3 september 2021

Een kwart van de organisaties heeft last van lasterlijke aanvallen op sociale media

Veiligheidsbarometer van Vias bevraagt online en offline veiligheidsproblemen bij bedrijven

Cybercriminaliteit is voor 4 op de 10 bedrijven het meest voorkomende veiligheidsprobleem. Ruim een kwart van de bedrijven kreeg recentelijk ook te maken met lasterlijke aanvallen op sociale media. Ook beschadiging van eigendommen of voertuigen blijft een groot probleem. In 1 op de 4 gevallen is de dader zelfs gekend door de onderneming. Dit blijkt uit de tweede veiligheidsbarometer van Vias institute.

252 Nederlands- en Franstalige ondernemingen uit verschillende sectoren namen in de periode van januari tot en met maart 2021 deel aan deze tweede Veiligheidsbarometer van Vias institute. Die bevraging kwam tot stand met de medewerking van het Verbond voor Belgische Ondernemingen, Unizo, Unisoc, Agrofront, Union des classes moyennes (UCM) en Union Wallonne des Entreprises (UWE), Federale Politie en de Cyber Security Coalition.

Cybercriminaliteit blijft het vaakst voorkomende veiligheidsprobleem

43% van de deelnemende ondernemingen werd in de 12 maanden voorafgaand aan de studie slachtoffer van één of meerdere vormen van cybercriminaliteit. Dat gaat van illegale toegang tot IT-systemen door bijvoorbeeld hacking of phishing tot een tussenkomst in data of systemen door middel van virussen. Ook cyberafpersing en bedrijfsspionage worden gemeld.
Er duiken internationaal steeds meer studies op die aangeven dat COVID 19 als opportuniteit wordt aangegrepen voor allerhande vormen van cybercriminaliteit.

84% van de bedrijven vindt IT-beveiliging belangrijk in de onderneming, dit is 10% minder in vergelijking met 2018. Dit is opvallend ondanks het hoge slachtofferschap en het gegeven dat dit als voornaamste risico wordt inschat. Slechts 52% antwoordt positief op de vraag of de onderneming een specifiek veiligheidsbeleid op IT-niveau heeft.

Top 5 van feiten waar een onderneming of medewerker van een onderneming slachtoffer van werd de laatste 12 maanden

2018	
Cybercriminaliteit	43%
Beschadiging van voertuig	42%
Geweld, agressie	40%
Beschadiging van eigendom	40%
Ongeoorloofde toegang zonder geweld	38%

2021	
Cybercriminaliteit	43%
Beschadiging van eigendom of vandalisme	38%
Beschadiging van voertuig	37%
Ongeoorloofde toegang zonder geweld	28%
Lasterlijke uitlatingen tegen de organisatie via de sociale media	27%

Beschadiging van eigendom (38%) of vandalisme en beschadiging van een voertuig wordt door 37% van de respondenten aangeduid. Er is dus een opvallend hoog slachtofferschap dat zich zowel situeert op online als offline niveau.

Een nieuw en groeiend fenomeen zijn laster/lasterlijke uitlatingen tegen ondernemingen via de sociale media. 27% van de organisaties krijgt er mee te maken. Dit fenomeen is erg moeilijk onder controle te krijgen omdat objectieve en waarheidsgetrouwe informatie niet altijd makkelijk voorhanden is. Een goede (crisis) communicatie op basis van feiten is op dat vlak belangrijk.

Kwart van de daders is een bekende

De veiligheidsbarometer toont aan dat ondernemingen die slachtoffer werden van een crimineel feit de dader ervan in 24% van de gevallen kenden. Het gaat vaak om een werknemer van de onderneming zelf, een contractor of een interim. Indien werknemerscriminaliteit aan het licht komt, zal het bedrijf/onderneming dit vaak zelf regelen.

Gebrek aan vastgelegde procedures binnen bedrijven

In 42% van de ondernemingen bestaat er geen procedure voor het melden van verdachte handelingen op of naast de werkvloer. In 53% van de bedrijven is er geen anoniem meldpunt voorzien. De vraag is dus of werknemers van deze ondernemingen voldoende weten waar ze terecht kunnen als ze slachtoffer of getuige zijn van een crimineel feit op de werkvloer.

61% geeft aan dat er psychosociale opvangmogelijkheden zijn en dat er en vertrouwenspersoon is. Iets meer dan de helft duidt aan dat er een extern aanspreekpunt is terwijl 44% beaamt dat er een intern aanspreekpunt is. Dit zijn vrij lage cijfers, te meer gezien dit een wettelijke verplichting is.

Bijna 1/5de neemt echter geen beveiligingsmaatregelen in de strijd tegen criminaliteit, in hoofdzaak omdat het risico op slachtofferschap als laag wordt inschat. Er is weliswaar een groeiend bewustzijn in bedrijven omtrent beveiliging maar desondanks neemt nog steeds niet ieder bedrijf maatregelen.

Vaak lage aangiftebereidheid

De helft van de organisaties doet geen aangifte van het meest ingrijpende feit. Vaak wordt aangegeven dat ze de zaak niet ernstig genoeg vonden of omdat er geen zichtbare schade was. De aangiftebereidheid dient gestimuleerd te worden. Enkel zo kan de politie een beter zicht krijgen op de grootte van bepaalde problemen.

Conclusie

De strijd tegen criminaliteit in een onderneming of bedrijf is ieders verantwoordelijkheid. Niet alleen directie, management maar evenzeer medewerkers zijn hierin cruciale schakels. Iedereen dient zich als het ware als potentiële risicomanager te gedragen. Zorgen voor duidelijke richtlijnen, zowel ter bescherming van de offline als online veiligheid kan veel leed voorkomen. Als er zich toch feiten voordoen, is het belangrijk dat die altijd aangegeven worden.

Contactpersoon:
Arne Dormaels, directeur Veiligheid en preventie Vias institute: 0497/64.92.25.
.