Opinie

N.B. Het kan zijn dat elementen ontbreken aan deze printversie.

Alle hacks voorkomen? Niet tegen elke prijs

Terwijl de kosten van medicijnen voortdurend onderwerp van debat zijn, horen we nauwelijks iemand over de rekeningen van softwarebeveiligers, constateert promovendus cybersecurity *Bernold Nieuwesteeg*.

21 december 2017

Het security operations center (SOC) van computer- en netwerkbeveiliger Fox-IT in Delft, dat veel werk doet voor het Rijk. In het SOC worden medewerkers van Defensie opgeleid in het herkennen van en strijden tegen cyberaanvallen.

Foto Lex van Lieshout/ANP

Eind oktober besloot de voormalige minister van Volksgezondheid het medicijn Orkambi na moeizame prijsonderhandelingen toe te laten tot het basispakket. Eerder stelde uitvoeringsorganisatie Zorginstituut Nederland dat de prijs van het middel tegen taaislijmziekte, 170.000 euro per patiënt per jaar, met 82 procent omlaag moest om kosteneffectief te zijn. Hoewel de prijsafspraken geheim bleven, bruiste het debat erover.

Bernold Nieuwesteeg is promovendus cybersecurity aan de Erasmus Universiteit en partner bij CrossOver.

Hoe anders is dat met *cybersecurity*, oftewel onze digitale gezondheid. Over de kosten daarvan is nauwelijks publieke verontwaardiging, politieke controle blijft nagenoeg uit. Ondertussen wakkeren softwarebeveiligingsbedrijven via de media, met eigen 'onderzoeksrapporten', de angst voor virussen en aanvallen van hackers aan. De strekking: de digitale apocalyps nadert als er nu niet flink geïnvesteerd wordt.

De onderbouwing van die commercieel gemotiveerde berichtgeving is op zijn zachtst gezegd niet altijd even duidelijk. Een voorbeeld: onlangs stelde softwarebeveiliger Gemalto dat maar liefst 52,4 miljard dollar (44,2 miljard euro) aan beurswaarde verdampt zou zijn bij 65 getroffen bedrijven na het publiek worden van datalekken. Uit wetenschappelijk onderzoek blijkt echter dat het effect van datalekken op de beurswaarde zeer marginaal is. Op de korte termijn is de impact zo'n 1 à 2 procent van de marktwaarde. Een blijvend effect is niet aangetoond.

Desalniettemin worden de gebeden voor meer investeringen verhoord. Bijvoorbeeld door de overheid. Rutte III maakt maar liefst 95 miljoen euro extra per jaar vrij voor cybersecurity. En dat is nog maar het topje van de ijsberg. De grootste uitgaven vinden plaats binnen de bestaande ICT-budgetten van de ministeries. Het woord 'cybersecurity' wordt wel zes keer genoemd in het regeerakkoord. Of de kosten in verhouding staan tot de baten - daarover geen woord.

Doorgaans geen kwestie van leven en dood

Natuurlijk, een kosten-batenanalyse is niet altijd even realistisch. Denk aan uitgaven voor cyberdefensie, nodig om mee te kunnen doen aan de 'digital arms race'. Het Defensie Cyber Commando, onze digitale strijdkracht, pareert dagelijks aanvallen uit Rusland, Iran en China. Als we een tank kopen, berekenen we ook niet hoeveel euro's in veiligheid we ervoor terugkrijgen. Maar in tegenstelling tot wat graag gesuggereerd wordt, is cybersecurity doorgaans geen kwestie van leven en dood. Veelal zijn de gevolgen van cyberaanvallen gemakkelijk te beperken, zeker voor organisaties die basale regels in acht nemen, zoals het updaten van computers. Petya, het virus dat deze zomer meer dan 100.000 computers infecteerde, had met een simpele Windowsupdate grotendeels gepareerd kunnen worden. De truc is dan om nuchter de totale veiligheidskosten (de som van investering vooraf en de schade achteraf) te minimaliseren. Helaas grijpt de cybersecurityindustrie deze aanvallen juist aan om te pleiten voor extra investeringen.

Dit is zorgwekkend. De kosten hiervoor zullen de komende jaren exponentieel stijgen vanwege nieuwe digitaliseringsgolven, zoals 'internet of things', kunstmatige intelligentie en robotisering. Dat vraagt om een publiek en politiek debat over de hoeveelheid sloten die we op onze digitale deuren willen. Een debat dat moet beginnen bij de investeringen van de overheid zelf, omdat die uit de gemeenschappelijke middelen komen.

Lees ook: **'Nederland geeft niet genoeg uit aan cyberbeveiliging'**

De uitgangspositie van de overheid hierin is lastig. Waar ze in de beheersing van zorgkosten een scheidsrechter is in de relatie farmaceut-burger, daar is ze bij cyberveiligheid direct afhankelijk van de fabrikant. Helemaal als er al een aanval gaande is, verzwakt dat de onderhandelingspositie. Beveiligers kunnen hun informatievoordeel dan maximaal uitspelen en de hoofdprijs vragen.

Toch zou de overheid deze beveiligers hetzelfde moeten behandelen als farmaceuten en eisen dat de kosten in verhouding staan tot de baten. De extra middelen voor cybersecurity dienen daarom aangewend te worden voor kennis over digitale kosten en baten. Zo kunnen we het rendement bepalen en angstzaaiende beveiligers van repliek dienen.