



Breng *cashflow* in je business

Hoe HR het verschil maakt in cybersecurity (ook al klinkt dat onlogisch)



Goed getrainde medewerkers: *de beste vorm van cybersecurity*

Dat maakt digitale veiligheid ook een verantwoordelijkheid van HR. Maar hoe kan de HR-professional op dit thema het verschil maken?

Er zijn twee soorten bedrijven: bedrijven die gehackt zijn, en bedrijven die dat niet door hebben gehad.' Zegt oud-FBI-directeur Robert Mueller. 'Bedrijven zijn vaak doelwit van digitale aanvallen, cybersecurity op de werkvloer is dus van wezenlijk belang'.

In de Verenigde Staten is 'Business Email Compromise', in het Nederlands: CEO-fraude, financieel gezien de op een na schadelijkste vorm van criminaliteit. (Beleggingsfraude staat op één.) Als het om digitale veiligheid gaat, is niet de technologie, maar de mens de zwakste schakel. Daarom is voor bedrijven de beste veiligheidsmaatregel het trainen van het personeel. Hierin kan HR het voortouw nemen.



De dreiging:

Phishing en CEO-fraude

Wat is CEO-fraude en phishing, en waarom zetten criminelen deze trucs in om bedrijven te misleiden?

Bij CEO-fraude wordt een medewerker van de financiële afdeling per e-mail gevraagd, zogenaamd door de baas, om een betaling uit te voeren. Minder bekend, maar ook veel voorkomend: frauduleuze mailtjes die uit naam van HR worden gestuurd, waarin de ontvanger herinnerd wordt vakantiedagen op te geven of - ironisch genoeg - een belangrijke cybersecuritytraining te volgen. Met deze mailtjes is het fraudeurs niet om een betaling te doen maar het ontfutselen van belangrijke (inlog)gegevens: 'phishing'.

Verreweg de meeste cybercriminaliteit draait niet om geavanceerde technologische aanvallen, maar om dit soort 'social engineering', oftewel psychologische manipulatie van medewerkers van bedrijven.

Het is verontrustend effectief: ruim een derde van de werknemers trapt in social engineering-trucs.



De rol van HR

in het thema cybersecurity

Als HR-professional doe je er goed aan om samen te werken met IT. Inhoudelijk blijft de IT-specialist namelijk hoofdvantwoordelijk op dit thema. Die is op de hoogte van phishingtrucs en -trends, weet wat er moet gebeuren als het fout gaat en kan belangrijke technische veiligheidsmaatregelen nemen om te voorkomen dat het zover komt. Dat gezegd hebbende, kan je als HR-professional op twee manieren jouw deel doen:

1. Zet een cybersecuritytrainingsprogramma op voor medewerkers. Uit [onderzoek van cybersecuritybedrijf KnowBe4](#) blijkt dat zulke trainingen op de werkvloer erg effectief zijn in het versterken van die menselijke schakel. Zonder training trapt gemiddeld één derde van de medewerkers wereldwijd in social engineering-trucs. Na training (en follow-ups) daalt dat percentage tot gemiddeld vijf procent.
2. Kies HR- en salarissoftware van een leverancier die haar digitale veiligheid op orde heeft en de privacygevoelige administraties van klanten veilig houdt.

Cybersecuritytrainingen voor medewerkers

Bij het opzetten en invullen van een cybersecuritytraining neemt HR het voortouw, maar vraag je hulp en input van externe specialisten en van IT-collega's. KnowBe4's Chief Human Resources Officer Ani Banerjee deelt in [dit artikel](#) enkele algemene aanbevelingen voor een effectief en voor medewerkers boeiend trainingsprogramma.

Samengevat:

1. Bepaal en communiceer doelen van de training. Zo kan HR de effectiviteit meten en snappen medewerkers het belang en nut van de training, wat hun betrokkenheid vergroot.
2. Betrek leidinggevenden bij het trainingsprogramma. Als zij het goede voorbeeld stellen, volgen medewerkers.
3. Zoek 'aanvoerders': medewerkers die gepassioneerd zijn over dit thema. Met hun hulp promoot je de training onder hun peers.
4. Maak de training interessant en vermakelijk door verhaaltechnieken te gebruiken, sprekende voorbeelden, humor en simulaties. Speltechnieken ('gamify') helpen ook: maak bijvoorbeeld van de training een competitie tussen afdelingen, laat medewerkers duidelijk hun voortgang zien, beloon, communiceer regelmatig resultaten en vier successen.
5. Deel een les op en verspreid de blokken over het jaar.

TIP:

Als onderdeel van de training kan je als steekproef nep-phishingmails sturen naar alle medewerkers. Collega's die in de val lopen, wijs je daar vriendelijk maar duidelijk op met een auto-reply. Dat zal ze waakzamer maken.

Verder kan je overwegen om:

1. De cybersecuritytraining onderdeel te maken van de onboarding
2. De training verplicht te maken en te herhalen
3. Een communicatiekanaal op te zetten waarin medewerkers verdachte berichten onderling kunnen delen en bespreken



HR- en salarisssoftware: *de digitale veiligheid van Cash*

Digitale veiligheid dient zwaar mee te wegen in de keuze voor HR- en salarisssoftware. Daarom tot slot iets over hoe wij bij Cash Payroll onze infrastructuur en de administraties van onze gebruikers veilig houden.

Cash is op het gebied van privacy en veiligheid degelijk en ervaren. We zijn namelijk onderdeel van de Noorse softwaregroep Visma en profiteren zodoende van hun kennis, middelen en ervaring.

- Onze servers staan in Europa. Alle data wordt dus gehost in Europa.
- Al het dataverkeer binnen Cash Payroll gaat via firewalls en verbindingen met de applicatie zijn versleuteld.
- Alle data is versleuteld, of het nu staat opgeslagen of onderweg is. De data kan dus niet leesbaar onderschept worden.
- Inloggen gaat zoveel mogelijk via twee-factor-authenticatie (2FA). Ons systeem is bovendien zo ingericht dat gebruikers alleen toegang hebben tot informatie en programma-onderdelen die ze écht nodig hebben.



Breng *cashflow* in je business

Ben je nieuwsgierig naar ons aanbod voor salaris- en HR-software in één? Onze adviseurs staan graag voor je klaar, per e-mail via verkoop@cash.nl of telefonisch via 070-3560570.



Alexanderstraat 3
2514 JL Den Haag

070 - 3 560 570
info@cash.nl