Cyberrisico’s in de detail- en groothandel

19-10-2023 12:50

Veel winkeliers en groothandelaren hebben moeilijke jaren achter de rug. De pandemie zorgde voor veel disruptie terwijl ook de digitalisering verder is toegenomen. Die digitalisering bracht in veel gevallen omzetgroei met zich mee, maar zorgt ook voor een risico dat je niet mag onderschatten: cybercriminaliteit. Eén verkeerde muisklik kan grote gevolgen hebben. Toch zijn veel ondernemers zich daar niet bewust van terwijl er tienduizenden mkb'ers actief zijn in deze sectoren. Cybercriminelen kunnen hun malware over het web schieten, op zoek naar achterdeurtjes. Dat maakt ook zelfstandige winkeliers een potentieel doelwit.

In september 2023 vond de Vedis kennissessie over cybersecurity plaats op Nijenrode Business University. Cybersecurity is behoorlijk on(be)grijpbaar. Het bestaat eigenlijk niet. Je kunt namelijk nooit garanderen dat je bedrijf 100 procent veilig is voor elk mogelijk risico. Wat je wel kunt doen, is de focus leggen op het beschermen van de hoogst gewaardeerde bezittingen.

Als ondernemer in de dynamische detail- en groothandel wil je eigenlijk niet te veel bezig zijn met dit onderwerp. Je wilt focus op waar het om draait: je product of dienst verkopen en mensen daarmee helpen. Om dat te bereiken maak je een plan en stel je doelen. Je meet de performance en kijkt hoe bepaalde artikelen lopen. Ook kijk je of je genoeg personeel hebt en of die op de juiste plek zitten. Wanneer je met diezelfde bril kijkt naar cybersecurity kom je erachter dat de benadering hiervan eigenlijk niet zoveel verschilt. En dat hoeft niet duur te zijn.

‘Het is belangrijk cybersecurity te adresseren als strategisch

onderwerp'

Uitdagende omstandigheden

De brutowinsten van veel ondernemers staan nu meer dan ooit onder druk door gestegen inkoopkosten gecombineerd met gestegen personeelskosten, energiekosten en huurstijgingen met dubbele cijfers. Belastingschulden hadden tot voor kort weinig prioriteit bij ondernemers die liever eerst leveranciers en verhuurders betaalden, maar dat is voorbij. Het gevolg is dat de liquiditeitsruimte van veel bedrijven sterk verkrapt nu de ontvangen steun of uitgestelde belastingen moeten worden terugbetaald. Als retailer of groothandelaar heb je dus wel iets anders aan je hoofd dan nieuwe privacy- en securityregelgeving.

Desalniettemin gaan bedrijfsdoelen, privacydoelen en securitydoelen vaak hand in hand. Non-compliance en onveilige systemen kunnen miljoenen kosten in boetes en misgelopen inkomsten. De grote hoeveelheid risico's en producten maakt het moeilijk om beslissingen te nemen over welke cybersecurity-oplossing het beste is. De meeste bieden vaak maar een oplossing voor 1 klein aspect, bijvoorbeeld een enkele end-point beveiliging. Het is daarom belangrijk om cybersecurity te adresseren als een strategisch onderwerp binnen je bedrijf. Doel is een overzicht te krijgen van de belangrijkste risico's waarna de cyberstrategie vertaald kan worden naar operationeel niveau en bijbehorende oplossingen.

Neem cyberrisico's serieus

Er is alle reden om cybercriminaliteit serieus te nemen. Zeker omdat winkels en groothandels steeds 'digitaler' worden. Dé trend in beide sectoren is omnichannel klantcontact. Waar er vroeger één raakpunt was met de klant, de fysieke winkel, heb je als winkelier maar ook als groothandel nu overal zogeheten 'online touchpoints' zoals mobiele apps, websites en grote online platformen. Dat is goed voor de omzet en zichtbaarheid bij klanten, maar wel een digitaal risico voor bedrijfsprocessen. Het maakt ondernemers extreem afhankelijk van digitalisering terwijl we vaak zien dat kennis over goede IT-beveiliging ontbreekt.

Ook op het gebied van voorraadbeheer is er veel veranderd. Daar waar vrijwel alle retailers hun spullen voorheen nog inkochten en lieten bezorgen, werken steeds meer ondernemers nu samen met merken of groothandels vanuit één centraal voorraadsysteem. Dit betekent vervolgens dat je afhankelijker bent van zo'n gedigitaliseerde oplossing. Als dat systeem platligt, kun je niks meer verkopen. De slag in efficiency brengt dus ook nieuwe risico's met zich mee.

Van phishing tot datalekken

Een cyberaanval kan invloed hebben op de gehele keten, van leverancier tot afnemer. Uit onderzoek van INretail blijkt dat ruim 70 procent van de winkeliers weleens in aanraking is gekomen met online criminaliteit. Het gaat dan bijvoorbeeld om:

- **Ransomware**: Dit is een vorm van malware, een geïnfecteerd stukje software dat als wapen geldt. Hiermee wordt je IT-systeem versleuteld en vergrendeld waardoor je bestanden plotseling niet meer kunt openen. Bij betaling belooft de tegenpartij je IT-systeem weer te ontgrendelen.

- **Phishing**: Een winkelmedewerker klikt per ongeluk op een link of opent een besmette e-mailbijlage. Zo lukt het de criminelen om toegang te krijgen tot vertrouwelijke gegevens en deze te stelen, geld afhandig te maken of om malware, zoals ransomware, te installeren. Maar liefst 91 procent van de datalekken start met een phishing mail.

- **Datalek**: Door een slecht beveiligde server of geslaagde phishingaanval liggen plotseling de persoonsgegevens van klanten op straat. Dit kan leiden reputatieschade en verlies van vertrouwen van klanten in je bedrijf. Bovendien heb je de plicht om de aanval aan je klanten en de Autoriteit Persoonsgegevens te melden. Doe je dit niet? Dan kun je een flinke boete krijgen.

- **Baiting**: Een hacker probeert iemand met een valse belofte te verleiden. Bijvoorbeeld door een usb-stick achter te laten met de belofte dat de vinder een geldbedrag krijgt. Wanneer de vinder de usb-stick in zijn computer plugt om de eigenaar te achterhalen, dan wordt er automatisch malware geïnstalleerd.

'Cybercriminelen maken geen onderscheid'

4 inzichten rondom ‘zero trust’

Never trust, always verify (vertrouw nooit, verifieer altijd). Dat is de kern van ‘zero trust’. Terwijl interne processen vaak als vanzelfsprekend worden vertrouwd, wantrouwt deze nieuwe standaard alle eentjes en nulletjes in het digitale domein. Naast dit sterke uitgangspunt helpt het om te denken aan ‘protect surface’ (beschermingsoppervlakken) in plaats van ‘attack surfaces’ (aanvalsoppervlakken). Klinkt ingewikkeld? We leggen het uit.

In plaats van een poging om alles te beschermen tegen alle mogelijke aanvallen, bepaal je eerst wat belangrijk is voor jouw bedrijf en focus je daar je inspanningen op. Inherent aan ‘zero trust’ is het gebruik om minimale digitale rechten toe te kennen aan alle medewerkers. Daarnaast wordt een extra stap toegevoegd als er grote veranderingen worden doorgevoerd. Als laatste: het is goed om vertrouwen te hebben in mensen, maar het is beter om de controle te behouden.

Oplossingen om de informatiebeveiliging te versterken

Het essentiële element om beveiligingsproblemen zoals hacks te voorkomen, is proceshygiëne. Dit zijn maatregelen die ervoor zorgen dat je de controle hebt. Het begint al aan de deur, met toegangsbeheer. Wie heeft er toegang tot een systeem? Waarom hebben ze die toegang en waarvoor precies? Tot wanneer, hoe laat en op welke manier? Daarnaast is het raadzaam om een scheiding aan te brengen in je IT-infrastructuur zodat de belangrijkste, kritische systemen los van elkaar staan. Zo kan een hacker niet van het ene naar het andere systeem wandelen als die eenmaal binnen is. Vervolgens kan configuratiebeheer helpen om te zorgen dat de systemen voldoen aan de laatste standaarden. Als laatste is het belangrijk om 24 uur per dag, 365 per jaar alle kritische systemen te surveilleren op abnormaal gedrag en mogelijke zwakke punten te ontdekken en versterken.

4 take-aways

Allereerst is het belangrijk om te weten wat je doelen zijn, welke bezittingen het meest waardevol zijn en welke risico’s eraan gerelateerd zijn. Ten tweede moeten de maatregelen die je neemt om die bezittingen te beschermen in verhouding zijn met aan de risico’s. Naast dit zogenaamde ‘protect thinking’ is het cruciaal dat je exact weet welke wetgeving op jouw bedrijf van toepassing is. Als laatste is het goed als je zelf weet dat je bedrijf digitaal in controle is, maar je moet dat ook aan anderen kunnen tonen. Een proactief ‘in control statement’ is daarvoor de oplossing. Deze laatste takeaway is de belangrijkste. De andere drie zijn voorwaarden om het ‘in control statement’ op de juiste manier te kunnen maken.

De juiste vragen stellen

Als ondernemer stel je jezelf continu vragen over je bedrijfsprocessen. Wat zijn mijn doelen? Wat verkoopt het best? Wat kunnen we beter doen? Je kan gelijksoortige vragen ook stellen over je digitale zekerheid rondom het waarborgen van de kwaliteit, betrouwbaarheid en veiligheid van je digitale systemen, software en processen.

- Welke doelen hebben wij onszelf gesteld als het gaat om informatierisico's, security en assurance?
- Wat zijn onze hoog gewaardeerde bezittingen? Kortom, wat heeft prioriteit om te beschermen?
- Welke lessen trekken we uit de afgelopen twaalf maanden en wat kunnen we beter doen?
- Hoe meten wij onze Informatiebeveiliging rondom het waarborgen van de vertrouwelijkheid, integriteit, beschikbaarheid en authenticiteit van die informatie (inclusief die van onze keten) en hoe draagt dat bij aan onze bedrijfsdoelen?
- Hoe gebruiken wij onze IT investeringen en hoe meten we dat?

Bescherm je tegen aanvallen

Of je nu een groot bedrijf of een kleine mkb'er bent met een paar mensen op de loonlijst, cybercriminelen maken geen onderscheid. Als winkelier of groothandelaar moet je daarom blijven investeren in digitale veiligheid. Dit doe je bijvoorbeeld door:

- Medewerkers te trainen op bewustwording van cyberincidenten en cyberveiligheid. In meer dan 90 procent van de cyberincidenten gaat het mis door menselijk handelen. Medewerkers klikken op een besmette link of hebben toegang tot bestanden die beter beveiligd moeten zijn. Programma's die inspelen op deze risico's zijn daarom erg belangrijk.
- Gebruik te maken van sterke wachtwoorden of wachtwoordzinnen, bij voorkeur in combinatie met meervoudige authenticatie. Dit is na het inloggen met een gebruikersnaam en wachtwoord een extra controlemoment in de vorm van bijvoorbeeld een sms.
- Helder te hebben wie verantwoordelijk is voor alle IT-gerelateerde zaken, zoals het toegangsbeheer, de cybersecurity en het incidentenbeleid.
- Het versleutelen van vertrouwelijke en persoonlijke informatie.
- Het opstellen van een incidentbeleid, zodat je weet wat te doen bij een aanval.
- Minimaal 1 keer per maand een back-up te maken en die op te slaan buiten je netwerk, bij voorkeur offline. Vergeet ook niet om deze back-up te testen.
- Het installeren van permanente antivirussoftware en een firewall.
- Updates - waar mogelijk - regelmatig uit te voeren en door systemen en applicaties te 'patchen'. Dit is een soort van APK voor software.

'Schade vanuit uit cyberrisico's kan een enorme impact hebben'

Het verzekeren van risico's

Het bespreken van cyberrisico's wordt ook vanuit financieringsoogpunt steeds belangrijker. Dit komt omdat bedrijven steeds meer afhankelijk zijn van technologie en het internet, waardoor ze een groter risico lopen op cyberaanvallen en datalekken. Een cyberverzekering helpt om de kosten en gevolgen van deze incidenten te beperken. Cyberincidenten kunnen een grote impact hebben en (in)direct leiden tot financiële- en reputatieschade voor organisaties. Bijvoorbeeld door het maken van extra kosten voor herstel van bestanden/documenten en het inhuren van een experts (IT, PR, Juridisch). Maar ook inkomstenderving als gevolg van bedrijfsstilstand, boetes als gevolg van een incident en aansprakelijkheidsclaims van derden.

Het ontstaan van cyberrisico's is onder te verdelen in 3 hoofdoorzaken:

- Operationele systeemstoringen zonder dat er sprake is van kwaadwillig handelen;
- Een aanval van buitenaf (bijv. ransomware, malware, een virus, DDoS-aanval);
- Al dan niet opzettelijk menselijk handelen (b.v. versturen email naar verkeerde ontvanger, uitval als gevolg van mislukte update, verlies laptop met vertrouwelijke informatie).

De schade die voortkomt uit cyberrisico's kan een enorme impact hebben. Cyberrisico's zijn tegenwoordig voor bedrijven en organisaties net zo voelbaar als het verlies van fysieke bezittingen én de kans op een incident is aanzienlijk groter. Hoe goed organisaties ook beveiligd zijn, elke organisatie blijkt in de praktijk kwetsbaar voor de risico's die horen bij het gebruik van computersystemen. Investeren in het voorkomen van cyberincidenten is de basis, het verzekeren van cyberrisico's is het sluitstuk.

Over de auteurs

Olaf Zwijnenburg is sectormanager retail en groothandel bij Rabobank Nederland en is daarvoor als directeur verantwoordelijk en betrokken geweest bij grote transities van internationale retailers en merken.
Peter van Heerde is sectormanager retail en groothandel bij Rabobank Nederland en heeft als bankier jarenlang retailers en groothandels gefinancierd.
Mark van Kampen is sectormanager ICT bij Rabobank Nederland en heeft als bankier jarenlang ervaring in de IT-en dienstverleningssector.
Dr. Yuri Bobbert is professor aan Antwerp Management School en betrokken bij ON2IT Zero Trust Innovators. Daarnaast is hij ceo van Anove International, een bedrijf dat zich toelegt op Digital Assurance.

Peter van Heerde, Olaf Zwijnenburg, Mark van Kampen en Yuri Bobbert