THE HACKER EXPERIENCE

NextLevelUP

CONNECT TO MAKE AN IMPACT!

business games

INTERACTIEF LEREN

Uit onderzoek blijkt dat experimenteel leren ervoor zorgt dat mensen informatie beter onthouden. De deelnemers ervaren een onvergetelijke training en nemen spelenderwijs alle belangrijke leerdoelen in zich op.

BANDEN VERSTERKEN

Tijdens de game komen mensen met verschillende achtergronden en ervaringen op informele wijze in contact. Door samen te werken worden banden versterkt. Ze halen het beste in zichzelf én elkaar naar boven.

VAARDIGHEDEN EN KENNIS ONTWIKKELEN

Het trainen van soft-skills en het overdragen van kennis is verweven in al onze game modellen. Wij gebruiken bewezen technieken die mensen motiveren, enthousiasmeren en doen stilstaan bij verbeteringen in hun gedrag.

SUCCESVERHALEN

Businessgames en NextLevelUP hebben in co-creatie dit programma opgesteld. Businessgames is de autoriteit in het maken van serious games, NextLevelUP (met docenten van Avans, University of Applied Science) in de laatste wetenschappelijke inzichten ten aanzien van blijvende gedragsverandering op basis van gamification.

THE HACKER EXPERIENCE

In het bedrijfsleven krijg je te maken met allerlei gevaren. Een van de grootste, waar mensen het minst alert op zijn, is cybercriminaliteit. Met deze training belichten we de gevaren vanuit het perspectief van de hacker,

Stel je voor: je bent de leider van een groep hackers en je hebt maar één doel voor ogen: het meeste geld verdienen. Jij en je team aan hackers gaan aan de slag en maken gebruik van verschillende hackvormen om verschillende bedrijven te hacken.

Weet jij wat de meest voorkomende hackvormen zijn en welke effectief zijn? Maak jij keuzes op basis van eigen belang, of streef je juist naar een hoger belang? Welk bedrijf hack je als eerst en waar weet je het meeste geld vandaan te halen?

Dit is precies waar de 'Hacker Experience' business game om draait: een spannende game waarin hackers de strijd met elkaar aangaan om het meest succesvol te zijn. Een uitdaging waarin veiligheid, samenwerking en oplettendheid centraal staan. En waar bewustwording en gedragsverandering de uitkomst bieden.

BELANG VAN DE GAME

Vijf redenen met cijfers waarom cybersecurity van belang is voor een bedrijf:

1. Financiële schade: In 2020 was de gemiddelde kostenpost van een datalek wereldwijd maar liefst 3.86 miljoen dollar, volgens het "Cost of a Data Breach Report" van IBM Security.

2. Reputatieschade: Volgens een onderzoek van SecurityScorecard in 2020 verloor 43% van de bedrijven hun klanten door een datalek, en 52% van de bedrijven verloor de vertrouwde relaties met hun partners.

3. Aanvallen op bedrijven groeien: Volgens de "SonicWall 2021 Threat Report" groeide het aantal cyberaanvallen op bedrijven in 2020 met 62%, en de kosten van ransomware-aanvallen stegen met 171% tot 312.493 dollar per aanval.

4. Compliance vereisten: In 2020 werd de AVG meer dan 160.000 keer overtreden in Europa, met boetes die opliepen tot 50 miljoen euro of 4% van de jaaromzet van een bedrijf, volgens het "GDPR Enforcement Tracker Report" van DLA Piper.

5. Toekomstige kosten: Uit een onderzoek van het Ponemon Institute uit 2021 bleek dat het gemiddelde bedrijf dat een datalek heeft meegemaakt, de komende twee jaar een additionele kost van 3,3 miljoen dollar kan verwachten als gevolg van verminderde vertrouwenswaardigheid, reputatieschade en lagere omzet.

VOORBEELD OPZET GAME

Uitleg game

Ronde 1 - De teams gaan kennis opdoen aan de hand van de beschikbare informatie. Met deze informatie gaan ze een strategie bepalen. Welk bedrijf hacken ze als eerst en welke hackvorm is hiervoor geschikt? Is alle informatie beschikbaar, of moet deze worden ingekocht? Maken zij de juiste afwegingen en bereiden ze zich goed voor op de eerste hackaanval?

Ronde 2 – Het is tijd om de strategie waar te maken. De hackers beginnen met hun eerste aanval. Hebben zij de juiste inschattingen gemaakt en is de aanval succesvol? Lukt het de teams om een geslaagde hackaanval te plegen, dan kunnen ze hun team naar een hoger niveau tillen. Hierdoor worden meer hackvomen beschikbaar waardoor er nog meer geld kan worden binnengehaald.

Tussentijdse evaluatie – In deze evaluatie krijgen de teams feedback op hun acties. Daarnaast is dit een moment voor de deelnemers om snel samen te komen en eventueel hun strategie aan te passen.

Ronde 3 & 4 – In deze versnelde rondes krijgen de deelnemers te maken met meer tijdsdruk. Hoe beïnvloedt deze tijdsdruk hun besluitvorming? Uiteindelijk zal er één hackerteam winnen

Evaluatie & Prijsuitreiking – De game facilitators zorgen voor een uitgebreide evaluatie waarin de link met de dagelijkse praktijk wordt gelegd. In deze interactieve evaluatie laten wij de teams ook aan het woord en zal het duidelijk zijn waar zij gezamenlijk alert voor dienen te zijn.

METAFOOR

De link naar uw organisatie in combinatie met cyber criminaliteit is doorgaans snel gelegd. Door de game in een metafoor te spelen, trekken wij de deelnemers uit de dagelijkse praktijk. De business game legt de focus op het perspectief van de hacker. Snappen de deelnemers wat een hacker kan, kunnen deelnemers het belang van cyber security beter begrijpen.

TRAINING DETAILS

- Live en interactief
- In teamverband
- Maatwerk concept
- Verspreiding over meerdere dagdelen is mogelijk

NIEUWSGIERIG?

Neem vrijblijvend contact met ons op voor vragen. Wij informeren u graag over de mogelijkheden!