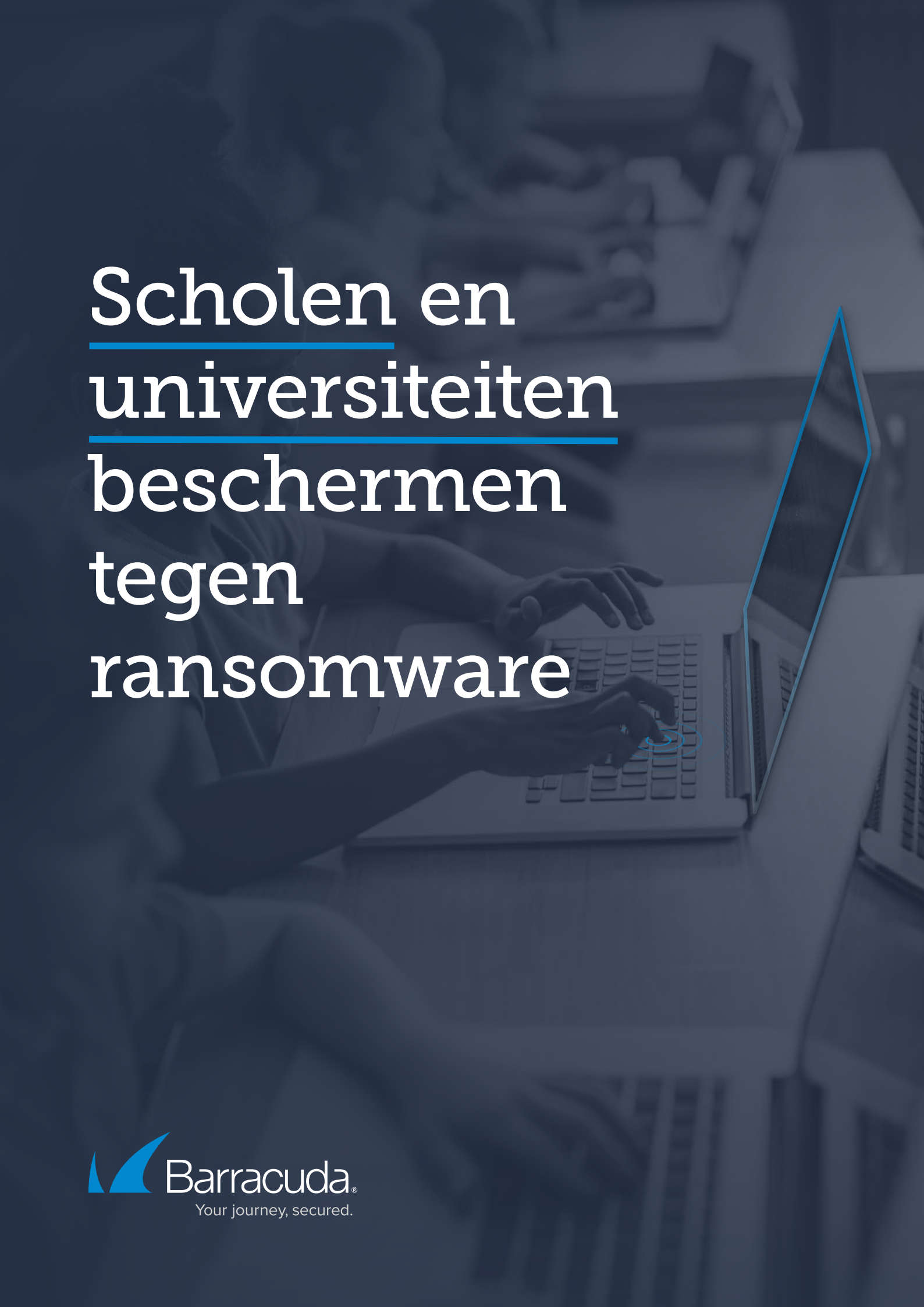


Scholen en universiteiten beschermen tegen ransomware

Barracuda®
Your journey, secured.

Inhoudsopgave

Ransomware en het onderwijs: lessen leren

Scholen en universiteiten hebben het zwaar te verduren gehad bij recente ransomware-aanvallen. Tussen 14 augustus en 12 september 2021 waren onderwijsinstanties het doelwit van meer dan 5,3 miljoen malware-aanvallen (inclusief ransomware), oftewel 63% van dergelijke aanvallen. Wereldwijd was 44% van alle onderwijsinstanties in 2020 doelwit van dergelijke aanvallen.

Ransomware is kwaadaardige software die uw gegevens versleutelt of er op een andere manier voor zorgt dat u geen toegang meer heeft tot uw eigen systemen. Vervolgens eisen criminelen losgeld in ruil voor de decoderingssleutel. In veel gevallen stelen aanvallers hierbij gegevens als persoonsgegevens. Deze exporteren ze om de organisatie die slachtoffer is voor nog meer geld af te persen of om ze op het dark web te verkopen, of allebei. Dit soort activiteiten zijn vooral verontrustend wanneer de gegevens betrekking hebben op kinderen. Bovendien kunnen organisaties die door ransomware worden getroffen, te maken krijgen met aanzienlijke onverwachte downtime, waardoor de kosten stijgen en in sommige gevallen de school of hogeschool moet worden gesloten totdat de situatie is opgelost.

Er werd een recente plotselinge stijging van het aantal ransomware-aanvallen op universiteiten en scholen opgemerkt bij aanvang van het nieuwe academische jaar. De timing van deze aanvallen was niet willekeurig. Door toe te slaan aan begin van het nieuwe schooljaar, wilden de aanvallers zoveel mogelijk chaos creëren, zodat de scholen snel zouden betalen.

Aangezien instanties afhankelijk zijn van IT-systemen om veilig toegang te verschaffen tot campusfaciliteiten, om nog maar te zwijgen van allerlei online onderwijs-, evaluatie- en beoordelingssystemen, kunnen succesvolle ransomware-aanvallen een universiteit letterlijk van de ene op de andere dag platleggen. De universiteit van Portsmouth werd aan het eind van de paasvakantie getroffen. De universiteit zag zich gedwongen de campus ruim twee weken te sluiten en toegang tot het netwerk op te schorten. Het opnieuw opbouwen van systemen, het controleren en opschonen van gegevens, het samenwerken met de politie, en het fysiek inspecteren en beveiligen van honderden laptops en andere apparaten betekende dat het weken duurde voordat de systemen weer volledig operationeel waren.

Barracuda.

Waarom het onderwijs?

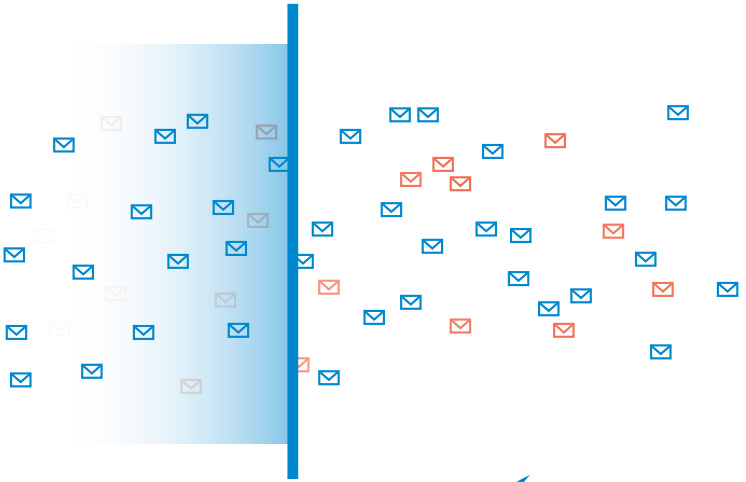
Als gevolg van de COVID-19-pandemie zag het onderwijs zich genoodzaakt in rap tempo thuiswerken en afstandsonderwijs te omarmen. Hoewel een dergelijke stap niet per se gevaarlijk hoeft te zijn, betekent dit wel degelijk een toename van mogelijke aanvalsvectoren voor kwaadwillenden.

Het National Cyber Security Centre (NCSC), een door de Britse overheid gesteund adviesorgaan, deed in juni 2021 een specifieke waarschuwing dat bendes hun pijlen op de onderwijssector hadden gericht na een sterke stijging in het aantal aanvallen op scholen, hogescholen en universiteiten. Het was ongebruikelijk dat het NCSC de waarschuwing aan bestuurders richtte, maar ook aan IT- en cyberbeveiligingspersoneel, wat schoolhoofden en rectoren deed beseffen dat dit niet alleen een theoretisch IT-probleem was, maar een ernstig institutioneel risico dat om actie vraagt.

Het NCSC adviseert het actief scannen van e-mails om schadelijke e-mails en uitvoerbare bijlagen te verwijderen, regelmatige training en voorlichting van het personeel, het maken van regelmatige back-ups van belangrijke bestanden, en het veilig en gescheiden bewaren van die back-ups, idealiter buiten van het hoofdnetwerk.

Veel professionele ransomwarebendes gebruiken geautomatiseerde tools die scannen op ongepatchte toepassingen die hun initiële toegang tot netwerken verschaffen. Het kan dus zijn dat zij zich niet rechtstreeks op een school of hogeschool richten, maar gewoon door hun bot gewaarschuwd worden dat iemand een deur tot het netwerk ontgrendeld heeft gelaten. Eenmaal binnen, kunnen zij hun machtigingen uitbreiden en zich door systemen heen bewegen om uw gevoeligste gegevens te achterhalen.

Cyberbeveiligingspersoneel moet een balans zien te vinden tussen de noodzaak om systemen potdicht te houden en de noodzaak om ze bruikbaar te houden voor personeel en studenten. Met een alsmaar veranderend rooster van zowel leraren als leerlingen en studenten is het een moeilijke uitdaging om de training en het bewustzijn op peil te houden. Maar er is hulp beschikbaar.



U moet nu actie ondernemen

Het moment om ransomware te bestrijden, is voordat het zover is. U wilt niet dat het zover komt dat u plannen moet maken tijdens een daadwerkelijke aanval. Barracuda kan u helpen een plan te ontwikkelen dat u beschermt tegen ransomware, dat belangrijke aanvalsvectoren omvat en dat uw gegevens beschermt.

Dit zijn de drie belangrijkste gebieden die u moet beveiligen om moderne ransomware-aanvallen te stoppen:

1. **Beveilig uw e-mail en train uw personeel**

2. **Bescherm uw webtoepassingen**

3. **Maak een back-up van uw gegevens**

Barracuda.

1. Beveilig uw e-mail en train uw personeel

E-mail is de meest voorkomende manier waarop ransomware een organisatie binnendringt. Er zijn 13 soorten e-mailbedreigingen die criminelen kunnen gebruiken om uw inloggegevens in handen te krijgen. Dit kan een geïnfecteerde link in een e-mail zijn waar een medewerker op klikt of een meer geraffineerde spear-phishing-aanval. De juiste e-mailbeveiliging kan u beschermen tegen zowel externe aanvallen als interne e-mails die al zijn aangetast. Zorg ervoor dat uw IT-personeel weet hoe zij in real time moeten reageren om aanvallen een halt toe te roepen en om te bepalen hoe een aanval heeft plaatsgevonden, zodat deze in de toekomst kan worden voorkomen. Leer werknemers hoe ze veelvoorkomende ransomwaretactieken kunnen herkennen en druk hen op het hart zorgen over potentiële aanvallen te escaleren. Dit geeft het IT-personeel de tijd om een aanval te onderscheppen of een werknemer extra training te geven. Beide scenario's zijn voordelig voor de organisatie.

2. Bescherm uw webtoepassingen

Webtoepassingen zijn een veelvuldig doelwit van aanvallers. Aanvallers kunnen beveiligingslekken in portalen voor studenten of personeel, online administratie- of onderwijssystemen, systemen voor externe toegang of andere webtoepassingen uitbuiten om initiële toegang tot netwerken te verkrijgen en ransomware te verspreiden. Als een toepassing eenmaal is gehackt, kunnen de aanvallers de malware zijdelings over de rest van uw netwerk verspreiden, en zo een ravage aanrichten. Een firewall voor webtoepassingen is een goede manier om dit deel van uw infrastructuur te beschermen.

3. Maak een back-up van uw gegevens

Als u het slachtoffer wordt van een ransomware-aanval en uw gegevens worden buitgemaakt, dan is de enige manier om ze te herstellen door back-ups te hebben van al uw gegevens, ook van cloud-gebaseerde en samenwerkingstoepassingen, en e-mail. En laat uw back-up niet een nieuw doelwit worden voor aanvallen. Versleutel de opgeslagen gegevens en bewaar meerdere kopieën op verschillende locaties. De toegang moet beperkt zijn tot essentieel personeel en moet multifactorauthenticatie omvatten. Zorg er ook voor dat u de back-upprocedures regelmatig test om te bevestigen dat u alles indien nodig snel en nauwkeurig kan herstellen.

De opleiders opleiden

In scholen en hogescholen is het, net als in elke andere organisatie, van vitaal belang dat de bestuurders het reële en aanwezige gevaar van ransomware begrijpen. Dit is geen strijd die de IT-afdeling in haar eentje kan voeren. Het heeft de steun en de actieve deelname van de hele organisatie nodig. Dat betekent dat u zowel het budget als de tijd moet vinden voor een degelijke training.

Barracuda kan bescherming bieden tegen e-mail- en phishingaanvallen, terwijl het ook netwerken beschermt en de vereiste back-up biedt. Deze uitgebreide bescherming helpt u zo veilig mogelijk te blijven, maar maakt ook een sneller herstel mogelijk als het ergste gebeurt.

Neem gerust contact met ons op als u vragen hebt over hoe wij uw school, hogeschool of universiteit beschermen tegen ransomware. Voor meer gedetailleerd advies over ransomware en hoe u uw organisatie kunt beschermen, kunt u Barracuda's eBook hier downloaden.

Over Barracuda

Bij Barracuda willen we van de wereld een veiligere plek maken. Wij geloven dat ieder bedrijf toegang verdient tot een cloud-enabled beveiligingsoplossing op bedrijfsniveau die makkelijk te kopen, 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, zodat zij zich kun richten op hun bedrijf. Ga voor meer informatie naar barracuda.com.

Barracuda
Your journey, secured.

Neem gerust contact met ons op als u vragen hebt over hoe wij uw organisatie beschermen tegen ransomware.