Productblad

Veilig Zakelijk Internetten II

MKB-Nederland en VNO-NCW organiseren met steun van het ministerie van Veiligheid en Justitie en het ministerie van Economische Zaken een vervolg op het project Veilig Zakelijk Internetten uit 2015.
Veilig Zakelijk Internetten II (VZI II) levert een bijdrage aan het vergroten van het bewustzijn van het midden- en kleinbedrijf (mkb) over de impact van cybercrime op hun onderneming en hoe zij zich daartegen kunnen weren. Tot slot moet het programma ondernemers ook daadwerkelijk tot actie aanzetten.

Achtergrond

Cybercrime is een containerbegrip met veel tentakels; het is razendsnel van kwajongenswerk uitgegroeid naar internationaal opererende netwerken die de hele digitale wereld gebruiken voor het stelen van geld, goederen, informatie, identiteiten en voor chantage, afpersing en fraude. De financiële schade, imagoschade, verlies van banen, en faillissementen in Nederland als gevolg van cybercrime worden niet systematisch onderzocht of bijgehouden. Wel blijkt uit een in april 2016 uitgevoerde analyse van adviesbureau Deloitte dat cybercriminaliteit Nederlandse bedrijven en de overheid jaarlijks ongeveer 10 miljard euro kost.

Het midden- en kleinbedrijf bestaat uit ondernemingen met maximaal 250 werknemers. Van alle 1,3 miljoen in Nederland gevestigde bedrijven, behoort 99 procent tot deze categorie. Samen zijn zij verantwoordelijk voor 58 procent van de omzet in ons land en bieden zij werkgelegenheid aan 60 procent van alle werknemers. Het overgrote deel van de mkb-ondernemers behoort tot de categorie met 1 tot 10 personeelsleden. In deze bedrijven is veelal weinig capaciteit voor het inrichten van de randvoorwaarden voor veilig ondernemen. In tegenstelling tot het grootbedrijf kent het mkb geen grote stafafdelingen met de nodige specialismen. Mkb-ondernemers ‘leunen’ sterk op de kennis en kunde van hun IT-leverancier en maken ook dankbaar gebruik van het informatieaanbod van organisaties als MKB-Nederland en VNO-NCW.

Uitgangspunten van het project

www.veiliginternetten.nl is de basis van het project. Deze website bundelt het op internet vaak al beschikbare maar zeer verspreide aanbod van informatie en tools. Hiermee krijgt de ondernemer overzichtelijkheid en duidelijkheid, en wordt verwarring voorkomen.

Het project zet in op een groot bereik van ondernemers met inzet van alle communicatiemiddelen van de betrokken stakeholders. Veilig Internetten zet de lijn van bundeling van alle informatie en tools op het gebied van cybersecurity voor mkb-ondernemers door richting ondernemers met behulp van een breed gedragen communicatiestrategie, met inzet van alle communicatiemiddelen van de betrokken stakeholders. Al deze communicatiemiddelen dragen dezelfde boodschappen over cybersecurity en verwijzen naar het integrale aanbod van informatie en tools, direct te bereiken via www.veiligInternetten.nl/academy.

Gericht aanspreken van ondernemers

Cybersecurity staat in de beleving van de gemiddelde ondernemer nog steeds ver van zijn of haar bed. De onderneming wordt meestal niet als een relevant doelwit van cybercrime beschouwd. Cybercrime is iets wat grote ondernemingen raakt en zich vaak op internationaal niveau beweegt, zo is de algemene gedachte. Met het toenemen van online zaken doen zijn echter veel meer ondernemers kwetsbaar voor cybercrime dan het aantal ondernemers dat zich dat terdege realiseert.

Voor het onderwerp veilig ondernemen, waaronder cybersecurity, geldt dat dit een ondernemer dit vaak pas als urgent ervaart als er sprake is van een inbreuk op de veiligheid van het bedrijf. Het is dus zaak ondernemers hierin te bereiken voordat van een dergelijke inbreuk sprake is.

MKB-Nederland en VNO-NCW zetten met Veilig Zakelijk Internetten II in op twee benaderingen:

1. Een branchespecifieke benadering, op basis van inzichten vanuit onderzoek door de Haagse Hogeschool;
2. Een generieke benadering van alle ondernemers op een zo gericht mogelijke manier, met inzet van kennis van TNO over de drijfveren en barrières van verschillende mkb-segmenten Inzicht hierin is nodig om ondernemers aan te spreken op wat zijzelf belangrijk vinden en hen daarmee aan te zetten tot het gewenste gedrag.

Ad 1 Branchespecifieke benadering

Veilig Zakelijk Internetten II maakt met informatie uit onderzoek door de Haagse Hogeschool inzichtelijk wat er op het gebied van cybercrime kenmerkend is voor vijf afzonderlijke branches. Er worden vragen en antwoorden ontwikkeld en voorbeelden van specifieke branche-impact gegeven. Bestaande tools worden op een voor de branche in kwestie herkenbare manier verpakt en ontwikkeld. Hiermee vergroot het project de kans op bewustwording en daadwerkelijke actie van ondernemers.

Invulling branchepakket:

- onderzoek binnen de branche voor het creëren van bewustwording en het verzamelen van relevante gegevens en uitdagingen op het gebied van cybercrime. Dit is nodig voor het schokeffect en het creëren van verandermanagers binnen branches
- op basis van onderzoek een branchespecifieke toolkit realiseren, gebaseerd op:
  - de uit het onderzoek volgende branchespecifieke kenmerken en aanbevelingen voor de branche
  - een scan met een persoonlijke branchespecifieke impactanalyse
  - aanpassing van beleid en procedures rond cybercrime
  - vertaling van technische risico's naar branchespecifieke communicatie
  - verandering van gedrag bij mensen binnen de branche.
  - de toolkit krijgt de vorm van een multimediaal online magazine. Hiermee kan op interactieve en aantrekkelijke wijze de achterban worden geïnformeerd.
- infographics per branche op basis van de scanresultaten.

In ruil voor facilitering en ondersteuning met informatie en tools vragen MKB-Nederland en VNO-NCW per branche commitment met concrete afspraken over contactpersoon, inzet en coördinatie. In annex I staat een uitgebreider overzicht van de mogelijkheden.

Overige branches worden zowel tijdens als na de campagne gefaciliteerd. Hiertoe wordt een toolkit ontwikkeld met daarin:

- introductie van de campagne
- beschrijving van de onderdelen
- verwijzing naar de diverse onderdelen
- een technische beschrijving voor het embedden in de eigen communicatiemiddelen.

Ad 2 Generieke benadering

In de generieke benadering spreken we ondernemers zo gericht mogelijk aan op basis van segmentatie qua:

- type ondernemer
- type organisatie en daaraan gekoppelde risico's (bijvoorbeeld branche)
- grootte van de organisatie
- gebruik van digitale mogelijkheden (contentmix)
- psychosociale kenmerken zoals heersende normen of percepties omtrent veiligheid in de onderneming, mate van kennis van het onderwerp en locus of control (wie wordt gezien als verantwoordelijk).

Het aanbod aan ondernemers: 2500 scans en een 'Academy' van tools

Alle ondernemers die vanuit de breed gedragen communicatiestrategie tot bezoek aan de website Veilig Zakelijk Internetten worden verleid, krijgen de volgende zaken aangeboden:

- een zorgvuldig samengestelde vragenset die de ondernemer bevraagt over specifieke kenmerken van de onderneming
- een scan om het cybersecuritylevel van de onderneming inzichtelijk te maken. De scan controleert op meer dan 70.000 bekende kwetsbaarheden. Door een heldere terugkoppeling zetten deze scans met de rapportages aan tot concrete actie
- score t.o.v. branche of soortgelijke bedrijven (benchmark)
- een 'Academy' waarin de ondernemer wegwijs wordt gemaakt op basis van branche, menselijke factoren en niveau. Denk hierbij aan contentvormen als E-books, whitepapers en video. De Academy brengt het aanbod van cybercrimetools voor ondernemers bij elkaar, zoals eerder door ECP is geïnventariseerd
- een persoonlijk dashboard via een integrale, beveiligde 'Mijn'-omgeving op Veilig Zakelijk Internetten, De Zaak, MKB Servicedesk en ZZP Servicedesk.

Duur van het project

Het project start op 11 oktober 2016, in de Week van de Veiligheid en eindigt op 30 september 2017.

Uitvoering van het project

MKB-Nederland/ VNO-NCW – projectmanagement

- Dutch Network Groep – platform voor mkb ondernemers/ content ontwikkeling
- Threadstone – cybersecurity
- TNO – onderzoek en advies
- Haagse Hogeschool – brancheonderzoek
- ECP – website veiliginternetten.nl

Meer informatie

Coen van den Berg, MSc.
Projectmanager
T. 070 – 3490 401 / 06 - 1135 1758
E. Berg@vnoncw-mkb.nl

Januari 2016

Annex I: ondersteuning VZI partners

Ook steunen?

Met deelname aan het project VZI II kunnen brancheverenigingen hun achterban informeren over de risico's van cybercrime en over oplossingen om dit te beperken. Het project biedt twee pakketten:

- Pakket A: communicatie + scan (kosteloos)
- Pakket B: pakket A + maatwerkpakket (niet kosteloos)

	Pakket A	**Pakket B**
Toegang tot VZI Academy		
Toegang tot technische scan digitale omgeving (max. 2.500 – op=op) inclusief rapport met mogelijke oplossingen		
Maandelijkse communicatie toolkit (kant-en-klare content voor website, nieuwsbrief en social media)		
Spreker/ presentatie/ workshop cybersecurity door TNO/ ThreadStone (min. 25 pers.)		
Logovermelding veiligzakelijkinternetten.nl		
Branche-informatie in rapportages		
Opname branche-informatie in rapportages		
Branche specifieke online multimediale brochure		
Branche specifieke business impact op meest voorkomende kwetsbaarheden in technische scan[1]		
1x per jaar managementrapport voor branche organisatie		
Brancheonderzoek door de Haagse Hogeschool	optioneel	optioneel
Kosten	**wel Kosteloos**	**Niet kosteloos**

Wat verwachten we van een steunende organisatie?

- Commitment en actieve houding om campagne tot succes te maken
- Communicatieplan met tenminste 6 uitingen

[1] Alleen mogelijk nadat het onderzoek door de Haagse Hogeschool is uitgevoerd.