DE GIDS OVER CYBERBEVEILIGING VOOR ELK BEDRIJF

EEN ANTWOORD OP AL UW VRAGEN

Nu cyberaanvallen jaarlijks toenemen, is het cruciaal voor zowel kleine als grote bedrijven om krachtige beveiligingsmaatregelen in te voeren voor e-mails, apparaten, bestanden en netwerken.

Bij Brick9 hebben we een jarenlange ervaring in het doeltreffend helpen bestrijden van geavanceerde cyberbedreigingen. Teneinde een waaier aan persoonlijke cyberbeveiligingsoplossingen te kunnen aanbieden om deze toegenomen criminaliteit te bestrijden, kozen we voor een samenwerking met de toonaangevende leverancier Barracuda.

Het is van kapitaal belang om de juiste oplossing te kiezen voor de specifieke behoeften van uw bedrijf. Daarom hebben we een overzicht gemaakt van alle belangrijke vragen die u uzelf zou moeten stellen om de beste oplossingen voor uw bedrijf te implementeren.

In dit e-book vindt u de nieuwste informatie en tips over cyberbeveiliging.

U krijgt een antwoord op uw vragen over:

WAAROM IS CYBERBEVEILIGING ZO BELANGRIJK?

91% van de bedrijven zegt dat de kosten van e-mailinbreuken oplopen.

78% van de hacks begint met een doelgerichte aanval via e-mail.

De gemiddelde kostprijs van een datalek bedroeg in 2019 maar liefst zo'n 3,2 miljoen euro en jaarlijks blijft het aantal cyberbedreigingen toenemen. Cyberbeveiliging is een slimme investering, niet alleen om uw gegevens te beschermen, maar ook om uw bedrijf mogelijks duizenden euro's te doen besparen.

Brick9 biedt haar klanten volledig beheerde, gecontroleerde en betrouwbare beveiligingsoplossingen aan van toonaangevende partners, waaronder Barracuda. Dit betekent dat u er zeker van kunt zijn dat we achter de schermen uw gegevens, apparaten en werknemers beschermen.

HOE KUNT U VEILIG TELEWERKEN?

Meer werknemers dan ooit doen nu aan telewerk. Het kan nochtans een echte uitdaging zijn om ervoor te zorgen dat ze zijn uitgerust om dat veilig te doen.

De meeste telewerkers hebben toegang tot de nodige bestanden, e-mails en gegevens via cloudtoepassingen zoals Microsoft 365. Hackers weten dat ook en richten zich specifiek op kwetsbare cloudnetwerken en cloudtoepassingen die niet beveiligd zijn.

1/3 van de bedrijven zegt dat ze gegevens zijn verloren van SaaS-applicaties, zoals Microsoft 365, omdat deze niet voldoende beschermd waren.

Hoewel het klopt dat Office 365 al een bepaald niveau van online bescherming biedt, is die bescherming beperkt en moeilijk te beheren voor een volledig personeelsbestand. Veel bedrijven ontdekken dat gegevensverlies nog altijd gebeurt omdat een back-up van gegevens niet op een veilige manier kon worden gemaakt.

Een ingebouwde, full-stack cloudbeveiligingsoplossing met netwerkbescherming is essentieel om ervoor te zorgen dat telewerkers vanaf eender welk apparaat veilig toegang hebben tot gegevens.

Barracuda Essentials voor Office 365 biedt een bijkomende bescherming voor e-mails en e-mailarchivering.
Hierdoor zal uw beveiliging niet onderworpen zijn aan Microsoft-beperkingen en kunt u er zeker van zijn dat al uw databases beschermd zijn.

Barracuda Cloud biedt een ecosysteem waarop bedrijven wereldwijd vertrouwen om anomalieën een stap voor te blijven en een veilige toegang vanop afstand te garanderen voor alle gebruikers.

HOE BESCHERM IK MIJN TEAM TEGEN PHISHING-AANVALLEN EN HACKERS?

De meest voorkomende vorm van cyberaanvallen zijn phishing-e-mails. Hackers stellen dergelijke e-mails op om een individuele gebruiker in de val te lokken en zo vertrouwelijke gegevens van hem te krijgen.

Een phishing-e-mail kan een schadelijke link bevatten of er kan in worden gevraagd om persoonlijke of financiële informatie aan de hacker te verschaffen. Die informatie kan daarna op het Dark Web worden verkocht.

van de cyberaanvallen begint met een e-mail.

E-mailbeveiliging

Bepaalde e-mailtoepassingen zoals Outlook of Gmail plaatsen spam- of junkmails automatisch in een aparte map voor u. Toch komen veel gerichte phishing-aanvallen nog steeds in inboxen terecht. Een krachtige filtering is nodig om ervoor te zorgen dat hackers worden opgemerkt en geblokkeerd, en dat verdachte inhoud proactief wordt opgespoord en risico's worden beperkt.

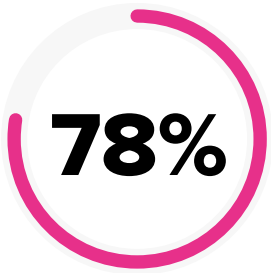
Barracuda beschermt elke dag meer dan een miljard e-mails met **Total Email Protection**. U kunt ook AI Phishing Protection implementeren via de Sentinel-oplossing die spear-phishing-aanvallen aanpakt door anomalieën te detecteren.

Traditionele antivirusproducten alleen bieden dit niveau van gespecialiseerde, innovatieve bescherming tegen oplichting niet.

KAN IEDEREEN EEN OPLEIDING IN CYBERBEVEILIGING VOLGEN?

De hoofdoorzaak van gegevensverlies zijn menselijke fouten. Niet alle succesvolle aanvallen of datalekken worden veroorzaakt door kwaadwillige of ontevreden werknemers – vaak gaat het gewoon om een simpele vergissing.

Cybercriminelen gebruiken steeds meer geavanceerde methoden, wat betekent dat aanvallen veel moeilijker te identificeren zijn.



van de mensen zei te weten dat onbekende links in e-mails een risico inhouden, maar ze klikken er toch op

Opleiding in cyberbeveiliging

In de meeste gevallen is uw eindgebruiker uw eerste lijn van verdediging. Als uw werknemers opgeleid en uitgerust zijn om cyberbedreigingen te identificeren, komt dit uw hele bedrijf ten goede. Hoewel het belangrijk is om te weten welke de meest voorkomende cyberbedreigingen zijn, raadt Brick9 haar klanten altijd aan om regelmatig opleidingen te volgen om op de hoogte te blijven van nieuwe, complexe risico's voor bedrijven.

Tijdens de **Security Awareness Training** leren werknemers hoe ze cyberbedreigingen kunnen herkennen en erop moeten reageren, in plaats van in de val van de hacker te trappen. Dankzij deze praktische opleiding vergaart uw team dergelijke kennis op basis van gesimuleerde, reële bedreigingsscenario's. Zo kunt u de resultaten van iedereen analyseren en de eventuele zwakke punten binnen uw team detecteren.

WAAROM MOET MIJN NETWERK WORDEN BEVEILIGD?

Netwerken worden steeds complexer, met meerdere sites, cloudplatformen en verbindingsproblemen waarmee rekening moet worden gehouden. Netwerken nemen snel toe, wat nieuwe beveiligingsproblemen met zich meebrengt, zoals het behoud van de controle over gegevens en de toegang ertoe.

Bijna 98 % van de bedrijven heeft te kampen met beveiligingsproblemen met een Wide Area Network (WAN)

Netwerkbeveiliging met een firewall

Ervoor zorgen dat uw personeel verbonden blijft via een beveiligd netwerk, is van cruciaal belang om de productiviteit in uw bedrijf op peil te houden. Vroeger blokkeerden firewalls enkel cyberbedreigingen, maar ze kunnen veel meer.

Het installeren van een **CloudGen-firewall in uw Wide Area Network (WAN)** zorgt voor een goede beveiliging, een permanente beschikbaarheid van uw netwerk en toegang tot cloudgebaseerde toepassingen. Het beheer is gecentraliseerd, wat wil zeggen dat u gemakkelijk een fijnmazig, waterdicht beveiligingsbeleid voor uw hele WAN kunt gebruiken.

HOE KAN CYBERBEVEILIGING MIJN BEDRIJF HELPEN OM ONDERBREKINGEN TE VOORKOMEN?

Uw gegevens beschermen is cruciaal voor een veerkrachtig bedrijf dat op lange termijn floreert. Elk bedrijf, klein of groot, is een potentieel doelwit voor cybercriminelen, en wanneer u een slachtoffer wordt, kan dat dure gevolgen hebben. Als een aanval slaagt, kunnen uw gegevens worden gegijzeld en kan het uren of zelfs dagen duren alvorens uw bedrijf terug operationeel is.

66%

van de bedrijven beweert dat aanvallen hen in 2019 geld hebben gekost en bijna 1/4 van hen zegt dat die kosten opliepen tot 82.000 euro of meer.

Gegevensback-up

Onderbrekingen kosten altijd geld, ongeacht de grootte van het bedrijf. Ransomware- en malwareaanvallen zijn bedoeld om gegevens te stelen of vervelende virussen te verspreiden die een volledig systeem kunnen platleggen. Als er geen doeltreffende back-up van uw gegevens werd gemaakt, kan de onderbreking tussen de aanval en het herstellen van wat nodig is om de activiteiten te hervatten, lang duren.

Beperk onderbrekingen en voorkom gegevensverlies met **Barracuda Backup**. Deze oplossing is cryptolocker-bestendig omdat het een gesloten ecosysteem is. Bestanden zijn alleen toegankelijk via een beveiligd toegangsplatform. Dit houdt in dat de gegevens tijdens een cyberaanval intact blijven, ongeacht of ze op hetzelfde netwerk zijn opgeslagen of niet. Hierdoor kunnen gegevens veel sneller worden hersteld dan wanneer u een back-up van uw gegevens op een andere site had gemaakt, zonder in te boeten op beveiliging.

Brick9 kan uw volledige back-upoplossing configureren en beheren, zodat u met een gerust hart weet dat uw bedrijf beschermd is. De back-up beschermt uw kritieke gegevens, zodat u ze snel en gemakkelijk kunt opvragen, mocht u ze ooit verliezen.

BRICK9

Barracuda
Your journey, secured.

VOLGENDE STAPPEN

Inzicht hebben in de cyberbedreigingen waarmee uw bedrijf te kampen heeft, is de enige manier om risico's te beperken en uw bedrijf langer en beter te beveiligen. Het risico op niets doen of minder waakzaam zijn, is groot en kan u veel geld kosten.

Brick9 werkt samen met Barracuda om cyberbedreigingen te bestrijden met behulp van de laatste, meest innovatieve oplossingen. Basissoftware is gewoon niet meer goed genoeg en **wij begrijpen wat er nodig is om uw gegevens te beveiligen**.

Als u een gesprek wenst met een specialist van Brick9, dan horen we graag van u. We weten hoe belangrijk uw gegevens zijn. Daarom bespreken we met plezier wat de volgende stappen best zijn voor uw bedrijfsbehoeften.
Word vandaag een veiliger bedrijf, samen met Brick9.

Neem vandaag nog contact met ons op.

Ask@brick9.com

+32 9 292 73 98

BRICK9

Barracuda
Your journey, secured.


BRICK9
Barracuda
Your journey, secured.