Herstel de mens als sterkste schakel

Al jarenlang is het een gevleugelde uitspraak binnen het cybersecuritydomein: de mens is de zwakste schakel. Die uitspraak is niet alleen onnodig negatief, maar doet bovendien meer kwaad dan goed. En is bovendien niet waar. Omdat veel van de incidenten waarvan mensen de schuld krijgen hun oorsprong helemaal niet vinden bij de eindgebruiker, maar bij andere elementen in het securitysysteem. Het is niet de mens, maar de heersende securityfilosofie die faalt.

Tekst: Dr. Rick van der Kleij

Veel organisaties zien securityoplossingen als het belangrijkste middel om het digitale kwaad te bestrijden. Anno 2023 mogen we echter best concluderen dat die hyperfocus op technologie heeft gefaald. Goede security is niet alleen een kwestie van bits en bytes. Naast krachtige securityoplossingen zijn een degelijk securitybeleid en veilig gedrag cruciaal om de oprukkende cybercriminaliteit de kop in te drukken. Want jazeker: de meeste cyberincidenten ontstaan door menselijk handelen.

Dat het vaak misgaat op 'veilig gedrag', ligt echter niet per se aan de mens zelf. Mensen worden namelijk niet vanzelf onderdeel van dat 'socio-technische' securitysysteem. Waar het misgaat? Allereerst bij de erkenning van de rol van de mens binnen cybersecurity.

Volgens Gartner ligt de verhouding tussen investeringen in technologie, processen en de mens op respectievelijk 85, 14 en 1 procent.

Security-awarenesstrainingen

Die gigantische scheefgroei is op zichzelf al zorgwekkend. Het wordt nog problematischer als organisaties die ene procent ook nog op een ineffectieve manier inzetten. Er valt vaak veel af te dingen op de manier waarop veel organisaties hun security-awarenesstrainingen inzetten. Zo zijn ze vaak eenmalig. Ook is er nauwelijks sprake van maatwerk. Iedereen ondergaat dezelfde training. En zonder goede metingen van de effectiviteit zijn de resultaten van zo'n training een blinde vlek.

Dat is niet het enige probleem met de meeste security-awarenesstrainingen. Veelal staan de verkeerde mensen voor de groep. Deze trainingen worden namelijk doorgaans gegeven door IT'ers. Hun insteek is kennisoverdracht. Niet verwonderlijk, want die kennis is hun specialiteit. Kennis alleen is echter niet genoeg. Het is niet kennis die

'Awarenesstrainingen worden vaak gegeven door de verkeerde mensen'

hackers buiten de deur houdt, maar veilig gedrag. IT'ers hebben niet per definitie verstand van menselijk gedrag, laat staan dat ze gedragsverandering kunnen realiseren.

Meer dan rationaliteit

Bovendien komt veilig gedrag niet alleen voort uit rationaliteit. Daar is meer voor nodig. Een veilige werksfeer bijvoorbeeld. Zo'n sfeer ontstaat niet door mensen te straffen als ze op een verkeerde link klikken. Die negatieve benadering zorgt er vooral voor dat mensen incidenten niet meer melden, met alle gevolgen van dien. In plaats daarvan zouden organisaties het melden van incidenten moeten aanmoedigen.

Daarnaast is securitybeleid vaak te ingewikkeld. Zo ingewikkeld dat mensen daarop falen wat juist zorgt voor onveiligheid. Denk aan een beleid dat om het gebruik van sterke – en dus ingewikkelde – wachtwoorden vraagt. Dat is op papier goed verdedigbaar, maar zorgt in de praktijk juist voor onveiligheid. Mensen zijn namelijk van nature slecht in het onthouden van ingewikkelde tekenreeksen. Met als gevolg dat ze wachtwoorden hergebruiken, of op post-its schrijven. In zo'n geval zorgt securitybeleid dus juist voor onveilig gedrag.

Veilig gedrag faciliteren

Technologie en beleid moeten veilig gedrag juist faciliteren, en dat zo eenvoudig mogelijk maken. Dat betekent onder andere dat deze zaken zo min mogelijk dagelijkse werkprocessen verstoren. Daarvoor zijn mogelijkheden genoeg. Zo bestaat al een tijd het idee om wachtwoorden te vervangen door een reeks zelfgekozen emoji's. Zolang de set emoji's groot genoeg is, heb je bij vier stuks al een zeer sterk 'wachtwoord'. Niet alleen kunnen wachtwoorden zo korter worden, emoji's zijn ook nog veel eenvoudiger te onthouden.

Gelukkig leeft dit besef bij een groeiende groep securityleveranciers. Er bestaan zelfs oplossingen die niet alleen de focus leggen op gebruiksvriendelijkheid, maar zelfs veilig gedrag actief stimuleren. Denk aan software die waarschuwt op het moment dat medewerkers privacygevoelige persoonsgegevens in hun e-mail verwerken. Zo'n waarschuwing maakt direct bewust en kan het aantal onbedoelde datalekken via e-mail flink verkleinen.

Organisaties zijn aan zet. Het is hun verantwoordelijkheid om de mens als sterkste schakel te herstellen. Een goede

Over de auteur

Dr. Rick van der Kleij is security-onderzoeker bij TNO. Vanuit die rol onderzoekt hij de menselijke factor binnen cybersecurity.

start is te kijken hoe mensen precies hun werk uitoefenen. Met welke processen en handelingen hebben zij dagelijks te maken? En ook: welke drempels ervaren zij als het gaat om security? Worden deze issues niet bij de kern aangepakt, dan bestaat het risico dat medewerkers manieren zoeken om eromheen te werken. Die 'workarounds' brengen weer nieuwe risico's met zich mee.

Nieuwe rol

Het is tijd voor een nieuwe rol binnen cybersecurity. Een die de menselijke factor serieus meeweegt in het socio-technische securitysysteem, en die mensen begeleidt naar veiliger gedrag. Belangrijk is om die rol weg te houden bij IT'ers, want het vertrekpunt is niet technologie. In plaats daarvan ligt hier een grote kans voor psychologen en gedragsexperts. Zij zijn immers bij uitstek de personen die menselijk gedrag kunnen veranderen. Is er geen budget voor dergelijke specialisten? Dan is het goed om je als cybersecurityprofessional te verdiepen in menselijk gedrag. Want uiteindelijk hebben we niet meer security-awareness nodig, maar meer human-awareness. Alleen zo maken we van de mens de sterkste schakel. "De hier gepresenteerde inzichten zijn mede tot stand gekomen door intensieve samenwerking binnen het Partnership for Cyber Security Innovation (pcsi.nl)." ‹‹

Cybersecurity nieuwe stijl

Het sturen van menselijk gedrag gaat het beste vanuit een positieve benadering. Een waarbinnen de mens onderdeel is van een socio-technisch securitysysteem. Dat betekent dat organisaties afscheid moeten nemen van veel traditionele denkwijzen over sturing van gedrag. Onderstaande tabel maakt dat duidelijk.

Traditioneel	Nieuwe stijl
Controle op naleven regels	Mensen helpen
Straffen	Belonen
Negatieve opdracht	Positieve businesscase
Mens als losstaand element	Systeembenadering
Bewustzijn als doel	Veilig gedrag als streven
IT-insteek/achtergrond	Psychologie als basis
Losstaande acties	Continu proces
Mens als probleem	Mens als onderdeel van de oplossing