TESORION

Moderne fraudeurs doen hun werk **online**. Ze worden steeds slimmer en professioneler. Voor dit type **cybercrimineel** zijn jouw medewerkers de prooi.

Daarbij speelt hij in op hun onbewuste drijfveren. Nieuwsgierigheid, hebzucht en medeleven kunnen je dingen laten doen zonder dat je er goed bij nadenkt. Ook van angst en respect voor autoriteit maakt de crimineel graag misbruik.

Vooral phishing groeit razendsnel. Daarbij probeert de crimineel je te verleiden om te klikken op een link in een mail of een chatbericht. Je komt op een website waar je bijvoorbeeld kunt inloggen. Als je dat doet, heeft hij je gegevens. En daar gaat hij dan mee aan de slag.

Dit is maar één voorbeeld van internetfraude. Je medewerkers moeten dus weten hoe ze zulke aanvallen herkennen. En ze moeten ervan doordrongen zijn hoe ze moeten handelen als het gebeurt.

Je medewerker van de financiële afdeling zit thuis te werken. Het is altijd behoorlijk druk in deze tijd van de maand. Hé, een mail van de directeur: er moet kennelijk snel een factuur worden betaald. Je medewerker aarzelt een fractie van een seconde, toch is het duidelijk dat het dringend is. Kortom, meteen maar even doen ...

Maatwerk in trainingen

Op basis van onze expertise hebben we een scala van trainingen en assessments ontwikkeld. Die stemmen we af op de leerstijl en de beschikbare tijd van je medewerkers. Met serious gaming laten we ze bijvoorbeeld ervaren hoe een hacker denkt. Of hoe het voelt als je wordt gechanteerd met ransomware.

Trainen is het aanleren van nieuwe gewoontes; daarom zit er een ritme in onze trainingen. Voor een vast bedrag per medewerker maken we je mensen weerbaar.

Waakzaam blijven

Bewustzijn moet geregeld gevoed worden. Daarom helpen we je organisatie om de security awareness te bewaken.

Met assessments testen we of je mensen nog steeds alert zijn. En welke aanpak het beste werkt bij jouw medewerkers. Zo kunnen we samen de cybercrimineel buiten de deur houden.

Hoe maak je mensen weerbaar?

Cybersecurity is mensenwerk. Ook de beste technologie werkt pas als je medewerkers weten hoe ze hem moeten gebruiken. Maar steeds vaker zijn mensen zelf het doelwit van een cyberaanval. Zelfs als de beveiliging goed op orde is, kunnen criminelen toch binnenkomen door op menselijke zwaktes in te spelen.

Hoe voorkom je dat? Met het trainingen, testen en toetsen van je medewerkers. Om ze bewust te maken van de gevaren. En ze te leren wat ze moeten doen.

TESORION

Fokkerstraat 4
3833 LD Leusden

T: +31 33 456 3663
E: sales@tesorion.com

www.tesorion.com

Tesorion 7 checklist

De basis op orde. Waar begin je als jij je wilt wapenen tegen cybercriminelen?

1. Maak **medewerkers** weerbaar
We weten dat we niet op dat linkje moeten klikken. Ook weten we dat we niet zomaar geld moeten overmaken. Toch letten we niet altijd even goed op en trappen we er misschien allemaal wel eens in.

2. Splits je **netwerk** op in **compartimenten**
Segmenteer je netwerk. Zie het als brandwerende compartimenten. Wanneer er brand in een bepaald deel is kan je de branddeur sluiten en gaat niet het hele pand verloren.

3. Beveilig apparaten, e-mail en social media
We werken overal waar we willen. E-mail is in veel organisaties het belangrijkste communicatiemedium. Daarom wil je direct kunnen ingrijpen op apparaten die vreemd gedrag vertonen of zijn geïnfecteerd.

4. Versleutel belangrijke data
Data is het nieuwe goud, waarom beschermen we het dan niet net zo? Zorg dat je belangrijke data versleuteld bewaart, zodat wanneer data op straat komt te liggen deze niet toegankelijk is voor derden.

5. Maak betrouwbare **back-ups**
Het maken van back-ups lijkt een open deur. Back-ups zijn belangrijk, zo niet essentieel, om binnen afzienbare tijd (deels) verder te kunnen werken in geval van bijvoorbeeld ransomware.

6. Regel **toegang** tot bedrijfsmiddelen
Alle medewerkers hebben ongetwijfeld een eigen gebruikersnaam en wachtwoord. Waarschijnlijk heb je ook al sterke authenticatie ingeschakeld. Alleen een wachtwoord is niet veilig genoeg.

7. Houd je software en apparaten **up-to-date**
Overal zit tegenwoordig software in. Er zijn legio voorbeelden van software die kwetsbaarheden bevatten. Juist hierdoor kunnen cybercriminelen binnenkomen. Kortom: hoe ga jij om met deze updates?

24/7 actief
180+ experts
500+ klanten
1.000+ sensoren
4+ mln beschermde apparaten
100% Europees

ISO/IEC 27001 Information Security Management · NEN 7510 Information Security in Healthcare
EUROPOL The No More Ransom Project · EC3 European Cybercrime Centre