VEILIG BANKIEREN IN HET MKB

Hoe werken cybercriminelen?

Hoe kun je je wapenen tegen cybercriminaliteit?

Bedrijven zijn steeds meer het doelwit van cybercriminelen. Ze worden eerst via het internet bespioneerd. Vervolgens concentreren cybercriminelen zich op specifieke werknemers die ze op slinkse wijze gaan manipuleren. Zo laten cybercriminelen bijvoorbeeld werknemers betalingen uitvoeren naar rekeningen die in handen blijken van criminelen. Lees in deze brochure verder hoe cybercriminelen te werk gaan en hoe u uw bedrijf kunt beschermen.

Hoe werken cybercriminelen?

Cybercriminelen maken vaak gebruik van social engineering om hun doel te bereiken. Social engineering omvat kwaadaardige telefoongesprekken, e-mails, sms'jes of andere vormen van manipulatie met als doel werknemers bepaalde acties uit te laten voeren of informatie prijs te geven. Veel van de oplichtingspraktijken worden pas gelanceerd nadat de criminelen informatie over uw bedrijf hebben verzameld via bijvoorbeeld de bedrijfswebsite, publieke registers (KvK) of sociale media. Hoewel er verschillen zijn in de wijze waarop aanvallen worden uitgevoerd, hebben ze één ding gemeen: de aanvallers maken misbruik van menselijke eigenschappen zoals behulpzaamheid, vertrouwen, angst, nieuwsgierigheid of respect voor autoriteit. Werknemers worden zo effectief gemanipuleerd dat ze in goed vertrouwen handelen, maar daardoor onbewust hun bedrijf benadelen.
Hieronder geven we vier voorbeelden van fraudevormen waarmee het MKB de laatste jaren te maken heeft gekregen.

Voorbeeld 1: Chief Executive Officer (CEO-)fraude

Een werknemer die bevoegd is om betalingen te doen (boekhoudafdeling of administratie) ontvangt een nepbericht bijvoorbeeld via e-mail of sms dat afkomstig lijkt van een hogergeplaatste manager, of zelfs van de algemeen of financieel directeur. De werknemer wordt gevraagd een vertrouwelijke betaling uit te voeren. De reden hiervoor kan bijvoorbeeld een geheime overnamedeal zijn of de betaling van een boete. Discretie gewenst, denkt de medewerker. Het is voor hem logisch dat hij niemand binnen het bedrijf iets mag vertellen over de transactie. Nadat het eerste contact tot stand is gekomen via e-mail, volgen daarna telefoontjes en e-mails van zogenaamde adviseurs of advocaten die door het bedrijf zijn ingehuurd. Vaak worden dergelijke transacties geloofwaardig gemaakt door het beschikbaar stellen van valse facturen en notariële aktes. Dit met maar één doel: de werknemer overtuigen een grote transactie uit te voeren naar een (meestal) buitenlandse bankrekening. Deze oplichtingstruc kan worden herhaald tot het betrokken bedrijf het opmerkt.

Voorbeeld 2: Factuurfraude

Een veel voorkomende vorm van factuurfraude is het doorgeleiden van legitieme betalingen naar een frauduleuze bankrekening. Dit kan simpelweg door facturen te onderscheppen in het posttraject en deze te voorzien van een sticker met een nieuw rekeningnummer. Ook komt het voor dat een MKB een e-mail ontvangt waarin wordt beweerd dat een bedrijf van wie hij producten of diensten afneemt en aan wie hij vaker betalingen doet, een nieuw rekeningnummer in gebruik heeft genomen. Om het voor de betaler betrouwbaar over te laten komen, wordt dan vaak gerefereerd aan een bestaand factuurnummer. Een meer omslachtige, maar geavanceerdere manier van het wijzigen van het rekeningnummer is het inbreken (hacken) in de administratie van het bedrijf dat de factuur verstuurt. Deze oplichtingspraktijken worden meestal pas gedetecteerd wanneer de legitieme begunstigde het bedrijf erop wijst dat zij niet het verwachte factuurbedrag heeft ontvangen.

Phishing en malware

Remote Access fraude

Naast bovengenoemde methoden versturen criminelen nepfacturen voor denkbeeldige diensten die qua inhoud en bedrag veelal overeenkomen met een factuur die wordt verwacht. Soms wordt dit gedaan met (niet van echt te onderscheiden) nagemaakte e-mailopmaak van zakelijke relaties waarin meerdere bankrekeninggegevens zijn opgenomen.

Voorbeeld 3: Phishing en malware

Werknemers ontvangen dagelijks veel e-mails. Door drukte, maar ook uit gewoonte kan het daarom eenvoudig gebeuren dat zij op links klikken waardoor kwaadaardige software wordt geïnstalleerd op de lokale computer, of – erger nog – op het bedrijfsnetwerk. Criminelen worden hierdoor in staat gesteld om van afstand het netwerkverkeer te filteren en vertrouwelijke bedrijfsinformatie of financiële gegevens te bemachtigen.

Een bijzondere, maar zeer actuele vorm van malware, is de gijzelsoftware (ransomware). Dit type malware blokkeert een computer en/of gegevens die erop staan en vraagt vervolgens van de gebruiker geld om de computer weer te 'bevrijden'. Betalen blijkt echter niet (altijd) tot vrijgeven van de gegevens, bestanden of de computer te leiden.
Verder moet u rekening houden met het gevaar van Remote Access Tools. Dit is software die de beheerder ervan (hacker of helpdesk) toegang geeft tot een andere pc. Het stelt criminelen in staat alles op een computer te volgen en geld weg te sluizen. De cybercrimineel verandert bij het internetbankieren één van uw zakelijke rekeningnummers in dat van hemzelf. Nietsvermoedend blijven u of uw medewerkers geld overmaken naar deze rekening. Net als in het verleden. Het gevolg is een grote financiële schade. In het algemeen begint een aanval met een e-mail. Soms is het een algemene e-mail, vaak ook een mailing gericht op een specifieke sector zodat deze eerder serieus genomen wordt. Het virus weet zich te installeren op de computer omdat het misbruik maakt van fouten (bugs) in het besturingssysteem, de webbrowser of andere op de computer aanwezige software.

Voorbeeld 4: Tech support scam

In dit geval doen criminelen zich voor als bankmedewerker of bijvoorbeeld als medewerker van Microsoft. Zij nemen contact op met een bedrijf en beweren dat de (bank)software moet worden bijgewerkt of dat er een probleem is gesignaleerd. Daarvoor moeten volgens de persoon aan de telefoon de benodigde autorisaties aan hem beschikbaar worden gesteld. Om de fraude te camoufleren, melden de criminelen dat door de software-update het online bankieren een paar dagen niet beschikbaar zal zijn.

Tips voor het beschermen van uw bedrijf

1. *Controleer risicogevoelige processen*

   Waar kan er een opening zijn voor dergelijke fraude in uw bedrijf? Niet alleen het invoeren of autoriseren van betalingen zijn beveiligingsgevoelige processen. Wijzigingen in bijvoorbeeld rekeningnummers en e-mailadressen moeten ook nauwlettend gecontroleerd worden.

2. *Creëer een open bedrijfscultuur: laat vragen toe*

   Als werknemers ongewone transacties of contracten opmerken, moeten ze deze altijd kunnen navragen bij het management. Bevestiging via de telefoon van een aangewezen contactpersoon of leidinggevende in het bedrijf kan fraude voorkomen.

Wijs medewerkers op risico's gebruik social media

Wees alert en voorzichtig bij onbekende e-mails

3. Wijs medewerkers op risico's gebruik social media

Uitnodigingen van onbekende personen moeten niet zonder meer geaccepteerd worden. Maak uw werknemers ervan bewust dat informatie die zij delen via sociale netwerken en internet mogelijk tegen hen kan worden gebruikt.

4. Wees alert en voorzichtig bij onbekende e-mails

Laat uw medewerkers weten dat ze voorzichtig moeten omgaan met e-mails van onbekende afzenders. Zelfs als de vermeende afzender echt en bekend lijkt te zijn, moet het e-mailadres worden gecontroleerd. Als het e-mailadres overeenkomt met de afzender, kan de e-mail worden geopend. Als dit niet het geval is, moet deze worden verwijderd. In het algemeen gesteld, moet de inhoud van elke e-mail geloofwaardig en aannemelijk zijn. Een dwingende of dreigende toon ("het is essentieel dat het geld vandaag nog wordt overgeboekt, anders verliezen we een belangrijke klant") kan bijvoorbeeld een indicatie zijn dat er iets niet in de haak is. Kijk daarnaast goed naar alle links en afbeeldingen in de e-mail; ook deze moeten geloofwaardig en aannemelijk zijn. Neem bij twijfel vooral telefonisch contact op met de afzender van de factuur.

5. Zorg ervoor dat uw IT-systeem veilig is

Bescherm uw systemen (met internetverbinding): installeer firewalls en antivirus-software, implementeer patchbeleid (voor software-updates) en wijzig regelmatig wachtwoorden. Beveilig telefoons, tablets en computers die u gebruikt voor bankzaken met een toegangscode. Regel goed welke rechten uw medewerkers en beheerders hebben binnen uw netwerk. Installeer geen software van onbekende bronnen.

6. Controleer regelmatig uw rekeningen en batchopdrachten

Controleer altijd zo spoedig mogelijk uw elektronische en papieren rekeninginformatie. Check alle transacties die u instuurt of autoriseert. Gebruik ook de controlemogelijk-heden voor batchopdrachten, zoals controlegetallen en hashwaardes.

7. Zorg voor betrouwbare gebruikersrechten en beveiliging van de autorisatieprocessen

Geef medewerkers alleen die gebruikersrechten die zij nodig hebben om hun taken uit te voeren. Het toestaan van te veel gebruikersrechten zorgt voor een hoger risicoprofiel. Pas het 'vier ogen' principe toe bij het autoriseren van transacties (en het 'zes ogen' principe indien het grote betalingen betreft). Zorg dat individuele medewerkers niet gemachtigd zijn om te handelen namens anderen.

8. Educatie van uw werknemers op cybercriminaliteit

Houd regelmatig trainingssessies voor (nieuwe) fraude- en oplichtingspraktijken zodat uw medewerkers dit kunnen herkennen.

9. Wijs op het 'gebruik gezond verstand'

Vraag uw medewerkers om hun gezond verstand te gebruiken wanneer ze iets ongewoon zien. Verhoogde waakzaamheid is de beste waarborg voor uw bedrijf.

Wat moet u doen, mocht u (vermoeden) onverhoopt slachtoffer te zijn van cybercrime

Bel direct uw bank zodat zij (vervolg)schade kunnen voorkomen. Daarnaast moet u van alle fraude(pogingen) aangifte doen bij de politie. Voor juridische stappen is immers altijd een proces-verbaal nodig.

Voor meer informatie:

- https://veiliginternetten.nl/
- https://www.veiligbankieren.nl/
- https://www.ncsc.nl/
- https://www.politie.nl/
- https://www.fraudehelpdesk.nl/
- De website van uw bank