City Deal
Lokale Weerbaarheid Cybercrime

POWERED BY CCV centrum voor criminaliteitspreventie en veiligheid

Evidence based cybersecurity gedragsinterventie

gericht op drie basisprincipes van veilig ondernemen

In dit project ontwikkelt de Haagse Hogeschool een interventie die gericht is op 3 basisprincipes van veilig digitaal ondernemen: inventariseer kwetsbaarheden, voer updates uit en voorkom malware. Onderdeel van de interventie is het aanbieden van een handelingsperspectief voor deze 3 maatregelen. Deze maatregelen zijn gemeten met een geautomatiseerde kwetsbaarhedenscan. Dankzij een voor- en nameting kan de effectiviteit van de interventie getoetst worden. De Haagse Hogeschool werkt in dit project samen met Threadstone (ontwikkelaar van de scan) en PVO Den Haag.

Probleem

Eén op de vijf ondernemers in Nederland heeft in het verleden te maken gehad met enige vorm van slachtofferschap van cybercrime. Ondernemers die de cyberweerbaarheid van hun onderneming willen verhogen, kunnen online kiezen uit een groot aantal cyberscans die door diverse organisaties worden aangeboden. Tot op heden is er weinig inzicht in de effectiviteit van deze cyberscans en of de cyberscans in combinatie met op maat gemaakt adviesrapporten ervoor zorgen dat ondernemers stappen nemen om hun cyberweerbaarheid te verhogen.

Aanpak

Het project ‘Evidence based cybersecurity gedragsinterventie gericht op drie basisprincipes van veilig ondernemen’ probeert een evidence based aanpak te creëren waarmee ondernemers in het mkb hun cyberweerbaarheid kunnen verhogen. Het doel van dit project is dan ook het ontwikkelen en meten van een cybersecurity gedragsinterventie die ondernemers aan moet sporen om het niveau van hun cyberweerbaarheid te verhogen. Het project wordt uitgevoerd in vier geografische gebieden in regio Den Haag en Utrecht.

Voorafgaand aan de interventie is een juridische risico-beoordeling uitgevoerd om te kunnen beoordelen of de interventie binnen de wettelijke kaders wordt uitgevoerd. De conclusie van deze beoordeling is dat er geen juridische bezwaren zijn gevonden van het uitvoeren van de cyberscan. Ook zijn er enkele interviews bij stakeholder afgenomen om de verwachtingen en inzichten van externe partijen in kaart te brengen.

De interventie bestaat uit drie stappen:

1. Eerst wordt er via de domeinnaam van de onderneming een geautomatiseerde kwetsbaarhedenscan uitgevoerd op de openbaar bereikbare digitale infrastructuur van ondernemers. Ondernemers hoeven zich hiervoor niet aan te melden. Hiermee wordt op een laagdrempelige manier een klein deel van de cybersecurity van deze ondernemers in kaart gebracht.
2. Hierna ontvangt de ondernemer een op maat gemaakte adviesrapportage waarin de eventueel gevonden kwetsbaarheden staan toegelicht, één van de drie varianten van de risicocommunicatie en een handelingsperspectief. Dit handelingsperspectief is bedoeld om de ondernemer aan te sporen met hun ICT- of cybersecurity leverancier in gesprek te gaan om de gevonden kwetsbaarheden te verhelpen, of om een ICT- of cybersecurity leverancier in de hand te nemen.
3. Er wordt een nameting gedaan om de effectiviteit van de interventie te kunnen meten. Dezelfde domeinnamen zullen hiervoor opnieuw worden gescand. Hiermee wordt geprobeerd vast te stellen of de ondernemers veranderingen hebben aangebracht aan hun cyberweerbaarheid.

Resultaten

Tijdens de eerste meting zijn 1.975 geautomatiseerde kwetsbaarhedenscans uitgevoerd. Vervolgens zijn naar 1.399 van deze ondernemingen op maat gemaakte adviesrapporten verstuurd, waarbij gevarieerd werd tussen drie vormen van risicocommunicatie (sociale norm, geanticipeerde spijt en geen risicocommunicatie). 576 gescande bedrijven fungeerden als controlegroep; deze bedrijven hebben geen adviesrapporten ontvangen. Zes weken later heeft een nameting plaatsgevonden bij alle 1.975 ondernemingen om de effectiviteit van de verschillende vormen van communicatie te kunnen testen. De dataverzameling is momenteel nog bezig, er kunnen om deze reden nog geen uitspraken worden gedaan over de effectiviteit van de interventie.

Vervolg

Indien uit dit onderzoek blijkt dat we kunnen spreken van een evidence based effectieve interventie voor het verhogen van de cyberweerbaarheid van de ondernemers, wordt beoogd om de interventie landelijk beschikbaar te stellen. Doordat de resultaten nog niet bekend zijn is het op dit moment niet mogelijk om concrete aanbevelingen voor de toekomst te doen.

Meer informatie

Meer weten over dit project? Neem contact op met:

- Dr. Susanne van 't Hoff-de Goede, M.S.vantHoff-deGoede@hhs.nl
- Maaike van der Wal, MSc M.L.vanderWal@hhs.nl

Het secretariaat van de City Deal Lokale Weerbaarheid Cybercrime wordt gevoerd door het Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Bekijk de CCV-database voor nog meer interessante cyberprojecten.

PVO ThreadStone CYBER SECURITY DE HAAGSE HOGESCHOOL