LESNOTA | TEACHING NOTES

CASE | Cyber security check MKB

Bedrijven (zouden moeten) weten dat cybersecurity heel belangrijk is. Alleen al in 2022 kreeg 56% van de Nederlandse mkb te maken met een aanval op hun digitale systemen. En dat is het percentage van wie we het weten. Bedrijven die getroffen zijn bekennen vaak achteraf dat de digitale veiligheid van hun organisatie minder goed georganiseerd was dan ze dachten. Het blijkt geen onderdeel van de veiligheidsroutine. Vaak zijn er plannen en heel veel aannames. De eerste stap naar een steeds veiliger bedrijf is te weten wie waarvoor verantwoordelijk is als het gaat om de cyberveiligheid van de organisatie.

Saxion heeft, in samenwerking met een aantal partners, een risicoscan ontwikkeld. Deze risicoscan kan de digitale veiligheid en weerbaarheid van bedrijven in kaart brengen, waaruit opvolgend een adviesrapport meegegeven wordt om de veiligheid en weerbaarheid te verhogen.

In samenwerking met het Centrum voor Veiligheid en Digitalisering, waar het Saxion Centrum voor Ondernemerschap als partner onderdeel van uitmaakt, worden ondernemende studenten opgeleid, met behulp van deze instructievideo's, om deze scans uit te voeren bij MKB-bedrijven in de regio. Eerst onder begeleiding vanuit Saxion, later als zelfstandig ondernemer.

DOELGROEP

De doelgroep is tweeledig: zowel studenten als regionale MKB bedrijven profiteren van deze ontwikkeling.

MKB Bedrijven

Het mkb in Oost-Nederland met 5 – 100 medewerkers. Er ligt focus op accountantskantoren, ICT-dienstverleners, advocatenkantoren, retail, installatiebedrijven en organisaties in de zorg.

Studenten

In eerste instantie wordt deze scan uitgevoerd door studenten van de opleidingen Integrale Veiligheid en Security Management en van de minor Digitale Revolutie. Daarnaast zijn er studenten van de Digitale Werkplaats die hier ook mee aan de slag gaan. Deze casus biedt studenten een eerste 'veilige' kennismaking met zelfstandig ondernemen, onder begeleiding vanuit Saxion.

In 2024 is er plek voor de check in de module Information at Risk van de opleiding Security Management.

LEERDOELEN EN KERNPUNTEN

De beoogde leerervaring is dat studenten kennis maken met de praktijk. Ze leren om te gaan met informatie die gevoelig zou kunnen zijn voor een bedrijf en op welke manier zij op een professionele wijze een interview met een verantwoordelijke binnen een bedrijf afnemen. Hiervoor worden de studenten begeleid bij het uitvoeren van de eerste scans. De studenten kunnen opgedane theoretische kennis toepassen en vragen beantwoorden, evenals een initieel advies uitbrengen richting de klant (bijv. ga in gesprek met je IT leverancier n.a.v. dit rapport).

LESSTRATEGIE

De lesstrategie voor deze casus is als volgt:

Na begeleiding van studenten, waarbij gebruik wordt gemaakt van de instructievideo's, gaan één of meerdere studenten langs bij een mkb'er voor een interview van ongeveer een uur. Het interview bestaat uit 36 vragen over hoe de digitale weerbaarheid van de organisatie is geregeld. Na het interview krijgt de organisatie een rapport waarin duidelijk staat wie binnen of buiten de organisatie verantwoordelijk is voor de belangrijkste maatregelen die genomen moeten worden voor de vergroting van de cybersecurity van het bedrijf. Daarin worden de volgende onderwerpen aangehaald:

1. Inventarisatie van kwetsbaarheden
2. Veilige instellingen
3. Updates
4. Toegangsbeperking
5. Beveiliging tegen virussen en andere malware

Nadat bedrijven het rapport met verbetermogelijkheden hebben ontvangen, wordt ze aangeraden in gesprek te gaan met hun IT-leverancier om de zwakheden binnen de organisatie verder te bespreken en tot oplossingen te komen.

DISCUSSIEVRAGEN

Voor de beeldvorming onderstaand enkele voorbeelden van vragen die tijdens het interview worden gesteld. Deze zullen in de lessen voorbereid worden.

- Wie is binnen de organisatie verantwoordelijk voor het maken van een inventarisatie van onderdelen en informatie die bedrijfskritisch en gevoelig zijn?
- Wie is binnen de organisatie verantwoordelijk voor het testen van het terugzetten van back-ups?
- Wie is binnen de organisatie aangewezen als contactpersoon voor het melden van verdachte situaties?
- Wie draagt zorg voor het gebruik van veilige, sterke en verschillende wachtwoorden?
- Wie stelt per medewerker vast tot welke systemen en data zij toegang zouden moeten hebben om hun werk te kunnen doen?