GEDRAG

Digitale weerbaarheid in het mkb: een serieus probleem?

Onlangs is het lectoraat 'Cybersecurity in het mkb' gestart aan de Haagse Hogeschool. De focus van het lectoraat ligt op de human factor in cybersecurity. Het doel van dit lectoraat is om de kennispositie van het mkb op het gebied van cybercrime en cybersecurity te vergoten om zo het slachtofferschap en de impact van cyberaanvallen onder mkb'ers te verlagen. Het lectoraat kent vier onderzoekslijnen, waarbinnen steeds het mkb centraal staat. Een belangrijke onderzoekslijn is het vergroten van de digitale weerbaarheid van het mkb.[1] Maar waar gaat het over als we het hebben over digitale weerbaarheid? Wat is een 'goed niveau'? Wordt dit niveau daadwerkelijk bereikt met de huidige voorzieningen? En hoe vergroot je de digitale weerbaarheid in het mkb?

Digitale weerbaarheid: een serieus probleem?

De digitale weerbaarheid in Nederland blijft achter bij de groei van dreigingen. Dat concludeert de Nationaal Coördinator Terrorismebestrijding en Veiligheid in het Cybersecuritybeeld Nederland 2017. Dat de digitale weerbaarheid moet worden vergroot blijkt ook uit het voorstel voor de Cybersecuritywet (Csw) van minister Grapperhaus (Justitie en Veiligheid), dat op 15 februari 2018 bij de Tweede Kamer is ingediend. Het doel van dit voorstel is om Nederland digitaal veiliger te maken. De Csw volgt uit de Netwerk- en Informatiebeveiligingsrichtlijn (NIB-richtlijn) van de Europese Unie. De NIB-richtlijn spoort lidstaten aan hun digitale weerbaarheid te vergroten.[2]

Vooral bij het mkb is het niet goed gesteld met die digitale weerbaarheid. Het mkb heeft onvoldoende middelen, kennis of toegang tot kennis om dreigingen te onderkennen en zich weerbaar te maken (Verhagen, 2016). Basale digitale beveiligingsmaatregelen, zoals het updaten van software, het gebruik van sterke wachtwoorden of het maken van back-ups van belangrijke bestanden, worden nog te vaak niet genomen (Munnichs, Kouw & Kool, 2017). Mkb-ondernemers achten zichzelf veelal niet interessant voor cyberaanvallen en zien cybercrime niet als een van de belangrijkste bedrijfsrisico's. Het zijn vooral de sociaaleconomische ontwikkelingen waar de ondernemer van wakker ligt (Van den Berg & Reijmer, 2015). Ook ontbreekt het aan inzicht in de risico's en in de mogelijkheden om daar iets aan te doen (Munnichs e.a., 2017). Risico's blijven daardoor ongrijpbaar en cybersecurity krijgt onvoldoende prioriteit. Het gebrek aan digitale weerbaarheid vormt daarmee een serieus probleem.

Het mkb: kwetsbaarheden en bedreigingen

Het midden- en kleinbedrijf (mkb) betreft 24% van de bedrijven in de Nederlandse economie (Smetsers & Van der Beek, 2017). Als ook ZZP'ers en parttime bedrijven (<15 uur) worden meegerekend, dan behoort meer dan 99% van de bedrijven in de Nederlandse economie hiertoe. Het mkb is dan ook de backbone van de Nederlandse economie. Mkb-bedrijven vormen 61% van het Nederlandse bruto binnenlands product (bbp), zorgen voor 70% van de werkgelegenheid en hebben een totale omzet van 888 miljard euro (CBS, 2015).

Het mkb is in zeer grote mate afhankelijk van ICT (Van den Berg & Reijmer, 2015). In het mkb gebruikt een groot deel van de medewerkers internet bij het uitvoeren van zijn of haar werkzaamheden.[3] Deze werkzaamheden betreffen bijvoorbeeld het beheer van persoonsgegevens en klantgegevens in databanken en het uitvoeren van digitale betalingen. Dat

1 De andere onderzoekslijnen zijn: Aard en omvang van slachtofferschap, Aard van cybercriminaliteit en De aanpak van cybercriminaliteit.
2 Zie: https://www.securitymanagement.nl/cybersecuritywet-naar-tweede-kamer/
3 Centraal Bureau voor de Statistiek (2014). ICT, Kennis en Economie 2014. Hardinxveld-Giessendam: Tuijtel.

digitalisering risico's met zich meebrengt wordt inmiddels wel onderkend. Enerzijds zijn er nieuwe delicten bijgekomen, bijvoorbeeld het hacken van een database met persoonsgegevens of het platleggen van websites of netwerken. Anderzijds zijn er traditionele vormen van criminaliteit waarbij ICT een steeds belangrijkere rol speelt bij de realisatie daarvan (Leukfeldt, 2017). Voorbeelden zijn het plegen van fraude via internet en afpersing door computervirussen. De bescherming van burgers en bedrijven tegen cyberaanvallen is de laatste jaren dan ook topprioriteit van de Nederlandse overheid. Diverse maatregelen zijn al genomen. Met de oprichting begin 2018 van een Digital Trust Centre komt het kabinet bijvoorbeeld tegemoet aan de wens van bedrijven om hen te helpen met actuele informatie over risico's en adviezen over digitale veiligheid.[4] Desondanks worden mkb'ers relatief vaak slachtoffer van cyberaanvallen. Een onderzoek van het Center of Expertise Cyber Security van de Haagse Hogeschool laat zien dat een op de vijf mkb-ondernemers die deelnamen aan het onderzoek slachtoffer zijn geworden van een cyberaanval.[5] Als sector is het mkb weliswaar groot, maar de omvang van individuele bedrijven is veelal beperkt. Dit brengt kwetsbaarheid met zich. Het is voor mkb'ers moeilijker dan voor grote ondernemingen om de secundaire processen in hun organisatie goed te organiseren. Dat geldt ook voor cybersecurity. Het mkb heeft veelal dan ook niet de capaciteit om zich te weren tegen cyberaanvallen.

Digitale weerbaarheid?

Van Dale definieert weerbaarheid als het vermogen om jezelf te verdedigen, om tegenstand te bieden. In het Engels wordt dit ook wel *defensibility* genoemd. Net als in de fysieke wereld zijn risico's in het digitale domein nooit volledig uit te bannen. Het valt bovendien niet te zeggen welke gedaante de dreigingen in de komende jaren zullen aannemen en wat ervoor nodig is om die het hoofd te bieden (Munnichs e.a., 2017). Dit betekent dat bedrijven niet alleen de capaciteit moeten hebben om weerstand te bieden tegen bekende en onbekende vormen van cybercrime, om robuust te zijn, maar ook het vermogen moeten bezitten om snel te kunnen herstellen van een crisis als gevolg van een aanval.

4 Zie : https://www.rijksoverheid.nl/actueel/nieuws/2017/09/23/digital-trust-centre-geeft-ondernemers-advies-over-cybersecurity.
5 https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/infographic-nulmeting-cybersecurity-mkb.pdf.

Dr. Rick van der Kleij

Dr. Rick van der Kleij is op 1 januari 2018 gestart als senior onderzoeker aan het lectoraat Cybersecurity in het mkb, Haagse Hogeschool. Zijn opdracht is om de digitale weerbaarheid van het mkb te vergroten.

Rick is ook werkzaam als senior onderzoeker bij TNO, waar hij onderzoek doet naar human factors in cybersecurity.
r.vanderkleij@hhs.nl

Veerkracht, *resilience* in het Engels, lijkt dan ook beter te omschrijven wat echt nodig is om digitaal weerbaar te zijn. Onder veerkracht wordt verstaan de capaciteit om tegenstand te bieden en snel te herstellen van bekende en onbekende dreigingen (Linkov, Eisenberg, Plourde, Seager, Allen & Kott, 2013, p. 2). Systemen die veerkrachtig zijn, worden veelal omschreven aan de hand van vier stadia van een cyclus: voorbereiden/plannen, monitoren, absorberen/herstellen en aanpassen aan bekende en onbekende dreigingen (National Academy of Sciences, 2012; Hollnagel, 2011). In de eerste fase staat een goede voorbereiding centraal: het kunnen anticiperen op (on)voorziene dreigingen; in de tweede fase staat het vermogen om incidenten te herkennen voorop; in de derde fase draait het om snel en adequaat reageren op het incident, het continueren van de bedrijfsvoering tijdens een incident en het herstellen van verstoringen; in de vierde fase, ten slotte, staat het lerend vermogen voorop: kennis die is opgedaan tijdens het incident kan worden gebruikt om systemen, protocollen en mensen veerkrachtiger te maken (Linkov e.a., 2013).

In mijn ogen dient een digitaal veerkrachtig bedrijf dan ook in voldoende mate de capaciteit te hebben om te: (1) anticiperen, (2) monitoren, (3) reageren en (4) leren. In andere woorden: het mkb moet weten hoe het incidenten kan voorkomen, wat incidenten zijn en hoe deze te herkennen, wat te doen en, na afloop, weten wat er is gebeurd. Digitale veerkracht is dus een proactief vermogen, waarbij het lectoraat niet alleen geïnteresseerd is in de adaptieve respons en lerend vermogen, maar ook in de factoren die bijdragen aan een effectieve voorbereiding op incidenten en het adequaat kunnen monitoren van cyberspace. Hieruit blijkt dat een *integrale aanpak* noodzakelijk is om digitaal veerkrachtig te zijn als mkb. Op zowel het niveau van de besturing, de techniek als de mens zijn maatregelen nodig.

Human factors en digitale veerkracht

Het lectoraat wil komen tot een raamwerk waarmee mkb'ers kunnen vaststellen hoe digitaal veerkrachtig ze zijn. Maar vooral ook willen we inzichtelijk maken welke factoren bijdragen aan digitale veerkracht en wat het mkb en stakeholders kunnen doen om dit vermogen te vergroten. Omdat onveilig gedrag vaak aan de basis staat van geslaagde cyber-aanvallen – iemand klikt op de link in een phishing e-mail, heeft de verplichte software-update te lang uitgesteld of een standaardwachtwoord nooit aangepast – is het bovendien van belang dat er zicht komt op waarom mkb'ers zich onveilig gedragen en wat zij hieraan kunnen doen. Hier ligt een interessante relatie met het vakgebied human factors: om veilig gedrag te stimuleren moet er gelegenheid worden geboden. Een deur met een slot dat niemand kan bedienen, leidt tot een onveilige situatie. Zo is het ook met cybersecurity. Slimme aanpassingen aan de sociotechnische omgeving kunnen naar mijn mening dan ook een belangrijke rol gaan spelen in het verhogen van de digitale veerkracht van het mkb.

Referenties

CBS (2015). *De staat van het mkb: 2015*. Centraal Bureau voor de Statistiek. Den Haag.

Hollnagel, E., Paries, J., Woods, D., & Wreathall, J. (2011). *Resilience engineering in practice: a guidebook*. Ashgate, United Kingdom.

Leukfeldt, E.R. (ed.) (2017). *Research Agenda: The Human Factor in Cybercrime and Cybersecurity*. The Hague: Eleven International Publishers.

Linkov, I., Eisenberg, D.A., Plourde, K., Seager, T.P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions, 33*(4), 471-476.

Munnichs, G., Kouw, M., & Kool, L. (2017). *Een nooit gelopen race: Over cyberdreigingen en versterking van weerbaarheid*. Rathenau instituut, Den Haag.

National Academy of Sciences (2012). *Disaster resilience: a national imperative*. Washington DC, United States.

Smetsers, D. & Beek, J.E. van der (2017). *Preventie door het mkb tegen digitale fraude*. Kamer van Koophandel.

Van den Berg, M. & Reijmer, T. (2015). *Cybersecurity in het MKB.* (NB: In opdracht van Interpolis). Verkregen op 15.02.2018 van: https://www.interpolis.nl/~/media/files/ebook_cybersecurity_in_het_mkb.pdf.

Veenstra, S., Zuurveen R. & Stol, W. (2015). *Cybercrime onder bedrijven. Een onderzoek naar slachtofferschap van cybercrime onder het Midden- en Kleinbedrijf en Zelfstandigen zonder Personeel in Nederland*. Leeuwarden: NHL.

Verhagen, H. (2016). *De economische en maatschappelijk noodzaak van meer cybersecurity. Nederland digitaal droge voeten*. Verkregen op 15.02.2018 van : https://www.cybersecurityraad.nl/binaries/CybersecurityAdviesHernaVerhagen_tcm56-122110.pdf.