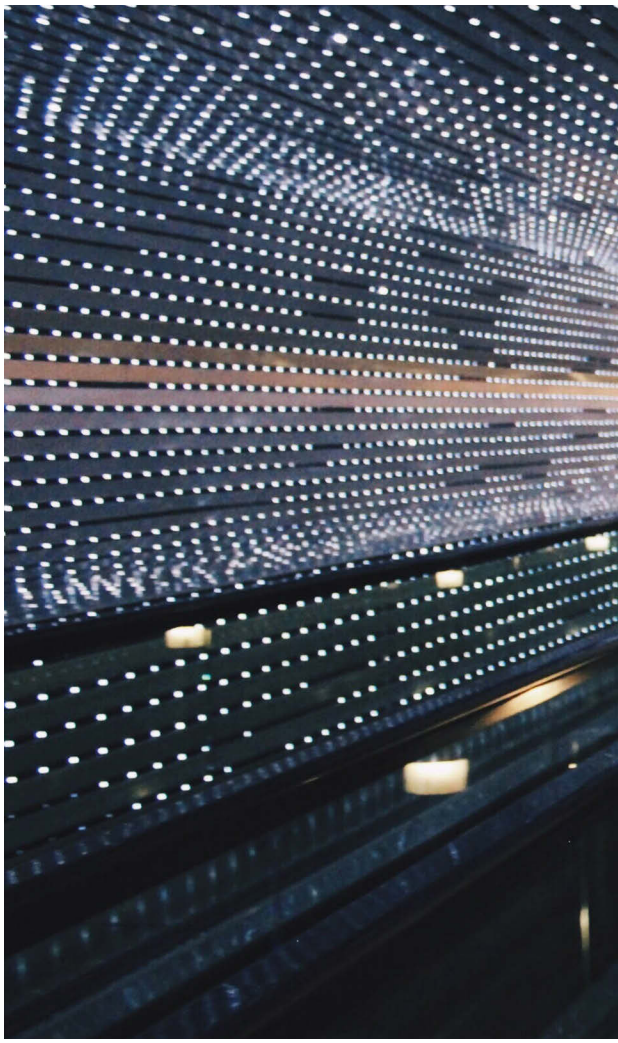
De menselijke factor is cruciaal, maar ook onderbelicht

Menselijke factor vaak doorslaggevend in cybercrime



De invloed van de menselijke factor op het slagen van een cyberaanval is groot. Middels social engineering proberen cybercriminelen een situatie te creëren waarbij een werknemer op een link klikt, een bestand download, of zelfs geld overmaakt naar een bankrekening. Veel medewerkers zijn onbewust onbekwaam. Middels awareness training worden medewerkers minder vatbaar voor social engineering en wordt de kans op een geslaagde cyberaanval kleiner.

Redactie Process Control

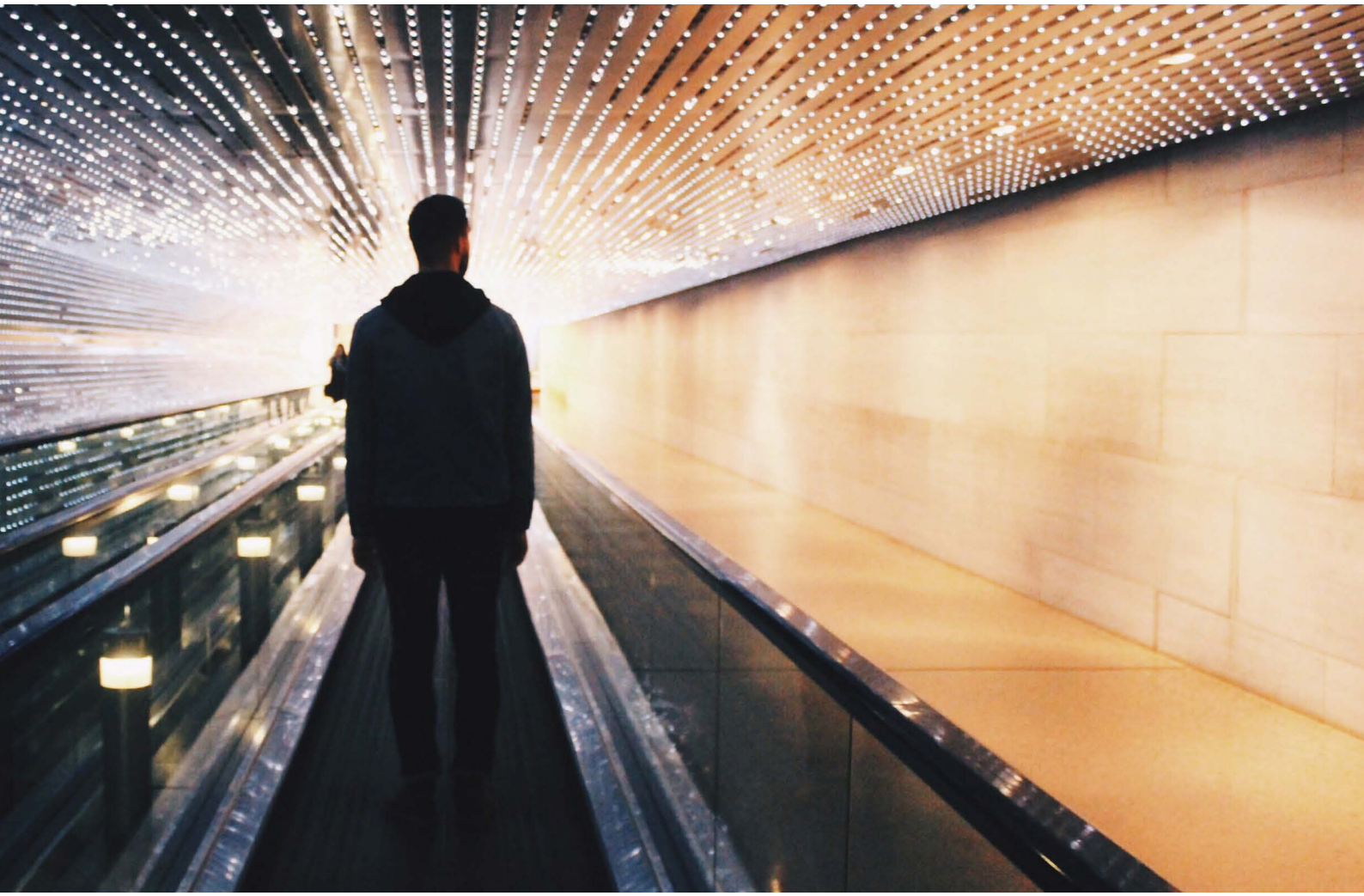
De 'human factor', of in goed Nederlands, de menselijke factor, is nog steeds een niet te onderschatten factor in (industriële) cybersecurity. Michael Theuerzeit, lead consultant bij Hudson Cybertec, vertelt: "We hebben het heel vaak over techniek; bijvoorbeeld hoe je OT en IT van elkaar gescheiden moet houden, hoe je zonering aanbrengt in je systemen, wat je met firewalls kunt, hoe Deep Packet Inspection werkt, enzovoorts. Cybersecurity wordt bepaald door mens, organisatie en techniek. Over die laatste twee hebben we het heel vaak, en terecht, maar het is belangrijk dat we ook het menselijke aspect niet overslaan. Dat is namelijk cruciaal."

Normen

In vrijwel alle gevallen van een geslaagde cyberaanval speelde een menselijke handeling een rol. En in veel gevallen is die menselijke rol doorslaggevend. "Ik schat in dat we het over zo'n negentig procent van de gevallen hebben", licht Theuerzeit toe. "Voor een geslaagde cyberaanval is het namelijk heel vaak noodzakelijk dat er ergens op een link wordt geklikt, een bestand wordt gedownload, of iemand iets verkeerd doet."
Doordat er de laatste jaren meer aandacht voor industriële cybersecurity is gekomen, zijn er veel dingen veranderd. Er zijn internationale normen gekomen, er is nationaal beleid voor cybersecurity en de industrie begint zich steeds meer te realiseren dat cybersecurity serieus dient te worden genomen. "Op het gebied van organisatie en techniek zijn er grote stappen genomen", vervolgt Theuerzeit. "Bedrijven voelen de noodzaak om te investeren in technische en organisatorische maatregelen om de kans op een geslaagde cyberaanval te verkleinen. Voor hackers is dat natuurlijk slecht nieuws: die moeten dus harder hun best doen om ergens binnen te komen."

Belletje rinkelen

De menselijke factor is vaak een ondergeschoven kind, weet ook Marcel Jutte, managing director bij Hudson Cybertec: "Nog steeds zie je een best grote groep mensen die onbewust onbekwaam zijn als het over cybersecurity gaat. Als je een mailtje krijgt van je collega met het verzoek de bijlage te downloaden en het document even door te lezen, gaat er niet altijd een belletje rinkelen."
En waar de techniek het voor hackers lastiger maakt om bedrijven te hacken, zorgt andere techniek er ook weer voor dat social engineering, het bewust misleiden van mensen om ze een bepaalde handeling te laten uitvoeren, ook weer eenvoudiger wordt.



"Denk maar aan deep fakes", verduidelijkt Theuerzeit. "Het kan zomaar zijn dat jij gebeld wordt door je leidinggevende met het verzoek om een bepaalde som geld over te maken op een bankrekeningnummer. In grote bedrijven kan het best zo zijn dat je die specifieke leidinggevende maar twee keer eerder hebt gesproken en dat je niet meer exact weet hoe die persoon praat. En wat doe je dan? Ga je dan drie verdiepingen omhoog op zoek naar die persoon om te checken of het wel echt is? In de praktijk komen dit soort gevallen van oplichting echt voor. De remedie is uiteraard vrij simpel: bel die specifieke persoon even op en begin het gesprek met: 'Ik had je net even aan de telefoon en heb ik goed begrepen dat dit en dat de bedoeling is?' Als die persoon aan de andere kant verbaasd vraagt waar je het over hebt, weet je vervolgens hoe laat het is."

"Als er op die USB-stick een label zit met daarop de tekst 'reorganisatie 2022' trek je nog steeds heel veel mensen over de streep"

Groot versus klein

Deep fakes worden steeds geraffineerder en er is steeds minder informatie nodig om een overtuigende deep fake te produceren. Als de belangrijkste klanken zijn geregistreerd is het mogelijk om een deep fake te maken. Vaak zijn daar maar enkele gesproken zinnen voor nodig. "Je moet niet de illusie hebben dat je dat kunt voorkomen", meent Theuerzeit. "Dat zou betekenen dat je geen telefoongesprekken meer zou kunnen voeren."

Grotere organisaties kunnen kwetsbaarder zijn voor social engineering dan kleinere bedrijven. Jutte: "Grotere organisaties hebben per definitie een groter aanvalsoppervlak. Maar ook heel praktisch: in een klein bedrijf waarbij iedereen op gehoorsafstand van elkaar zit, leidt een mailtje van de leidinggevende met een verzoek ergens geld naar over te maken zeer waarschijnlijk tot de vraag waarom die leidinggevende dat niet even door het kantoor heen kan roepen."

Michael Theuerzeit

Marcel Jutte

USB-stick

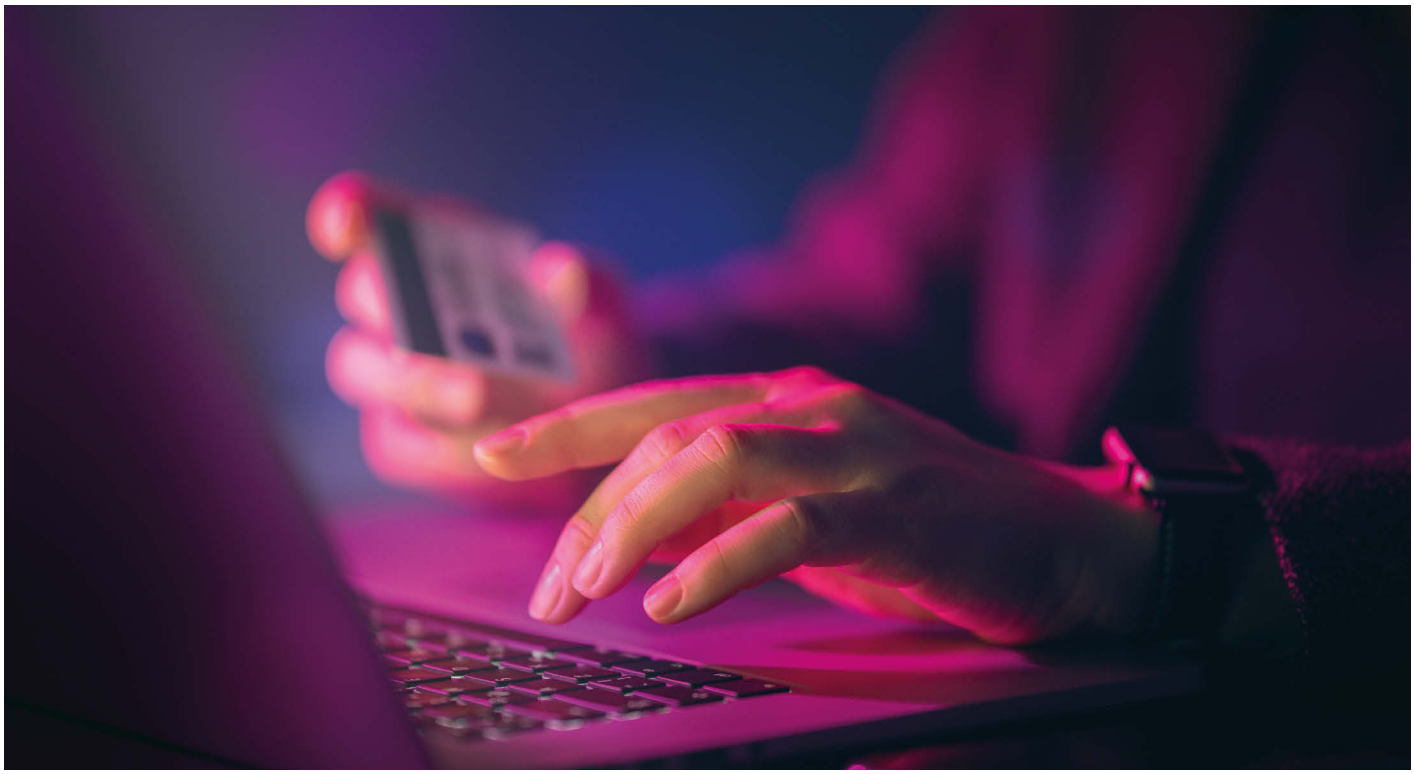
Ook de 'old school' achtergelaten USB-stick op de parkeerplaats sorteert nog altijd effect. "Iedereen die een awareness-training heeft gehad, weet dat je die USB-stick niet in een computer moet stoppen, maar als jij iemand weet te triggeren om dat toch te doen, weet ik zeker dat sommige mensen er intrappen," vertelt Theuerzeit.
Dat triggeren kan soms op een verbluffend simpele manier gebeuren: "Als er op die USB-stick een label zit met daarop de tekst 'reorganisatie 2022' trek je nog steeds heel veel mensen over de streep." En als die tekst nog niet voldoende is, kan een logo, of een veelgebruikte afkorting van een afdeling binnen het bedrijf het restant van de twijfel alsnog wegnemen.

Serious gaming

Zo'n negentig procent van de cyberaanvallen is, zoals Theuerzeit al eerder zei, afhankelijk van de menselijke component. Dat betekent dus ook dat het investeren in die menselijke component een enorme pay-off heeft. "Ik zeg niet dat je dan meteen minder cyberaanvallen hebt, maar wel dat de kans op slagen van een cyberaanval significant kleiner wordt", verduidelijkt Theuerzeit.
Een interessante manier om awareness te vergroten is het zogenaamde 'serious gaming', waarbij op een speelse manier de kennis van medewerkers wordt verruimd. Jutte: "Dat kan gaan om het simuleren van een calamiteit, wat in de procesindustrie vrij gebruikelijk is, maar serious gaming kan ook worden toegepast op awareness training."
Bij Hudson Cybertec werd de afgelopen tijd hard gewerkt aan een serious game dat specifiek gericht is op de menselijke component bij cyberaanvallen. Jutte: "We hebben een spel ontwikkeld dat we inmiddels inzetten bij onze awareness programma's. Het spel bestaat uit vragen met een aantal mogelijke antwoorden. Mensen worden daarbij getriggered om op een andere manier na te denken over cybersecurity. Daarnaast komt er ook een competitief element bij. Het interessante is dat het spel door de hele organisatie heen kan worden ingezet, van procesoperators tot directieleden."
Er wordt zeer positief gereageerd op het spel. "Je ziet dat mensen op een andere manier gaan denken over social engineering", vertelt Theuerzeit. "Wat ook interessant is dat het spel ertoe leidt dat mensen ineens gaan praten over eerdere social engineering ervaringen. Iemand zegt dan: 'Ik heb een jaar geleden precies zo'n raar mailtje gehad en toen heb ik dit en dat gedaan.' En andere collega's blijken dan ook ervaringen te hebben met verschillende social engineering methodes, zonder dat ze toen wisten dat het om social engineering ging. Het spel is enerzijds een eyeopener en anderzijds een breekijzer om de discussie aan te zwengelen."

Screening

Ook de normeringen in cybersecurity hebben vooral betrekking op de technische en organisatorische kant van cybersecurity. Theuerzeit: "Als je kijkt naar de WBNI en de NIS zie je dat het ook daar vooral om techniek en organisatie gaat. Wat mij betreft is de menselijke factor onderbelicht."
Volgens Jutte zouden daar op een relatief eenvoudige manier grote stappen in gezet kunnen worden. "Het is van groot belang om je personeel goed te



screenen voordat je ze een functie geeft. Daarbij is een Verklaring Omtrent Gedrag (VOG, red.) een prima begin, maar op kritische functies kan het noodzakelijk zijn om een zwaardere screening in te zetten. Niet alleen als het personeel de organisatie binnenkomt, maar ook op het moment dat ze van functie wisselen."
Uit een screening kan blijken dat mensen misschien bovengemiddeld beïnvloedbaar zijn voor social engineering. Iemand die grote schulden of andere problemen heeft, zou bijvoorbeeld makkelijker kunnen worden overgehaald tot bepaald gedrag. En waar een geslaagde cyberaanval in een IT-afdeling erg vervelend kan zijn, leidt een geslaagde cyberaanval in het OT-domein van een chemische plant zeer wel mogelijk tot serieuze safety issues. Hoe groter de consequenties, hoe relevanter een goede screening is."

Witte overhemden, blauwe overalls

Een ander probleem dat ook sterk met de menselijke factor samenhangt is de aloude tegenstelling tussen IT en OT, weet Theuerzeit. "IT-afdelingen zijn vaak veel mondiger dan OT-afdelingen. Ik kom heel vaak tegen dat IT'ers OT-cybersecurity er wel even naast denken te kunnen doen, maar zo simpel gaat dat niet. OT-domeinen zitten echt anders in elkaar en de consequenties bij storingen zijn vele malen groter dan in het IT-domein. Ook de directie is vaak gevoeliger voor argumenten vanuit de IT-afdeling dan die van de OT-afdeling. We zien helaas te vaak dat er door interventie vanuit de IT-afdeling verkeerde OT-cybersecurity beslissingen worden genomen. Je krijgt daarmee een soort schijnveiligheid."
Die complexe verhoudingen tussen IT-afdelingen, OT-afdelingen en directies kunnen worden verbeterd door de partijen met elkaar in gesprek te brengen en ze echt naar elkaar te laten luisteren. Maar dat is soms behoorlijk lastig. Theuerzeit: "Ik heb meegemaakt dat ik zowel de IT- als OT-afdeling in één meeting wilde betrekken. Eerst kwamen de witte overhemden en stropdassen binnen. Die gingen aan één kant van de tafel zitten. Daarna kwamen de blauwe overalls binnen en die gingen aan de andere kant van de tafel zitten. Wij werden als externen begroet, maar onderling werd er zelfs geen gedag gezegd. Dan weet je dat je een serieuze taak hebt om de partijen samen te brengen. De spanning was daar te snijden en er was een compleet gebrek aan begrip voor elkaar. Omdat wij in zo'n situatie als externen aan tafel zitten om advies te geven, kunnen we het gesprek sturen en voorkomen dat mensen elkaar niet eens laten uitpraten. We helpen ze echt naar elkaar te luisteren met als doel de digitale weerbaarheid van de organisatie te vergroten."

> "Voor hackers is dat natuurlijk slecht nieuws: die moeten dus harder hun best doen om ergens binnen te komen"

Meer weten over awareness training en heeft u ook interesse in serious gaming? Kijk dan op www.hudsoncybertec.com

Hudson Cybertec en de Kiwa Groep

Hudson Cybertec maakt sinds kort onderdeel uit van de Kiwa Groep, een bekende mondiale speler op het gebied van certificeringen. Kiwa is actief in meer dan 40 landen en heeft ruim 10.000 medewerkers in dienst.
Kiwa heeft met Hudson een sterke speler aan boord die gespecialiseerd is in OT Cybersecurity. Bij Hudson kan men door de overname gebruik maken van het grote netwerk van Kiwa en putten uit een veel grotere pool van werknemers.
Marcel Jutte, managing director bij Hudson Cybertec licht toe: "Door de overname krijgen we de mogelijkheid om sterk te groeien. Niet alleen omdat we nu midden in een netwerk van prospects komen te zitten, maar ook omdat we bij Kiwa de beschikking krijgen over meer slagkracht. We hebben namelijk ook de nodige mensen nodig om die groei te kunnen doormaken."