HELDEN VAN . NU
de provider voor het mkb

Digitalisering in de detailhandel, hier moet je aan denken

Whitepaper

Welkom

Waarom dit whitepaper?

Uit onderzoek onder een brede range van bedrijven, variërend in grootte, branche en businessmodel, blijkt dat de uitbraak van het coronavirus de digitale transformatie heeft versneld met zeven jaar. Zelfs binnen e-commerce, waar digitalisering niet nieuw meer is, is de ontwikkeling met een factor drie versneld. Dat betekent dat ook binnen de retailsector meer aandacht nodig is voor digitalisering. Snel internet, wifi, scheiding van netwerken voor bedrijfsvoering, leveranciers en gasten, netwerkbewaking, camerabewaking, IT-management en vaste en mobiele telefonieoplossingen: het is niet niks. In dit whitepaper nemen we je stap voor stap mee in de wereld van digitalisering binnen retail. Waar schuilen de gevaren, waar moet je aandacht voor hebben en wat kun je doen om de uitdagingen het hoofd te bieden?

Inhoudsopgave

HOOFDSTUK 1

Veiligheid boven alles

1. Veiligheid boven alles

Dataverbindingen zijn cruciaal voor de retailbranche. Kassa's, pinbetalingen, voorraadsystemen, alarmering voor en bewaking van pand, koelingen en vriesunits, weegschalen, verzin het en het maakt gebruik van een dataverbinding. Leveranciers loggen vanaf afstand in op hun apparatuur in de winkel. Veel detailhandelaars bieden bovendien een gratis wifi-netwerk aan hun klanten aan. Daar ligt meteen een groot gevaar op de loer: cybercriminaliteit.

1.1. Retail onweerstaanbaar doelwit

Deloitte onderzocht hoe het staat met cybersecurity binnen de retailsector. Bijna een derde van de 1.800 ondervraagde bedrijven is niet goed voorbereid op een cyberaanval en slaagt er niet in een goed preventie- en voorbereidingsbeleid neer te zetten. Dat is opvallend, zeker gezien het feit dat een bedrijf na een cyberaanval gemiddeld 57 dagen nodig heeft om weer normaal tot de normale, dagelijkse gang van zaken terug te keren. En aangezien creditcardgegevens het nieuwe goud zijn voor hackers en criminelen, is Retail een bijna onweerstaanbaar doelwit voor cyberaanvallen.

30%
VAN DE RETAILBEDRIJVEN IS NIET GOED VOORBEREID OP EEN CYBERAANAL

1.2. Gevaar ligt overal op de loer

Veiligheid is niet alleen cruciaal om aanvallen van buitenaf te weren. Insider-bedreigingen in de detailhandel nemen ook toe. Het personeelsverloop is hoog en het aantal vestigingen en distributiecentra neemt toe. Gegevens die niet goed bewaakt worden, staan in no time op een USB-stick of externe harde schijf die vervolgens in een willekeurige broekzak het pand verlaat. En hoeveel van je bedrijfsprocessen zijn er niet uitbesteed aan derden? Heb je leveranciers die hun apparatuur in jouw winkel op afstand beheren. Ook dat brengt een risico met zich mee, zelfs als je je leveranciers voor de volle honderd procent vertrouwt. Want hoe veilig is hun netwerk? Als zij worden gehackt, zit zo'n cyberboef in no time ook op jouw netwerk. Tenslotte vormen ook gebruikers van het gasten-wifinetwerk een potentieel gevaar. Zij mogen natuurlijk nooit en te nimmer bij de bedrijfsinformatie kunnen komen. Met behulp van fysiek gescheiden netwerken of het gebruik van VLAN's en het implementeren van diverse beleidsmaatregelen omtrent het netwerk stel je dit veilig..

1.3. Zorg voor veilige communicatie

Of een aanval nu eenvoudig of verfijnd is, de resultaten kunnen desastreus zijn. Toch zijn er genoeg mogelijkheden om veilige communicatie, met het hoofdkantoor en met vestigingen onderling, mogelijk te maken. Denk daarbij aan firewalls, VPN-verbindingen en SD-WAN-oplossingen, maar ook aan een goed inlogbeleid, goede beveiligingssoftware, monitoringtools, bijgewerkte software. Tenslotte is elk netwerk zo sterk als z'n zwakste schakel, dus zorg ook dat je medewerkers zich bewust zijn van de gevaren die op de loer liggen. Vijf tips om te zorgen voor veilige communicatie.

Case: Hackers stelen kaartgegevens van miljoenen klanten

Bij een grote retailer die diverse food- en non-foodproducten verkoopt, installeerden hackers malware op de point-of-sale-systemen van de winkel. De geïnfecteerde systemen registreerden de gegevens van elke kaart die door het pinapparaat werd gehaald, inclusief pincodes. De malware verspreidde zich door de hele organisatie en infecteerde uiteindelijk alle kassasystemen. Zo werden enorme hoeveelheden pasgegevens verzameld en voor illegale doeleinden doorverkocht voor grof geld. De aanval kreeg wereldwijde media-aandacht, waardoor het bedrijf ernstige reputatieschade opliep en de verkoopcijfers drastisch daalden.

bron: https://www.nu.nl/internet/2063003/hackers-stelen-miljoenen-creditcardnummers.html

Vijf tips voor veilige communicatie.

1.3.1. Scheid de netwerken

Zorg ervoor dat de netwerken voor bedrijfsvoering, leveranciers en gasten goed afgescheiden worden. Immers, het is niet de bedoeling dat je leveranciers jouw gevoelige bedrijfsinformatie kunnen zien en je wil ook niet dat het winkelende publiek eens lekker kan rondneuzen op jouw bedrijfsnetwerk. Zorg daarom dat je een goede router en firewall hebt geïnstalleerd, juist zijn geconfigureerd en up-to-date blijven.

1.3.2. Werk met een VPN

Een VPN is een Virtual Private Network, die het mogelijk maakt je bedrijfsnetwerk te verbinden met het internet, zonder in te leveren op veiligheid. Door al je locaties onder te brengen in één gesloten VPN-netwerk, zorg je dat de data die je uitwisselt, niet op straat komen te liggen. Op deze manier wordt het dataverkeer van de verschillende vestigingen van elkaar en van het internet gescheiden. Dat zorgt dat je netwerk volledig is afgeschermd, en daarmee dus ook belangrijke data zoals kassa- of persoonsgegevens

1.3.3. Zorg voor bijgewerkte software

Als je wil voorkomen dat je zorgvuldig verzamelde gegevens op straat komen te liggen, moet je ook zorgen dat je software altijd up-to-date is. Of misschien is dit een mooi moment om over te stappen naar de cloud. Je cloudprovider doet dan de hardware-investeringen, en zorgt voor onderhoud, beheer, de meest recente software-updates en back-ups. De server staat niet langer onder een bureau of in een meterkast. Storingen worden direct geconstateerd en opgelost. Allemaal voor een vast bedrag per maand. Groeit (of krimpt) je bedrijf, dan is het eenvoudig op- of afschalen.

Digitalisering in de detailhandel, hier moet je aan denken

HELDEN VAN . NU
de provider voor het mkb

1.3.4. Vergeet je hardware niet

Vergeet vooral je hardware niet. Hoe ouder de computer, hoe kwetsbaarder. Vaak is het niet meer mogelijk om updates uit te voeren, waardoor de computers niet meer goed beveiligd zijn. En we hoeven je niet te vertellen dat je anno nu een fikse boete riskeert als je niet alles doet om datalekken te voorkomen. Denk er wel aan dat oude hardware – dat zijn ook oude harde schijven of USB-sticks – op de juiste manier vernietigd moet worden, anders liggen je data alsnog op straat.

1.3.5. Stap over op een digitale alarminstallatie

Als we het over veiligheid hebben, moeten we natuurlijk ook fysieke bedreigingen denken. Vergeet daarom je alarminstallatie niet. Als je overstapt op een digitale IP-melder, kan de alarminstallatie een eventueel alarm doorgeven via de internetverbinding.

Nieuwsgierig?

Benieuwd naar hoe wij jouw bedrijf kunnen helpen met onze hoogwaardige digitale dienstverlening? Neem gerust contact met ons op via 088 – 40 88 400 of stuur een mail naar sales@heldenvan.nu. We denken graag met je mee!

HOOFDSTUK 2

Zonder bereikbaarheid geen business

2. Zonder bereikbaarheid geen business

Een snelle – en betrouwbare! – internetverbinding is dus cruciaal voor elke retailer. Veiligheid staat voorop, maar zonder online en telefonische bereikbaarheid geen business. Zeker niet in een wereld waar de digitalisering zo explosief groeit. Maar een internetverbinding kan uitvallen. Door te zorgen voor een goede back-up-verbinding vang je dit op. Vijf zaken die je niet mag vergeten.

2.1. Zorg voor een back-up-verbinding

Voor optimale betrouwbaarheid worden hoofd- en back-up-verbindingen over verschillende netwerken getransporteerd. Denk aan kabel, glasvezel en 4G. De kans op een gelijktijdige storing op beide netwerken is te verwaarlozen. Zorg dat bij een storing op de hoofdverbinding, al het internet-, pin- en telefoonverkeer automatisch via de back-up verbinding wordt afgehandeld. En zoek een partner die je verbinding monitort en direct contact opneemt als een storing zich voordoet.

2.2. Zorg voor noodstroomvoorzieningen

Om de gevolgen van stroomuitval op te vangen kun je alle actieve apparatuur aansluiten op noodstroom-accupacks. Vergeet daarbij je camerasysteem niet aan te sluiten!

2.3. Vergeet je alarm niet

Werk je met een digitaal alarmsysteem, dan moet ook die natuurlijk terug kunnen vallen op een back-up-verbinding. Met een back-up-verbinding over 4G wordt een mogelijk alarm via het mobiele netwerk afgehandeld. Dit kan zelfs een vereiste van de verzekeringsmaatschappij zijn. De installateur van de alarminstallatie kan je precies vertellen wat de voorwaarden bij jouw verzekeringsmaatschappij zijn.

2.4. Geef telefoonverkeer voorrang

Ook telefonie gaat tegenwoordig vaak via internet. Dat kan veel voordelen met zich meebrengen. De abonnement– en gesprekstarieven zijn laag. Je belt volgens de laatste digitale techniek. Je telefooncentrale zit in de cloud. Onderhoud, beheer en updates laat je aan je partner over. Zorg dan wel dat telefoonverkeer altijd voorrang heeft boven het internetverkeer. Alleen dan heb je optimale gesprekskwaliteit! Je wil toch niet riskeren dat je net met die ene belangrijke klant aan de lijn zit en de verbinding wordt weggedrukt!

2.5. Zorg voor een goed Service Level Agreement

Goede afspraken met je leverancier zijn natuurlijk ook cruciaal. Dankzij een goed SLA weet je onder welke voorwaarden je kunt terugvallen op de ondersteuning door je leverancier. In een SLA worden niet alleen de te leveren diensten en het overeengekomen kwaliteitsniveau beschreven, maar ook de rechten en de plichten van zowel de aanbieder als de afnemer.

Een goede voorbereiding is het halve (maat)werk

Geen bedrijf is hetzelfde. Dus ook de geboden oplossing niet. Een nieuw project moet daarom altijd starten met het creëren van gezamenlijk inzichtelijk: wat is de gewenste functionaliteit? Aan de hand hiervan kan een ontwerp en een proof of concept gemaakt worden en alle risico's en afhankelijkheden in kaart gebracht. Pas als iedereen overtuigd is van de gewenste werking, kun je overgaan tot implementatie. Ook in het implementatietraject moet elke stap overwogen worden genomen, zodat de business gewoon doorgaat.

Nieuwsgierig?

Benieuwd naar hoe wij jouw bedrijf kunnen helpen met onze hoogwaardige digitale dienstverlening? Neem gerust contact met ons op via 088 – 40 88 400 of stuur een mail naar sales@heldenvan.nu. We denken graag met je mee!

Te veel bomen? Helden Van Nu tonen je het bos!

We snappen dat het je kan duizelen. Welke maatregelen zijn een must en hoe voer je ze door? Helden Van Nu is gespecialiseerd in het leveren van hoogwaardige digitale dienstverlening binnen de retailsector. Met snel internet, wifi, scheiding van netwerken voor bedrijfsvoering, leveranciers en gasten, netwerkbewaking, camerabewaking, IT-management en vaste en mobiele telefonieoplossingen bieden wij een totaaloplossing voor winkelketens. Net als jij gaan wij voor optimale kwaliteit. Wij leveren een internetverbinding waar je altijd op kunt vertrouwen, maken bellen tegen lage kosten mogelijk en zorgen voor een pinverbinding die het altijd doet. Zodat je zorgeloos kunt doen waar je goed in bent: je klanten helpen.

Wij zitten boven op de bal

Technische storingen zijn helaas niet altijd te voorkomen. Zelfs niet met onze actieve monitoring. Maar continuïteit is cruciaal. Daarom bewaken wij elke verbinding actief. Is er toch een storing? Dan merkt ons bewakingscentrum dat direct. We nemen contact met je op per telefoon, mail of sms. Zo ben je direct op de hoogte van wat er aan de hand is en wat de vervolgstappen zijn. Via een app op je smartphone of via een webbrowser krijg je bovendien toegang tot ons monitoringsysteem. Alsof je naast ons in ons bewakingscentrum zit.

Wij zijn onafhankelijk van andere partijen

Bovendien zijn onze monteurs bevoegd wijzigingen door te voeren in de wijkcentrales van KPN voor DSL of FTTH glasvezel. Dit zorgt voor een aanmerkelijke versnelling van de oplostijd. We zijn immers niet afhankelijk van andere partijen, zoals KPN.

Wij lossen het gewoon op

Het verschil tussen providers komt naar boven als je ze nodig hebt. Voor advies. Voor de internetverbinding van je nieuwe vestiging. Bij een storing. Daar onderscheiden wij ons van de rest. Met betrokken mensen die begrijpen dat een storing van je internetverbinding desastreus is voor jouw organisatie en die van de hoed en de rand weten en het simpelweg voor jou oplossen.

HELDEN VAN . NU
de provider voor het mkb