Auteurs: Luuk Bekkers, MSc. PhD-kandidaat, hij is te bereiken via: l.m.j.bekkers@hhs.nl. Dr. Susanne van 't Hoff-de Goede, onderzoeker, zij is te bereiken via: m.s.vanthoff-degoede@hhs.nl. Dr. Rutger Leukfeldt, directeur & lector. Allen werken zij voor het Centre of Expertise Cyber Security, De Haagse Hogeschool. Rutger is ook senior onderzoeker bij het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving. Rutger is te bereiken via: e.r.leukfeldt@hhs.nl. Dr. Remco Spithoven is lector, Lectoraat Maatschappelijke Veiligheid, Hogeschool Saxion en te bereiken via: r.spithoven@saxion.nl.

Wat motiveert mkb'ers om actie te ondernemen tegen ransomware?

Slachtofferschap van ransomware – software die bestanden of systemen versleutelt als drukmiddel om slachtoffers losgeld te laten betalen – is een groeiend probleem voor bedrijven in Nederland. Tot wel 17% van de Nederlandse mkb'ers zegt ooit slachtoffer te zijn geworden van dit delict. Toch nemen ondernemers nog te weinig maatregelen om hun bedrijf tegen ransomware en andere vormen van cybercriminaliteit te beschermen. Hoe kunnen we de weerbaarheid van het mkb vergroten?

Tegenwoordig behoort ransomware tot de meest voorkomende vormen van cybercriminaliteit onder het mkb (1,2). Ransomware is kwaadaardige software die data of een computer(systeem) versleutelt, waardoor de toegang tot die data wordt ontzegd (3). Pas als het slachtoffer een geldbedrag betaalt ('losgeld'), maken criminelen de gegevens weer beschikbaar. Midden- en kleinbedrijven vormen in het bijzonder een doelwit omdat hun cybersecurity vaak onvoldoende is. Vaak ontbreekt cybersecuritybeleid, worden wachtwoorden opnieuw gebruikt en zijn de maatregelen die worden genomen onder de maat of worden deze slecht geïmplementeerd (2,4,5). Met andere woorden: Nederlandse ondernemers hebben doorgaans een lage mate van cyberweerbaarheid en zijn daarom kwetsbaar voor slachtofferschap van ransomware.

Onbekend is echter nog hoe het komt dat ondernemers maar weinig maatregelen nemen en hoe ze gemotiveerd kunnen worden hun bedrijf beter te beschermen tegen ransomware. Daarom hebben De Haagse Hogeschool en Hogeschool Saxion recent met verschillende partners (o.a. gemeenten, regionale veiligheidsnetwerken, de FraudeHelpdesk en het CCV) een onderzoek uitgevoerd naar psychologische processen die kunnen verklaren waarom ondernemers zich wel of niet beschermen tegen ransomware. Hierbij is ook onderzocht wat verschillen zijn tussen ondernemers die een extern cybersecuritybedrijf inschakelen en ondernemers die dat niet doen. Met deze kennis zijn overheidspartijen en IT-professionals beter in staat om ondernemers te helpen zich te wapenen te voorkomen om slachtoffer te worden van ransomware. In dit artikel bespreken we de belangrijkste bevindingen van het onderzoek.

Factoren die een rol spelen bij zelf-beschermend gedrag: PMT

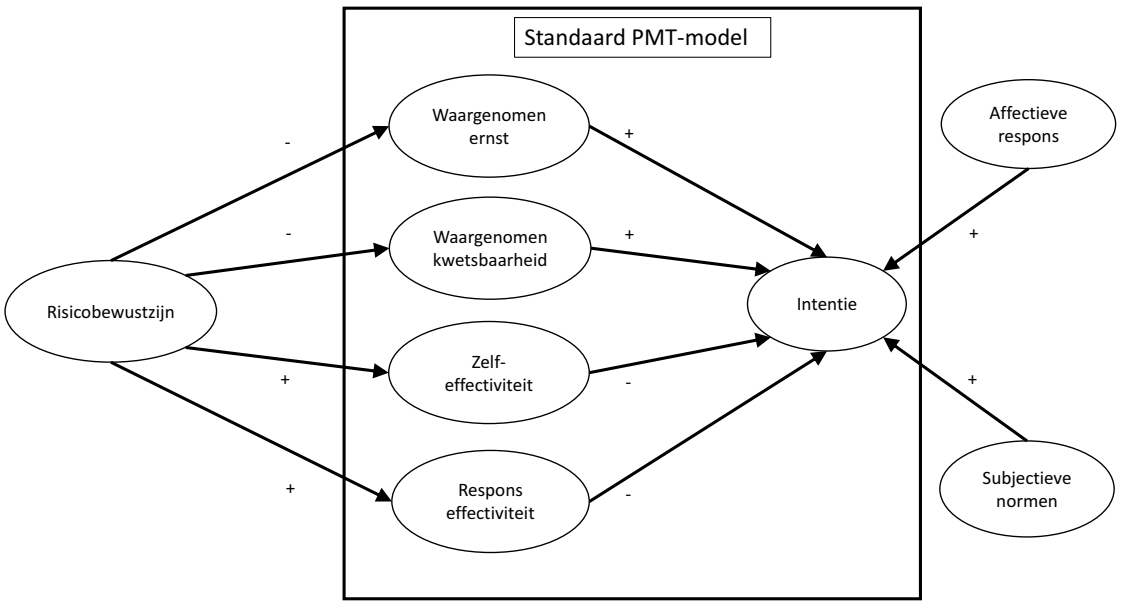
In het onderzoek fungeert de 'Protectie-Motivatie Theorie' (PMT) als het theoretisch raamwerk (6,7). PMT tracht te verklaren waarom mensen de intentie hebben om zich tegen een bepaald risico te beschermen. Toegepast op ransomware, veronderstelt de theorie dat ondernemers zelf-beschermend gedrag vertonen als ze denken dat hun bedrijf kwetsbaar is voor ransomware (waargenomen kwetsbaarheid) en als ze overtuigd zijn dat blootstelling aan ransomware ook ernstige gevolgen kan hebben voor hun bedrijf (waargenomen ernst). Daarnaast is ook respons effectiviteit van belang, ofwel de mate waarin ondernemers van mening zijn dat het zin heeft om hun bedrijf te beschermen tegen ransomware. Ten slotte veronderstelt de theorie dat mensen een schatting maken over hun eigen capaciteiten (zelf-effectiviteit): pas als ondernemers zichzelf in staat achten hun bedrijf te kunnen beschermen, gaan ze dat ook doen. Samen spelen deze vier factoren van het PMT-model mogelijk een rol bij de intentie van ondernemers om cybersecuritymaatregelen te nemen tegen ransomware.

Uitbreiden PMT-model

Hoewel het PMT-model waardevolle inzichten biedt, is het niet volledig bruikbaar als we deze toepassen op de weerbaarheid van het mkb tegen ransomware, want ook andere factoren hebben mogelijk een invloed op het zelf-beschermend gedrag van ondernemers. Daarom hebben we voor dit onderzoek op basis van bestaande literatuur drie factoren toegevoegd aan het PMT-model: 'risicobewustzijn' (8,9), 'affectieve respons' (8) en 'subjectieve normen' (9,10). Risicobewustzijn gaat over de mate waarin ondernemers weten wat de risico's zijn van ransomware. Affectieve respons heeft betrekking op de gevoelsmatige reactie op ransomware, ofwel de mate waarin ondernemers zich zorgen maken: de verwachting is dat hoe meer zorgen ze zich maken, hoe groter de kans dat ze maatregelen nemen. Ten slotte refereert subjectieve norm aan de waargenomen sociale druk van mensen uit de sociale omgeving om maatregelen te nemen. We veronderstelden dat wanneer ondernemers denken dat branchegenoten of ketenpartners van hen verwachten dat ze hun eigen bedrijf beschermen, de ondernemers eerder geneigd zijn dat ook te doen.

Unieke dataset

Op basis van wetenschappelijke literatuur is een vragenlijst ontwikkeld om de genoemde factoren te meten. Deze vragenlijst is vervolgens uitgezet onder een groot panel van 2000 Nederlandse zzp'ers en eigenaren van bedrijven tot 250 werknemers. In totaal hebben 1020 respondenten de vragenlijst volledig ingevuld. Deze unieke, grote dataset geeft inzicht in een populatie die relatief kwetsbaar is voor slachtofferschap van cybercriminaliteit, maar doorgaans zeer moeilijk is te bereiken voor wetenschappelijk onderzoek. Nadat de data was verzameld, zijn statistische analyses uitgevoerd om een gedetailleerd beeld te krijgen van de invloed van de bovengenoemde factoren op de gedragsintentie ten aanzien van het nemen van maatregelen tegen ransomware in de toekomst.



Figuur 1 - Resultatenanalyse.

Bevindingen

Figuur 1 betreft een overzicht van de resultaten van de analyse. Een + (plus) geeft een positief verband weer: hoe hoger de score op de ene variabele, hoe hoger de score op de ander. Een – (min) daarentegen vertegenwoordigt een negatief verband: hoe hoger de score op de variabele aan het begin van de pijl, hoe lager de score op de variabele aan het einde van de pijl.

Uit onze analyse blijkt dat de intentie om meer maatregelen tegen ransomware te nemen direct wordt verhoogd wanneer ondernemers zich zorgen maken over de risico's (affectieve respons) en wanneer ze ervan overtuigd zijn dat andere mensen in hun omgeving verwachten dat zij maatregelen nemen (subjectieve normen). Ook is de kans groter dat ondernemers hun bedrijf beschermen tegen ransomware wanneer zij hun bedrijf kwetsbaar achten voor slachtofferschap van ransomware (waargenomen kwetsbaarheid) en als zij van mening zijn dat dit kan leiden tot ernstige gevolgen in termen van verlies van geld en tijd (waargenomen ernst). Al deze bevindingen waren in lijn met onze verwachtingen. Dit beeld bleek echter wel anders te zijn voor de groep ondernemers die hun cybersecurity uitbesteedt: zij beschouwen hun bedrijf minder kwetsbaar voor ransomware, waardoor ze minder gemotiveerd zijn om zelfbeschermend gedrag te vertonen.

Verder komt naar voren dat ondernemers juist minder geneigd zijn zich te beschermen tegen ransomware als zij geloven dat zij daartoe in staat zijn (zelf-effectiviteit) en overtuigd zijn dat het nemen van maatregelen ook zin heeft (respons effectiviteit). Deze bevindingen stonden haaks op onze verwachtingen. Een mogelijke verklaring hiervoor is dat ondernemers zichzelf overschatten: zodra ondernemers denken dat zij hun bedrijf inderdaad kunnen beschermen tegen ransomware, zien ze mogelijk minder risico in ransomware en nemen ze dus minder snel actie. De notie van overschatting komt ook terug bij de rol van risicobewustzijn in de analyse: als ondernemers meer weten over de risico's van ransomware, beschouwen zij zichzelf minder kwetsbaar en schatten ze de gevolgen van een ransomware aanval minder hoog in, waardoor ze geen aanvullende maatregelen nemen. Meer onderzoek is nog wel nodig om de mogelijke rol van overschatting bij ondernemers beter in kaart te brengen.

Hoe weerbaarheid tegen ransomware verhogen?

Onze resultaten wijzen erop dat het informeren van ondernemers over ransomware een uiterst gevoelige benadering vereist. Het verstrekken van informatie kan er immers toe leiden dat ondernemers hun eigen capaciteiten onrealistisch hoog inschatten, zichzelf veilig wanen en hun bedrijf daarom juist minder goed beschermen. Dat is in het bijzonder het geval voor ondernemers die hun cybersecurity extern hebben belegd. Het uitbesteden van cybersecurity wil echter niet zeggen dat een bedrijf ook veilig is en geen slachtoffer meer kan worden. Daarom is het belangrijk dat IT-dienstverleners een open en eerlijke relatie onderhouden met hun cliënten, specifiek benadrukken dat ondernemers zelf de eindverantwoordelijkheid hebben om slachtofferschap van ransomware te voorkomen en naast het nemen van technische en organisatorische maatregelen ook het personeel alert maken. Bovendien blijken ondernemers gevoelig voor invloeden vanuit hun omgeving. Benoem dus expliciet dat andere ondernemers hun bedrijf ook beschermen: dat is de norm. Collega-ondernemingen die maatregelen hebben genomen, eventueel nadat zijzelf slachtoffer van ransomware zijn geworden, kunnen als rolmodel fungeren.

Verder komt uit ons onderzoek naar voren dat tijd, geld en complexiteit van cybersecurity belangrijke barrières zijn voor ondernemers. Adviseer ondernemers daarom over gebruiksvriendelijke maatregelen en biedt ze perspectief op hoe zij concreet kunnen handelen om het risico op ransomware in hun specifieke situatie te beperken. Hierbij kan het helpen om een emotionele reactie onder de ondernemers teweeg te brengen, bijvoorbeeld door te benoemen dat ook de individuele ondernemer kans heeft om slachtoffer te worden en door uit te leggen dat slachtofferschap grote consequenties kan hebben voor het bedrijf.

Conclusie

In deze studie hebben wij onderzocht hoe het komt dat Nederlandse ondernemers hun bedrijf vaak slecht beschermen tegen ransomware en hoe ze gemotiveerd kunnen worden meer maatregelen te nemen. Hieruit is gebleken dat de motivatie van ondernemers wordt beïnvloed door een vrij complex samenspel van verschillende sociaalpsychologische factoren. Zo zijn ondernemers van plan zich beter te beschermen tegen ransomware wanneer zij zich zorgen maken over de risico's, wanneer ze denken dat andere mensen in hun omgeving van ze verwachten dat ze maatregelen nemen, wanneer ze hun bedrijf kwetsbaar achten en wanneer ze ervan overtuigd zijn dat slachtofferschap grote gevolgen kan hebben. Ondernemers nemen opvallend genoeg juist minder snel maatregelen wanneer zij geloven dat ze daartoe in staat zijn en wanneer ze overtuigd zijn dat het zin heeft om maatregelen te nemen. Dat komt mogelijk omdat ondernemers zichzelf overschatten. Professionals kunnen onze resultaten gebruiken om het gedrag van ondernemers te veranderen en daarmee de weerbaarheid tegen ransomware-aanvallen te verhogen.

Referenties

(1) Notté, R. J., Slot, L., van 't Hoff-de Goede, S. & Leukfeldt, E. R. (2019). Cybersecurity in het mkb. De Haagse Hogeschool.

(2) Johns, E. (2021). Cyber Security Breaches Survey. Department for Digital, Culture, Media & Sport.

(3) Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), 10-21.

(4) Rohn, E., Sabari, G., & Leshem, G. (2016). Explaining small business InfoSec posture using social theories. Information & Computer Security, 24(5), 434-556.

(5) Osborn, E., & Simpson, A. (2018). Risk and the small-scale cyber security decision making dialogue- UK case study.

(6) Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93-114.

(7) Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A Revised theory of protection motivation. In J. T. Cacioppo, & R. E. Petty (Eds.), Social Psychophysiology: a source book (pp. 153-176).

(8) De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2021). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour & Information Technology, 1-13.

(9) Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. Computers in Human Behavior, 92, 139-150.

(10) Barlette, Y., Gundolf, K., & Jaouen, A. (2017). CEOs' information security behavior in SMEs: Does ownership matter? Systemes d'Information Management, 22(3), 7-45.