Position Paper:

Nederlands Cyber Security Lab Labsessie #4

Hoe kunnen we organisaties helpen om geen losgeld meer te betalen?

Bernold Nieuwesteeg (*Directeur Centre for the Law and Economics of Cyber Security - Erasmus Universiteit Rotterdam*)
Arwi van der Sluijs (*Algemeen Directeur - NFIR B.V.*)
Danny Damen (*T-CERT Case Manager - Tesorion*)
Henk Ferwerda (*Inhoudelijk Directeur - Bureau Beke*)
Michiel van der Donck (*Information Security Officer - Erasmus Universiteit Rotterdam*)
Petra Oldengarm (*Directeur - Cyberveilig Nederland*)
Rutger Leukfeldt (*Directeur Centre of Expertise Cyber Security - Haagse Hogeschool*)

14 OKTOBER 2022

Inleiding

Ransomware (gijzelsoftware) vormt één van de grootste cyberdreigingen voor organisaties. Het lijkt erop dat het betalen van losgeld bij een ransomware-aanval steeds vaker voorkomt. Recent stelde het Nationaal Cyber Security Center dat het fenomeen ransomware onze nationale veiligheid bedreigt.[1] We kunnen dus wel stellen dat dit een groot maatschappelijk probleem is. Organisaties betalen soms losgeld. Zij denken dat dit voor hen goedkoper is dan het opschonen of vervangen van de hele IT-infrastructuur. Dit laatste zou immers tijd kosten, tijd waarin de organisatie geen producten of diensten levert. En soms heeft een organisatie weinig keuze, omdat er anders essentiële gegevens verloren gaan die het voortbestaan van de organisatie bedreigen.

Met elke losgeldbetaling dragen organisaties echter bij aan het versterken van een crimineel businessmodel. Cybercriminelen investeren in die criminele activiteiten die een hoge economische verwachtingswaarde hebben. Wanneer het betalen van ransomware tot norm verwordt, kan dit ervoor zorgen dat het aantal aanvallen en de hoogte van het losgeld omhoog gaan. Als cybercriminelen daarentegen ontdekken dat Nederland een land is waar weinig losgeld wordt betaald, zullen ze wellicht hun pijlen op andere plekken richten. De Nederlandse maatschappij zou dus beter af zijn als er geen losgeld meer wordt betaald aan cybercriminelen.

Losgeldbetalingen simpelweg verbieden lijkt in 2022 geen haalbare maatregel. Sommige organisaties staan namelijk met de rug tegen de muur en kunnen bijna niet anders dan betalen. Maar er zijn ook organisaties die wel over de streep getrokken kunnen worden om niet te betalen die dat in de huidige situatie nog wel doen. Vaststaat dat we iets zullen moeten verzinnen om de status quo te veranderen. Als we niets doen, blijven de gelden binnenstromen bij de cybercriminelen en blijft hun verdienmodel dus in stand. Op dit moment nemen ransomware aanvallen alleen maar toe. Veel ondernemers krijgen hiermee te maken. Zelfs als een deel niet gaat betalen staat het verdienmodel voor de criminelen nog altijd als een huis. Dit vraagstuk is dus een grote uitdaging voor onze maatschappij. Het lab boog zich daarom over de vraag hoe we ervoor kunnen zorgen dat meer organisaties die slachtoffer worden van een ransomware-aanval de keuze gaan maken om niet te betalen.

1. https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021

Onze positie: onderzoek een ‘anti-ransomware fonds’ dat onder voorwaarden organisaties ondersteunt die geen losgeld te betalen.

Organisaties die slachtoffer worden van een ransomwareaanval zullen de kosten van betalen afwegen tegen de kosten van niet betalen. Middels het fonds willen we het aantrekkelijker maken om niet te betalen door organisaties daarin te ondersteunen.

In het fonds worden middelen, kennis en kunde vrij beschikbaar gemaakt om herstel mogelijk te maken. Hulp bij herstel zou zowel in kind (digitale brandweer, expertise) als cash kunnen zijn. Het voordeel bij hulp in kind is dat het bedrijf ook gelijk het cyberkennisniveau verhoogt. Het fonds kan bijvoorbeeld aangesloten worden bij een bestaande centrum voor cybersecuritykennisdeling, dat, mits voldoende bekend, het portaal kan zijn om de hulp bij ransomware te verlenen.[2]

Het doel van het fonds is niet om te zorgen dat er nooit meer losgeld wordt betaald, maar grosso modo te zorgen dat er minder losgeldbetalingen worden gedaan. Hierdoor wordt Nederland mogelijk een minder aantrekkelijk land voor cybercriminelen.

Cruciaal hierbij is wel dat organisaties niet laks worden omdat ze verwachten toch wel een uitkering uit een fonds te krijgen. Daarom zou een vergoeding alleen mogen worden uitgekeerd als een organisatie reeds aan een basisniveau van cybersecurity voldoet (een cybersecurity ‘baseline’). IT en de beveiliging ervan is namelijk nog steeds niet topprioriteit bij bedrijfsleven en overheid. Men zegt van wel, maar het lab ziet teveel voorbeelden waar er nog te weinig gebeurt. Een groot deel van cyberaanvallen lijkt het gevolg van achterstallig onderhoud of fouten. De voorwaarden voor hulp/uitbetaling zouden dynamisch bepaald kunnen worden, zoals ook bepleit in ons position paper van labsessie 1. [3]

De ondersteuning dient als een steuntje in de rug om die organisaties die nu twijfelen over wel of niet betalen over te halen om geen betaling te doen. Het gaat daarom ook niet om organisaties die nu met de rug tegen de muur staan. Daarvoor zou de uitkering vermoedelijk te klein zijn. Vanzelfsprekend mag de uitkering niet gebruikt worden voor het betalen van het losgeld en hiervoor zullen dus waarborgen moeten worden ingebouwd.

Een uitdaging is nog wel hoe we er voor zorgen dat organisaties die toch al niet zouden betalen (op dit moment, zonder een fonds) er niet oneigenlijk gebruik van gaan maken. En hoe maken we het systeem makkelijk uitvoerbaar? Dit rechtvaardigt verder onderzoek en dat is derhalve onze call to action.

2. Zoals bijvoorbeeld het Digital Trust Centrer
3. Position Paper: Nederlands Cyber Security Lab Labsessie #1. “Op naar een zorgplichtstandaard voor cybersecurity”.

Call to action

"Experimenteer met een fonds om bedrijven te stimuleren geen losgeld te betalen"

1. Experimenteer met verschillende vormen van hulp.
2. Onderzoek:
    a. de wijze van hulp (in kind versus cash)[4]
    b. de voorwaarden waarop uitgekeerd wordt, zoals minimale beveiligingsmaatregelen
    c. hoe oneigenlijk gebruik kan worden bestreden.
3. Maak voldoende middelen beschikbaar voor het inzetten van zo'n fonds
4. Onderbouw in welke mate Nederland een minder aantrekkelijk land kan worden voor gerichte cyberaanvallen als er minder losgeld betaald wordt.

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.

Het NCSL is een initiatief van Bernold Nieuwesteeg (Erasmus Universiteit Rotterdam), Petra Oldengarm (Cyberveilig Nederland) en Rutger Leukfeldt (Haagse Hogeschool // NSCR)

4. Bijvoorbeeld door die bedrijven te onderzoeken die wel losgeld hebben betaald, en te identificeren met welke hulp ze in de positie zouden zijn gekomen om geen losgeld te betalen.