Netwerkbeveiliging die past bij de retail.

Barracuda
Your journey, secured.

Netwerkbeveiliging is een uitdaging voor de retail

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, in verspreide vestigingen of winkels, of vanuit huis, was al in opmars en is door de COVID-19-pandemie in een stroomversnelling gekomen. Retailaren moeten een veel groter aanvalsoppervlak beveiligen, waarbij vaak apparaten en netwerken worden aangesloten die niet onder hun directe beheer staan. Netwerkbeveiliging is vooral een uitdaging voor retailers met complexe banden met leveranciers en logistieke partners.

Barracuda.

De specifieke uitdaging voor de retail en hoe deze aan te gaan

Voor beveiligingsteams in de retail vormt zelfs het afbakenen van het netwerk (laat staan de verdediging ervan) een uitdaging. Beveiligingsprofessionals hebben aan winkels, e-commerce, logistieke systemen en connecties met andere leveranciers een hele kluif. Dit is een van de redenen waarom huidige verdedigingopties niet uitsluitend zijn gebaseerd op de beveiliging van de perimeter. Hoe goed u de afbakening ook maakt, u moet in de diepte verdedigen en binnen uw hele netwerk, en niet alleen eromheen, systemen hebben ingesteld.

- **Meerdere locaties:** Grote winkelketens tellen soms tientallen, honderden of zelfs duizenden locaties. Een enorm groot oppervlak om te verdedigen. Het gaat hierbij om winkels, kantoren, magazijnen en distributiecentra. Al die locaties moeten zijn beveiligd tegen aanvallen terwijl ze wel gewoon open moeten blijven voor het winkelend publiek en personeel.

- **Toegankelijke locaties:** Winkels, warenhuizen, shop-in-shops en zelfs kiosken vormen allemaal een potentieel netwerkbeveiligingsrisico. Betaalautomaten, handheld-betaalapparaten, voorraadterminals en andere apparatuur maken allemaal deel uit van het netwerk en moeten altezamen worden beveiligd tegen sabotage en aanvallen. Bovendien moeten op al deze locaties ook wifinetwerken worden beveiligd.

- **Online toegang:** De netwerken van retailers beperken zich niet tot alleen maar de winkels. Websites, e-commercetoepassingen, portals voor klantaccounts en toegang tot de toeleveringsketen zijn allemaal manieren waarop aanvallers systemen kunnen binnendringen.

- **Druk om te integreren:** De niet-aflatende druk van de retail op de marges betekent een nauwe integratie in het netwerk van e-commerce, IoT en andere slimme systemen, zoals POS, CCTV, zelfbedieningskiosken, tijdklokken, handscanners en HVAC-besturingen, om er maar een paar te noemen. De digitale transformatie betekent een nauwere integratie met leveranciers, waardoor het netwerkrisico nog groter wordt.

- **Er is training nodig voor uw personeel:** Uw medewerkers, of ze nu in de winkel, op kantoor of in een magazijn werken, 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.

- **Kwetsbaarheid opdrachtnemers:** Veel grote retailars besteden sommige taken betreffende de basisinfrastructuur uit aan opdrachtnemers en zakenpartners. Denk bijvoorbeeld aan het onderhoud van de verwarming, ventilatie en airconditioning of vitrines van diepvriezers en koelkasten. Het is van cruciaal belang dat ook die partijen een goede netwerkhygiëne handhaven en idealiter alleen gedeeltelijke toegang of Zero Trust Network Access krijgen. Zo niet, dan kunnen die externe partijen het startpunt 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.

Moderne winkels zijn afhankelijk van een enorme hoeveelheid IT-systemen om simpelweg te kunnen functioneren. Een IT-storing betekent niet alleen dat de kassa's buiten werking zijn en dat de voorraadsystemen niet werken. De realiteit is dat winkels hun deuren hebben moeten sluiten vanwege aanvallen op hun netwerken.

Een geslaagde aanval op een retailers is een pijnlijke openbare aangelegenheid. Shoppers zullen u zonder aarzeling de rug toekeren als uw diensten niet toegankelijk zijn. Dit vormt een serieuze bedreiging voor het voortbestaan van uw bedrijf, maar is niet onoverkomelijk.

Netwerkveiligheid is een aanpak, niet een product

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. De beveiliging moet werkbaar zijn voor het personeel, anders zullen zij simpelweg manieren vinden om deze te omzeilen. Daarnaast moeten beveiligde websites van retailers soepel functioneren voor klanten.

Een enkele beveiligingslaag, hoe sterk dan ook, werkt ook niet. Een crimineel die een enkele e-mailaccount binnendringt en dan vrij door het netwerk kan bewegen, is natuurlijk ook niet de bedoeling. De verdediging moeten de bewegingen binnen het netwerk controleren en bewaken, niet alleen in en uit het netwerk.

De juiste aanpak is het implementateren 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 (Secure Access Service Edge) mogelijk, een aanpak die de beveiliging decentraliseert en in elk deel van de organisatie plaatst, waar gebruikers zich ook bevinden.

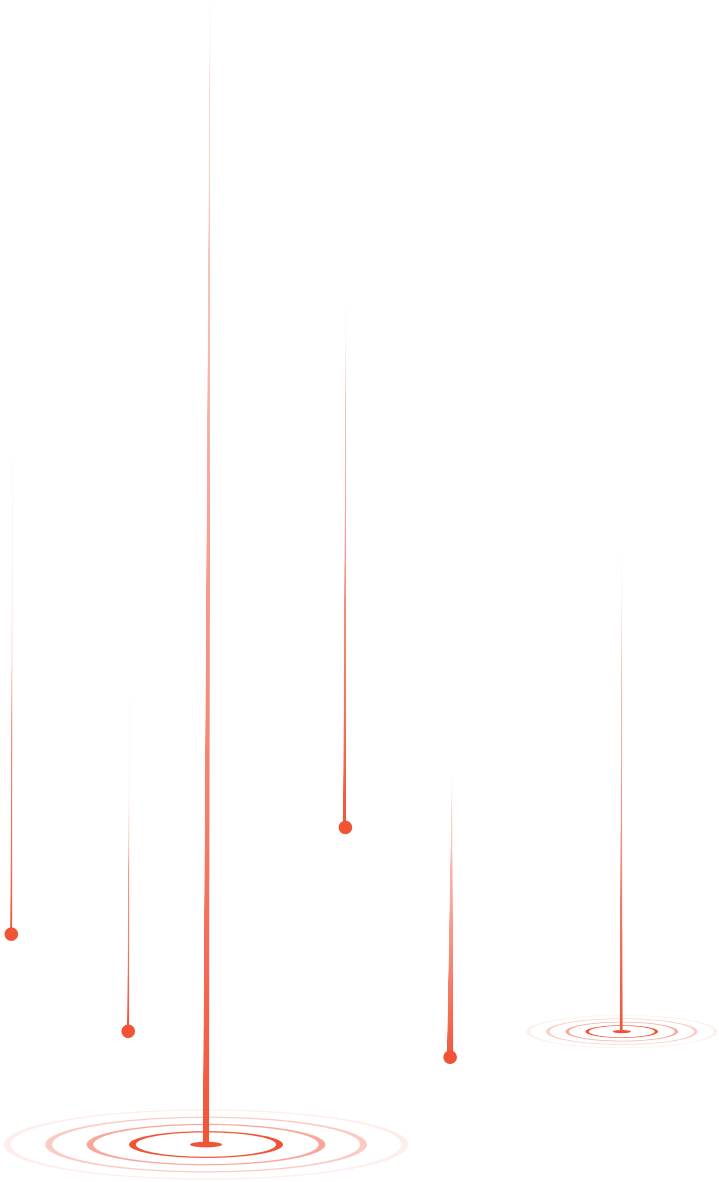
Netwerkbeveiliging komt voort uit robuuste componenten die samenwerken. Krachtige firewalls en mechanismen voor toegangscontrole houden indringers buiten de deur, terwijl netwerksegmentatie de laterale bewegingen van gebruikers of potentiële indringers beperkt, mochten zij langs het toegangsbeheer glippen. 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, externe werklocaties, winkels en vertrouwde partners met elkaar verbinden via meerdere versleutelde verbindingen en is veel goedkoper dan pseudo-veilige MPLS (Multiprotocol Label Switching) of andere geleasede lijnen.

Conclusie

De retail heeft te maken met een overvloed aan bedreigingen van cybercriminelen die voor winstdoeleinden inbreuk proberen te maken op hun netwerken. Malware, ransomware en allerlei andere soorten cyberaanvallen richten een ravage aan in de industrie. 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 de retail een kosteneffectieve manier heeft 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.

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.