AUDIT MAGAZINE

ARTIKELEN | 1 DECEMBER 2022

SLECHTNIEUWSBOODSCHAPPEN EN CYBERSECURITYBESLISSINGEN

Auteur: Drs. Marc van der Veen RA RO RE CIA RMFI

Leestijd: 5 min



In dit artikel zijn de resultaten van mijn onderzoek in het kader van de afronding van de post-master IT-Auditing & Advisory aan de Erasmus Universiteit weergegeven. Centraal in het onderzoek staat de vraag hoe een internal IT-auditor, een journalist (media) of gedragsvalkuilen de beslissingen van besluitvormers bij het treffen van cybersecuritymaatregelen kunnen beïnvloeden.

Cybersecurity was nog niet zo lang geleden voor veel mensen een ver-van-mijn-bedshow. Inmiddels kan niemand er meer omheen en is het bewust dan wel onbewust, gewenst dan wel ongewenst, onderdeel van ons dagelijks leven. Al is het alleen maar omdat de kranten bijna dagelijks volstaan met organisaties die zijn getroffen door een cyberaanval. Voorbeelden van cyberaanvallen met een grote impact in Nederland zijn die bij de universiteit van Maastricht, de gemeente Hof van Twente en bij VDL Nedcar. En ook buiten Nederland zijn cyberaanvallen aan de orde van de dag.

Not if, but when

Zoals gezegd zijn cyberaanvallen momenteel niet meer weg te denken uit ons dagelijks bestaan. Het lijkt erop dat geen organisatie er meer aan ontkomt. Een veelgehoorde frase is dan ook: ‘the question is not IF you are going to be hacked,

© AuditMagazine.nl

but WHEN!' Kunnen organisaties dan helemaal niets doen tegen cyberaanvallen? Er is veel tegen cyberaanvallen te doen, maar het is de vraag of deze aanvallen volledig zijn te voorkomen. Door de steeds toenemende complexiteit van informatietechnologie, bijvoorbeeld als gevolg van artificial intelligence (AI) en blockchain, en interdependenties binnen netwerken, is het volledig voorkomen van cyberaanvallen een utopie. Echter, in een omgeving die volatiel, onzeker, complex en ambigu is, ook wel de VUCA-omgeving genoemd, wordt het bewuster en anders omgaan met (cyber)risico's daarom steeds belangrijker.

Welke maatregelen?

Besluitvormers staan veelal voor de vraag welke maatregelen ze moeten treffen om de organisatie te wapenen tegen dergelijke cyberaanvallen. Het treffen van maatregelen gaat vooraf door een besluitvormingsproces bij het nemen van een beslissing door de besluitvormer. Een signaal, risicowaarschuwing of slechtnieuwsboodschap is dan vaak een impuls voor dat besluitvormingsproces.

Uit onderzoek blijkt dat de bron van de slechtnieuwsboodschap een rol speelt in het nemen van een beslissing

Uit eerdere toonaangevende onderzoeken blijkt dat mensen bij het nemen van beslissingen vuistregels toepassen, en daarbij maken ze systematische fouten. Deze zogenoemde heuristieken en biases spelen in het nemen van beslissingen door besluitvormers een belangrijke rol. Daarnaast blijkt uit onderzoek dat de bron van de slechtnieuwsboodschap een rol speelt bij het nemen van een beslissing. Ofwel, is deze boodschap afkomstig van binnen de 'groep' van de besluitvormer, ook wel de 'ingroup' genoemd, of is deze boodschap afkomstig van buiten de 'groep' van de besluitvormer, ook wel de 'outgroup' genoemd. Bij het nemen van beslissingen hebben besluitvormers dus te maken met informatie afkomstig uit verschillende bronnen en is sprake van persoonlijke voorkeuren die het nemen van beslissingen beïnvloeden. Deze complexiteit en het gebrek aan inzicht daarin kan leiden tot onjuiste beslissingen.

Effect

Recent heb ik eerdere onderzoeken op het gebied van besluitvorming gecombineerd en onderzocht in hoeverre een slechtnieuwsboodschap met betrekking tot een cyberaanval invloed heeft op het nemen van een beslissing om binnen organisaties maatregelen te treffen om dergelijke aanvallen in de toekomst te voorkomen. In het door mij uitgevoerde onderzoek staat het effect van slechtnieuwsboodschappen op de besluitvorming door zogeheten besluitvormers (managers, leidinggevenden, toezichthouders, et cetera) centraal. Ik heb onderzocht in hoeverre een slechtnieuwsboodschap van een internal IT-auditor een ander effect heeft op het nemen van een beslissing door een besluitvormer dan wanneer deze boodschap afkomstig is van een journalist (media). Daarbij wordt een internal IT-auditor beschouwd als onderdeel van de 'ingroup' van een besluitvormer en een journalist als onderdeel van de 'outgroup' van een besluitvormer.

Daarnaast heb ik onderzocht in hoeverre de waargenomen relevantie en het herkennen van problemen in een slechtnieuwsboodschap invloed hebben op de beslissingen van besluitvormers om cybersecuritymaatregelen te treffen.



Verband

De slechtnieuwsboodschap (afkomstig van een internal IT-audit of een journalist) is als onafhankelijke variabele in het onderzoeksmodel meegenomen. Daarbij is het rechtstreekse verband met het nemen van een beslissing voor het treffen van cybersecuritymaatregelen onderzocht. In het onderzoeksmodel zijn tevens twee mediërende variabelen opgenomen, te weten de waargenomen relevantie ('perceived message relevance') en het herkennen van problemen ('problem recognition'). Aan de hand van een experiment is het onderzoeksmodel onderzocht. Hierbij is aan de hand van twee scenario's met behulp van een casus en een vragenlijst bij veertig besluitvormers onderzocht welke verbanden in het onderzoeksmodel aangetoond konden worden.

Actie

Uit het onderzoek komt naar voren dat een besluitvormer eerder tot actie overgaat om cybersecuritymaatregelen te treffen op het moment dat deze boodschap afkomstig is van een internal IT-auditor dan wanneer de boodschap afkomstig is van een journalist (vanuit de media). Meer specifiek kiest een besluitvormer er dan voor om awarenesstrainingen te organiseren als maatregel om de organisatie te beschermen tegen cyberaanvallen in plaats van te investeren in of de verbetering van patchmanagement of logische toegangsbeveiliging.

De waargenomen relevantie van de slechtnieuwsboodschap is van belang om de besluitvormer daadwerkelijk een beslissing te laten nemen. Op het moment dat de besluitvormer de slechtnieuwsboodschap niet als relevant ervaart, speelt deze boodschap geen rol bij het nemen van de beslissing door de besluitvormer. Daarnaast is in het onderzoek geen significant verband gevonden tussen het herkennen van problemen in de slechtnieuwsboodschap en het nemen van een beslissing door een besluitvormer om cybersecuritymaatregelen te treffen.

Op het moment dat de besluitvormer de slechtnieuwsboodschap niet als relevant ervaart, speelt deze boodschap geen rol bij het nemen van een beslissing

Inzicht

Met dit onderzoek is getracht om besluitvormers, maar ook internal IT-auditors, meer inzicht te geven in welke factoren een rol spelen bij het nemen van beslissingen om cybersecuritymaatregelen te treffen. Daar kan een besluitvormer in het

besluitvormingsproces en een internal IT-auditor in de uit te voeren audits rekening mee houden. Zo is het voor besluitvormers waardevol om zich te realiseren dat de bron (ingroup of outgroup) van de slechtnieuwsboodschap van invloed is op het nemen van een beslissing, ondanks dat de inhoud van die bron niet anders is.

Daarnaast zijn de uitkomsten van dit onderzoek voor de internal IT-auditor waardevol, omdat de internal IT-auditor goed moet beseffen dat de relevantie van zijn slechtnieuwsboodschap van invloed is op de beslissing die een besluitvormer neemt. Het is eveneens belangrijk dat een internal IT-auditor zich realiseert dat hij zich binnen de groep van een besluitvormer bevindt. Immers, de internal IT-auditor heeft in dat opzicht impact op de besluitvormer en zijn audits hebben daarmee effect op het nemen van beslissingen.

Vervolgonderzoek

Eventueel vervolgonderzoek kan zich richten op een andere samenstelling van de outgroup. Zo kan bijvoorbeeld worden onderzocht of de resultaten uit dit onderzoek ook standhouden op het moment dat een externe auditor of externe toezichthouder (los van elkaar) deel uitmaakt van de outgroup. Daarnaast zijn andere heuristieken en biases, bijvoorbeeld overconfidence of de status quo bias, waardevolle en interessante concepten om binnen de context van cybersecurity nader te onderzoeken.

Over
Drs. Marc van der Veen RA RO RE CIA RMFI is eigenaar van Audit & Risk Solutions en helpt organisaties met vraagstukken op het gebied van audit, risicomanagement en cybersecurity.

Het gedetailleerde onderzoeksdocument is te raadplegen op de site van Audit & Risk Solutions.

Tags: Cyber resilience

Bron url: https://auditmagazine.nl/artikelen/slechtnieuwsboodschappen-en-cybersecuritybeslissingen/