De strijd tegen cybercrime in de retail

03-05-2016 12:13

Door Rob Pronk
Regional Director Northern Europe bij LogRhythm

De afgelopen jaren zijn er verschillende ernstige datalekken geweest bij retailorganisaties in het buitenland. Daardoor kwamen duizenden creditcardgegevens en andere persoonlijke informatie van klanten op straat te liggen. Bij het ene datalek ging het om malware, terwijl een ander het gevolg was van kwaadaardige activiteiten van binnenuit of het gebruik van gestolen inloggegevens. En ook in Nederland zijn retailers steeds vaker het doelwit van cyberaanvallen. Cybercriminelen worden steeds gewiekster met hun technieken, waardoor het voor retailers ook steeds lastiger wordt de ontwikkelingen bij te houden. Daarom is het noodzakelijk om netwerkbeveiliging op een andere manier aan te pakken. Retailers moeten zich realiseren dat de verdedigingstechniek die eerder goed werkte, niet in staat is zich snel aan te passen aan opkomende bedreigingen. En dat terwijl het landschap met bedreigingen nu juist razendsnel verandert. Aan retailers de taak proactiever te zijn en volledig inzicht in hun netwerk te creëren.

Vaststellen dat een activiteit inderdaad kwaadaardig is, vereist een goede uitrusting en monitoring van de complete infrastructuur die betrokken is bij creditcardverwerking. Hieronder valt alles van point-of-sale-systemen (POS) tot de betalingsverwerker, maar ook de backoffice- en netwerkinfrastructuur. Stel, er is malware geïnstalleerd op een POS-systeem; die malware kan proberen contact te leggen met een Command and Control-server – geen gebruikelijke communicatie vanaf een POS. Of de malware initieert een verdachte verwerkingsactiviteit of brengt wijzigingen aan in het bestandssysteem van de POS. Een andere indicator: een gebruiker die probeert ongebruikelijke toegang te krijgen tot een backoffice-server waarop gevoelige klantdata staat. In al deze scenario's komt een inconsistente activiteit aan het licht die – bij goede monitoring en analyse ervan – organisaties waarschuwt dat er geprobeerd is in te breken.

POS en de backoffice beschermen
Het is zaak om POS-endpoints te monitoren. Deze moeten allemaal dezelfde processen draaien, en hun bestandssystemen moeten identiek zijn aan elkaar en alleen wijzigen tijdens geplande updates. Zijn ze niet volledig identiek? Dan betekent dat meestal dat er malware op het systeem aanwezig is.

In veel gevallen communiceren de POS-endpoints van een organisatie rechtstreeks met betalingsverwerkers van derde partijen, de payment service providers. Vaak communiceren deze endpoints echter ook met backoffice-systemen die verschillende doelen hebben, vooral in grotere organisaties. Het kan zijn dat ze transacties verzamelen van meerdere POS-endpoints voor verwerking, de aankopen van een klant volgen in het kader van loyaliteitsprogramma's, een klant in staat stellen zich aan te melden voor een lidmaatschap of e-mailnotificaties, of informatie in een voorraadvolgsysteem updaten. Hoewel deze backoffice-systemen niet altijd creditcardgegevens verwerken, hebben ze meestal wel toestemming om te communiceren met POS-endpoints, wat hen interessante aanvalsvectoren maakt. Bovendien staan er misschien ook wel andere persoonlijke gegevens op deze systemen die naast creditcarddata beschermd moeten worden.

Netwerkcommunicatie identificeren
Naast POS- en backoffice-systemen is het ook van belang netwerkcommunicatie tussen componenten in de creditcardverwerkingsketen nauwgezet in de gaten te houden – een proces dat wordt vereist door de Payment Card Industry Data Security Standard (PCI-DSS). Omdat POS- en backoffice-systemen zulke specifieke taken hebben, is het identificeren van ongeautoriseerde netwerkcommunicatie essentieel en relatief eenvoudig vast te stellen. POS-endpoints moeten dus alleen betrokken worden bij bepaalde communicatie, zoals met backoffice-systemen en of payment service providers. Als er een nieuw soort netwerkcommunicatie te zien is,

zoals malware die gegevens probeert door te sturen of een hacker die een poging doet data te stelen, zijn beveiligingsmedewerkers direct op de hoogte te stellen.

Ongeacht de steeds geavanceerdere bedreigingen en de toenemende hoeveelheid data die retailorganisaties genereren, is het sowieso raadzaam continu op de hoogte te zijn van de kleine veranderingen die zich voordoen in het IT-netwerk. Door de volledige IT-infrastructuur die betrokken is bij de verwerking van creditcardtransacties goed te monitoren, kunnen beheerders elke kwaadaardige activiteit in de betaalverwerkingsketen identificeren. De systemen die deze transacties verwerken, hebben heel specifieke taken en horen te werken volgens een zeer beperkt en een voorspelbaar patroon. Of het nu gaat om een inbreker die toegang tot data wil waar hij geen toegang tot mag hebben. Of om malware die data probeert te stelen. Of om een simpele verkeerde instelling van de firewall waardoor een backoffice-server blootgesteld is aan het internet. In alle gevallen veranderen de endpoints en/of het gedrag van het netwerk. Retailers moeten in staat zijn deze gedragsveranderingen te herkennen zodra ze zich voordoen. Zo kunnen ze aanvallen tegen hun betaalverwerkingsketen een halt toeroepen voordat klantdata aangetast worden.