Cybercriminaliteit is big business

Fraude treft steeds vaker bedrijven

De tijd dat oplichtersbendes nog ten strijde trokken met amateuristische phishingmails in gebrekkig Nederlands, ligt ver achter ons. Fraude is tegenwoordig big business geworden. Bovendien worden oplichters steeds creatiever en bedenken ze continu nieuwe technieken om nietsvermoedende slachtoffers in de val te laten lopen. Hilde Pottie van het Fraud Competence Center bij Belfius gidst ons door de donkere krochten van de fraudewereld en geeft praktische tips om uw bedrijf zo goed mogelijk te beveiligen.

Mailbox hacking

"De term zegt het zelf: in dit geval wordt de mailbox van tegenpartijen of leveranciers gehackt, waardoor bedrijven mails binnenkrijgen die op het eerste gezicht van hun leveranciers lijken te komen, maar eigenlijk vals zijn. Ofwel zit er een - uiteraard vervalste - factuur bij de mail, ofwel wordt er vermeld dat de leverancier de facturen voortaan via factoring zal innen. Er wordt dan een nieuw rekeningnummer opgegeven, dat vaak naar het buitenland leidt", aldus Hilde.

"Daarnaast gebeurt het ook dat mailboxen gewoon nagebootst worden. De afzender is plots Jan Janssens in plaats van Janssen. Of de letter l (van Lima) in een bedrijfsnaam is vervangen door een hoofdletter i, iets wat je op het scherm nauwelijks van mekaar kunt onderscheiden."

Factuurfraude

"Er zijn grosso modo twee vormen van factuurfraude: ofwel komt een elektronische factuur binnen via een gehackte mailbox (zie ook het stukje over 'Mailbox hacking', nvdr) ofwel wordt een papieren factuur onderschept tijdens het posttraject", zegt Hilde. "Vervolgens worden er gegevens op de factuur gewijzigd of wordt de factuur gewoon volledig nagebootst. Het probleem met factuurfraude is dat er vaak weken verstrijken vooraleer duidelijk wordt dat het om oplichting gaat. De opdrachtgever denkt dat hij de factuur correct heeft betaald, terwijl de begunstigde een tijdje blijft wachten op het geld. Tegen de tijd dat de fraude aan het licht komt, valt het geld meestal niet meer te recupereren."

WAT TE DOEN?

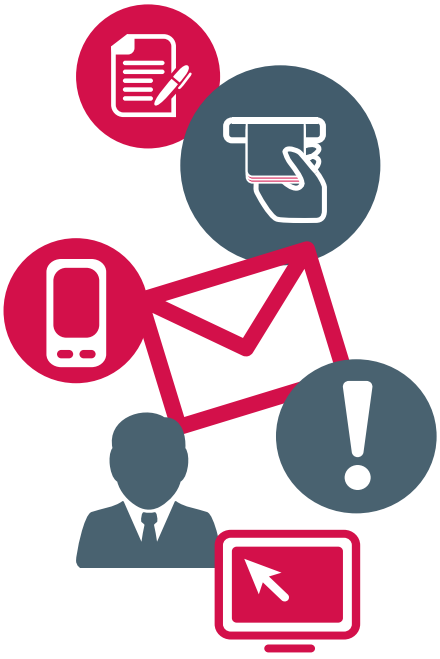
Eigenlijk heeft elk bedrijf een overzicht nodig van al z'n tegenpartijen, waarin alle contactpersonen, telefoonnummers en rekeningnummers vermeld staan. Elke factuur die betaald wordt, kan dan gedubbelcheckt worden met dat overzicht. Of u kunt via online banking uiteraard ook met 'bewaarde begunstigden' werken, dan merkt u meteen als een leverancier plots op een ander rekeningnummer betaald wil worden. Wijkt het rekeningnummer van de begunstigde af, neem dan contact op met de tegenpartij via de gegevens uit het algemeen overzicht, niet via de gegevens die op de dubieuze factuur staan.

Social engineering

"CEO-fraude is het meest bekende voorbeeld van social engineering. In zo'n geval worden medewerkers van een bedrijf eerst benaderd door een fraudeur die zich uitgeeft als vertrouwenspersoon van de CEO of CFO. Vaak doen de oplichters zich in die eerste contacten voor als advocaat, consultant of notaris. Nadien volgt dan een frauduleuze e-mail om een dringende en vertrouwelijke betaling uit te voeren, zogezegd in opdracht van de CEO of CFO. Het geld vertrekt vaak naar buitenlandse rekeningen, waarna de fraudeurs met de noorderzon verdwijnen."

WAT TE DOEN?

Breng uw medewerkers op de hoogte dat deze fraudetechniek bestaat en verduidelijk dat u nooit via mail of aan de telefoon zou vragen om een dringende en vertrouwelijke transactie uit te voeren. Maak werk van een duidelijk protocol in geval van dringende betalingen en volg dit altijd consequent. Spreek bijvoorbeeld een codewoord af, dat u enkel in dergelijke gevallen gebruikt. Zorg er bovendien voor dat alle (grote) verrichtingen een dubbele handtekening nodig hebben. Vier ogen zien altijd meer dan twee.



Interne fraude

Bij interne fraude komt de dreiging niet van buitenaf, maar wel van binnenin het bedrijf. "Het zijn vaak de moeilijkste gevallen om op te sporen en op te lossen", weet Hilde. "Een klassiek voorbeeld dat helaas nog al te vaak voorkomt: een medewerker met toegang tot de rekeningen van het bedrijf, maakt daar misbruik van door af en toe geld door te sluizen naar z'n eigen privérekeningen, of de rekeningen van vrienden en familie."

WAT TE DOEN?

Zorg voor duidelijke interne procedures, want goede afspraken maken goede vrienden. Dubbele handtekeningsbevoegdheid voor grote bedragen is zeker geen overbodige luxe. Voer regelmatig een interne audit uit, en laat de medewerkers bij wijze van afschrikking weten dat er controles zijn.

Phish a card

"Ook op het vlak van phishing verschuift het actieterrein van de fraudeurs continu. Bij bankkaartphishing krijgen de klanten een bericht dat hun bankkaart op vervaldag gaat komen en dat ze moeten aanloggen via de pc om bepaalde gegevens in te voeren, waaronder hun pincode. Daarna wordt hen gevraagd om hun kaart op te sturen naar een bepaald adres. Op die manier hebben de phishers zowel de kaart als de code in handen, en wordt het wel erg gemakkelijk om rekeningen te plunderen", zegt Hilde.

WAT TE DOEN?

Laat u niet misleiden, banken zullen nooit vragen om uw bankkaart op te sturen en tegelijk online uw pincode te registeren. Wanneer u twijfelt, neem dan contact op met uw vertrouwde aanspreekpunt bij de bank, via de gebruikelijke kanalen. Zorg ervoor dat uw medewerkers ook op de hoogte zijn van dergelijke phishingpraktijken.

Boilerroomfraude

"Met deze vorm van fraude viseren de oplichters vooral bedrijfsleiders of financieel directeurs in hun hoedanigheid als privépersoon. De CEO's of CFO's worden meestal vanuit het buitenland benaderd door zogezegde specialisten die vrij complexe beleggingen aanbieden met veel betere rendementen dan diegene die de Belgische banken momenteel kunnen geven", vertelt Hilde.

"De fraudeurs zijn absoluut geen amateurs, ze beheersen het financieel jargon tot in de puntjes en komen bijzonder professioneel over. Ze hebben mooie websites, glossy brochures en een waterdicht verhaal aan de telefoon. Slachtoffers schrijven al snel geld over naar het buitenland, verblind door de potentiële opbrengst en gerustgesteld door het plausibele verhaal. Aanvankelijk gaat het om bedragen van een paar duizend euro, maar al snel gaat de bal aan het rollen. Voor je het weet, gaat het om gigantische bedragen, terwijl de slachtoffers vaak niet eens beseffen dat ze werden opgelicht. Pas op het moment dat de klant een deel van z'n geld terug wil om er een grote aankoop mee te financieren, wordt alle contact verbroken en blijkt het geld in rook te zijn opgegaan."

WAT TE DOEN?

Wees niet te goedgelovig. Klinkt een verhaal te mooi om waar te zijn? Dan is het dat waarschijnlijk ook.

Bent u toch in de val gelopen? Praat erover met uw vaste contactpersoon bij de bank en gooi uw verhaal niet zomaar online. Op het internet lezen de fraudeurs immers ook mee. Er zijn intussen gevallen bekend van zogeheten recovery fraude, waarbij de oplichtersbendes online hun 'hulp' aanbieden om een deel van het verloren geld te recupereren. Het enige wat de klant hoeft te doen, is vooraf een bepaald bedrag overschrijven om alvast een deel van de kosten te dekken. Resultaat: dubbele winst voor de fraudeurs en een nog grotere financiële kater voor de slachtoffers.

BENT U TOCH HET SLACHTOFFER GEWORDEN VAN FRAUDE?

1. Neem onmiddellijk contact op met uw vaste contactpersoon bij de bank en vermeld daarbij zo veel mogelijk details over wat u is overkomen. Op die manier kan ons Fraud Competence Center proberen om (een deel van) het geld te recupereren.

2. Ga meteen langs bij de politie om een proces-verbaal te laten opstellen. Als u het geld achteraf wilt recupereren, hebt u een officieel pv nodig om te kunnen bewijzen dat er effectief fraude heeft plaatsgevonden.

Dergelijke onaangename verrassingen in de toekomst vermijden?

Praat erover met uw Corporate Banker!
Belfius heeft tal van producten en diensten in z'n gamma die oplossingen aanreiken in de strijd tegen fraude. U ontdekt ze ook in ons dossier ***Veilig bankieren***.

EN U?

Neem deel aan onze anonieme enquête (slechts 3 vragen) door hier te klikken en laat ons weten of u al bepaalde gevallen van, of pogingen tot fraude hebt meegemaakt.