Position Paper:

Nederlands Cyber Security Lab Labsessie #3

Hoe kan cyberweerbaarheid binnen een keten van bedrijven worden vergroot?

Petra Oldengarm *(Directeur - Cyberveilig Nederland)*
Bernold Nieuwesteeg *(Directeur Centre for the Law and Economics of Cyber Security - Erasmus Universiteit Rotterdam)*
Rutger Leukfeldt *(Directeur Centre of Expertise Cyber Security - Haagse Hogeschool)*
Dave Maasland *(Chief Executive Officer - ESET Nederland)*
Evert Stamhuis *(Senior Fellow- Jean Monnet Centre of Excellence on Digital Governance)*
Jan Heijdra *(Technology evangelist security- Cisco)*
Jelle Niemantsverdriet *(National Security Officer- Microsoft)*
Roos Dijkxhoorn *(Chief Operating Officer – PuraSec B.V.)*

8 FEBRUARI 2022

Inleiding

Al jarenlang roepen cybersecurity-experts hetzelfde: het is nodig dat mkb-ondernemers structureel aandacht besteden aan cybersecurity. Ondernemingen zijn in toenemende mate afhankelijk van digitale middelen. Uitval van deze middelen of schade aan digitale informatie zijn daarmee reële risico's die een grote impact kunnen hebben op de bedrijfsvoering. Ook neemt de dreiging toe. Cybercriminelen gaan dusdanig professioneel te werk dat de kans op incidenten met veel impact steeds groter wordt. Bijvoorbeeld door het uitvoeren van aanvallen waarbij ze via een bedrijf diens klanten compromitteren. Ook zien we bijvoorbeeld dat cyberspionnen zich steeds vaker richten op economische belangen en daarmee op het bedrijfsleven.

Als mkb-bedrijven toeleverancier zijn van grotere ondernemingen heeft hun cyberweerbaarheid in sommige gevallen direct invloed op de weerbaarheid van die grotere organisaties. Denk aan de recente aanval van een ransomware groepering op het bedrijf Kaseya, die de klanten van Kaseya rechtstreeks raakte . Door misbruik van een kwetsbaarheid in de software van Kaseya raakte een grote groep klanten besmet met ransomware.

In toenemende mate maken grotere organisaties zich terecht druk over dit soort afhankelijkheden die zij hebben in de keten van bedrijven waarmee zij samenwerken. Sommige van hen zijn initiatieven gestart onder het motto 'groot helpt klein'. Daarin worden bijvoorbeeld toeleveranciers opgeleid in basismaatregelen of mogen zij gebruik maken van de cybersecurityexpertise van de grote partijen. Het is goed te zien dat er aandacht is voor het bieden van hulp en ondersteuning. Aan de andere kant zijn er ook ondernemingen die meer eisen en voorwaarden willen stellen om zekerheid in te bouwen.

Het lab boog zich over de vraag op welke wijze een keten van bedrijven versterkt moet worden om de cyberweerbaarheid te verhogen tegen redelijke kosten en kwam tot een belangrijk inzicht. Als we willen dat de weerbaarheid van een keten groter wordt dan houdt dit onder andere in dat de individuele schakels in de keten ieder zelf hun weerbaarheid zullen moeten verhogen. Concreet betekent dit dat zij ervoor moeten zorgen dat ze de digitale infrastructuur die zij gebruiken bij het leveren van hun eigen producten en diensten goed hebben beveiligd. Deze infrastructuur bestaat veelal uit ingekochte producten en diensten, zoals routers, servers, software, enz. Als die als vanzelfsprekend veilig zouden zijn, dan zou de weerbaarheid van elke schakel in de keten enorm toenemen. Echter, deze is nu niet vanzelfsprekend veilig. En dus moeten organisaties die behoefte aan vanzelfsprekende veiligheid expliciet gaan maken. Dit overstijgt dus de ketenspecifieke issues, maar is wel de essentie van waar we in de toekomst naar toe zouden moeten. Daarnaast zijn er ook specifieke acties in de keten mogelijk, waardoor de weerbaarheid van de gehele keten kan worden versterkt.

1. https://nos.nl/artikel/2387724-zeker-200-bedrijven-getroffen-door-grote-ransomware-aanval
2. https://fd.nl/ondernemen/1383893/asml-geeft-zijn-leveranciers-bijles-over-het-weren-van-hackers

Onze positie: maak de behoefte aan vanzelfsprekende veiligheid expliciet aan ontwikkelaars van producten en diensten

Steeds meer ondernemers zijn (groten)deels afhankelijk van technologie. De droom van iedere ondernemer zou moeten zijn dat veiligheid als het ware ingebakken zit in de oplossingen die hij gebruikt en daarmee een vanzelfsprekendheid is. In andere domeinen is dit al zo. We accepteren bijvoorbeeld geen nieuwe auto's meer zonder autogordels op de voor- en achterbank, zonder airbags of kreukelzones. Als we een auto kopen vragen we in veel gevallen niet eens meer welke veiligheidsmaatregelen genomen zijn en een auto kopen zonder autogordel is tegenwoordig zelfs onmogelijk. Voor wat betreft digitale veiligheid moeten we dezelfde ambitie hebben, zo stelt het lab. En die ambitie gaat om de volledige breedte van het onderwerp. Dus niet alleen over technologie, maar ook om gedrag en organisatie, beleid en bestuur en juridisch kader.

Het klinkt wellicht als een utopie, vanzelfsprekende (cyber)veiligheid, maar het begint bij het stellen van de behoefte. Als je deze wens niet nu al expliciet uitspreekt, dan wordt er voorlopig niets op dit gebied ontwikkeld, tenzij dit door bijvoorbeeld wetenschappers als een lange termijn uitdaging wordt gezien en er langzamerhand oplossingen voor worden ontwikkeld. Door de behoefte hieraan nu al duidelijk te formuleren richting productleveranciers en dienstverleners, zullen ontwikkelaars hierop moeten inspringen en wordt het gat tussen de ideale situatie en de realiteit verkleind.

Het mogelijk maken van vanzelfsprekende cybersecurity-oplossingen moet deels gericht zijn op het ontwikkelen van nieuwe technische mogelijkheden, maar dus niet alleen. De oplossingen moeten zodanig worden ontworpen dat gebruikers ervan als vanzelf de veilige optie kiezen (denk aan het knipperende lampje en de irritante pieptoon in een auto als je de gordel vergeet vast te doen). De gedragsprikkels om veilig gedrag uit de weg te gaan moeten zo laag mogelijk zijn en een veilige optie moet als standaard beschikbaar zijn in de markt. Ook het juridisch kader is van belang. Het helpt bijvoorbeeld als er vanuit de overheid duidelijke voorschriften komen over de minimale eisen aan de beveiliging van producten en diensten (denk aan de verplichtingen die autoleveranciers hebben als het gaat om veiligheid), zowel aan de diensten van IT-leveranciers, als aan producten en diensten in bredere zin.

Naast de behoeftestelling aan vanzelfsprekende veiligheid is het van belang om ook keten-specifieke acties te nemen om veiligheid in de keten te vergroten. Een voorwaarde daarvoor is het hebben van voldoende cybersecuritykennis. Binnen het mkb is deze kennis echter nog beperkt, zo ziet het lab. Specialistische cybersecuritykennis is echter essentieel bij het nemen van de juiste beslissingen, bijvoorbeeld voor het kiezen van passende cybersecurity-oplossingen en -diensten. Deze kennis is bij mkb-ondernemers echter lastig op te bouwen.

Call to action

Het lab roept ondernemers op om bij haar product- en dienstleveranciers de behoefte uit te gaan spreken aan vanzelfsprekende veiligheid. Door deze behoefte expliciet te maken, zullen deze leveranciers anders over cybersecurity moeten gaan nadenken en nieuwe oplossingen moeten ontwikkelen of vragen van de markt.

Het lab ziet daarnaast een aantal specifieke mogelijkheden voor wat betreft het verbeteren van de cyberweerbaarheid in een keten van bedrijven op de kortere termijn, rekening houdend met het gebrek aan cybersecuritykennis binnen deze doelgroep:

1. **Ontwikkelen standaard met minimale cybersecurity-eisen.**
   Het is van belang dat mkb-bedrijven de fundamenten op orde hebben als het gaat om cybersecurity. Op dit moment is dit vaak nog vrijblijvend en verstrekt de overheid slechts adviezen over welke fundamentele maatregelen zinvol kunnen zijn. Het lab adviseert om deze adviezen meer impact te laten hebben in de praktijk. Dat zou kunnen door het ontwikkelen van nieuwe wetgeving, maar ook doordat afnemers van deze leveranciers of consumenten zo'n standaard gaan eisen. Wel is het van verstandig als niet iedere afnemer een eigen aanpak ontwikkelt, maar dat er een standaard komt waaraan alle bedrijven in een keten moeten voldoen, wellicht met een focus op een specifiek domein. Samen optrekken zou namelijk het belang van een minimale veiligheidsgarantie bevorderen en de kans bieden om de ontwikkelkosten te spreiden. Ook kan het zinvol zijn kennis op te doen in andere domeinen, zoals de autobranche, om te komen tot een bruikbare standaard. Brancheorganisaties zouden hierin een voortrekkersrol kunnen nemen.

2. **Gezamenlijke inkoop van cybersecuritydiensten binnen een keten of branche.**
   Bij veel mkb-ondernemers ontbreekt

3. Zie ook ons Position Paper #1, zorgplichtstandaard in cybersecurity https://cyberveilignederland.nl/upload/user-files/files/Position-Paper-NCSL-Labsessie-cyberveilig-nederland-bv2021.pdf

kennis op basis waarvan een goede keuze voor cybersecurity oplossingen kan worden gemaakt. Bij de kleinere mkb-ondernemingen is er daarnaast vaak grote druk op de kosten ervan. Toeleveranciers binnen een bepaalde keten of branche zouden gezamenlijk diensten kunnen inkopen, zowel vanwege het tekort aan kennis, als vanwege het beperken van kosten.

3. **Groot-helpt-kleinrichtlijnen en best practices.** In het verlengde van diverse individuele activiteiten van grote ondernemingen zou het goed zijn als de overheid samen met grote ondernemingen richtlijnen en best practices ontwikkelt voor hoe grote bedrijven hun toeleveranciers kunnen helpen bij het verhogen van de cyberweerbaarheid. Er valt te denken aan het doen van een toets van beveiligingsplannen, het verzorgen van webinars over maatregelen, het gezamenlijk oefenen van een crisis, het eisen van diverse basismaatregelen en het organiseren van slimme contracten waarin effectieve prikkels worden gegeven en kennis wordt gedeeld.

4. **Programma gericht op het verhogen van cybersecuritykennis binnen de IT-sector.** Het is belangrijk dat het kennisniveau op gebied van cybersecurity binnen de IT-sector verder omhooggaat. Mkb-ondernemers kijken steeds vaker naar hun IT-leverancier als het gaat om cybersecurity. Veel van deze IT-leveranciers zijn echter nog niet goed op de hoogte van de laatste ontwikkelingen en mogelijkheden om op efficiënte wijze in te zetten op het verhogen van de cyberweerbaarheid. Daarom is het nodig dat de overheid samen met de wetenschap, brancheorganisaties in de IT-sector en de cybersecuritysector komt met initiatieven om dit kennisniveau te vergroten en kennisdeling te stimuleren.

Over het Nederlands Cyber Security Lab (NCSL)

Nederland heeft behoefte aan maatschappelijke oplossingen voor optimale cybersecurity buiten de bestaande kaders. Door wetenschappers en bedrijfsleven bijeen te brengen combineert het NCSL wetenschappelijke inzichten met best practices vanuit het bedrijfsleven. De overheid is klankbord. Het Lab bestaat uit een bureau dat labsessies organiseert. Het bureau selecteert thema's en genodigden per labsessie. Tijdens de labsessie faciliteert het bureau het creatieve proces. Na de labsessie wordt een position paper met een kernachtige weergave van de oplossingen openbaar gemaakt en verspreid.