RECENTE VOORBEELDEN CYBERCRIME IN DE DETAILHANDEL

Als een ondernemer in de detailhandel te maken krijgt met cybercriminaliteit, is de gemiddelde schade **€ 54.000,-.**

Voor één op de twaalf winkeliers is dit zelfs meer dan € 250.000,-. Het gaat onder meer om herstelkosten, omzetverlies, tijdverlies en extra beveiligingskosten. Het aantal DDos-aanvallen nam in 2018 met 15% toe. Uit onderzoek komt naar voren dat 2.500 webshops in de drukke decembermaand de dupe waren van een aanval.

MALWARE IN KASSASYSTEMEN

Een kledingwinkel blijkt maandenlang met gehackte kassasystemen te hebben gewerkt. Vanaf de kassa's die besmet waren met malware werden betaalgegevens van klanten gestolen. De malware heeft enkele maanden op een aantal kassa's gedraaid.

De kledingwinkel werd gealarmeerd door een beveiligingsrapport dat melding maakte van ongeautoriseerde toegang tot betaalkaartgegevens. Nader onderzoek wees uit dat de encryptie uit bleek te staan en dat er malware op diverse kassapunten was geïnstalleerd. Hoe de malware op de kassa's terecht is gekomen en hoe de encryptie buiten werking gesteld kon worden, is nog niet bekend.

UITVALLEN KOELING SLAGERIJ

Een slager regelt de temperatuur van zijn koeltoonbank en koelcellen met een computersysteem. Hij kan dit op afstand bedienen en krijgt een waarschuwing als de temperatuur te hoog is. Op een morgen blijkt de temperatuur in de koelcellen te zijn opgelopen tot 45 graden. Een hacker is het systeem binnengedrongen en heeft de temperatuur verhoogd. De voorraad van twee dagen is bedorven. Het computersysteem en de temperatuurregeling moeten worden vervangen. De winkel moet noodgedwongen een aantal dagen sluiten en loopt omzet mis.
Klanten gaan naar een andere slager of de supermarkt.

GEHACKTE KASSAPRINTER

In 2017 begonnen overal ter wereld duizenden printers ineens vreemde berichten te printen. In plaats van een kassabon verscheen een plaatje van een robot. Hoeveel printers er geïnfecteerd waren is niet bekend, maar de hacker Stackoverflowinm die de aanval uitvoerde, spreekt van 150.000 printers. De hacker was een tiener die zich verveelde, gelukkig geen kwaad in de zin had en alleen de aandacht wilde vestigen op de printerveiligheid. Toch konden duizenden winkels hun klanten geen fatsoenlijke kassabon of factuur geven.

CYBERAANVAL OP WEBSHOP

De eigenaresse van een webshop wordt het slachtoffer van een DDos-aanval. Hierdoor is haar webshop twee dagen niet bereikbaar. Alle gegevens van aankopen gaan verloren. Tijdens deze dagen wordt er niets verkocht en geen omzet gerealiseerd. Klanten ontvangen hun bestelde producten niet en kunnen de webshop niet bereiken.
(Potentiële) klanten gaan naar een andere webshop.

.

RANSOMWARE DROGIST

De ransomware GrandCrab heeft duizenden Windows-computers van particulieren én bedrijven gegijzeld. De ransomware werd verspreid via bijlagen in e-mails. Zo werd de eigenaresse van een drogist ook het slachtoffer. Plotseling verscheen er een bericht op haar kassa dat de computer was overgenomen en ze € 500,- moest betalen om haar bestanden terug te krijgen. Alle kassa's werden geblokkeerd, net als de toegang tot haar boekhouding.

De winkel kon openblijven, maar klanten konden alleen contant afrekenen en alle verkochte producten werden bijgehouden op papier. De eigenaresse heeft de cybercriminelen niet betaald, omdat ze niet zeker wist of ze dan de sleutel tot haar gegevens kreeg. Ze raakte al haar zakelijke bestanden kwijt. In het vervolg is ze extra voorzichtig en maakt zij elke dag een back-up van haar gegevens.

VIRUS OP BETALINGSSYSTEEM WEBSHOP

Op een maandagmorgen ontdekt een financiële medewerker van een webshop in designmeubels dat er **€ 27.000,-** is overgemaakt naar een voor hem onbekend bankrekeningnummer in het buitenland. Hij neemt direct contact op met de bank. Die kan de betaling echter niet meer terugdraaien. De bank neemt contact op met de buitenlandse bank,maar het geld blijkt alweer te zijn overgeboekt naar een andere bankrekening. Het bedrijf is het slachtoffer geworden van cybercrime. De financiële medewerker heeft nietsvermoedend op eenlink geklikt in een phishing-mail. Daardoor is op zijn computer een 'banking trojan horse'-virus geïnstalleerd.

Waarschijnlijk heeft de medewerker hierna een betaling uitgevoerd via internetbankieren. Ongemerkt is hij doorgelinkt naar een goed nagemaakte kopie van de website van de bank en heeft hij zijn inloggegevens achtergelaten. Het bedrijf is het bedrag van **€ 27.000,-** kwijt. Gelukkig was de financiële medewerker zo alert dat hij deze foute betaling direct heeft opgemerkt en alarm heeft geslagen. Anders was het bedrijf waarschijnlijk meer geld kwijt geweest