INFORMATIEBESCHERMING IN NEDERLAND

proofpoint.
Protect people. Defend data.

Een perspectief van binnenuit:

Wanneer ik met klanten spreek over de ontwikkeling van hun beveiligingsstrategie, zijn we het er meestal over eens dat elke aanpak op data moet zijn gebaseerd. In cyberbeveiliging, een domein dat voortdurend aan veranderingen onderhevig is, kan die data snel veranderen. Bovendien komt die informatie uit een groot aantal verschillende bronnen. Ik hoor veel klanten worstelen met het gebrek aan inzicht in dat veranderende dreigingslandschap: Waar lopen we risico? Hoe groot is dat risico? Wat kunnen we doen om dat te verkleinen?

Om organisaties te helpen, bevraagden we 75 hogere leidinggevenden in Nederland om erachter te komen hoe zij over het risico van binnenuit denken. We wilden inzicht krijgen in gegevenslekken, zowel oorzaken als gevolgen, maar ook weten hoe leidinggevenden hun beveiligingscultuur ontwikkelen en hoe zij tegen bedreigingen van binnenuit aankijken.

Robbert Bouman,
Regional Director Benelux, Proofpoint

Een derde weet niet of er een gegevenslek is geweest

Een volledig verslag van ons onderzoek vindt u **hier**. De resultaten zijn ontnuchterend. Bijna de helft van de organisaties waarmee spraken, gaf aan in de afgelopen twaalf maanden te maken hebben gehad met een gegevenslek. Dat is op zich al veel, maar het onthutsende was dat meer dan een derde niet eens wist of er een lek was geweest of niet.

Dat wijst op een gebrek aan interne communicatie (niet alle mensen met wie we hebben gesproken, hadden een specifieke beveiligingsfunctie) ofwel een gebrek aan tools en processen om gegevenslekken snel en onomstotelijk te identificeren.

Diefstal van inloggegevens was een terugkerend thema bij gegevenslekken. Het was zowel de hoofdoorzaak als het belangrijkste gevolg. Deze aanvallen vormen dus een cyclus. Aanvallers bemachtigen inloggegevens (bijvoorbeeld door ze op het dark web te kopen) om toegang te krijgen tot organisaties, waar ze nog meer inloggegevens kunnen 'oogsten', die ze dan weer doorverkopen, en zo gaat de cyclus door.

Fouten door gebruikers kunnen kostbaar zijn

Ik denk dat organisaties het risico van dataverlies door handelen van mensen binnen het bedrijf onderschatten. Ze hebben vaak een beperkt beeld van bedreigingen van binnenuit en denken dat het alleen om ontevreden of kwaadwillende medewerkers gaat die gegevens lekken of stelen. Veel bedrijven gaan ervan uit dat hun eigen medewerkers dat niet doen. Dat is mogelijk, maar uit onze enquête blijkt dat het risico van slordigheid van gebruikers net zo groot is. Medewerkers kunnen gemakkelijk fouten maken, bijvoorbeeld door niet de juiste beveiligingsprocedures te volgen en dat is hoe een gegevenslek vaak ontstaat.

Door werken op afstand worden deze risico's nog eens vergroot. 56% van de leidinggevenden met wie wij hebben gesproken, gaf aan dat medewerkers lakser zijn geworden met de beveiligingsprocedures sinds ze thuis zijn gaan werken. Daarnaast zei 76% dat ze door het werken op afstand minder inzicht hebben in wat hun medewerkers doen.

Een mes dat aan twee kanten snijdt als bescherming tegen insider-risico's

Het tegengaan van bedreigingen van binnenuit vergt kennis en de juiste tools. Als medewerkers begrijpen welke risico's achteloos gedrag met zich meebrengt, kunnen ze hun acties beter in de context plaatsen. Als tweede, minstens even belangrijke, bescherming zijn er tools om de risico's van binnenuit te identificeren voordat deze een probleem worden.

Gelukkig gaf bijna twee derde (63%) van de leidinggevenden in onze enquête aan dat ze hun medewerkers trainen in bedreigingen van binnenuit. Bovendien lijken organisaties zich bewust te zijn van de andere bedreigingen voor medewerkers die vanuit huis werken, zoals aanvallen op cloudsystemen en ransomware. Dit zijn onderwerpen die in training aan de orde komen bij respectievelijk 64% en 61% van de organisaties.

De meeste organisaties (68%) hebben een oplossing om gegevensverlies te voorkomen (DLP, oftewel Data Loss Prevention). Deze zorgt ervoor dat gevoelige gegevens het bedrijf niet verlaten. Een gebrek aan specifieke technologie om bedreigingen van binnenuit aan te pakken, is echter de belangrijkste factor bij het insider-risico in het bedrijf. 77% was het hiermee eens.

Met moderne oplossingen voor bedreigingen van binnenuit kunnen organisaties het risico en de frequentie van deze bedreigingen verkleinen. Ze kunnen snel reageren wanneer er toch problemen ontstaan en ze kunnen al deze activiteiten efficiënter beheren.

Lees vooral het volledige rapport van ons onderzoek: **Bedreigingen van binnenuit - Uitdagingen en prioriteiten voor organisaties in Nederland.**