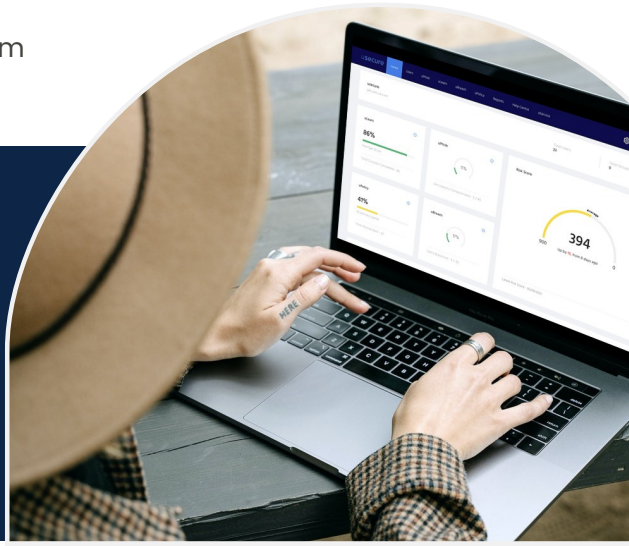
LOGO

www.eengoedewebsite.com

HUMAN RISK MANAGEMENT (HRM) CASE STUDY

Een kijk op hoe HRM het veiligheidsgedrag van werknemers in dit bedrijf heeft veranderd.



DOELSTELLINGEN VAN DE KLANT

- Bepaal welke werknemers een groot risico lopen om slachtoffer te worden van een phishing aanval
- Een continu overzicht hebben van welke werknemers kwetsbaar zijn voor phishing aanvallen
- Regelmatige trainingen over beveiligingsbewustzijn om gebruikers weerbaarder te maken tegen phishing aanvallen en om het algemene beveiligingsgedrag te verbeteren
- Aantonen dat de ISO 27001-clausule 7.2.2 wordt nageleefd

AANPAK

Training in Beveiligingsbewustzijn

- Analyseer de huidige sterke en zwakke punten van de beveiliging van elke gebruiker met behulp van een Gap Analysis Quiz.
- Aan de hand van de resultaten van de quiz krijgt iedere werknemer om de vier weken een nieuwe cursus over veiligheidsbewustzijn, het bepalen van de eerste cursussen is afhankelijk van de zwakste resultaten.
- Op regelmatige tijdstippen zullen er ook aangepaste nalevingscursussen worden gegeven.

Gesimuleerde Phishing Oefeningen

- Er zal minstens iedere zes weken een phishing simulatie worden uitgevoerd om het effect van de training te testen en eventuele gebruikers met een hoog risico op te sporen.
- Er wordt een directe vervolgtraining gegeven aan alle medewerkers die tijdens een phishing simulatie hun inloggegevens hebben prijsgegeven, om het risico zo snel mogelijk te verminderen.

Toezicht op het Dark Web

- Het dark web zal voortdurend worden bewaakt om aanvallen, waarbij er gebruik wordt gemaakt van gestolen werknemersgegevens zoals gekraakte gebruikersnamen en wachtwoorden, in een vroeg stadium op te sporen en te voorkomen

KLANTENPROFIEL

Sector

- Bouw

Aantal Gebruikers

- 250 Werknemers

Gebruik van de Dienst Sinds

- Augustus 2020

UITDAGINGEN/ DRIJFVEREN

- Een personeelslid werd slachtoffer van een phishing aanval door middel van een 'Cadeaubon'
- Het huidige opleidingsmateriaal voor beveiligingsbewustzijn is niet boeiend en ondoeltreffend
- De huidige aanpak van traning voor beveiligingsbewustzijn is te tijdrovend

DE IMPACT - RISICOSCORE

Om de impact van het Human Risk Management programma van de klant te meten, werden zowel bij de start van het programma als na zeven maanden van training de belangrijkste risicometingen uitgevoerd.

Hieronder ziet u de risicoscore voor het bedrijf (alle risicomaatstaven zijn samengevoegd), een risicoscore voor opleidingen (een combinatie van cijfers voor cursussen en percentages van voltooide cursussen), een risicoscore voor phishing (de cijfers van geopende, aangeklikte en beschadigde bestanden tijdens phishing simulaties) en een risicoscore voor het dark web (gebaseerd op de mate waarin gevoelige gegevens van uw bedrijf op het dark web zijn blootgesteld).

RISICOSCORE

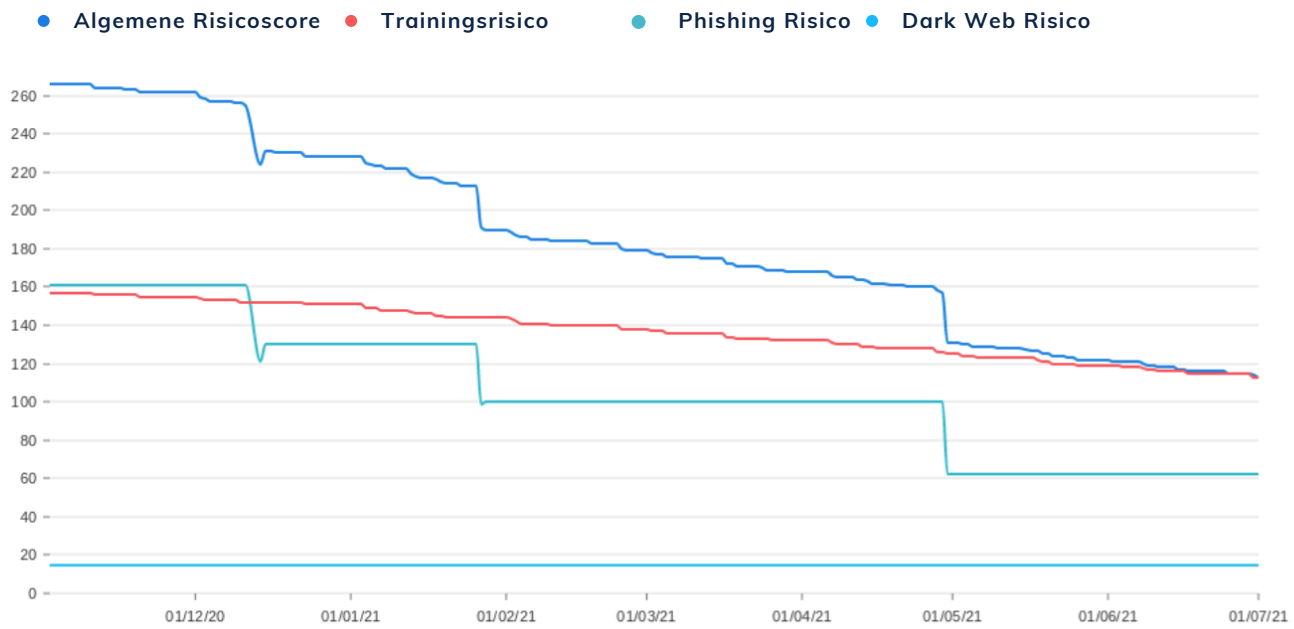
Na zeven maanden van training in beveiligingsbewustzijn, periodieke gesimuleerde phishing oefeningen en het scannen van inbreuken op het dark web, werd de totale menselijke risicoscore van de klant met 152 punten verlaagd - waardoor het risico veranderde van 'gemiddeld' naar 'laag'.

Het phishing risico binnen het bedrijf daalde aanzienlijk met 100 punten, wat betekent dat de werknemers beduidend beter waren in het herkennen, vermijden en melden van verdachte aanvallen.

EERSTE RISICOSCORE		RISICOSCORE NA 7 MAANDEN
270/900	»	**118**/900
Gemiddeld		Laag

BELANGRIJKSTE GEGEVENS

- BEDRIJFSRISICO | -152
- TRAININGSRISICO | -40
- PHISHING RISICO | -100
- DARK WEB RISICO | GEEN VERANDERING



DE IMPACT - TRAINING & PHISHING RESULTATEN

Om het menselijke cyberrisico te verminderen, was het belangrijk om ervoor te zorgen dat de werknemers hun cursussen beveiligingsbewustzijn zo snel mogelijk voltooiden en de minimumscore van 80% haalden in hun follow-up vragenlijsten.

Om ervoor te zorgen dat dit ook gebeurde, werden het aantal werknemers die de cursus hadden voltooid en de cursuscijfers bijgehouden. Er werder ook automatische herinneringsmails verstuurd naar alle werknemers die hun cursus niet binnen een paar werkdagen hadden afgerond.

De resultaten van de continue phishing simulaties werden ook opgevolgd om er zeker van te zijn dat de training voor beveiligingsbewustzijn het gewenste effect bereikte.

TOEPASSING VAN DE TRAINING

Gem. tijd om een cursus af te ronden na inschrijving	Cursus Gestart	Cursus Voltooid	Gemiddeld Cijfer
3 Dagen	97%	97%	92%

PHISHING SIMULATIE PRESTATIES

	Verstuurd	Geopend	Bezocht	Besmet
1st Simulatie	146	74	40	9
2de Simulatie	172	34 -74%	4 -163%	2 -127%

Van de 250 personeelsleden begon 97% aan hun cursus en zij voltooide deze ook. Na hun inschrijving hadden zij gemiddeld slechts drie dagen nodig om hun cursus af te ronden, terwijl zij gemiddeld 92% scoorden.

Zoals u kunt zien in de tabel van de Phishing Simulatie Prestaties, waren werknemers veel minder geneigd om een phishing simulatie te openen, erop te klikken of erdoor besmet te raken.