

Mkb ondernemingen gezocht die hun cyberweerbaarheid willen vergroten

Het mkb is in toenemende mate slachtoffer van cyberaanvallen en datalekken (CBS, 2022; SIDN, 2020). Door de relatief beperkte middelen en expertise is het voor het mkb doorgaans lastiger om een goede combinatie te maken tussen maatregelen op het gebied van techniek, organisatie en gedrag. Hogeschool Utrecht, Hogeschool Saxion en consortiumpartners starten daarom een onderzoek om mkb bedrijven in Nederland weerbaarder te maken tegen cyberdreigingen. Hierbij gaat het zowel om het voorkomen als het kunnen omgaan met incidenten. In ons onderzoek richten we ons specifiek op het vergroten van cyberweerbaar gedrag.

Waar zijn wij naar op zoek?

Wij zijn hiervoor op zoek naar 24 mkb bedrijven met 5-49 medewerkers die willen participeren in dit onderzoek. Het uiteindelijke doel van dit onderzoek is om de deelnemende mkb bedrijven weerbaarder te maken op het gebied van cybersecurity. Wij zullen dit doen in een aantal stappen:

- Een intakegesprek
- Risico-inventarisatie op het gebied cyberveiligheid (nulmeting)
- Voor iedere deelnemende mkb onderneming een eigen routekaart naar verbetering.
- Een simulatie van cyberdreigingen in de vorm van goedaardige phishing mails en goedaardige hacks
- Workshops om digitaal weerbaar gedrag te stimuleren
- Risico-inventarisatie op het gebied cyberveiligheid (eindmeting)

Voor onderzoeksdoeleinden worden de deelnemende mkb ondernemingen onderverdeeld in twee groepen. Deze twee groepen doorlopen in essentie hetzelfde traject. Alleen de timing van de workshop(s) is anders. Dit wordt gedaan om het effect van de workshop(s) zuiver te kunnen meten.

Wat levert het u op?

Door deel te nemen aan dit onderzoek krijgen u en uw medewerkers een beter inzicht in de cyberrisico's die uw onderneming loopt. Daarnaast bieden wij u, in de vorm van een praktische routekaart naar verbetering, heldere handvatten om uw onderneming weerbaarder te maken. Tot slot helpen wij u en uw medewerkers aan de hand van één of meer workshops gedragsaanpassingen te maken die u in staat stellen effectiever om te gaan met cyberdreigingen.

Wat vragen we van u?

Het onderzoek neemt ongeveer 14 maanden in beslag. Voor het welslagen van het onderzoek is het van belang dat u en een aantal medewerkers gedurende deze periode ongeveer 6 middagen beschikbaar zijn. In deze periode voeren wij onder leiding van een IT-auditor twee cyberrisico-inventarisaties bij uw onderneming uit. Om deze risico-inventarisaties adequaat uit te voeren hebben wij toegang tot uw onderneming nodig en is het belangrijk om u en een aantal medewerkers een aantal vragen op dit gebied te stellen. Daarnaast vragen wij uw toestemming om een aantal goedaardige phishing mails en een tweetal goedaardige hacks uit te voeren. Tot slot vragen wij u en een aantal medewerkers deel te nemen aan een drietal workshop gericht op cyberweerbaar gedrag. Vanzelfsprekend worden tijdens het gehele onderzoek alle bedrijfs- en persoonsgegevens geanonimiseerd en zijn daardoor niet te herleiden naar specifieke bedrijven of personen.

Aanmelden?

Wij hopen van harte dat u wil deelnemen aan dit onderzoek. U kunt zich aanmelden door een mail te sturen naar Myrna Jacobs (myrna.jacobs@hu.nl). Mocht u nog aanvullende vragen hebben dan kunt u deze naar hetzelfde adres sturen.

Met vriendelijke groet,

Ralph van Mechelen

Projectleider “Digitale weerbaarheid mkb”

Consortiumpartners:



Koninklijke Nederlandse
Beroepsorganisatie
van Accountants

