Werk & geld • 06:00

Cybersecurity: 'Je bent zo sterk als je zwakste schakel'

Claartje Vogel

Digitale dieven worden sneller, slimmer en geavanceerder. Hoe bescherm je jouw bedrijf anno 2024 tegen cyberaanvallen?

In 2023 had bijna driekwart van de Nederlandse bedrijven te maken met een cyberaanval. Illustratie: FD Studio

Stel je voor: je krijgt een WhatsApp-bericht van een onbekend nummer op je werktelefoon, ondertekend met de naam van de hoogste baas. Hij wil je spreken over een aanstaande deal. Je bent huiverig, maar dan gaat je telefoon over en hoor je de stem van je ceo. Na een kort gesprek vraagt hij je om discreet te zijn en klaar te staan om een overeenkomst te tekenen. Die komt zo binnen in je mailbox. Wat zou jij doen?

In dit geval bleek het een poging tot oplichting, bij de Italiaanse autofabrikant Ferrari. Deze zomer was het bedrijf bijna slachtoffer van deepfakefraude. De medewerker die het telefoontje kreeg, vertelt aan persbureau Bloomberg dat de stem heel overtuigend was, met hetzelfde Zuid-Italiaanse accent als de echte ceo, Benedetto Vigna. Toch had hij wat argwaan jegens het verhaal van de 'bijzondere deal'. Hij besloot een persoonlijke vraag te stellen: 'Welk boek heb ik je onlangs aangeraden?' De nep-ceo verbrak onmiddellijk de verbinding en de medewerker meldde de poging tot oplichting.

Dit soort geavanceerde digitale fraude neemt toe. In 2023 had bijna driekwart van de Nederlandse bedrijven ermee te maken (zie kader *'Cyberaanvallen in opkomst'*). Uit onderzoek van ABN Amro en onderzoeksbureau MWM2 blijkt dat maar liefst 86% van de Nederlandse grootbedrijven en 71% van het mkb doelwit was van een hack of een andere digitale aanval. Bij 59% van alle grootbedrijven en 43% van het mkb leidde een cyberaanval tot schade, zoals inkomstenverlies door stilstand van het bedrijf of reputatieschade door gelekte klantgegevens.

Cyberaanvallen in opkomst

- De aanvalsmethoden van cybercriminelen veranderen in rap tempo, blijkt uit een analyse van ABN Amro (april 2024). Phishen blijft een populaire manier om binnen te komen bij bedrijven. Gijzelsoftware en fraude met AI zijn in opkomst.
- In totaal is **37%** van de Nederlandse bedrijven al eens geïnfecteerd met malware, waarvan 19% vorig jaar.
- **26%** van de bedrijven heeft ervaring met gijzelsoftware, waarvan 19 procent-punt de afgelopen 12 maanden.
- **25%** van de bedrijven verloor al eens vertrouwelijke gegevens door datalekken. Bij 15% gebeurde dit afgelopen jaar.
- Meer dan **50%** van de bedrijven ziet AI als een bedreiging voor de cyberveiligheid van de organisatie. In 2023 was dit nog geen kwart. Grote bedrijven maken zich het meest zorgen.

Niet of, maar hoe

Dat cyberaanvallen lastiger af te wenden zijn, blijkt ook uit een recent rapport van de Cyber Security Raad (CSR). Zij adviseren vooral de 'cyberweerbaarheid' te vergroten: het vermogen van organisaties om digitale risico's te beperken, cyberincidenten te voorkomen en schade eenvoudig te herstellen.

'Het is niet de vraag of en wanneer je slachtoffer wordt van een cyberaanval, maar hoe je de schade kunt beperken', zegt Joey Fennis, Head of Incident Response bij cybersecuritybedrijf DataExpert. Met zijn team helpt hij bedrijven zich te wapenen tegen cyberaanvallen. Fennis werkt al meer dan tien jaar als cyberveiligheidsspecialist, voorheen bij ING. 'Bij de bank zagen we de opkomst van de huis-tuin-en-keukenhacker. Ook een minder digitaalvaardige crimineel kan online eenvoudig een doe-het-zelfphishingkit kopen en onder valse voorwendselen vertrouwelijke gegevens achterhalen.'

Snelle ontwikkelingen maken het moeilijker om nepberichten, telefoontjes en zelfs videogesprekken te herkennen, aldus Evert van Essen. Hij is ceo van Brooklyn Partners, een bedrijf dat onder andere overheden en financiële instellingen helpt onlineoplichting te voorkomen. 'Voorheen leerden we mensen dat je nepberichten herkent aan slecht Nederlands, maar die vlieger gaat allang niet meer op', vertelt hij.

Ook *deepfakes* worden steeds echter. Met kunstmatige intelligentie zijn criminelen in staat om razendsnel bijna exacte kopieën van gezichten en stemmen te maken. Zo kunnen ze zich voordoen als een manager of zelfs een directielid.

Ook Bunq Bank en het Britse reclamebureau WPP werden bijna slachtoffer van ceo-fraude via deepfakes. Het internationale ingenieursbureau Arup raakte er zelfs $25 mln door kwijt. Van Essen: 'De grens tussen nepberichten en realiteit vervaagt. Maar het principe blijft hetzelfde: een crimineel probeert je te verleiden om van het proces af te wijken.'

> **'Eén ding is zeker: het gaat een keer mis, ook in jouw organisatie, dus maak een draaiboek en bereid je voor'**

Luister naar je onderbuik

Om weerbaar te zijn tegen cyberaanvallen heb je veel meer nodig dan een antiviruspakket. 'Het gaat er in het begin om dat iedereen zich bewust en verantwoordelijk voelt voor de digitale veiligheid van de organisatie', zegt Fennis. 'Je bent zo sterk als je zwakste schakel.' Voor managers is het belangrijk om nieuwe informatie te delen en incidenten te bespreken met hun team. Elke werknemer moet kennis hebben van cyberveiligheid.

Maar iedereen dezelfde e-learning geven is niet genoeg, volgens Van Essen. 'Het is beter om medewerkers te trainen op basis van het risico dat ze lopen. Wie het hoogste risico loopt, heeft specifieke coaching nodig.'

Medewerkers met een hoog risico op digitale fraude zijn de mensen met budgetten en financiële bevoegdheden, en de directie. In organisaties die werken met intellectueel eigendom zijn het de werknemers die toegang hebben tot gevoelige data. 'In een hightechbedrijf zijn dat de productontwikkelaars of bijvoorbeeld de technici met bepaalde marktkennis', zegt Van Essen. Hoe train je dit soort medewerkers?

'Houd ze op de hoogte van nieuwe technieken en deel informatie over recente aanvallen. Leer ze naar hun onderbuikgevoel te luisteren en bij enige twijfel de oorsprong van berichten te verifiëren. Vertrouw je een e-mail van een leverancier niet? Bel hem dan via het vertrouwde telefoonnummer.'

Gijzelacties

Kunstmatige intelligentie vergroot niet alleen de kans op phishing, maar ook die op ransom-aanvallen. Vooral in de maakindustrie zijn dit soort gijzelacties een ramp, vertelt Fennis. 'Hackers gebruiken AI om het internet af te speuren naar achterdeuren die openstaan. Vervolgens dringen ze binnen, stelen ze de data, verwijderen de back-ups, gooien alles op slot en vragen losgeld of verkopen de gegevens door. Zo kunnen ze de hele productie van een maakbedrijf platleggen of zelfs een brug of sluis blokkeren.'

Van Essen adviseert het risico te beperken door medewerkers alleen toegang te geven tot de systemen en info die ze echt nodig hebben. 'Veel datalekken ontstaan doordat mensen per ongeluk iets doormailen naar de verkeerde persoon. Ook werken met generatieve AI is een risico, want dit soort systemen onthoudt alle informatie die je erin stopt. Zo kan gevoelige bedrijfsinformatie zomaar bij je concurrent terechtkomen.'

Cloudtoepassingen en samenwerkingen met leveranciers zijn risico's waar je weinig grip op hebt. Een voorbeeld is de recente storing bij Defensie, Eindhoven Airport, NCSC (National Cyber Security Centre), DigiD en P2000. Door een storing bij Defensie lag het civiele onderdeel van Eindhoven Airport plat, waardoor er geen vliegtuigen konden aankomen of vertrekken.

'Zulke ketenreacties komen steeds vaker voor. Denk aan de wereldwijde Microsoft-storing door een fout in een beveiligingsupdate van Crowdstrike', waarschuwt Fennis. 'Eén ding is zeker: het gaat een keer mis, ook in jouw organisatie. Maak een draaiboek en bereid crisiscommunicatie met je medewerkers, zakenpartners en klanten voor. Je kunt trainen op deze rampen, zoals je ook een brandoefening doet.'

Dit artikel is gemaakt door de redactie van FD Persoonlijk. Lees al onze verhalen op fd.nl/persoonlijk.

Laatste nieuws

09:01
KLM grijpt in om resultaat met €450 mln op te krikken

08:01
VS en G7 waarschuwen voor aanval Israël op Iraanse kerncentrales

08:00
Co-ouderschap: samen apart zorgen

07:10
Live: AEX-index daalt in eerste handel op Damrak

06:00
Cybersecurity: 'Je bent zo sterk als je zwakste schakel'

Lees al het laatste nieuws