Social engineering gevaar op de werkvloer

RendementOnline

Door redactie FA Rendement

4 oktober 2023 | 5 minuten

Cybersecurity staat steeds hoger op de agenda, zowel bij de overheid als bij ondernemingen. Daarnaast is digitalisering toegenomen sinds er veel meer vanuit huis gewerkt wordt. Het belang van digitale veiligheid is daardoor ook verder toegenomen. Een van de lucratieve methoden voor cybercriminelen is social engineering. Dat kan beginnen met een vlotte babbel aan de telefoon. Maar ook wat u op social media deelt, is een bron.

Een cybercrimineel kan op allerlei manieren proberen gevoelige, vertrouwelijke informatie los te peuteren. De informatie die cybercriminelen vergaren, proberen ze vervolgens te interpreteren en te combineren tot bruikbare gegevens. Er is dan sprake van social engineering. Eigenlijk is een social engineer een soort spion voor wie niets te gek is om aan de gewenste gegevens of informatie te komen.

Niet de enige

Voor de social engineer kan het vergaren van persoonlijke gegevens bij de juiste combinatie, vergelijking en interpretatie uiterst bruikbare informatie opleveren. En die informatie heeft hij sneller dan u denkt. U bent echt niet de enige die denkt dat u er niet in zult trappen als iemand u telefonisch vraagt naar gevoelige bedrijfs- of persoonsgegevens.

> **De social engineer kan zijn ‘onderzoek’ al starten geheel buiten uw gezichtsveld**

Onbewuste informatie

Een social engineer denkt daar heel anders over en zal verschillende methoden en technieken op u loslaten, waardoor u toch iets prijsgeeft. De social engineer kan zijn ‘onderzoek’ al starten geheel buiten uw gezichtsveld. Als u uw eigen naam googelt, komt u mogelijk al heel wat informatie te weten.

Dat hoeft niet alleen om privézaken te gaan (zie kader), maar ook (semi)officiële, professionele en commerciële instanties verzamelen allerlei gegevens over u die opvraagbaar kunnen zijn, zoals gegevens van het kadaster, de Kamer van Koophandel, domeinnaamregistraties of telefoon- en bedrijfsgidsen. Mocht iemand bij een dergelijke instantie gegevens over u opvragen, dan hoeft u er niet op te rekenen dat de betreffende instantie u daarvan op de hoogte zal brengen.

Let op de privégegevens op social media

Ook de informatie die op uw socialemediapagina’s staat – uw gezinssamenstelling, hobby’s of nevenwerkzaamheden – kan een schat aan gegevens bevatten. De social engineer verdiept zich vergaand in de interesse, belevingssfeer en omgeving van zijn potentiële slachtoffer of doelgroep.

Inbreken en de manieren

Als bepaalde gegevens die de social engineer zoekt niet direct op internet te vinden zijn, kan hij proberen die informatie boven tafel te krijgen via direct contact met u of uw collega als gebruiker van het systeem of het netwerk waarop hij wil inbreken. Vooral in grotere ondernemingen kan een social engineer ook iemand benaderen die vanwege zijn functie niet helemaal op de hoogte is van alle ICT-procedures en de bijbehorende beveiligingsinstructies. Denk bijvoorbeeld aan (wisselende) krachten, de baliemedewerker, representatieve functies, maar ook nieuwe werknemers.

Nieuwe werknemers zijn namelijk meestal nog niet zo bekend met alle veiligheidsprotocollen en met wat binnen de bedrijfscultuur al dan niet normaal is. Voor nieuwe personeelsleden is het behoorlijk lastig in te schatten of bepaalde vragen indiscreet of risicovol zijn voor uw onderneming. Sommige social engineers zijn zelfs zo brutaal dat ze hun vragen inleiden met een praatje dat het heel normaal is om bepaalde vragen in het kader van het beveiligingsbeleid te stellen aan nieuwe werknemers.

Tips

Omdat het zo lastig is social engineering te herkennen (en te voorkomen) is het belangrijk om de kans hierop zo klein mogelijk te maken. De volgende tips kunnen daarbij helpen.

- Gebruik altijd sterke wachtwoorden voor toegang tot netwerken of webpagina's met gevoelige of cruciale gegevens en bestanden.
- Verander regelmatig uw wachtwoord. Dit kan bijvoorbeeld verplicht worden gesteld met behulp van software in de netwerkomgeving.
- Hang wachtwoorden nooit en te nimmer op een briefje aan de monitor of iets dergelijks, maar gebruik een wachtwoordbeheerprogramma (zoals NordPas, Keeper of Dashlane) als u ze niet allemaal kunt onthouden.

> **Werknemers voorlichting geven over social engineering help het eerder te herkennen**

Herkenning tegen social engineering

Uw onderneming beschermen tegen social engineering gaat niet met speciale software, zoals die wel bestaat voor malware. Werknemers voorlichting geven over het fenomeen kan wel helpen om social engineering te herkennen. Enkele tips:

- Verklein de kans op diefstal of verlies van mobiele apparatuur, want dergelijke apparatuur is nu eenmaal een belangrijk doelwit van social engineers.
- Wees voorzichtig met het verspreiden van persoonlijke en gevoelige gegevens via sociale media. Ook al lijken uw persoonlijke zaken niets te maken te hebben met uw werk, de social engineer vindt er vaak nog allerlei interessante informatie in.
- Maak in uw onderneming duidelijke afspraken of stel een beleid op over het afhandelen van persoonlijke en zakelijke relaties en bezoeken. Geef daarbij aan wat wel en niet hoort in de dagelijkse bedrijfsvoering. In een contactenbeleid kunt u laten vastleggen dat in ieder geval nooit direct aan een veiligheidsgerelateerd verzoek van relatief onbekende personen mag worden voldaan.

Bewustzijn en herkenning

Deze aandachtspunten spelen een extra belangrijke rol als u of uw collega's veel op beurzen, congressen of in de openbare ruimte zijn. Overtuig de directie ervan om werknemers bewust te maken van het fenomeen social engineering en de gevaren ervan.

Iedereen binnen uw onderneming moet op de hoogte zijn van de mogelijke bedreigingen van uw ICT-infrastructuur en systemen, de informatiegevoeligheid en de verschillende methoden van cybercriminelen. Daarbij hoort dus ook een bewustzijn met betrekking tot de dreiging van malware en phishing.

> **Bespreek de gevaren van en risico's van cybercriminelen**

Controletips met collega's

Gebruik eventueel de volgende controle- en leertips samen met uw collega's:

- Stuur een voorbeeld rond van een phishingmail en kijk of uw collega's die herkennen, en hoe ze erop reageren. Een spookfactuur rondsturen kan een eyeopener zijn.
- Check of uw collega's ook eigen software of procedures gebruiken (vooral de thuiswerkers). Zijn die net zo veilig en betrouwbaar? Past dit wel in uw automatiseringsbeleid of ICT-infrastructuur? Het verzamelen van die (deel)informatie kan via hengelberichten (phishing) of kwaadaardige scripts (malware).
- Bel of mail een collega en probeer gevoelige informatie los te peuteren. Doe uzelf voor als een ICT'er en vraag bijvoorbeeld om het wachtwoord waarmee kan worden ingelogd.
- Geef uw collega's een lijstje met sterke en zwakke wachtwoorden en laat hen aangeven welke wachtwoorden niet veilig zijn. Geef hier ook feedback op.
- Herhaal overlegsessies of trainingen over bewust en veilig datagebruik en online gedrag. Bespreek daarin de gevaren en risico's, de (nieuwste) trends en dreigingen, de methoden en technieken van cybercriminelen en beveiligingsmogelijkheden.

Al bent u misschien niet verantwoordelijk voor het beleid binnen de hele organisatie, iedereen zal snappen dat juist iemand van de financiële afdeling cybersecurity (tools) belangrijk vindt en daarover aan de bel trekt!

Dit is een artikel van de redactie van FA Rendement

FA Rendement is dé informatiebron voor administrateurs, boekhouders, controllers en andere financiële professionals. Wat is er veranderd op het gebied van financieel-administratieve wet- en regelgeving, en hoe kunt u als specialist deze informatie direct in uw dagelijkse werk toepassen? Daarnaast moet u op de hoogte zijn van onder meer de fiscaliteit, automatisering, de loon- en salarisadministratie, sociale voorzieningen, debiteurenbeheer en inkoop.

De onafhankelijke en ervaren redactie van FA Rendement zit bovenop het nieuws en vertelt u als eerste wat de ontwikkelingen zijn. Altijd in heldere taal en met een praktische insteek, zodat u de informatie direct kunt vertalen naar uw eigen werksituatie. FA Rendement is daarnaast multimediaal. De voor uw vakgebied relevante informatie verschijnt:

- ✓ dagelijks op het digitale platform Rendement Online, waar u onder meer het laatste nieuws, checklists, rekentools, maatwerkbrieven en verdiepingsartikelen tot uw beschikking heeft;
- ✓ wekelijks gebundeld in een e-mailnieuwsbrief;
- ✓ maandelijks in het vakblad FA Rendement, boordevol nieuws en achtergrondartikelen, digitaal en op de mat;
- ✓ tweemaandelijks in een handzaam themadossier: een pocketboekje dat iedere editie een complex onderwerp uitdiept.