Finance professionals extra alert op phishing praktijken

10-12-2021

Phishing praktijken komen steeds vaker voor bij bedrijven. We zien ze niet alleen vaker opduiken, maar ook in steeds meer verschillende vormen. Denk aan CEO-fraude, het klikken op nep-emails, het misbruiken van creditcard gegevens of overmaken van facturen naar verkeerde bankrekeningen. Ook worden e-mailadressen en namen van gerechtsdeurwaarders regelmatig gebruikt als afzender door criminelen.

Gelukkig zijn veel finance professionals extra alert op phishing. Dat blijkt uit een onderzoek van AG Connect en Financieel Management van afgelopen zomer onder de bezoekers van de website. In dit artikel gaan we dieper in op de vormen van phishing en wat u zelf kunt doen als finance professional.

Vormen van phishing

Er is bijvoorbeeld sprake van phishing wanneer mensen worden opgelicht door gegevens in te vullen op een vervalste website. In verreweg de meeste gevallen gaat het om een kopie van een website die goed bekend is bij de persoon in kwestie. Deze persoon ziet niet dat het om een kopie van de vertrouwde website gaat en logt in met zijn gegevens. Criminelen kunnen die zo eenvoudig onderscheppen.

Op deze manier kunnen inloggegevens en creditcardgegevens in verkeerde handen terecht komen, waardoor organisaties worden opgelicht. Deze vorm van internetfraude noemen we phishing. Maar liefst 16 procent van de Nederlandse organisaties geeft aan wel eens getroffen te zijn door phishing praktijken.

Schade door internetfraude loopt hoog op

Internetfraude bestaat tegenwoordig in veel verschillende vormen. Kijken we naar de vormen van internetfraude waar bedrijven het vaakst mee te maken krijgen in Nederland, dan zien we dat aanvallen met ransomware en phishingmails het meest voorkomen.

Het doel van de hackers is niet altijd hetzelfde. Het kan de hackers te doen zijn om het verkrijgen van gevoelige data, wat aan de opdrachtgever of een hoogste bieder kan worden verkocht. Anderzijds kan het ook gaan om het gijzelen van gevoelige data, waarbij de hackers het doel hebben om een grote som geld te vragen voor het vrijgeven van de date. In sommige gevallen is een aanval vooral bedoeld om de systemen voor enige tijd plat te leggen.

Grote schade bij veel bedrijven

De schade door dergelijke vormen van internetfraude kan behoorlijk in de papieren gaan lopen. Wordt gevoelige data gegijzeld, dan moet een bedrijf vaak een aanzienlijk bedrag aan de hackers betalen. Vervolgens kan het bedrijf de eigen computers weer in en ontstaat er weer toegang tot de eigen data. Daarnaast is er in veel gevallen ook sprake van reputatieschade. Internetfraude kost organisaties in vrijwel alle gevallen veel geld en hier komt verdere imagoschade nog bij. De vraag is dan ook in hoeverre Nederlandse bedrijven en organisaties maatregelen nemen om phishing praktijken tegen te gaan. Wat is hierbij de rol van de finance professional?

Controle en opleiding binnen bedrijven

Volgens het onderzoek van AG Connect en Financieel Management is er nog veel ruimte voor verbetering als het gaat om het voorkomen van internetfraude, waaronder phishing. Meer dan 4 op de 10 organisaties geeft aan dat er geautomatiseerde emailchecks worden uitgevoerd. Slechts bij iets meer dan een kwart van de deelnemende bedrijven vinden er automatische controles op bankrekeningnummers plaats en overboekingen van bedragen boven een bepaalde grens worden nog handmatig gecontroleerd binnen 34 procent van de deelnemende bedrijven.

Van alle 200 deelnemende organisaties geeft 16 procent aan wel eens door een phishing aanval te zijn getroffen. Bijna een derde van de bedrijven geeft aan regelmatig phishingmails te ontvangen en 6 op de 10 bedrijven geven aan dat al deze mails worden gemeld binnen de organisatie. Dit betekent dat er binnen 4 op de 10 bedrijven eigenlijk geen controle op bestaat.

Phishing preventie hoger op de agenda

Het onderzoek laat duidelijk zien dat er nog veel ruimte voor verbetering is binnen veel Nederlandse bedrijven en organisaties. Bij 62 procent van de deelnemers is er bijvoorbeeld geen sprake van afspraken over data in financiële software tussen de finance afdeling en de ICT afdeling. Maar liefst 64 procent van de medewerkers van de finance afdeling verstuurt nog regelmatig gevoelige informatie naar externe partijen en 38 procent slaat bedrijfsgevoelige data nog altijd op privéapparaten op. Finance professionals moeten dan ook extra alert zijn op phishing praktijken en andere vormen van internetfraude, vooral omdat internetfraude steeds meer voorkomt.

Meer controle, ook over de financiën

Er is meer controle nodig, zeker op het gebied van financiën. Dit heeft niet alleen betrekking op het nemen van maatregelen om internetfraude tegen te gaan, maar bijvoorbeeld ook in het dieper graven in financiële statussen van nieuwe én bestaande klanten.

Wilt u voorkomen dat facturen onbetaald blijven, dan is er een maximale controle nodig. Blijven er toch facturen openstaan? Wacht dan niet te lang met het inschakelen van een incassobureau. Willems Gerechtsdeurwaarders & Incasso uit Utrecht staat dan graag voor u klaar. Neemt u gerust eens vrijblijvend contact met ons op voor meer informatie of advies.