

Hoe retailers cybercriminelen een stap voor kunnen blijven

02-10-2019 14:35



Door: David van den Berg
Associate director en head of Benelux region bij Verizon

Nieuwe technologische ontwikkelingen veranderen de retailsector op ongekende wijze. De fysieke en digitale wereld raken steeds verder verstrengeld en de klantervaring blijft zich ontwikkelen. Naarmate de sector verandert, veranderen ook de methoden die cybercriminelen gebruiken om gevoelige gegevens van bedrijven en consumenten te stelen.

Uit gegevens over cybersecurity blijkt dat Point Of Sale-aanvallen (POS) vóór 2018 het meest voorkomende type incident in de retailsector waren. Dit betrof onder meer aanvallen op afstand van POS-omgevingen en de bijbehorende malware en diefstal van betaalkaartgegevens. Recente gegevens tonen echter aan dat aanvallers tegenwoordig nieuwe en verbeterde methoden gebruiken om retailers aan te vallen. Hierdoor zitten retailers na afloop van een incident opgescheept met een puinhoop.

Aanvalspatronen veranderen

Volgens het Verizon Data Breach Investigations Report (DBIR) van dit jaar, hebben aanvallen op webapplicaties POS-aanvallen ingehaald als de meest voorkomende cyberaanval. Sinds 2014 is het aantal POS-incidenten met een factor tien gedaald. Tegelijkertijd is de kans dertien keer groter dat webapplicaties worden aangevallen en nietsvermoedende retailers worden getroffen. Dus hoe slagen cybercriminelen er in om

deze web-aanvallen uit te voeren?

Ze dringen eerst het betalingssysteem van een website binnen om vervolgens een code te installeren die de gegevens van klanten steelt wanneer zij hun aankopen doen. Dit zijn alledaagse aanvallen die niet altijd de voorpagina's halen, maar wel grote gevolgen hebben. De huidige cybercriminelen zijn op zoek naar kwetsbare e-commerce-applicaties die een middel kunnen zijn voor efficiënte en geautomatiseerde aanvallen. Er zijn zelfs criminelen die gespecialiseerd zijn in dit soort simpel uitvoerbare aanvallen.

Wat kunnen bedrijven hieraan doen?

Om de gegevens veilig te houden, moeten retailers passende maatregelen nemen om cyberaanvallen te voorkomen. Hoewel er geen allesomvattende oplossing bestaat, zijn hier een paar stappen die bedrijven kunnen nemen om de risico's te beperken.

1. Ken het belang van software voor bestandsintegriteit. Cybercriminelen die webapplicaties aanvallen, zijn niet uit op bestaande gegevens. In plaats daarvan implementeren ze een code om klantgegevens vast te leggen op het moment van invoer. Om dit tegen te gaan, moeten bedrijven software voor bestandsintegriteit toevoegen aan hun malwarebescherming op betalingssites, het patchen van besturingssystemen en de code van betaalapplicaties.

2. Omarm het nieuwe. Blijf nieuwe technologieën omarmen zodat criminelen POS-systemen niet meer als laaghangend fruit zien. Denk hierbij aan Europay MasterCard Visa (EMV) en mobile wallets, of een andere methode die gebruik maakt van een eenmalige transactiecode, in tegenstelling tot Primary Account Numbers (PAN).

3. Onthoud dat het niet alleen om de betaalkaarten gaat. Hoewel criminelen vaak uit zijn op betaalkaartinformatie, is het niet de enige soort gegevens die zij nuttig vinden. Beloningsprogramma's waarbij gebruik wordt gemaakt van een puntensysteem zijn ook potentiële doelwitten, net als de persoonlijke informatie van klanten.

Voor veel, vooral kleinere, retailorganisaties is het implementeren van uitgebreide security-maatregelen noch betaalbaar, noch haalbaar. Maar elke stap op het gebied van security, hoe klein ook, kan grote gevolgen hebben voor het opsporen en afschrikken van cybercriminelen. Het is belangrijk om personeel te trainen in het identificeren van potentiële bedreigingen. Het is een eenvoudig maar waardevol begin om ervoor te zorgen dat iemand in de organisatie een bedreiging kan detecteren.

In de wereld van cybersecurity bevinden retailers zich in de ongunstige positie dat ze niet alleen rekening moeten houden met hun eigen gegevensbeveiliging, maar ook met die van hun vele klanten. In een steeds digitalere wereld is het belangrijk om zoveel mogelijk beveiligingsmaatregelen te installeren als mogelijk. Maar minstens zo belangrijk is het om bewust te zijn van wat cybercriminelen zoeken en hoe ze dit bereiken. Een open houding ten opzichte van de nieuwste technologieën is van onschatbare waarde om potentiële aanvallers altijd een stap voor te zijn.

David van den Berg