Security Awareness: waar mensen werken, ontstaan kwetsbaarheden

In dit artikel gaan wij in op het menselijk gedrag en leggen wij uit wat het belang van security awareness is als onderdeel van een effectief informatiebeveiligings-managementsysteem.

De meeste bedreigingen van informatiebeveiliging zijn gericht op het manipuleren van menselijk gedrag. Dit blijkt uit de social engineering-technieken die cybercriminelen toepassen om toegang te verkrijgen tot gevoelige informatie en -systemen. Een van de meest voorkomende technieken is phishing, waarbij cybercriminelen via een e-mail proberen om mensen te overtuigen om op een link te klikken of een bijlage te openen. Cybercriminelen proberen het gedrag van mensen te manipuleren door bijvoorbeeld een e-mail te gebruiken die eruitziet als een legitieme e-mail van een vertrouwde organisatie of door urgentie te creëren om snel te handelen.

Beweegredenen achter het klikken

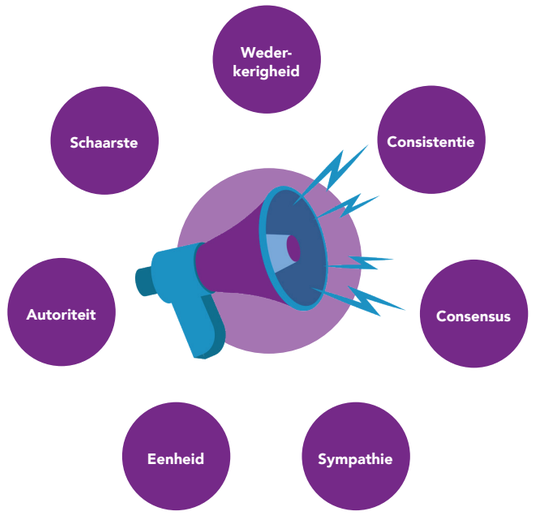
Maar waarom klikken er nog steeds mensen op links in phishing e-mails terwijl veel aandacht wordt besteed aan de risico's die hiermee gepaard gaan? En wat kunnen we eraan doen om dit te voorkomen? Veel keuzes die mensen maken zijn gebaseerd op emoties. Emoties kunnen de interpretatie van informatie en besluitvorming beïnvloeden. Als mensen tijdens het openen van een phishing e-mail niet anders denken dan dat het een 'echte' e-mail is en de inhoud automatisch vertrouwen, zal de kans groot zijn dat zij onbewust de phishinglink of bijlage openen. Dit is immers de makkelijkste weg. En hoewel er in toenemende aandacht voor het creëren van awareness voor dergelijke praktijken, lijkt het kiezen voor de makkelijkste weg ook vaak aan te sluiten bij de gewenste beleving van mensen, namelijk het handelen uit vertrouwen. Daarnaast kan het een trigger zijn om een phishing mail te openen omdat medewerkers een zekere urgentie ervaren; zij kunnen zich zorgen maken over het missen van belangrijke informatie en zouden daarom de phishinglink kunnen openen. Al is het alleen maar om het gevoel te krijgen dat zij niets missen; óók wanneer de klikker de mail niet helemaal vertrouwt.

Naast bovengenoemde redenen kan de druk van een groep, bijvoorbeeld van collega's of de verwachtingen van anderen, invloed hebben op het menselijk gedrag. Gedrag wordt in dit geval beïnvloed vanuit een sociaal perspectief. Sociale beïnvloeding wordt bewust ingezet bij het ontwerpen van phishing mails. Zo wordt zo'n mail vaak verstuurd uit naam van een collega of een bekende. Dit vergroot de kans dat op de mail geklikt wordt, bijvoorbeeld om niet onbeleefd gevonden te worden en uit betrokkenheid naar de betreffende collega.

Lang niet alle phishingmails zijn overigens zorgvuldig opgesteld en vormgegeven. Je kunt als kwaadwillende ook gewoon geluk hebben: er wordt uit automatisme of door slordig handelen heel vaak onbewust op een link geklikt, ondanks eenvoudig te herkennen punten die zo kenmerkend zijn voor een phishing e-mail.

De beïnvloedingsprincipes van Cialdini (zie afbeelding) helpen ons bij het inzichtelijk maken van hoe phishing e-mails werken en waarom mensen vaak in de val lopen. Een aantal van deze principes zijn:

- Consensus: phishing e-mails kunnen medewerkers proberen te overtuigen om op een link te klikken door het zo te laten lijken dat veel mensen dit eerder hebben gedaan;
- Autoriteit: phishing e-mails kunnen verzonden worden uit de naam van een bedrijf met een bekende naam;
- Schaarste: phishing e-mails kunnen het gedrag van medewerkers manipuleren door te benadrukken dat de link voor een beperkte tijd toegankelijk is.



De 7 beïnvloedingsprincipes van Cialdini

Security awareness beleid

Een cyberaanval kunnen wij niet voorkomen, we kunnen de kans daarop echter wel verkleinen door in te spelen op het menselijk gedrag. Dit vereist een combinatie van verschillende methodes.
Zo zou elke organisatie in onze ogen een security awareness campagne moeten ontwikkelen die past bij de organisatie en diens medewerkers (zie pagina 18 over de Pubquiz Cyberellende). Door regelmatig security trainingen te ontwikkelen en deze regelmatig op de agenda te zetten, wordt het veiligheidsbewustzijn van medewerkers vergroot. Het is het van belang dat alle medewerkers de trainingen volgen. Dit geldt uiteraard ook voor nieuwe medewerkers maar zeker ook voor het hoger management. De resultaten van deze trainingen kunnen vervolgens steeds weer worden geëvalueerd om te bepalen of deze effectief zijn en daadwerkelijk een bijdrage leveren aan het kennisniveau en de handelingsbekwaamheid van de medewerkers. De security trainingen bevatten informatie over alle soorten dreigingen waar de organisatie aan kan worden blootgesteld, waarvan de meest bekende voorbeelden phishing en social engineering technieken zijn. Door na afloop van de training de opgedane kennis te toetsen door een quiz of een game, kan een spelelement worden toegevoegd.

Ook het ontwikkelen van phishing simulaties kan bijdragen aan de kennis van de medewerkers. De phishing simulaties helpen de medewerkers om in staat te zijn phishing e-mails te herkennen en voorbereid te zijn in het geval dat er een echte phishing e-mail binnenkomt. Daarnaast kunnen phishingsimulaties medewerkers meer vertrouwen geven om een melding te maken als zij onverhoopt op een phishing e-mail hebben geklikt. De beleidslijnen en procedures die een organisatie hanteert zijn van belang om de juiste gedragscodes en richtlijnen te laten naleven. Door duidelijk beleid en heldere procedures op te stellen rond het veilig omgaan met (vertrouwelijke) informatie en het melden van incidenten, bied je duidelijkheid en handelingsperspectief.

Maar het is ook belangrijk dat medewerkers voldoende tijd (kunnen) nemen voor het lezen van hun e-mail om te voorkomen dat een medewerker haastig op een phishing link klikt. Het kan medewerkers helpen om hen er bewust van te maken dat het in dit licht zinvol kan zijn om een vast tijdstip aan te houden voor het controleren van en reageren op e-mails. Daarnaast is het verstandig om de resultaten van een phishing simulatie met de desbetreffende medewerker te bespreken. Daarbij geef je reflectie, maar ook laat je zien dat de organisatie belang hecht aan hetgeen wordt aangeboden.

Veiligheid op de werkvloer

De ervaren veiligheid op de werkvloer is een bepalende factor voor het gedrag en de ontwikkeling van medewerkers. Naast het herkennen van (cyber)dreigingen, is het van belang dat medewerkers deze melden aan de verantwoordelijke(n) en hierover openlijk durven te praten, zonder angst om te worden afgerekend. Dit zorgt ervoor dat als een dreiging daadwerkelijk plaatsvindt, bijvoorbeeld in de vorm van een phishinglink die wordt geopend door een medewerker, de medewerker dit durft te melden.

Vaak durven medewerkers in een onveilig werkklimaat niet aan te geven dat ze op een phishing link geklikt hebben of ze weten niet bij wie ze terecht kunnen op het moment dat er sprake is van een beveiligingsincident. Het niet weten of durven vertellen van de gebeurtenis draagt bij aan de afbreuk van het zelfvertrouwen van de medewerker. Deze kan zich schamen en zich zorgen maken over de gevolgen die zijn actie heeft voor de organisatie. Om te kunnen anticiperen op dergelijke incidenten is het belangrijk om medewerkers regelmatig te informeren over de procedures die zij moeten volgen wanneer zij te maken krijgen met een beveiligingsincident. Daarnaast is het belangrijk om een cultuur te ontwikkelen waarin medewerkers zich voldoende vertrouwd voelen om ook minder positieve zaken te delen met de organisatie. Dus: ontwikkel een degelijk awareness-programma. Het vroegtijdig op de radar hebben van dreigingen voorkomt immers verdere schade! We willen u daarbij graag helpen en ondersteunen.

Annebeth Groen, Frederike Gieles & Anna Navasardyan