Publicatie : Banking Review
Datum : 31 dec 2015 Pagina : 51
cm2 : 296 Advertentiewaarde : € 1.567,00
Regio : Nederland
Frequentie : 4x per jaar
Oplage : 3.964

Column

Onno de Vrij, onno.de.vrij@sas.com
Onno de Vrij is Head of Risk and Fraud bij SAS.

Bedrijfsprocessen

Cybercrime bestrijden? Speel niet volgens de regels!

Angst, onzekerheid en twijfel zijn gevoelens die vaak komen kijken bij cybercrime. En dat is logisch; in iedere organisatie leeft *angst* dat vertrouwelijke informatie op straat komt te liggen door een datalek. Daarbij is er doorgaans veel *onzekerheid* of je nou echt voorbereid bent op een volgende aanval, hoe deze aanval eruit ziet en hoe je je er het beste tegen kunt wapenen. Ook is er *twijfel* of er voldoende middelen in huis zijn om de slimme aanvaller te kunnen pakken voordat deze toeslaat. Als u de afgelopen jaren de media hebt gevolgd weet u dat al deze gevoelens niet ongegrond zijn.

Er zijn veel organisaties ten prooi gevallen aan cyberaanvallers. Je ziet dan ook dat investeringen in middelen die tegen aanvallen moeten beschermen sterk toenemen. Daarbij ligt de focus echter vooral op het voorkomen van incidenten op basis van regels die zijn ingesteld om aanvallen te signaleren. Een reactieve benadering dus. Aanvallers zoeken continu naar nieuwe manieren om de organisatie binnen te dringen, maar onze verdediging is gericht op aanvallen die we al eens hebben gezien.

Ofwel de cybercrimineel heeft altijd een voorsprong. U blijft daarmee in onzekerheid en weet niet wanneer de eerstvolgende aanval plaatsvindt, welke strategie hierbij wordt gebruikt en welke organisatie het doelwit zal zijn. Maar dat er slachtoffers gemaakt worden en schade ontstaat, dat is zeker. Hoe moet u dan omgaan met deze 'zekere onzekerheid'? Door het gedrag van de cybercrimineel te voorspellen.

Het voorspellen van gedrag lijkt een onmogelijke opgave. Maar door slim om te gaan met de data die de organisatie al heeft, is het mogelijk abnormaal gedrag binnen het bedrijfsnetwerk te herkennen en indringers snel op te sporen. Dit kan door het toepassen van behavioral analytics-technologie. Daarmee baseert u uw verdediging niet op vooraf ingestelde regels, maar bent u de crimineel een stap voor.

Om gedrag te kunnen voorspellen verzamelt u data over de systemen en het gedrag van de mensen die deze gebruiken. Vervolgens analyseert u deze gegevens en kunt u in kaart brengen wat voor iedere medewerker als normaal gedrag gezien kan worden.

Als een indringer zich toegang verschaft tot uw systemen gaat deze direct op zoek naar de kortste route naar de data die hij wil stelen. Omdat dit afwijkt van het normale gedrag van de gebruikers binnen uw netwerk wordt deze zoektocht direct zichtbaar. Zo zijn aanvallers snel ontmaskerd en is de kans op schade aanzienlijk verminderd.

Op deze manier zijn de rollen omgedraaid: u heeft de voorsprong. De cybercrimineel blijft nieuwe manieren ontwikkelen om data te verkrijgen. In plaats van telkens te proberen op tijd de tactische regels voor detectie aan te passen, vertrouwt u op een proactieve strategie.

En, laten we eerlijk zijn: we voelen ons allemaal een stuk zekerder als we zelf de spelregels bepalen. «