

Het prijskaartje van lakse online beveiliging

11-05-2015 11:50

Door Pieter Lacroix

Managing director bij IT- en databeveiligingsbedrijf Sophos Nederland

Twee derde van de grootste webshops heeft de online beveiliging niet op orde. Met een beetje digitale vakkundigheid zijn klantgegevens zo te bemachtigen. Dat blijkt uit een recent onderzoek van de Consumentenbond. Een aantal van die webwinkels lijkt het onderzoek af te doen als een beperkt gevalletje imagoschade. Dat is een gevaarlijke houding. De gevolgen van slechte gegevensbeveiliging zijn nu nog redelijk te overzien. Als de nieuwe EU-privacywetgeving binnenkort van kracht is, riskeren bedrijven enorme boetes.

Het onderzoek van de Consumentenbond voor de Digitaalgids van mei 2015 toont aan dat een ruime meerderheid van de grootste webshops in Nederland onvoldoende beveiligd is. Bij een derde van de 109 onderzochte websites is er zelfs sprake van ernstige veiligheidslekken. Klantgegevens zijn vrij gemakkelijk te achterhalen en soms is zelfs het complete klantbestand toegankelijk. De nadruk bij de berichtgeving ligt op de gevaren voor de consument - niet verwonderlijk gezien de initiatiefnemer van het onderzoek. Het risico voor de winkels krijgt minder aandacht. Ook dat is logisch, omdat naast de negatieve pers, de consequenties vrij gering zijn. Voorlopig althans, daar komt namelijk snel verandering in.

Boetebevoegdheid CPB uitgebreid

Retailers die klantgegevens slecht beschermen krijgen te maken met het College bescherming persoonsgegevens (CBP). Die geeft nu nog een waarschuwing of legt in het uiterste geval een last onder dwangsom op: een boete als de retailer het lek niet dicht. Dit jaar wordt de boetebevoegdheid van het CBP uitgebreid. Als dan wordt geconstateerd dat de beveiliging van gegevens niet deugt, kan een retailer een boete krijgen van maximaal 810 duizend euro of tien procent van de jaaromzet.

Strengere EU-privacywet

Daarnaast gaat naar verwachting in 2016 in de hele Europese Unie de General Data Protection Regulation (GDPR) van kracht. Die EU-wet is bedoeld om burgers meer grip op hun online gegevens te geven en gebruik van persoonsgegevens transparanter en verantwoordelijkheden 'afrekenbaar' te maken. Burgers moeten op verzoek volledige inzage krijgen in alle informatie die door een bedrijf of instelling over hen is vastgelegd.

Als burgers willen dat hun gegevens niet meer worden bewaard en verwerkt, en er zijn geen wettelijke gronden die dat tegenhouden, dan dienen die gegevens op verzoek direct verwijderd te worden. Verder moeten retailers kunnen aantonen dat ze technische en organisatorische maatregelen hebben genomen om de beveiliging te garanderen. Bovendien moeten ze proactief dataveiligheid controleren en klanten binnen 24 uur informeren als er een veiligheidslek wordt geconstateerd. Voldoen retailers niet aan de nieuwe privacyregels dan kan de EU boetes opleggen van 250 duizend tot honderd miljoen euro of vijf procent van de jaaromzet.

Consequenties dringen nog niet overal door

Dat betekent nogal wat voor retailers. Het heeft impact op de hele winkelorganisatie. Het gaat om de mensen in je organisatie, de processen en om technologie. Retailers moeten de verzoeken van klanten om inzage, wijziging en verwijdering van data kunnen honoreren en te allen tijde verantwoording kunnen afleggen over hoe ze klantdata zijn omgesprongen. De consequenties van de nieuwe wetgeving zijn nog lang niet bij alle retailers doorgedrongen.

Serieuze veiligheidsmaatregelen

Ieder retailer, groot of klein, moet zijn datamanagement opnieuw bekijken. Het gaat bijvoorbeeld om het

invoeren van een duidelijk veiligheidsbeleid: hoe gaan medewerkers om met klantgegevens, wie mag daarbij? Eén medewerker moet aangesteld worden als intern en extern aanspreekpunt voor dataveiligheid en er zal echt gekozen moeten worden voor een volwassen technologie om de klantdata te beschermen. Encryptie (versleuteling van data) is een belangrijk wapen in de strijd om gegevensbescherming. Wereldwijd wordt encryptie erkend als de beste methode om privacygevoelige data te beschermen, ook als er toch datalekken ontstaan. Met versleuteling tonen retailers bovendien aan dat ze serieuze veiligheidsmaatregelen hebben genomen.

De Consumentenbond heeft alle webwinkels waar veiligheidslekken werden geconstateerd, benaderd met de onderzoeksresultaten. Een aantal winkels kwam direct in actie. De helft van de webwinkels nam echter niet eens de moeite om te reageren op de bevindingen. Zo'n laconieke houding kan retailers in de nabije toekomst zeer duur komen te staan.