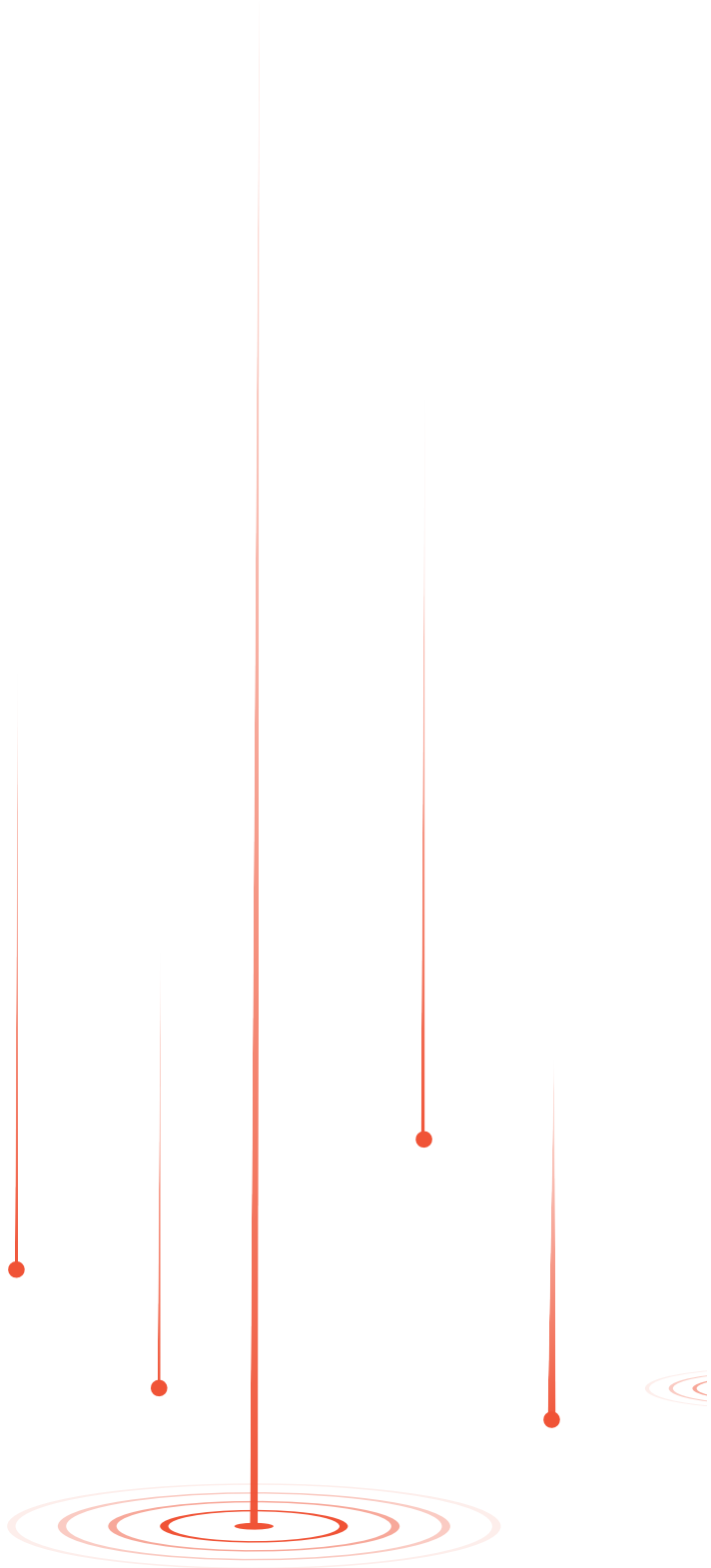
- **Waardevolle gegevens:** Hoewel sommige aanvallen niet veel meer dan een slechte vorm van kattenkwaad zijn, zijn de meeste cybercriminelen uit op financieel of materieel gewin. Onderwijsinstellingen bezitten grote hoeveelheden waardevolle gegevens, waaronder persoonlijk identificeerbare informatie (PII) over studenten, ouders, docenten en personeel, betalings- en rekeninggegevens, en in veel gevallen waardevol intellectueel eigendom in de vorm van onderzoeksgegevens. Dit kan hen tot doelwit maken van afpersing, cyberspionage en zelfs door aanvallen die worden gesponsord door de overheid.

- **Openbare of semi-openbare netwerktoegang:** Veel instellingen bieden wellicht openbare wifitoegang voor ouders en bezoekers en/of gedeelde terminals in openbare ruimten.

- **Gebruikers hebben training nodig:** Gebruikers vormen uw eerste, en misschien wel beste, verdedigingslinie tegen inbreuken. Bied gebruikers (studenten, personeel en docenten) training in het herkennen en melden van bedreigingen tegen de netwerkbeveiliging.

- **Kwetsbaarheid leveranciers/partners:** Onderwijsinstellingen hebben betrekkingen met leveranciers, opdrachtnemers en onderzoekspartners in de openbare en particuliere sector. Het is van cruciaal belang dat ook die partijen een goede netwerkhygiëne handhaven. Zo niet, dan kunnen die externe partijen de basis vormen voor een zogenaamde 'island-hopping attack', waarbij de aanvallers het netwerk van de leverancier of partner gebruiken om toegang te verkrijgen tot uw netwerk.

Een aanvaller kan puur kwaadwillig zijn en geen ander motief hebben dan ontregeling en vernietiging. Het is echter waarschijnlijker dat aanvallers uit zijn op een of andere vorm van gewin. Denk aan een bende die geld probeert af te persen om door hen versleutelde gegevens vrij te geven. Of identiteitsdieven die uw persoonlijk identificeerbare informatie (PII) proberen te stelen om deze vervolgens te verkopen. Ook kunnen het bedrijfs- of door de overheden gesponsorde agenten zijn die intellectueel eigendom willen exfiltreren. Onderaan de streep betekent dit dat onderwijsinstellingen de netwerkbeveiliging moeten verbeteren door in lagen en in de diepte te verdedigen.



Met netwerkbeveiligingslagen blijven onderwijsinstellingen veilig en toch wendbaar

Netwerkbeveiliging is geen product, programma of checklist. Het is een holistische aanpak waarbij verdedigingslagen worden opgebouwd om organisaties veilig en toch effectief te houden. Als onderwijsinstellingen de beveiliging dusdanig aanscherpen (denk aan tal van checkpoints, wachtwoorden en authenticaties) en het te moeilijk wordt voor studenten om toegang te krijgen tot hun lessen, e-mail te gebruiken of referentiemateriaal in te zien, dan slaan ze de plank mis. Een enkele beveiligingslaag, hoe sterk dan ook, werkt ook niet. Het is natuurlijk ook niet de bedoeling dat een crimineel het e-mailaccount van een professor binnendringt en dan vrij door het netwerk kan bewegen.

De juiste aanpak is het hele netwerk omvattende beveiligingslagen om verschillende soorten beveiliging te bieden voor de hele organisatie. Meerlaagse beveiliging, inclusief sandboxing voor volledige emulatie, biedt doeltreffende bescherming tegen geavanceerde bedreigingen en beperkt het risico om slachtoffer te worden van een ransomware-aanval. De overstap naar de cloud biedt grote voordelen met een deskundig beheerde beveiliging die altijd up-to-date is.

Netwerkbeveiliging komt voort uit robuuste componenten die samenwerken. Krachtige firewalls en mechanismen voor toegangscontrole houden indringers buiten de deur, terwijl netwerksegmentatie de laterale bewegingen van gebruikers of potentiële indringers beperkt, mochten zij door de mazen van de beveiliging glippen. Idealiter wordt de toegang tot alle toepassingen, binnen het netwerk, in de cloud of zelfs SaaS, gecombineerd met Zero Trust-principes, waarbij telkens de gebruikers-ID, apparaatstatus en andere vitale parameters worden gecontroleerd voordat er versleutelde toegang tot de toepassing wordt gegeven. Daarnaast zorgt Zero Trust Network Access (ZTNA) er voor dat de juiste gebruiker uitsluitend toegang heeft tot de benodigde toepassingen, zodat ongecontroleerde vergaring van toegangsrechten wordt vermeden.

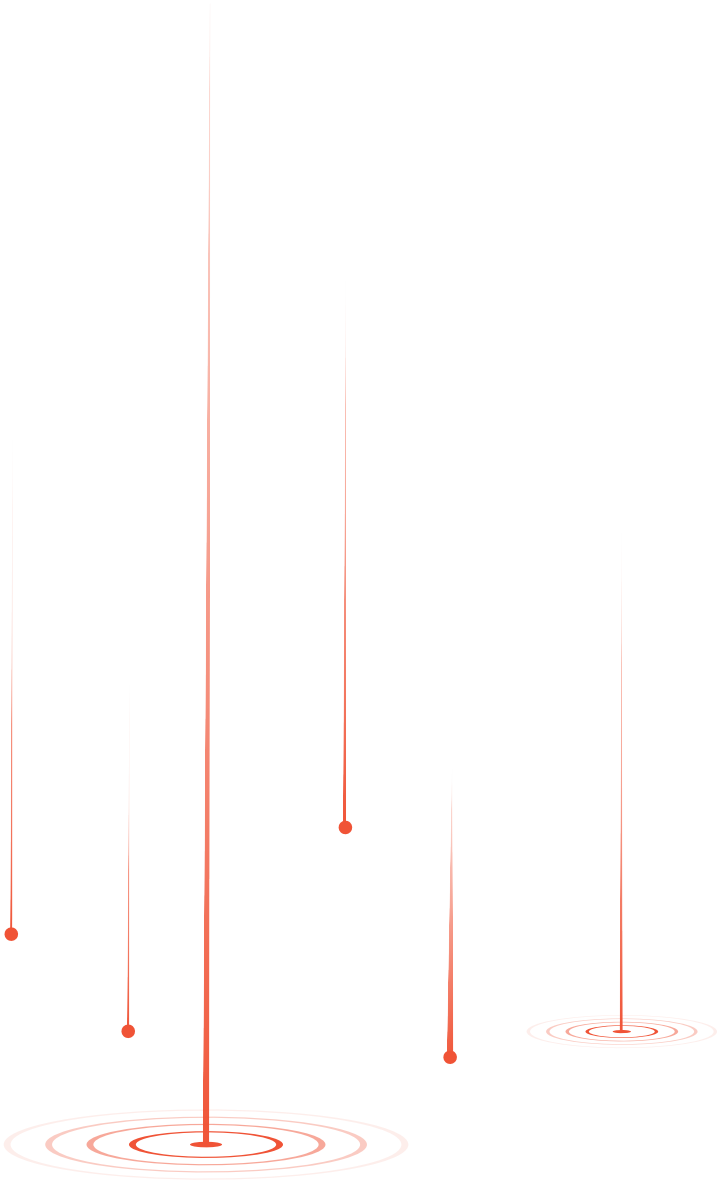
Barracuda.

Een SD-WAN-oplossing (Software-Defined Wide Area Network) kan gebouwen, verspreide locaties of campussen en vertrouwde partners met elkaar verbinden via meerdere versleutelde verbindingen, en is veel goedkoper dan pseudo-veilige MPLS of andere geleasede lijnen.

Een veilige leeromgeving vereist veilig computergebruik. Ransomware en andere malware kunnen uw netwerk infecteren via sociale media of gecompromitteerde websites. Microsoft Security Intelligence meldt dat het overgrote deel van de apparaten in de onderwijssector zijn besmet zijn met adware of backdoor trojans. Webbeveiliging is een wettelijke vereiste voor veel scholen en biedt verschillende voordelen als dit correct is geconfigureerd. Het filteren van content blokkeert afleidende sites en helpt leerlingen en studenten te beschermen tegen cyberpesten en online kinderlokkers.

Conclusie

De onderwijssector heeft te maken met een overvloed aan bedreigingen van cybercriminelen die inbreuk proberen te maken op hun netwerken voor winstdoeleinden. Malware, ransomware en allerlei andere soorten cyberaanvallen richten een ravage aan in onderwijsinstellingen. Eén ding is zeker: het is nú tijd om u te beveiligen tegen deze bedreigingen.



Netwerkbeveiliging lijkt een hele klus, en dat is het ook. Maar het is te doen. Bovendien kan deze beveiliging cloudgebaseerd zijn en via een as-a-service model worden geleverd, zodat overspannen IT-personeel minder wordt belast en onderwijsinstellingen een kosteneffectieve manier hebben om ervoor te zorgen dat de beveiliging up-to-date blijft.

Ontdek hoe u een effectieve netwerkbeveiligingsstrategie kunt ontwikkelen met de krachtige beveiligingstools van Barracuda. Wij staan klaar om u te helpen.

Over Barracuda Netwerkbeveiliging

De oplossingen van Barracuda omvatten drie kernproducten: Barracuda CloudGen Firewall, Barracuda CloudGen WAN en Barracuda CloudGen Access. Hiermee voldoet u aan alle huidige vereisten voor moderne netwerkbeveiliging.

Barracuda CloudGen Firewall combineert de beste geavanceerde beveiliging met een complete set van veilige SD-WAN-mogelijkheden. Barracuda CloudGen WAN is het enige cloud-native SASE-platform op de markt dat een wereldwijde veilige SD-WAN-dienst biedt die vanaf de basis is ontwikkeld op Azure. Barracuda CloudGen Access is een innovatieve Zero Trust Access-oplossing die vanaf elk apparaat en elke locatie beveiligde toegang biedt tot toepassingen en workloads.

Barracuda CloudGen Access™

Barracuda CloudGen Firewall™

Barracuda CloudGen WAN™

Over Barracuda

Bij Barracuda willen we van de wereld een veiligere plek maken. Wij zijn van mening dat ieder bedrijf toegang verdient tot een cloud-first beveiligingsoplossing op bedrijfsniveau die makkelijk aan te schaffen, te implementeren en gebruiken is. Wij beschermen e-mails, netwerken, gegevens en applicaties met innovatieve oplossingen die meegroeien en zich aanpassen aan het traject van onze klant. Meer dan 200.000 organisaties over de hele wereld vertrouwen op Barracuda om hen veilig te houden, zelfs wanneer ze niet eens weten dat iets een risico vormt. Zo is er ruimte om te kunnen focussen op hun bedrijf. Ga voor meer informatie naar barracuda.com.

Barracuda
Your journey, secured.

Neem gerust contact met ons op als u vragen heeft over hoe uw toepassingen kunnen worden beveiligd.