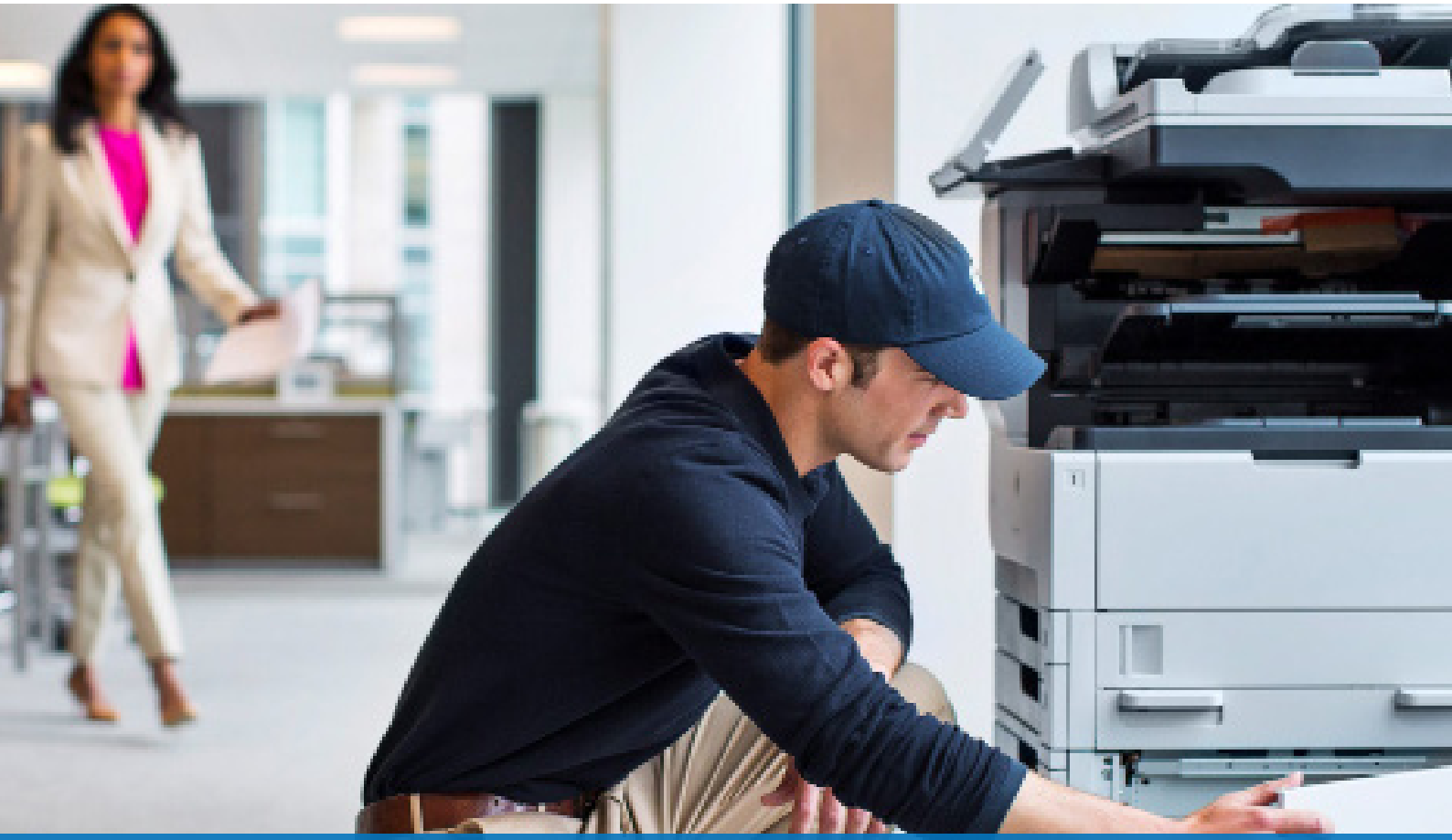
ateron®



WHITEPAPER

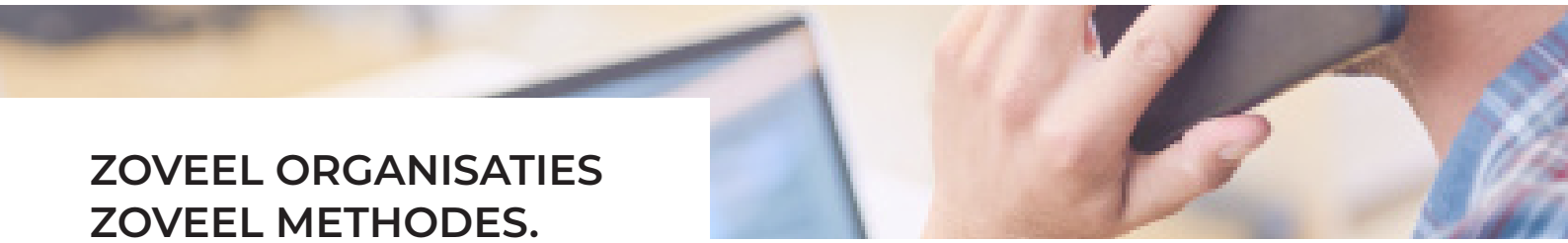
Social Engineering: Wie was toch die printermonteur?

Organisaties investeren steeds meer in hoogwaardige technische oplossingen om cybercriminelen en cyberaanvallen tegen te houden. Het gevolg is dat cybercriminelen steeds verder gaan om een aanval te laten slagen en misbruik maken van menselijke eigenschappen om zo vertrouwelijke gegevens te verkrijgen of om medewerkers bepaalde handelingen te laten verrichten: social engineering. **SOCIAL ENGINEERING** - ook wel human hacking genoemd - is hot. Lees in deze whitepaper over de verschillende social engineering technieken, waarom het zo succesvol is, de gevolgen ervan en wat we kunnen doen om ons te wapenen.

SOCIAL ENGEERING:
WIE WAS TOCH DIE PRINTERMONTEUR?

Technische oplossingen bieden weinig garantie om cybercriminelen buiten te houden en cyberaanvallen tegen te gaan. Ruim 70% van alle informatiebeveiligingsincidenten wordt namelijk nog altijd veroorzaakt door de eigen medewerkers. Vaak veroorzaken medewerkers deze incidenten onbewust, bijvoorbeeld door het delen van inloggegevens met een cybercrimineel. Criminelen gaan ook steeds verder in hun handelen en richten zich specifiek tot medewerkers om een aanval te laten slagen. Ze maken misbruik van menselijke eigenschappen om gegevens te ontfutselen of om mensen bepaalde handelingen te laten verrichten. Dit fenomeen staat bekend als **SOCIAL ENGINEERING**.

Er bestaan tal van verschillende technieken en methodes die criminelen, vaak succesvol, inzetten om personen te misleiden. Wat is het geheim hierachter en wat kunnen organisaties doen om hun medewerkers ertegen te wapenen?



ZOVEEL ORGANISATIES ZOVEEL METHODES.

PHISHING

De meest bekende vorm van **SOCIAL ENGINEERING** is natuurlijk phishing. In een e-mail worden ontvangers verleid om op een malafide link te klikken, een bijlage te openen of een andere handeling te verrichten. Wanneer er geklikt wordt probeert de aanvaller om vertrouwelijke gegevens te stelen, geld afhandig te maken of om malware en ransomware te installeren. Phishingmails zijn bijna niet meer van echt te onderscheiden. Maar liefst 91% van de datalekken wordt veroorzaakt door een phishingmail. Daarbij wordt volgens telecommunicatieconcern Verizon 30% van de verzonden phishingmails daadwerkelijk geopend. Vaak worden e-mailadressen “gespoofed”. Bij e-mail spoofing wordt een e-mailadres nagebootst en daarmee wordt de afzender vervalst. Dit kan een organisatie zijn of een persoon uit de eigen organisatie.

SMISHING

Dezelfde werkwijze wordt gebruikt bij sms phishing of smishing. Bij deze vorm van phishing krijgen slachtoffers in plaats van een e-mail een sms-bericht gestuurd met daarin een link naar een website of betaalverzoek. Het zorgwekkende is dat elk nummer vervalst kan worden.

WHALING

Whaling, beter bekend als CEO-fraude, wordt steeds vaker succesvol ingezet. Denk bijvoorbeeld aan het schandaal bij Pathé. Bij deze vorm van spearphishing (een gerichte phishing-aanval op een afdeling of individu) doet de crimineel zich voor als iemand van het topmanagement, waarbij vaak de vraag wordt gesteld of er snel een bedrag kan worden overgemaakt, bijvoorbeeld ten behoeve van een overname. De crimineel heeft hierbij veel kennis van de organisatie en weet goed aan wie van de financiële afdeling de mail gericht moet worden.

VISHING

Dan is er telefonische phishing, ook wel vishing (voice phishing) genoemd. Denk bijvoorbeeld aan de welbekende Microsoft scam, waarbij een zogenaamde Microsoft medewerker opbelt om een geconstateerd computerprobleem op te lossen, of een telefoontje van de ICT-afdeling met de vraag om inloggegevens te verstrekken. Vaak wordt vishing ook gebruikt als voorbereiding op een aankomende spearphishing-aanval. Phishing, vishing en smishing worden vaak gecombineerd om een zo legitiem mogelijke uitstraling te creëren.

USB DROP

Draagbare geheugens worden door medewerkers onderling nog steeds vaak gebruikt om informatie uit te wisselen. Daarom maken criminelen ook graag misbruik van USB-sticks. Bij deze vorm van **SOCIAL ENGINEERING**, ook wel “baiting” genoemd, worden USB-sticks verspreid in of nabij kantoorpanden of zelfs door promotieteams op parkeerplaatsen. Als de USB-stick eenmaal wordt aangesloten wordt geprobeerd om systemen te infecteren met malware of om gevoelige bedrijfsinformatie te stelen.

MYSTERY GUEST

Dan zijn er nog de mystery guests. Succesvol in al zijn eenvoud. Een crimineel doet zich voor als printermonteur, klant of medewerker van de serviceprovider en probeert zo fysiek toegang te krijgen tot het kantoorpand. Binnen 10 minuten staat de crimineel weer buiten met twee laptops, drie telefoons en een tablet met gevoelige informatie.

HET SUCCES ACHTER SOCIAL ENGINEERING.

Criminelen gaan steeds gerichter te werk. Veel van de informatie over bedrijven, afdelingen en werknemers die cybercriminelen gebruiken om een aanval op te zetten is te achterhalen via social media. De junior medewerker van de Finance afdeling is gemakkelijk op te sporen en de serviceprovider van een organisatie is eenvoudig traceerbaar. Daarnaast zijn criminelen heer en meester in het manipuleren van mensen. Dit doen ze door handig in te spelen op factoren waar mensen gevoelig voor zijn. Een aantal aspecten waar criminelen graag misbruik van maken zijn:

- Zakelijke of persoonlijke gevolgen door dreigementen
- Tijdsdruk (directe call-to-action)
- Goedgelovigheid van medewerkers
- Het uitstralen van autoriteit (bepaalde functie)
- Behulpzaamheid van medewerkers

DE GEVOLGEN.

De gevolgen van een succesvolle **SOCIAL ENGINEERING** aanval zijn vaak groot. Wellicht de grootste schadepost is de reputatieschade die een organisatie oploopt. Hoe kunnen zij nou vatbaar zijn voor een dergelijke truc? Andere gevolgen betreffen natuurlijk het verlies van vertrouwelijke informatie of geld en geïnfecteerde systemen.

Daarnaast is er nog de downtime na een incident: de tijd die nodig is om het incident te herstellen waardoor de organisatie niet bezig kan zijn met de dagelijkse business. De grootste schade die organisaties oplopen gaat dus veel verder dan geld alleen.

HOE KUNNEN ORGANISATIES ZICH WAPENEN?

Het antwoord is makkelijk en moeilijk tegelijkertijd: start met veiligheidsbewustwording en stel duidelijke procedures op. Maak medewerkers er bewust van hoe criminelen te werk gaan, zorg dat zij beveiligingsrisico's kunnen herkennen en daadwerkelijk zorgvuldiger en veiliger gaan werken. Test hen ook regelmatig. Maak daarnaast ook duidelijk bij wie medewerkers zich moeten melden als zij geconfronteerd worden met een vorm van **SOCIAL ENGINEERING**. Daar ligt gelijk het moeilijke aspect; het doorlopend aandacht besteden aan security awareness. Het is een proces, geen eenmalig project. Een eenmalige actie bereikt niet het gewenste resultaat, omdat de kennis op termijn wegzakt. Daarnaast bedenken criminelen continu nieuwe methoden om mensen te manipuleren en hun doel te bereiken.

OVER ATERON.

Organisaties worstelen vaak met de betrokkenheid van medewerkers op het gebied van informatiebeveiliging en privacy. 70% van alle informatiebeveiligingsincidenten wordt immers veroorzaakt door menselijk handelen. **Ateron** is specialist in het creëren van bewustwording en gedragsverandering rondom informatiebeveiliging.

Wij testen het gedrag van medewerkers, geven inzicht in het veiligheidsniveau en trainen uw medewerkers. Dit doen we met security awareness programma's en -meetmethoden. Leer medewerkers beveiligingsrisico's herkennen, maak van hen de sterkste schakel in informatiebeveiliging en creëer een (cyber)veilige werkomgeving.

CONTACT

Ateron
Bergerweg 170
6135 KD SITTARD

+31 (0)46 475 93 05
info@**ateron**.nl