Retail & Betalen: Cybercriminaliteit

14-03-2014 00:00

EtailTrends 2 geeft in het thema Betaaltrends een tussenstand van de nieuwste betaalmogelijkheden. RetailNews belicht deze week vijf onderwerpen rond betalen. Vandaag: cybercriminaliteit.

Criminelen die transactiegegevens en persoonlijke informatie van klanten wegsluizen via POS-systemen: voor een retailer klinkt dit als een horrorscenario. Het overkwam de Amerikaanse winkelketen Target vorig jaar rond de feestdagen. Gedurende drie weken stalen hackers informatie van ongeveer veertig miljoen credit- en betaalkaarten, waarmee betaald werd in de winkels.

De cybercriminelen maakten volgens computerbeveiliger McAfee bij deze aanval gebruik van malware die gebaseerd is op zogenoemde BlackPOS malware. Wat McAfee met name zorgen baart is dat deze malware gemakkelijk verkrijgbaar en relatief eenvoudig aan te passen is. Bovenal is de aanval op Target voor het concern een teken dat cybercriminaliteit en de 'dark web' marktplaatsen volwassen zijn geworden. Een onder criminelen geliefde handelsplaats is de zogenoemde Lampeduza Republic. McAfee ziet daar veel van de data van Target-klanten verkocht worden. De transacties worden afgerekend in bitcoins.

Deze virtuele valuta is naast een onder retailers steeds vaker geaccepteerd betaalmiddel een populair hulpmiddel voor criminelen. Thuiswinkel.org luidde begin dit jaar nog de noodklok over een nieuwe oplichtingtruc waarbij malafide webshops online shoppers met bitcoins om de tuin leiden.

Daarbij wordt een klant die zijn online bestelling wil afrekenen in euro's doorgeleid naar een site waar bitcoins worden verkocht. Terwijl de online shopper denkt een product te betalen, schaft hij in werkelijkheid deze digitale munten aan. Die belanden vervolgens in de digitale portemonnee van de internetoplichter.

Cybercriminelen worden dus steeds sluwer in hun handelswijze. En de kans dat zij hun pijlen richten op de retailbranche is redelijk groot, stelde Etiënne van der Woude van WatchGuard Technologies eerder al op RetailNews.

Internetcriminelen verleggen hun aandacht namelijk steeds meer naar organisaties met veel klanten en een hoog transactievolume, zoals retailers. De POS-systemen zijn voor hen een prachtig doelwit, omdat daar transactiegegevens en persoonlijke informatie van klanten samenkomen.

Voor een retailer die zich wil wapenen tegen cyberaanvallen op zijn kassasysteem is de eerste stap het loskoppelen van de POS-systemen uit de overige IT. "Als een kassasysteem is aangesloten op een pc die ook voor browsen en e-mailen wordt gebruikt, maar u het cybercriminelen erg gemakkelijk", aldus Van der Woude.

Daarnaast is het belangrijk te realiseren dat Windows XP binnenkort niet meer door Microsoft ondersteund wordt. Beveiligingslekken in de software worden dan niet langer gedicht. Kassa's die op dit systeem draaien, zijn dus extra kwetsbaar. Een ander belangrijk verdedigingsmechanisme is het gebruik van software die voorkomt dat data zoals creditcardgegevens weggesluisd worden.

Een volledig veilige retailomgeving is volgens Van der Woude onmogelijk. "Op het terrein van IT-security bestaat geen waterdichte beveiliging. Maar met deze betrekkelijk eenvoudige maatregelen wordt het cybercriminelen een stuk lastiger gemaakt."