Auteurs: Nicole van Deursen is hoofdredacteur van iB-Magazine en bereikbaar via nicolevandeursen@pvib.nl. Fook Hwa Tan is Chief Quality Officer van Northwave en bereikbaar via fookhwa.tan@northwave-security.com.

De onmeetbare impact van ransomware

De vorige uitgave van ons magazine (iB5) opende met een interview over het Data Breach Investigations Report van Verizon. Al in de eerste paar zinnen leek te worden gezegd dat de impact van de meeste ransomware aanvallen wel meevalt. Slechts 10% van de ransomware-aanvallen leidt daadwerkelijk tot financiële schade, aldus het rapport, waarbij de mediaan van betaalde bedragen slechts $11.150 is. In deze woorden gesteld lijkt het wel alsof een organisatie de kans op schade en hoogte van mogelijke schade van ransomware kan indelen op laag-laag in hun risicoanalyse

In Nederland kijken we op een andere manier naar de situatie: bij cybersecurity bedrijven staat de telefoon roodgloeiend met hulpvragen van slachtoffers van ransomware en de overheid noemt ransomware een bedreiging voor de nationale veiligheid. Wetenschappers doen onderzoek naar het thema en er is een constante stroom van televisie-uitzendingen, artikelen, rapporten en podcasts. Wij maken ons allemaal heel druk over ransomware, maar niet alleen vanwege de hoogte van het losgeld of de financiële schade.

Als je een cyberverzekeringspolis hebt, dan valt het betalen van het ransom onder de vergoeding van de polis. Een aantal jaren terug was het voor de verzekeraar een rekensom die ze vaker hebben uitgerekend, ook in andere domeinen. Ze maken een inschatting van de kosten van de schade en herstel en op basis van de kans van uitkeren kunnen ze een premie bepalen. De laatste twee jaar merk je echter, waarschijnlijk door het hoge aantal incidenten, dat ook verzekeraars voorzichtiger zijn. Bij sommige verzekeraars kunnen organisaties binnen vitale sectoren zich al niet meer verzekeren en bij andere moet een organisatie eerst een grondig onderzoek doorstaan door een cybersecurity bedrijf voordat een polis wordt afgesloten.

De onderzoekspopulatie van het Verizon rapport (1) is wellicht wel opgewassen tegen een financiële tegenvaller, zeker als ze een verzekering hebben afgesloten. Echter, door het betalen van het losgeld ben je als organisatie natuurlijk niet ineens uit de problemen. Los van de vraag of het überhaupt lukt om daarna alles weer te ontsleutelen zijn er nog de indirecte kosten, zoals de maatschappelijke en persoonlijke impact.

Maatschappelijke en persoonlijke impact

Een beschrijving van de maatschappelijke of persoonlijke impact zie je bijna nooit terug in financiële rapporten en statistieken. Toch kan die impact enorm zijn. Het PvIB organiseerde in juni een talkshow waarin een ondernemer vertelde hoe een cyberaanval zijn bedrijf, gezondheid en gezin had geschaad. Wanneer een onderneming failliet gaat laat dat diepe sporen na bij de ondernemers, hun klanten, maar ook bij de medewerkers die hun baan verliezen, en dus ook bij hun gezinnen. Een ander voorbeeld kennen we uit Duitsland, waar een jaar geleden in Düsseldorf een vrouw kwam te overlijden omdat het dichtstbijzijnde ziekenhuis onder een aanval met ransomware lag. Daarnaast valt een hack, malware of phishing bijna altijd aan te merken als een datalek, waarbij los van de mogelijke boete er ook persoonsgegevens kunnen worden gepubliceerd of misbruikt, met alle gevolgen van dien. Bovendien kan ransomware ook gevolgen hebben in een keten waar een organisatie deel van uitmaakt. Geen kaas in de schappen van de supermarkt, veroorzaakt door ransomware in de distributieketen staat voorgoed als nationaal trauma (en als 'kaas-hack') in ons collectief geheugen gegrift. Stel je voor dat de volgende keer die keten onze drinkwatervoorziening of elektriciteit is?

Maatschappelijke impact kan ook gaan over de stress waaronder incident responders moeten opereren na een ransomware aanval. De gezondheid van deze medewerkers leidt eronder als ze wekenlang onder hoge druk moeten werken, soms dag en nacht, om de gevolgen van de aanval te verwerken. Ook het andere uiterste komt voor: medewerkers die dagenlang juist niet mogen werken en worden verzocht hun verlofdagen op te nemen. Wanneer we deze indirecte schade meenemen in de risico-afweging, dan kan deze schade zwaarder wegen dan een concreet geldbedrag.

Meten is weten?

Het gestructureerd bijhouden en delen van data over de financiële en maatschappelijke impact van ransomware ontbreekt in Nederland. Zelfs als getroffen organisaties alle gevolgen administreren, dan delen ze die niet publiekelijk. Dat levert het risico op dat organisatorische maatregelen en zelfs overheidsbeleid worden gebaseerd op onvolledige risicoanalyses, onderbuikgevoel en publieke opinie. Ook in het Verizon rapport wordt de financiële impact niet verder uitgesplitst. Het uiteindelijke losgeldbedrag is natuurlijk een meetbare kostenpost. Maar of je dat nu betaalt of niet: bijna geen enkele organisatie kan verder zonder de hulp van ingehuurde cybersecurity bedrijven, juristen, en eventueel woordvoerders en bedrijfsartsen. Vervolgens zijn er andere concrete kosten zoals de (mogelijke) boete van de Autoriteit Persoonsgegevens, gedaalde beurswaarde, schade van het niet kunnen leveren van diensten aan de klanten, de nieuw aan te schaffen bedrijfsmiddelen, overuren en overwerkte medewerkers, inhuurkrachten, de communicatie en voorlichting, en versnelde afschrijving van bedrijfsmiddelen. Deze kosten zijn meetbaar, het is alleen veel werk om het bij te houden. De vraag is ook wanneer het voorbij is: wanneer ben je klaar met het repareren van de schade? De burgemeester van de Gemeente Hof van Twente vertelde in een recente televisie-uitzending (Zembla) dat de gemeente wel twee jaar nodig zal hebben om volledig van de gevolgen van de ransomware aanval te herstellen.

In openbare bronnen zijn maar beperkte gegevens beschikbaar en die gegevens missen soms ook context. Bijvoorbeeld in de Cybersecuritymonitor 2020 van het CBS (2) lijkt het aantal aanvallen van buitenaf (waar ransomware onder valt) de laatste jaren juist af te nemen. Op basis van die beperkte data kan men geneigd zijn te denken dat het dus inderdaad allemaal wel meevalt met de incidenten en dat we steeds beter zijn voorbereid. We moeten echter niet vergeten dat deze cijfers niet het hele verhaal vertellen en dat we veel meer zouden moeten weten over het fenomeen ransomware om er conclusies aan te kunnen verbinden.

Goed meten van ransomware impact is ingewikkeld maar niet onmogelijk. Het zal veel tijd kosten, maar het levert onmisbare kennis op over het fenomeen. Het aggregeren en delen van die data draagt bij aan bewustwording voor de urgentie van preventieve maatregelen. Jaren geleden werden risicoanalyses altijd kwalitatief uitgevoerd, omdat we geen data hadden om het kwantitatief te kunnen doen. Als we er met elkaar in slagen om meer van die data wel boven tafel te krijgen kunnen we completere risicoanalyses uitvoeren, beter beleid maken en bestuurders overtuigen tot investeren in preventieve maatregelen. We hebben daarbij wel hulp nodig van data professionals, want kijken naar alleen een mediaan van financiële schade (zoals in het Verizon rapport (1)) heeft weinig betekenis gezien de complexiteit van het fenomeen. We moeten ook kijken naar context, gemiddelden, uitsplitsingen in categorieën en naar outliers in de data (die vaak juist worden uitgesloten van analyse) omdat die leerzame verhalen vertellen. Laten we elkaar blijven steunen en in openheid informeren over incidenten en de gevolgen ervan, zodat we in de toekomst allemaal weerbaarder kunnen worden.

Referenties

(1) https://www.verizon.com/business/resources/reports/dbir/

(2) https://www.cbs.nl/nl-nl/publicatie/2021/18/cybersecuritymonitor-2020