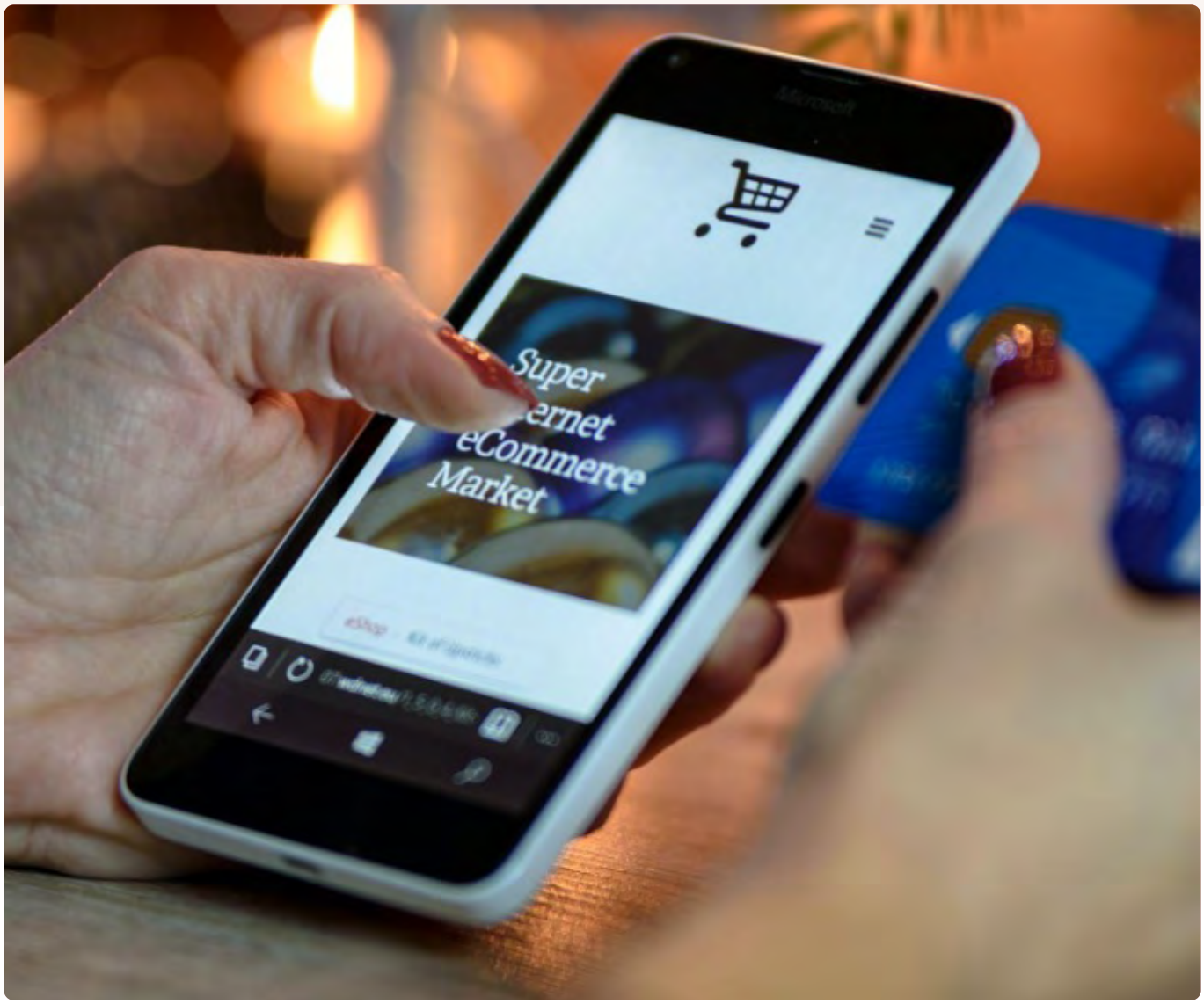
Perfect Day

Cybercrime in e-commerce

Trends, ontwikkelingen en tips voor bedrijven met webshops



www.perfectday.nl

Waarom is cybersecurity zo'n heet hangijzer voor webshops?

Volgens cijfers van de Kamer van Koophandel zijn in 2021 nieuwe 27.000 webshops ingeschreven in het handelsregister. De omzet uit online verkopen is met 86% gestegen. Dat zijn duizelingwekkende cijfers en een teken dat consumenten gretig gebruik maken van e-commerce. Dit is goed voor de economie en de ondernemers achter online winkels. Maar ook voor cybercriminelen die kansen zien in een markt die blijft groeien, met bedrijven die zich niet goed beschermen.

Je leest deze whitepaper ongetwijfeld om twee redenen. De eerste reden is dat je nieuwsgierig bent naar het fenomeen cybercrime. De andere reden is dat je benieuwd bent wat er zoal voor dreigingen zijn en hoe je jouw webshop hiertegen kunt beschermen. Hierover gaat deze whitepaper. Voor we je laten zien hoe jij jouw webshop optimaal beschermt tegen cyberincidenten, eerst wat context.

Cyberincidenten webshops

Volgens cijfers van de Kamer van Koophandel zijn in 2021 nieuwe 27.000 webshops ingeschreven in het handelsregister. De omzet uit online verkopen is met 86% gestegen. Dat zijn duizelingwekkende cijfers en een teken dat consumenten gretig gebruik maken van e-commerce. Dit is goed voor de economie en de ondernemers achter online winkels. Maar ook voor cybercriminelen die kansen zien in een markt die blijft groeien, met bedrijven die zich niet goed beschermen.

Je leest deze whitepaper ongetwijfeld om twee redenen. De eerste reden is dat je nieuwsgierig bent naar het fenomeen cybercrime. De andere reden is dat je benieuwd bent wat er zoal voor dreigingen zijn en hoe je jouw webshop hiertegen kunt beschermen. Hierover gaat deze whitepaper. Voor we je laten zien hoe jij jouw webshop optimaal beschermt tegen cyberincidenten, eerst wat context.

De incidenten die het nieuws halen, zijn nog maar het topje van de ijsberg. Door de jaren heen hebben ontelbare cyberincidenten bij webshops wereldwijd plaatsgevonden. Ook in Nederland zijn enkele webshops in verlegenheid gebracht.

Cijfers en feiten over e-commerce:

- In 2021 waren er 77.890 webwinkels in Nederland. Het grootste deel van de webwinkels verkoopt kleding (17.940) of non-foodartikelen (13.780).
- Bijna 70% van de ondernemers in e-commerce voldoen niet aan de wet ter bescherming van persoonsgegevens AVG. Bij 10% van de ondernemers is de situatie rondom wetgeving zelfs heel slecht.

Enkele voorbeelden:

Januari 2020 Een beveiligingsonderzoeker krijgt persoonlijke gegevens van 7000 klanten van verschillende webshops in handen. Hij kwam erachter dat hij klantgegevens kon ophalen door de URL van zijn eigen profiel op één van de webshops iets aan te passen. Op deze manier kon hij de klantgegevens van 7000 andere klanten inzien.

Februari 2021 Blokker heeft voor de tweede keer te maken met een datalek. Een oplettende ethical hacker had toegang tot persoonsgegevens van Blokker klanten. In totaal zou het gaan om 720.000 orders waarvan alle data inzichtelijk werd voor de hacker. Hiervoor hoefde hij slechts het ordernummer de URL aan te passen. Door een slimme query toe te passen kon hij een gigantische lijst met klantdata downloaden.

Voorjaar 2021 Bij een online kledingwinkel vond in 2021 een ransomware aanval plaats. Hierdoor werden bestanden op de NAS ontoegankelijk. Er stonden belangrijke gegevens op, zoals zakelijke gegevens, content en productfotografie. Het bedrijf moest een bepaald bedrag in Bitcoins overmaken om weer toegang te krijgen tot de bestanden. Dit heeft het bedrijf uiteindelijk ook gedaan, in de hoop dat ze geen verdere kosten hoefden te maken om de toegang tot de gegevens op een andere manier te herstellen. Maar helaas gebeurde er helemaal niets nadat het losgeld was betaald.

april 2022 Tientallen webshops van Allekabels.nl werden getroffen door een datalek. Door een hack heeft een cybercrimineel toegang gekregen tot de database, waarin persoonsgegevens gevonden werden. Van gedupeerden zijn niet alleen e-mailadres en huisadres bekend geworden. Ook de IBAN-gegevens van klanten van DutchDo zijn in verkeerde handen terecht gekomen.

De geschiedenis van e-commerce

E-commerce bestaat sinds de jaren '90, maar nam pas de afgelopen jaren een vlucht. De pandemie heeft hier nog een schepje bovenop gegooid, met als gevolg dat er nu rond de 80.000 webshops in Nederland actief zijn. Van grote corporates als Bol.com en Amazon, tot de webshop van de buurvrouw op haar zolderkamer. Ook bedrijven als Facebook (waar je online kunt kopen) en Marktplaats zijn e-commercebedrijven.

Het verzamelen van data voor marketingdoeleinden

Zolang er via het internet wordt verkocht, spreken we van e-commerce. Het principe is: iemand komt naar je website, kiest een product en voltooit de betaling. Maar tijdens deze reis heeft de consument al op verschillende manieren en op verschillende momenten gegevens achtergelaten, die jij zorgvuldig moet behandelen. Daarom is het belangrijk om te weten wat je op welke plek verzamelt, met welke middelen en vooral hoe je klantdata beschermt. Daarover later meer. Eerst nemen we je graag mee in de meest actuele ontwikkelingen bij webshops.

Cyber ontwikkelingen bij webshops

Persoonlijke aanbevelingen

Steeds meer webshops gebruiken de koophistorie en persoonlijke gegevens van klanten om aanbevelingen te doen voor andere producten die wellicht in het kooppatroon vallen. Hierdoor is de kans op herhalingsaankopen groter. . Het is van belang om voorzichtig met deze gegevens om te gaan, omdat hier ook persoonsgegevens in kunnen voorkomen. Zorg ervoor dat je klanten goed informeert over het gebruik van hun persoonsgegevens. Zet dit in de verplichte privacyverklaring.

Third-party cookies

Third-party cookies gaan de komende maanden verdwijnen. Dit komt mede omdat gegevensbeschermingsautoriteiten steeds strenger worden over het gebruik van third-party cookies. Hierdoor kan adverteren lastiger worden. Momenteel doet men onderzoek naar een goede vervanger voor cookies, zeker om de gepersonaliseerde marketing te kunnen blijven gebruiken. De verwachting is dat third-party cookies pas in 2023 verwijdenen. Maar houd er wel rekening mee dat het gebruik van cookies veel beperkter kan worden in de komende maanden. Wanneer je cookies gebruikt op je website, moet je daarvoor toestemming vragen aan je websitebezoeker, via een keuze in de cookiemelding.

Augmented Reality

Steeds meer bedrijven in de detailhandel gaan gebruik maken van Augmented Reality. Augmented Reality is een beeld van de werkelijkheid waaraan virtuele elementen worden toegevoegd door een computer. Hierdoor kan een klant bijvoorbeeld precies zien hoe een kledingstuk staat of hoeveel ruimte een bepaalde bank inneemt in de woonkamer. Op deze manier is het makkelijker voor een klant om een keuze te maken en is de kans op retournering van producten kleiner.

Afhankelijkheid van andere partijen

Je bent sterk afhankelijk van andere partijen zoals bijvoorbeeld je leveranciers of aanvullende dienstverleners zoals pakketbezorgers. Een cyberaanval op een van deze partijen binnen je keten kan ook een grote impact hebben op jouw bedrijf. Bijvoorbeeld omdat bepaalde producten of diensten niet meer geleverd kunnen worden. Maar ook omdat jouw gegevens in de handen kunnen vallen van cybercriminelen. Het is dus belangrijk om goede afspraken te maken met de ketenpartners over verantwoordelijkheden in het geval van een cyberaanval.

De top 5 cyberrisico's voor webshops

1

Spookfacturen Factuurfraude

Factuurfraude wordt op meerdere manieren toegepast. Zo sturen cybercriminelen facturen naar willekeurige bedrijven in de hoop dat er geen goede controle plaatsvindt op de authenticiteit. Door drukte binnen het bedrijf of de lage factuurbedragen, wil er nog wel eens een doorheen glippen. Dit noemen we spookfacturen. Een andere methode is CEO-fraude waarbij een valse betaalopdracht wordt gedaan uit naam van de CEO, of CFO van die organisatie. Tenslotte is er nog de gepersonaliseerde nepfactuur. Men doet zich voor als een leverancier van de onderneming, past het rekeningnummer op de factuur aan en hoopt op slechte controle bij de financiële administratie van het betreffende bedrijf. Vooral CEO-fraude en gepersonaliseerde nepfacturen zijn de laatste tijd een succesvolle methode geweest.

2

DDoS aanvallen

DDoS staat voor Distributed Denial of Services. Het is een cyberaanval waarbij heel veel verkeer tegelijkertijd naar computers, computernetwerken of servers wordt verstuurd waardoor deze overbelast raken en niet meer te gebruiken zijn. Hierdoor raakt je website onbereikbaar, wat tot een verlies van inkomsten kan leiden. Ook krijg je waarschijnlijk te maken met reputatieschade omdat klanten je website onbetrouwbaar vinden omdat die tijdelijk niet bereikbaar was na een cyberaanval.

3

Ransomware

Ransomware is schadelijke software die je binnenhaalt door op een verkeerd linkje te klikken of een geïnfecteerd bestand te downloaden. Dit kunnen ook afbeeldingen zijn. Bijvoorbeeld een afbeelding van een schade, of een pdf met zogenaamd retourlabel. Dankzij de software die zo op jouw computer terecht komt, kunnen criminelen jouw bestanden en systemen versleutelen. Ze eisen losgeld in bitcoins om je gegevens weer te ontsleutelen. Hierdoor kan je de toegang tot belangrijke gegevens en systemen verliezen, waardoor je niet meer (naar behoren) kunt werken en leveren. Ook kun je hierdoor productomschrijvingen en -foto's van je producten kwijtraken, waardoor het aanbod op de website niet meer volledig is.

4

Hacks

Een crimineel dringt je systemen binnen en heeft hierdoor toegang tot het systeem en alle gegevens die in dit systeem te vinden zijn. Hierdoor kan een crimineel dus aan gevoelige bedrijfsinformatie komen, die bijvoorbeeld met concurrenten of op het darkweb verkocht kan worden. Ook kan de crimineel gegevens in de systemen aanpassen of cruciale gegevens op je website aanpassen. Bijvoorbeeld door betalingen om te leiden of prijzen aan te passen. Ook kan er malware op de website worden geplaatst die je bezoekers besmet bij bezoek.

5

Datalekken

Datalekken kunnen op diverse manieren plaatsvinden, bijvoorbeeld bij het verliezen van een telefoon of laptop, door per ongeluk informatie naar de verkeerde persoon te sturen of door een hack. Hierdoor kunnen persoonlijke gegevens van klanten en medewerkers op straat komen te liggen, met alle gevolgen van dien. Dit kan leiden tot reputatieschade en een boete van de Autoriteit Persoonsgegevens wanneer er niet op de juiste wijze wordt gehandeld.

Hoe bescherm je jouw bedrijf tegen deze risico's?

Voordat je aan de slag kunt met cybersecurity moet je weten wat je moet beschermen. Met welke apparaten werk je, en wat doe je met de apparaten. Welke applicaties gebruik je, en waar worden je gegevens opgeslagen? Als je bijvoorbeeld met OneDrive werkt, worden gegevens dan alleen in de cloud opgeslagen, of ook op je harde schijf? Werk je ook op een NAS, zet je een klantenlijst op een USB-stick, app je even wat adresgegevens door omdat een e-mail niet is aangekomen?

Beveilig je website

Het is erg belangrijk dat de beveiliging van jouw website altijd volledig up-to-date is. Zorg ervoor dat de juiste standaarden en certificaten ingesteld staan en up-to-date zijn. Dit kan meestal worden geregeld door de websitebouwer of de hostingpartij. Zorg ervoor dat je duidelijke afspraken met hen hebt gemaakt over de updates en de beveiliging van de website. Ook kan je zelf controleren hoe het met de basisinstellingen van je website is via www.internet.nl.

IT Up-to-date en back-ups

Zorg ervoor dat je computers up-to-date zijn, er een firewall aanwezig is en er antivirus software op iedere computer staat geïnstalleerd. Ook moet je back-ups van je systemen hebben voor het geval dat het toch misgaat. Een verwijderd bestand of een ontoegankelijk systeem kan op die manier worden teruggehaald, mits je de back-ups op de juiste wijze hebt gemaakt. Zorg ervoor dat de back-ups ver genoeg teruggaan in de tijd en dat je meerdere versies bewaart, zowel online als offline op een harde schijf. Test ook regelmatig de back-ups om te kijken of deze goed werken.

95% van de cyberincidenten zijn direct gevolg van menselijk handelen."

Bewustzijn van medewerkers

Zorg ervoor dat medewerkers op de hoogte zijn van de cyberrisico's van jouw bedrijf. Ga hiervoor het gesprek met hen aan: hoe herken je een phishing e-mail? Wat moeten de medewerkers doen wanneer ze op een verkeerd linkje klikken? Maak afspraken met de medewerkers over hoe zij veilig omgaan met gegevens en systemen, bespreek dit regelmatig en volg trainingen waar nodig.

Afspraken met ketenpartners

Het is belangrijk om goede afspraken te maken met de partijen waarmee je samenwerkt. Wat kan je van hen verwachten wanneer er iets misgaat? Stellen ze je dan meteen op de hoogte? Wie is er verantwoordelijk als er schade wordt geleden? Dit zijn allemaal belangrijke zaken om op papier te hebben staan. Zo ben je op de hoogte van wat je van ze kan verwachten en kan je waar nodig ook zelf maatregelen treffen. Zorg er ook voor dat het uitwisselen van gegevens, bijvoorbeeld persoonsgegevens en financiële gegevens op een veilige wijze gebeurt. Denk hierbij bijvoorbeeld aan het gebruiken van een beveiligd portaal.

De 10 quick-wins van cybersecurity voor jouw webshop

1. **Maak een noodplan**
   Wat ga je doen als je netwerk plat ligt? Of als je een datalek hebt? Wie moet je waarschuwen en wie moet het oplossen? Met een goed noodplan beperk je altijd schade!

2. **Installeer goede antivirussoftware en firewalls**
   Lijkt een open deur, maar blijkt het niet te zijn. Schaf het aan, ook als je op een Mac werkt. Een snelle manier om risico's te verkleinen.

3. **Zorg dat alle software up-to-date is**
   Via bekende beveiligingslekken is het makkelijk binnenkomen voor criminelen. Vergeet niet om naast de voor de hand liggende devices ook apparaten als je router, Sonos speakers, slimme thermostaat etc. te updaten.

4. **Maak een wachtwoord protocol**
   Gebruik sterke, unieke wachtwoorden. Wij raden het gebruik van een wachtwoordmanager aan.

5. **Investeer in goede back-ups**
   Back-uppen is niet hetzelfde als synchroniseren naar de cloud. Zorg voor een goede faciliteit die is los staat van je netwerk en systemen.

6. **Test met het terugzetten van back-ups**
   Belangrijk en vaak vergeten. Probeer een paar keer per jaar of je de back-ups teruggezet krijgt en of alles dan nog goed werkt.

7. **Inventariseer welke apparaten er allemaal in je netwerk hangen**
   Vergeet ook hier de slimme thermostaat, draadloze speakers en ipads van de kinderen niet.

8. **Versleutel (encrypt) alle apparaten**
   Zo blijft de data beschermd en kan de harde schijf niet zomaar worden uitgelezen. Belangrijk als een apparaat verloren of gestolen is.

9. **Zet waar mogelijk 2 factor authenticatie aan**
   Zelfs als iemand jouw login en wachtwoord heeft, kan hij niet in je account omdat hij een code van bijvoorbeeld je telefoon nodig heeft.

10. **Gebruik een (extra beveiligde) applicatie voor vertrouwelijke informatie overdracht**
    Verzend je (gevoelige) persoonsgegevens via e-mail? Dat is volgens de AVG onveilig. Gebruik hier een speciale applicatie voor, of neem bijvoorbeeld een pro-abonnement op wetransfer.

Perfect Day

Over Perfect Day

Perfect Day is de partij voor cyber & data security in het mkb. Je kunt bij ons terecht voor advies en oplossingen. Daarvoor brengen we altijd eerst het grote plaatje van jouw bedrijf in kaart. Dat bestaat uit techniek, medewerkers, noodprocessen, wetgeving (avg) en ketenveiligheid. We maken dreigingen en kwetsbaarheden inzichtelijk. En helpen ze aan te pakken. Met een effectieve mix van persoonlijk advies en de juiste producten. Praktisch, persoonlijk en betaalbaar.

Afspraak maken?

Dit is hét moment om door te pakken! Maak een afspraak met onze cyber expert of boek eerst een gratis intake.

Contactgegevens

E: contact@perfectday.nl
T: 085 048 61 09