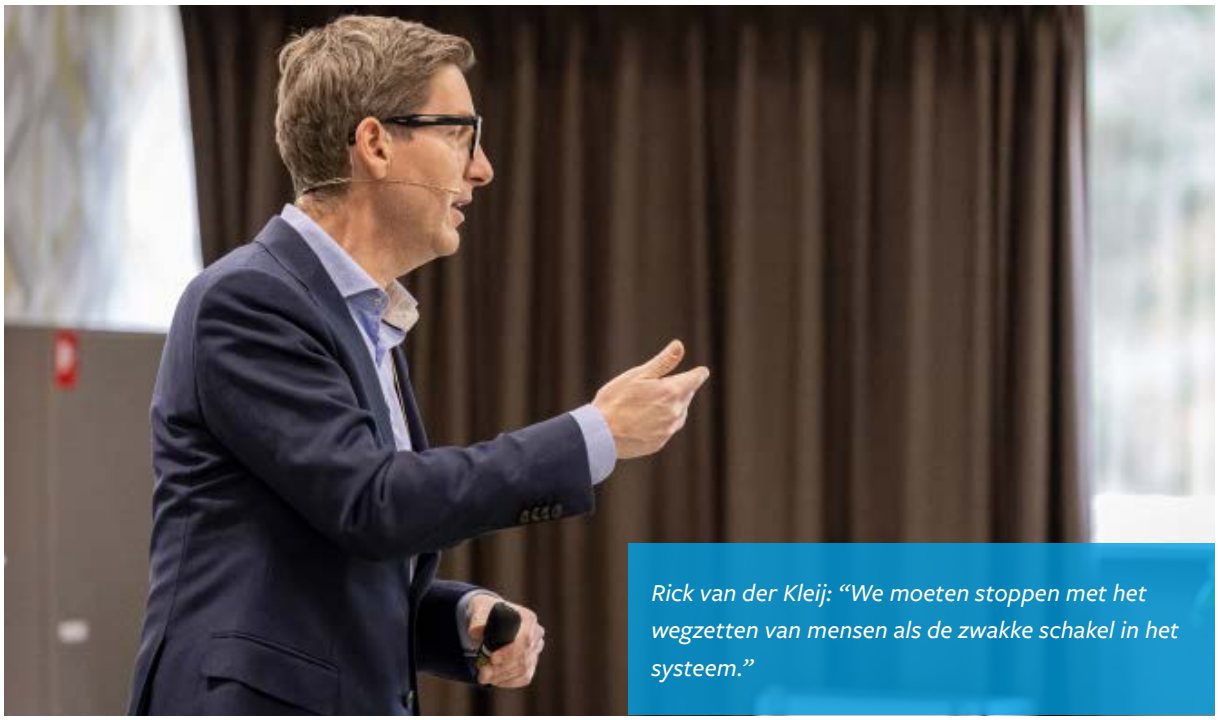
Interview met Rick van der Kleij, onderzoeker TNO

“Cybersecurity is meer dan **technologie alleen**”

In 2021 zijn er 735.000 fietsen gestolen. Dat lijkt veel, maar in hetzelfde jaar zijn volgens het Centraal Bureau voor Statistiek (CBS) bijna 2,5 miljoen Nederlanders slachtoffer geworden van online criminaliteit. Nederland is dus niet meer het land van traditionele misdaad, maar van cybercriminaliteit. Dus moet er meer in de bestrijding van cybercriminaliteit geïnvesteerd worden. Maar hoe? Security Management spreekt hierover met dr. Rick van der Kleij, gepromoveerd psycholoog en cybersecurity-onderzoeker bij TNO.

Door Betty Rombout

Beloon mensen die niet op een phishingmail klikken.



Rick van der Kleij: "We moeten stoppen met het wegzetten van mensen als de zwakke schakel in het systeem."

Samen met andere partijen onderzoekt TNO manieren om de maatschappij veiliger te maken door middel van innovaties op het gebied van cybersecurity. Zo is een security-awareness-aanpak nieuwe stijl ontwikkeld binnen het partnership van het PCSI (Partnership for Cybersecurity Innovation). Van der Kleij. "We hebben samen met partners gekeken naar een nieuwe rol op het gebied van security-awareness die hoort bij deze aanpak nieuwe stijl. De rol is succesvol getest binnen een van de partnerorganisaties."

Traditionele benadering

Sinds 2012 is het aantal slachtoffers van online criminaliteit met 22 procent toegenomen. En dat cijfer stijgt nog steeds. De gevolgen zijn enorm. Steeds meer bedrijven zijn slachtoffer van bijvoorbeeld ransomware. Een tandartsketen moest onlangs 2 miljoen euro betalen om weer toegang te krijgen tot systemen met daarin onder meer patiëntgegevens, nog los van de reputatieschade, wat ook een nadelig gevolg is. "Als bedrijf kun je er helaas niet vanuit gaan dat je veilig bent en gevrijwaard blijft van cybercriminaliteit. Dat vergeten veel bedrijven. Ze weten niet wat ze moeten doen als het misgaat", aldus Van der Kleij.
Hij vervolgt: "Oplossingen worden traditioneel vaak gezocht in de technologische hoek. Digitale veiligheid is nog veelal een IT-feestje. Dat doen we al jaren, maar dat werkt niet. Wat moet dan anders? Gelukkig vinden we allen wel dat er meer geïnvesteerd moet worden in cybersecurity. Maar waar investeer je dan in en hoe?"

Van der Kleij: "We moeten accepteren dat cybersecurity een sociotechnisch systeem is met veel verschillende elementen die de veiligheid beïnvloeden. Niet alleen technologie maar ook mensen, procedures en beleid spelen een belangrijke rol. De meeste investeringen zitten echter in technologie: 85 procent; 14 procent gaat naar processen, slechts 1 procent gaat naar de mensen. De balans is helemaal zoek. Ik denk dat er veel te winnen is als we investeren in alle componenten, dus ook in de mens. We moeten stoppen met het wegzetten van mensen als de zwakke schakel in het systeem. Dat is niet waar. Veiligheid hebben we zo ingewikkeld gemaakt dat mensen hierdoor falen. We moeten mensen onderdeel maken van het systeem. Trainen van personeel in cyberbeveiliging is een goede stap, maar daar moet het niet bij blijven. We hebben een security-awareness nieuwe stijl nodig die van de mens een belangrijke pijler maakt in cybersecurity."
Maar hoe doe je dat dan? "Mensen hebben beperkingen, dat hoor je te weten. We hebben moeite om ingewikkelde maar sterke wachtwoorden te onthouden. Maar dat wordt vaak wel van mensen verwacht, met als gevolg dat ze stiekem toch simpele en makkelijk te kraken wachtwoorden gebruiken, hun wachtwoord ergens opschrijven of wachtwoorden hergebruiken, om maar wat voorbeelden te noemen. Dit brengt risico's met zich mee. Als systeemontwerper hoor je er rekening mee te houden dat mensen fouten maken. Er moet een vangnet zijn. Wat te doen? Met kennis van de mensen het systeem herontwikkelen."
Van der Kleij verduidelijkt: "We zien dat er een kloof is

tussen kennis en gedrag. Met alleen kennisoverdracht zet je mensen niet aan tot veiliger gedrag. Mensen handelen niet alleen op basis van kennis. Meer aspecten spelen een rol om te komen tot veiliger gedrag. Gelegenheid, motivatie en kennis leiden tot bepaald gedrag. Kennis is de basis, maar de gelegenheid tot veilig gedrag moet er ook zijn. Zoals daadwerkelijk een slot op een deur. Motivatie? Als mensen melding maken van een phishingmail bij de IT-afdeling en daar geen feedback op krijgen, haken ze af. Ze zijn dan niet meer gemotiveerd. Als je van de mens een belangrijke pijler wilt maken in cybersecurity, wilt zorgen voor meer veiligheid, dan moet je deze aspecten ook meenemen in een security-awareness-programma."

Niet straffen maar belonen

Een ander belangrijk aspect van security-awareness nieuwe stijl is mensen niet te straffen. "Straffen mag dan effectief zijn, maar de effecten van belonen zijn veel sterker. Negatieve sancties kennen een grote beperking. Je dwingt mensen op te houden met bepaald gedrag, maar stimuleert hen niet om te zoeken naar nieuw gedrag. Met belonen doe je dat wel. Beloon mensen bijvoorbeeld die niet op een phishingmail klikken. Dan zet je ze in hun kracht, in plaats van de mensen die wel op een phishingmail klikken, verplicht een training te laten volgen. Ook kun je het mensen gemakkelijker maken aan veiligheid te doen, door bijvoorbeeld het verplicht melden van phishingmails makkelijk te maken via een meldknop in Outlook. En koppel vervolgens ook terug wat er met die melding gedaan wordt", aldus Van der Kleij. Er is bij security-awareness-activiteiten ook weinig sprake van maatwerk. De ene organisatie is de andere niet. Of de medewerkers nu veel of weinig affiniteit hebben met cybersecurity, iedereen krijgt dezelfde training. Activiteiten zijn ook vaak eenmalig. De dag erna hebben mensen het er nog over, en vervolgens is het weer zoals altijd. De resultaten worden ook veelal niet gemeten. Hoe weet je dan of wat je doet het juiste is?
"Het effect van veel awareness-trainingen is maar van korte duur. Elke week zou er bijvoorbeeld enige aandacht moeten zijn voor security, een korte vraag, een korte update op een onderwerp dat actueel is. Zo creëer je constant een stukje awareness binnen de organisatie", verklaart Van der Kleij.

Geen IT'ers

Waarom missen cybersecurity-awareness-activiteiten vaak hun doel? Van der Kleij licht toe: "Ten eerste omdat we deze activiteiten vaak laten leiden door mensen met de verkeerde vaardigheden. De cybersecurity-IT-specialist doet dit vaak naast het technische werk in deeltijd. Maar je vraagt mij als psycholoog toch ook niet om een computerprogramma te schrijven? Je moet mensen met een IT-achtergrond niet vragen om gedrag van eindgebruikers in relatie tot cybersecurity te laten onderzoeken."

Meetbaar

Van der Kleij: "Security-awareness-trainingen hebben vaak een verkeerde focus. Ze richten zich op wat fout gaat: eindgebruikers die simpele wachtwoorden gebruiken of op een phishingmail klikken. Dit is verkeerd in mijn ogen. Dit legt de verantwoordelijkheid niet bij de mensen die er over gaan, die het beleid bepalen, maar bij de eindgebruikers. We moeten stoppen om security-awareness-specialisten met een negatieve opdracht op pad te sturen. Als het maar niet fout gaat. Security-awareness-specialisten moeten op zoek gaan naar een positieve businesscase. Wat leveren de inspanningen op? En maak dat meetbaar."

Rol securitymanager

We hebben een aantal aspecten genoemd van cybersecurity-awareness nieuwe stijl. De vraag is natuurlijk: wat is de rol van de securitymanager in deze? "Een goede vraag", zegt Van der Kleij, want "wie moet hier nu iets mee?" Securitymanagers bepalen mede het (veiligheids)beleid. We hebben al heel wat gewonnen als de securitymanager meer *human awareness* heeft. Dat hij of zij snapt wat mensen in beweging zet en dat je security-awareness-specialisten nodig hebt die de mens en zijn gedrag begrijpen om de security op een hoger plan te brengen."

Betty Rombout is freelance journalist

Samenwerking

Het Partnership for Cyber Security Innovation (PCSI) is een publiek-privaat samenwerkingsverband en speelt door innovatie op het gebied van cybersecurity een essentiële rol om te komen tot een veilige en veerkrachtige digitale samenleving. Het partnership bundelt krachten om toepasbare en innovatieve cybersecurity-oplossingen te ontwikkelen waarmee bedrijven en organisaties in de Nederlandse samenleving zich kunnen beschermen tegen de cyberaanvallen van morgen.

Meer informatie: www.pcsi.nl