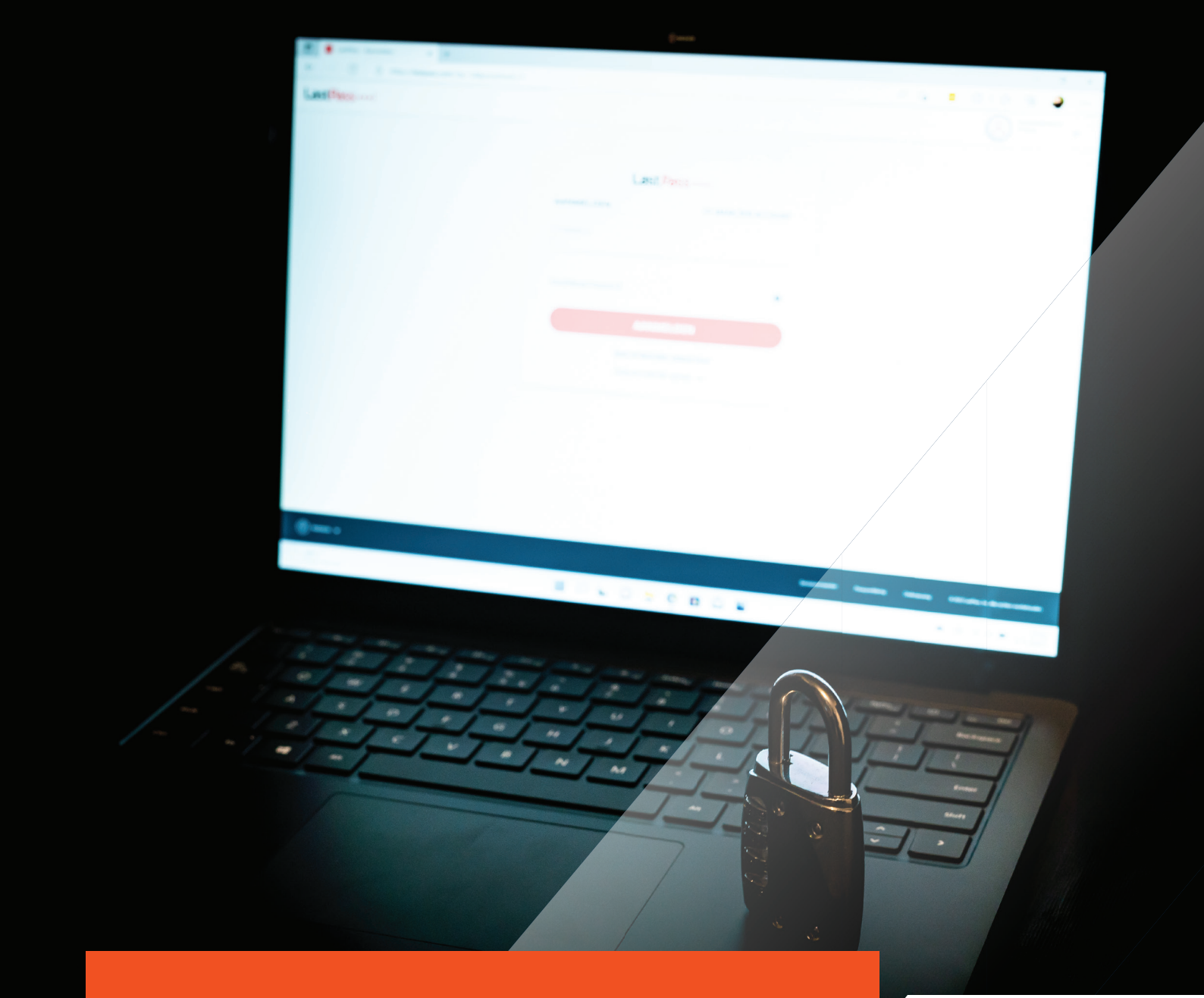


Verlaag cyberrisico's op de werkvloer met security awareness

TREDION

WHITEPAPER

Cybersecurity awareness: menselijk schild in de cyberstrijd

Je kunt je organisatie technisch gezien nog zo goed beveiligen tegen cyberaanvallen, het heeft pas zin als je personeel meedoet. Want bij het binnenkomen in jouw systemen hebben medewerkers een sleutelrol. Verreweg de meeste gemelde cybersecurity incidenten worden veroorzaakt door onwetendheid of onjuist handelen van mensen.

Bioscoopgigant Pathé werd in 2018 slachtoffer van CEO-fraude: er leek een e-mail verstuurd te zijn door de CEO, waarin hij om een geldbedrag vraagt. De fraudeurs hebben in korte tijd maar liefst 19 miljoen euro buitgemaakt. Hoe heeft dit zo kunnen gebeuren? En wat kan jij doen om een soortgelijke situatie in jouw bedrijf te voorkomen?

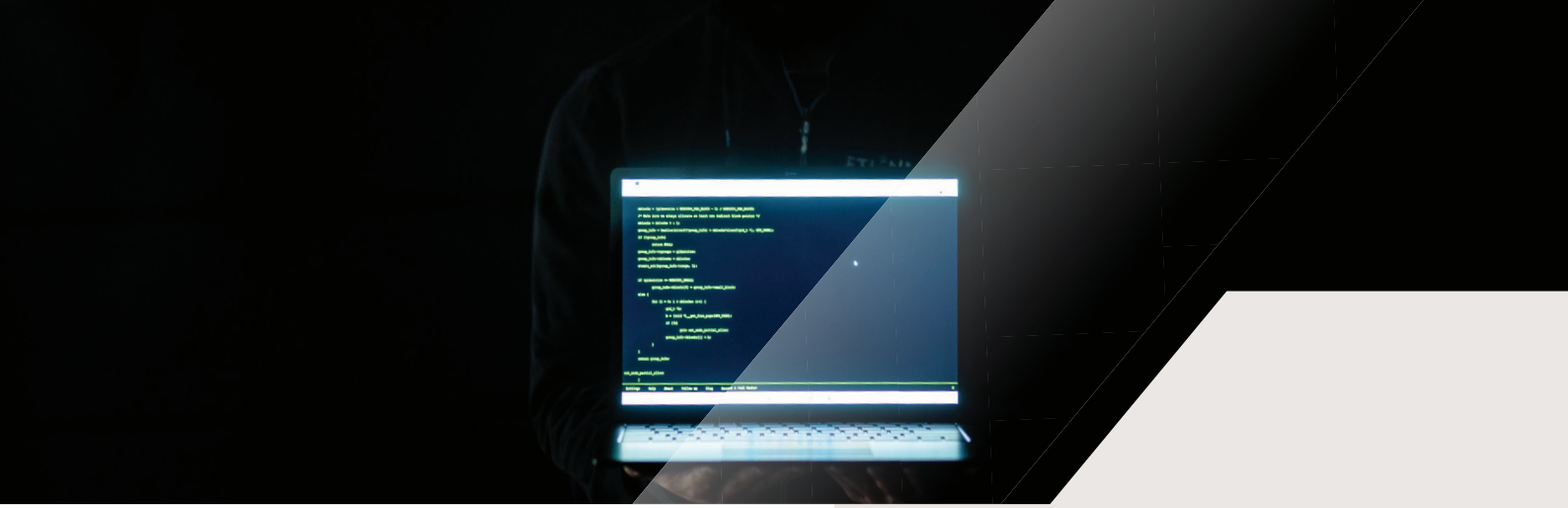
CEO-fraude: het verhaal van Pathé

Toenmalige directeur Dertje Meijer krijgt op 8 maart 2018 een e-mail binnen van de CEO van Pathé Europa. In de e-mail stond de vraag: “heeft KPMG al contact met je opgenomen vanochtend?”. Ze speelt de vraag door naar de CFO in Nederland, Edwin Slutter, en die weet ook van niets. Ze stuurt een e-mail terug. “Nee, hoezo. Wat is er aan de hand?” dan volgt de e-mail:

“We zijn op dit moment bezig met een financiële transactie die betrekking heeft op de overname van een buitenlandse onderneming in Dubai. De transactie moet strikt vertrouwelijk blijven. Communicatie moet alleen via mijn persoonlijke e-mailadres plaatsvinden. Na de deal zal het geld op de 26e weer teruggestort worden naar Amsterdam.”

Er moet direct een bedrag van € 826.000 worden gestort, en ook al twijfelen ze beiden over de gang van zaken, ze luisteren wel naar de baas. Het geld wordt overgemaakt naar het hoofdkantoor.
Een week later volgt een nieuw verzoek, dit keer voor enkele miljoenen euro’s. Dit herhaalt zich nog een aantal keer. Op deze manier is er in totaal zo’n 19 miljoen euro buitgemaakt.

Na enige tijd komen er vanuit het Pathé-hoofdkantoor vragen: waar is dit geld eigenlijk naartoe gegaan? Er vindt een spoedoverleg plaats. Dan wordt duidelijk: de Nederlandse top is om de tuin geleid door de fraudeurs. Zowel de CEO Dertje Meijer als de CFO Edwin Slutter worden ontslagen.



Hoe kan dit gebeuren? Bedrijfscultuur en social engineering

Om niet door de mand te vallen, hebben de fraudeurs zich uitgebreid verdiept in de bedrijfscultuur van Pathé. Zo wisten ze dat er tussen de CEO in Frankrijk en de directeur in Nederland voornamelijk mailverkeer plaatsvond. Ook bestaat in het hoofdkantoor van Frankrijk een cultuur waarin geen vragen aan de baas worden gesteld. Hier zijn de hackers achter gekomen door in te breken in de systemen en een tijdlang het mailverkeer te monitoren. In de verzoekmail wordt ingespeeld op het verantwoordelijkheidsgevoel van de medewerker: de informatie is 'strikt vertrouwelijk'. Deze aanpak heet ook wel 'social engineering'.

Hiërarchische organisaties met internationale vestigingen zijn kwetsbaar voor CEO-fraude, omdat er onderling beperkt gecommuniceerd wordt, vaak via e-mail.

Hoe makkelijk kunnen cybercriminelen jouw bedrijf binnendringen?

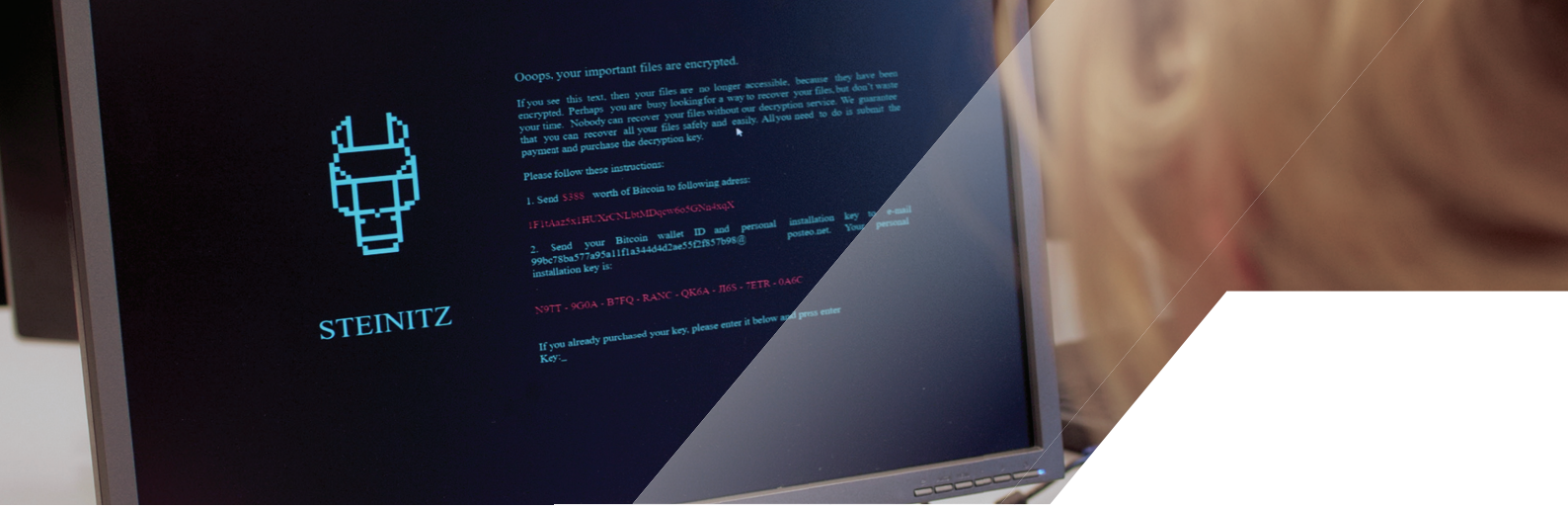
Vanwege schaamte worden CEO-fraude en andere vormen van cybercrime vaak binnenshuis gehouden. Daarom lijkt het alsof het minder vaak voorkomt dan het in werkelijkheid gebeurt. Maar het kan elk bedrijf overkomen. Menselijke fouten en een gebrek aan awareness op de werkvloer vormen verreweg het grootste cyberrisico. Een serieuze bedreiging, waar je als organisatie dus mee aan de slag moet!

Word je gehackt? Dat kost je geld én klanten

Het doel van cybercriminelen: jouw waardevolle (bedrijfsgevoelige of privacygevoelige) informatie stelen. Bijvoorbeeld om zich uitgebreid te kunnen voorbereiden op een grootschalige CEO-fraude zoals bij Pathé, of om die informatie rechtstreeks te verkopen op het darkweb. Afgelopen jaar zijn wereldwijd 1,4 miljard digitale bestanden ontvreemd, 86% meer dan een jaar geleden (Van Gils & Van Wijnen, 2021).

De gevolgen

Een cyberaanval heeft grote gevolgen voor organisaties. Volgens een **IBM rapport** zijn de gemiddelde kosten van een datalek inmiddels opgelopen tot maar liefst 4 miljoen dollar. Naast directe en indirecte financiële schade heeft een hack vaak enorme reputatieschade als gevolg. En wat dacht je van een afname van het klantenbestand. Want wie wil er nog met je samenwerken als hun data vervolgens op straat komt te liggen?



Verschillende typen cyberaanvallen

Om mensen aan te sporen om veilig gedrag te gaan vertonen in jouw organisatie, is meer kennis over cybercriminaliteit de eerste cruciale stap. Zo is het goed om te weten dat criminelen over het algemeen op drie manieren je systeem proberen te kapen. Ze schenden hiermee respectievelijk je CIA: Confidentiality (vertrouwelijkheid), Integrity (integriteit) en Availability (beschikbaarheid):

- Je identiteit: wachtwoorden of andere manieren van authenticatie (C)
- Uitvoering: iets uitvoeren op jouw systeem of netwerk, zoals malware (I)
- Een denial of service-aanval, waarmee ze je toegang tot je eigen systemen en informatie blokkeren (A)

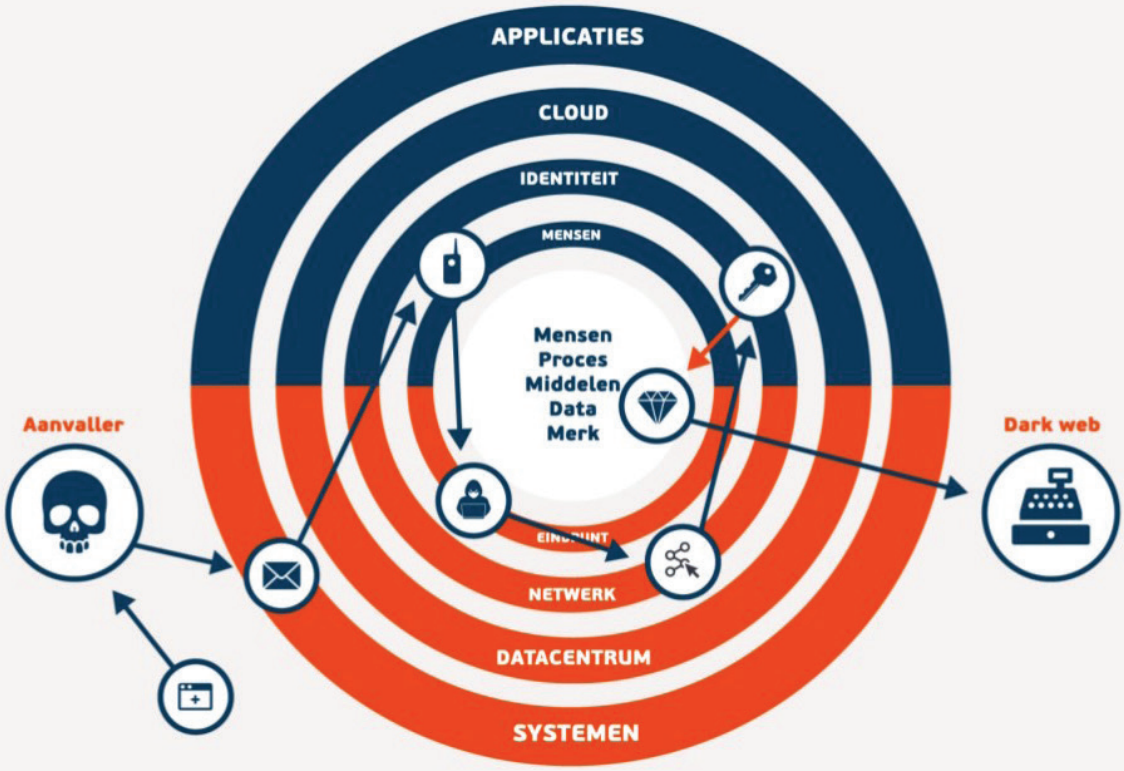
Voor al deze gevallen geldt: het binnenkomen in jouw systemen is altijd de eerste stap, waarbij jouw medewerkers een sleutelrol hebben. Denk aan het klikken op een malafide link in een e-mail die op het eerste gezicht van een vertrouwde partner lijkt te zijn. De link wordt geopend en zo begint de aanval op jouw vertrouwelijke informatie.

Omgaan met cyber-gevaren

De eerste stap om mogelijke fraude of een hack te voorkomen, begint bij de eindgebruiker. Die moet zich bewust zijn van cybergevaren en weten hoe hij hiermee om moet gaan. Lastig. Want hoewel een fysiek risico altijd heel zichtbaar is – als je de deur open laat staan, kan er een dief naar binnen komen en jullie laptops stelen – is dit digitaal een stuk ongrijpbaarder. De impact daarentegen kan veel groter zijn. En ook al heb je sloten op je deur, een alarm dat de laatste persoon die vertrekt moet inschakelen en een verzekering tegen inbraak – als een medewerker de deur open laat staan, heeft dit allemaal geen zin.

Ook kun je je bedrijfsnetwerk nog zo goed afschermen, maar als je medewerkers thuis op de bank zitten met hun zakelijke telefoon, dan kunnen hackers ook via die weg binnenkomen. Zo is spoofing (een nep e-mail, zogenaamd van een bedrijf) op je mobiel nauwelijks te onderscheiden van echt.

De hacker wil jouw systemen binnenkomen om jouw 'diamant' (belangrijke data) te stelen. Die verkoopt hij tot slot op het darkweb. Onderweg kan hij nog veel meer schade aanrichten aan je bedrijf.



Digitale fraude voorkomen begint bij security awareness

De meest voor de hand liggende – maar ook lastige – manier om cyberrisico's te minimaliseren is om je medewerkers zó van de risico's te doordringen, dat ze zich online veilig gaan gedragen. Iedereen in je bedrijf moet **security awareness** ademen. Je bedrijfscultuur speelt hierin een belangrijke rol: een op cybersecurity gefocuste cultuur moet je blijven motiveren en ondersteunen. Zo creëer je een optimaal samenspel van compliance, de medewerker en de techniek. En dat begint natuurlijk met training.

Een security awareness-training verkleint de kans op hacks

Op de bouwplaats worden mensen steeds gecorrigeerd als ze geen helm op hebben. Dit zorgt ervoor dat ze zich telkens opnieuw bewust worden van de risico's. Op dezelfde manier kun je mensen ook trainen als ze bijvoorbeeld hun scherm niet locken: zodat ze hier elke keer even goed bij nadenken.

Een goede security awarenesstraining verkleint aantoonbaar de kans dat je medewerkers op een malafide link klikken en zorgt ervoor dat ze zich online veiliger gaan gedragen. Maar zelfs de meest getrainde medewerkers kunnen op links blijven klikken. Dit ga je nooit helemaal voorkomen. Het doel is juist dat de organisatie de bewustwording gaat ademen.

Dit onveilige gedrag wil je dus niet meer in je organisatie...:

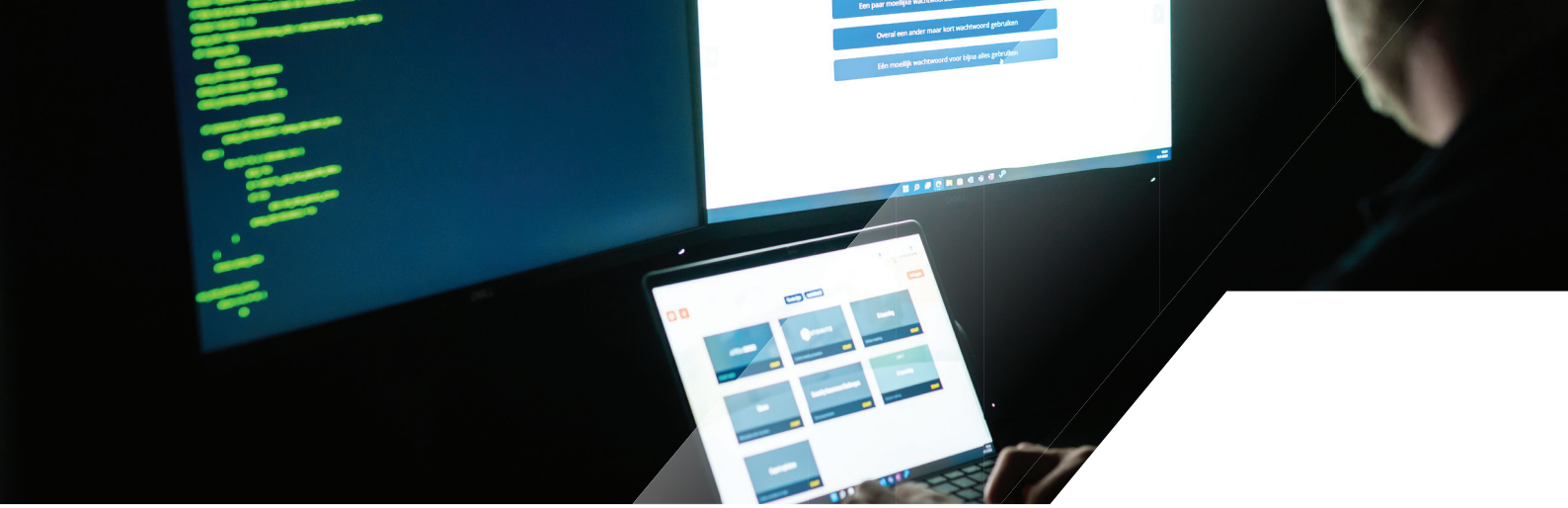
- In phishing e-mails trappen;
- Onveilige wachtwoorden gebruiken;
- Wachtwoorden delen;
- Per ongeluk gegevens lekken via e-mail of andere applicaties;
- Klikken op kwaadaardige links.

...en hier moet je personeel dus op getraind worden

Hieruit volgen belangrijke zaken die elke medewerker zou moeten leren:

- Onveilige e-mails/sms'jes/social mediaberichten herkennen en melden;
- Verantwoord omgaan met gevoelige bedrijfsinformatie;
- Geen onbevoegden toegang geven tot belangrijke documenten;
- Veilig omgaan met bedrijfsmiddelen, zoals laptops en telefoons;
- CEO-fraude kunnen herkennen, zoals in het voorbeeld van Pathé;
- Zich bewust worden van het belang van AVG en de impact van datalekken.

Al deze zaken komen spelenderwijs langs in onze awareness e-learning. Op diverse manieren wordt je personeel uitgedaagd om steeds meer te leren over cybersecurity. Het spelelement (gamification) helpt hierbij: zichtbare scores zorgen voor plezier en een gezonde competitiedrang.



De voordelen van onze trainingen in het kort

Het awarenessprogramma dat wij aanbieden loopt minimaal drie jaar, en medewerkers kunnen de vragen en challenges in hun eigen tijd doen. De prestaties van je personeel worden doorlopend getest met phishing e-mails. We zorgen ervoor dat de kennis goed over de tijd verspreid wordt, waardoor het security bewustzijn écht in je organisatie verankerd wordt. Onze online awareness training is uniek en uiterst effectief, want:

- Content is specifiek ontwikkeld voor de Nederlandse markt;
- Ook Engelse ondertiteling beschikbaar;
- De aangeboden informatie is volledig up-to-date;
- Gamification om de medewerker te verleiden en te motiveren;
- Echte cases ter referentie bij de vragen;
- Diverse expert-interviews;
- Resultaten meetbaar door middel van phishingtesten.

Benieuwd wat zo'n training jouw organisatie oplevert? **Bekijk hier de mogelijkheden** van security awareness.

Meer weten?

Neem contact op met Marc van Erp
marcvanerp@tredion.nl

Ontvang persoonlijk advies

TREDION

Avelingen-West 11
4202 MS Gorinchem

0183 610 555
info@tredion.nl