3 manieren om een webshop te beschermen tegen fraudeurs

29-03-2021 08:00

Steeds meer retailers zijn ook online te vinden. De coronacrisis heeft veel ondernemers gedwongen ook hun online aanwezigheid onder de loep te nemen. Webshops werden in mum van tijd uit de grond gestampt. Een fantastische kans voor fraudeurs om schade te berokkenen. Retailers zouden alles op alles moeten zetten om de veiligheid te waarborgen. Sterker: bedrijven zijn zelfs verplicht om actie te ondernemen. De wet Algemene Verordening Gegevensbescherming (AVG) verplicht alle ondernemers het nodige te doen om de gegevens van hun klanten en medewerkers te beschermen.

Gebruik een zakelijke VPN

Een Virtual Private Network (Virtueel Particulier Netwerk) is precies wat de naam zegt: een privé en anonieme verbinding met het internet. Het maskeert het echte IP-adres van degene die met de VPN verbonden is, waardoor de kans kleiner is dat de ondernemer of het bedrijf zelf slachtoffer wordt van cyberdreigingen. Daarnaast voegt het een extra beveiligingslaag toe: alle verzonden en ontvangen data wordt door een tunnel versleuteld, waardoor cybercriminelen minder gemakkelijk mee kunnen kijken op de verbinding, data kunnen onderscheppen en uitlezen.

Zelfs kleine bedrijven en zzp'ers zouden het gebruik van een VPN moeten overwegen. Voor de zakelijke markt zijn aparte VPN-aanbiedingen, die de online veiligheid nog beter waarborgen. Het is een investering die de moeite waard is. Het is niet alleen slim, maar ook een manier om bij te dragen aan het voldoen aan de Algemene Verordening Gegevensbescherming.

Gebruik een veilig platform

Voordat ondernemers denken aan het starten van een webshop, is het zaak dat ze zich verdiepen in het platform dat ze gaan gebruiken. Tegenwoordig zijn er veel verschillende platforms, zoals Woocommerce,

Shopify en Magento. Voor ieder platform valt wel iets te zeggen als het gaat om voor- en nadelen.

Kijk bij de keuze naar het platform niet alleen naar betaalbaarheid, maar zeker ook naar de beveiligingsaspecten. Hoe veilig is het platform dat mogelijk gebruikt zal worden? Welke extra beveiligingsmogelijkheden zijn er? Hoe gaat het platform om met de privacy van ondernemers, diens medewerkers en klanten? Het zijn zaken om zich van te vergewissen alvorens het platform in gebruik te nemen.

Werk met SSL-certificaten
Gegevens van klanten moeten altijd beschermd zijn. Daar mag geen twijfel over bestaan. Daarom is het een goede eerste stap SSL-certificaten toe te voegen aan de webshop en HTTPS te gebruiken. Wanneer deze combinatie wordt gebruikt, komt er een veilige verbinding tot stand, waarbij de verzonden en ontvangen data tussen de klant en de webshop wordt versleuteld.

Een gewoon SSL-certificaat is niet voldoende. Werk met een uitgebreide validatie of met een zogenaamd ‘EV SSL’. De klant ziet dat de verbinding veilig is, door de groene adresbalk en het hangslot met de naam van het bedrijf in de URL-balk. Dat stelt klanten gerust: ze weten dat ze op een extra beveiligde manier bestellen en betalen.

Hoe veilig is de webshop?
Alleen beveiligingsmaatregelen treffen is niet voldoende om een webshop te beschermen tegen fraudeurs. Beveiliging is geen kwestie van ‘set and forget’, maar een steeds doorgaand verbeteringsproces. Criminelen zullen altijd proberen om manieren te vinden om te kunnen profiteren van mogelijke fouten. Wees altijd bereid om deze problemen snel aan te pakken.

Test regelmatig hoe veilig de webshop is door beveiligingsaudits uit te voeren. Deze audits vertellen meer over de kwaliteit van de maatregelen, of ze nog voldoende werken en of er misschien iets bijgewerkt moet worden.