Toonaangevende netwerkbeveiliging voor lokale overheden.

Barracuda®
Your journey, secured.

Netwerkbeveiliging kan de belangrijkste handhaver zijn voor lokale overheden

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 verwijst naar tal van verschillende technologieën en beginselen. Het is niet een kwestie van simpelweg het juiste product kopen. Hieronder vallen geavanceerde firewalls, maar netwerkbeveiliging gaat verder dan het beveiligen van de perimeter. Dit omvat ook het controleren van het netwerkverkeer, het beheren van het bandbreedtegebruik en het detecteren en in quarantaine plaatsen van internetbedreigingen. In de huidige wereld waarin mensen van waar dan ook kunnen werken, kan SASE (Secure Access Service Edge) de beveiliging optimaliseren en tegelijk de prestaties voor gebruikers op een gedistribueerd netwerk verbeteren.

Werken op afstand (op verspreide locaties of kantoren, of vanuit huis) was al in opmars en de invoer ervan 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. Netwerkbeveiliging is met name een uitdaging voor overheidsinstanties, met beperkte budgetten, in de schijnwerpers van de publieke opinie en met de vraag van burgers naar diensten op retailniveau.

Barracuda.

De uitdaging voor de lokale overheid en hoe deze aan te gaan

Nieuwe technologieën evolueren voortdurend en worden steeds meer een integraal onderdeel van bijna alle overheidsinstanties. Of het nu gaat om personeel dat een mobiel apparaat gebruikt om telefoontjes aan te nemen en e-mails te versturen, of om burgers die apps downloaden om toegang te krijgen tot bepaalde overheidsdiensten; er is een steeds groter aanvalsoppervlak waar cybercriminelen zich op kunnen richten en mogelijk gevoelige gegevens uit kunnen overhevelen.

Bij de ransomware-aanval op de gemeente Hackney in 2019 werd geen losgeld betaald, maar toch kostte het miljoenen ponden om te herstellen. En dit is niet alleen een probleem voor gemeenten. Volgens recente berichtgeving zou een netwerkinbreuk toegang hebben verschaft tot systemen in het kantoor van de Britse premier, met als gevolg de exfiltratie van enkele van de meest gevoelige gegevens van Engeland.

Sterke netwerkbeveiliging zou wel eens het meest vitale onderdeel kunnen zijn van elke overheidsoperatie in deze moderne tijd. Bewustzijn van de veelvoorkomende risico's is de sleutel om ze te verminderen. Deze risico's omvatten:

- **Een voortdurend veranderend landschap:** In de huidige netwerken veranderen hard- en software voortdurend. De tijd van beveiliging 'instellen en vergeten' ligt achter ons. Ook het bedreigingslandschap verandert met de dag, of het nu gaat om nieuwe kwetsbaarheden of geopolitieke veranderingen en overheidsactoren die nieuwe gevaren opleveren.

- **Meerdere locaties:** Eén overheidsdienst moet een enorm oppervlak kunnen verdedigen. Dat kunnen meerdere politiebureaus zijn of gemeenten die een regio bestrijken. Al die locaties moeten zijn beveiligd tegen aanvallen, terwijl ze wel gewoon open moeten blijven voor inwoners en personeel.

- **Waardevolle gegevens:** Hoewel sommige aanvallen niet veel meer dan een slechte vorm van kattenkwaad zijn, draait het bij de meeste cyberaanvallen om financieel of materieel gewin. Overheidsinstanties bezitten grote hoeveelheden waardevolle gegevens, waaronder persoonlijk identificeerbare informatie (PII) over inwoners en personeel, evenals betalings- en rekeninggegevens. Dit kan hen tot doelwit maken van afpersing

en mogelijk zelfs door aanvallen die door overheden worden gesponsord.

- **Online toegang:** Overheidsnetwerken reiken vaak verder dan de lokale kantoorruimte. Websites, toepassingen, klantaccountportalen, links naar leveranciers en online servicemogelijkheden bieden aanvallers stuk voor stuk manieren om het systeem binnen te dringen.

- **Onbewuste integratie:** De COVID-19-pandemie heeft deze netwerkuitbreiding versneld. Het gebruik van werklaptops, mobiele telefoons en computernetwerken buiten het kantoor is in sommige gevallen onvermijdelijk geworden om op hetzelfde niveau te kunnen blijven werken. De digitale transformatie betekent een nauwere integratie met externe apparaten, wat het netwerkrisico nog verder vergroot.

- **Er is training nodig voor uw personeel:** Uw medewerkers vormen uw eerste, en misschien wel beste, verdedigingslinie tegen inbreuken. Het is van essentieel belang dat de training van het personeel up-to-date blijft en dat er een sfeer van vertrouwen blijft bestaan, zodat de mensen zich zelfverzekerd genoeg voelen om aan de bel te trekken. Een afgeschermd budget voor veiligheidstraining op nahouden is moeilijk, maar van cruciaal belang. De beste tools te hebben, maar niet de vaardigheden om ze te gebruiken is zinloos.

- **Onderling verbonden diensten en agentschappen:** Engeland telt 333 lokale autoriteiten, 413 agentschappen en andere overheidsinstanties, 20 niet-ministeriële departementen en 23 ministeriële departementen die de Britse overheid bestrijken. Zij zijn op talloze manieren met elkaar verbonden en delen informatie en operationele communicatie. Toegang tot één netwerk kan mogelijk leiden tot de laterale verspreiding van een aanval.

Een aanvaller kan puur kwaadwillig zijn en geen ander motief hebben dan ontregeling en vernietiging, maar het is waarschijnlijker dat aanvallers uit zijn op een of andere vorm van gewin.

Wat de reden ook is, een geslaagde aanval op een overheidsinstantie kan schade toebrengen aan het personeel, de inwoners, het hele land en daarbuiten. Omdat zoveel agentschappen en overheidsinstanties gevaar lopen als er ook maar op een klein onderdeel wordt ingebroken, is het verbeteren van de beveiliging van overheidsnetwerken een must.

Netwerkbeveiliging die beschermt en optimaliseert

Netwerkbeveiliging is geen product, programma of checklist. Het is een holistische aanpak waarbij verdedigingslagen worden opgebouwd om organisaties veilig en toch effectief te houden. Het gaat erom uw netwerk te beschermen en te optimaliseren. Als overheidsinstanties de beveiliging dusdanig aanscherpen (denk aan tal van checkpoints, wachtwoorden en authenticaties) en het te moeilijk wordt voor medewerkers om toegang te krijgen tot de database van hun afdeling, om e-mail of toepassingen te gebruiken, dan slaan ze de plank mis. Een enkele beveiligingslaag, hoe sterk dan ook, werkt ook niet. Een crimineel die de e-mailaccount van een ambtenaar binnendringt en dan vrij door het netwerk kan bewegen, is natuurlijk ook niet de bedoeling.

De juiste aanpak is de implementatie van beveiligingslagen die het hele netwerk omvatten om verschillende soorten beveiliging te bieden voor de hele organisatie. De overstap naar de cloud biedt grote voordelen met een deskundig beheerde beveiliging die altijd up-to-date is. Het maakt de implementatie van SASE mogelijk, een aanpak die de beveiliging decentraliseert en in elk deel van de organisatie plaatst, waar gebruikers zich ook bevinden.

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 langs het toegangsbeheer glippen. Idealiter wordt de toegang tot alle toepassingen binnen het netwerk, in de cloud of zelfs SaaS, gecombineerd met Zero Trust-principes, waarbij voortdurend de gebruikers-ID, apparaatstatus en andere vitale parameters worden gecontroleerd, voordat er versleutelde toegang tot de toepassing wordt gegeven. Daarnaast zorgt ZTNA (Zero Trust Network Access) ervoor dat de juiste gebruiker uitsluitend toegang heeft tot de vereiste toepassingen, zodat ongecontroleerde vergaring van toegangsrechten wordt vermeden.

Barracuda.

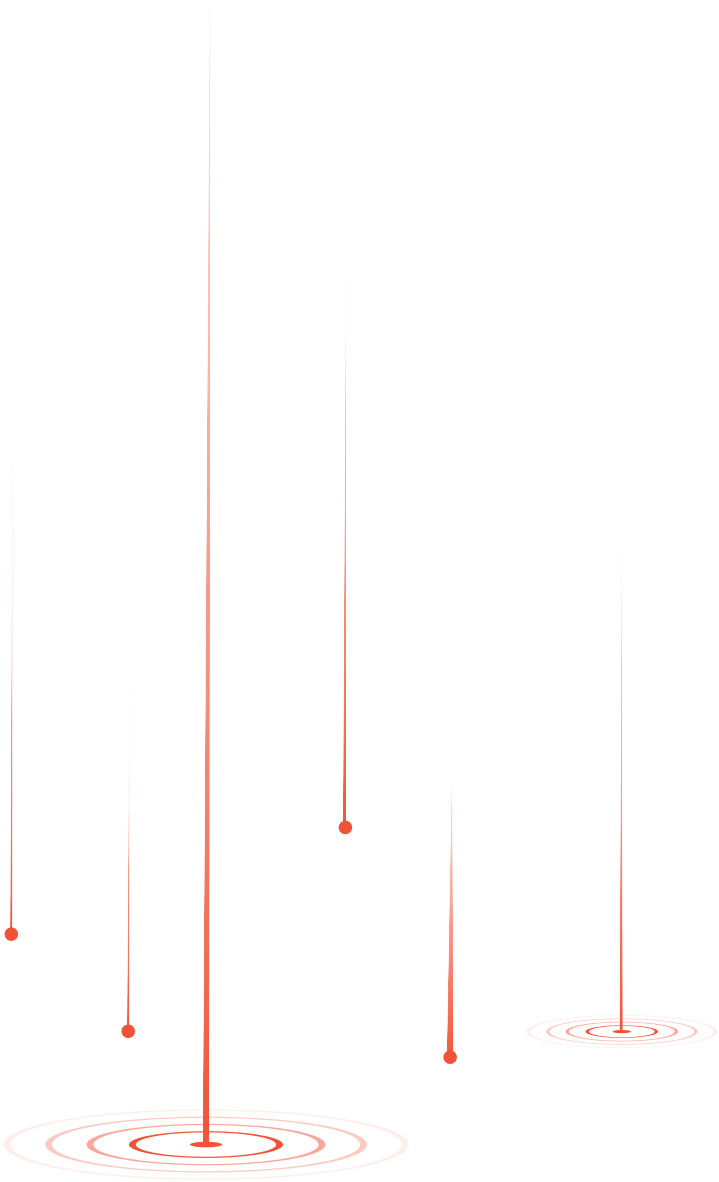
Een SD-WAN-oplossing (Software-Defined Wide Area Network) kan gebouwen, verspreide werklocaties en vertrouwde partners met elkaar verbinden en het gebruik van Zero Trust Network Access verbetert de beveiliging door gebruikers alleen toegang te geven tot de bronnen die ze nodig hebben om hun werk te doen, en alleen na authenticatie en via een versleuteld kanaal.

Conclusie

Lokale overheden lijken misschien geen voor de hand liggend doelwit voor cybercriminelen. Maar de sector wordt dagelijks aangevallen. De consument verwacht steeds eenvoudiger digitale toegang tot diensten, maar lokale overheden moeten het beperkte budget zo goed mogelijk gebruiken om de verdediging optimaal te houden.

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 lokale overheden een kosteneffectieve manier hebben om ervoor te zorgen dat de beveiliging up-to-date blijft. Het kan bijdragen tot een beter en een veiliger netwerk.

Ontdek hoe u een effectieve netwerkbeveiligingsstrategie kunt ontwikkelen met de krachtige beveiligingstools van Barracuda. Wij staan klaar om u te helpen. Lees hier meer over onze aanpak van netwerkbeveiliging.



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.