Slimme cybersecurity-strategie: een kwestie van keuzes maken

De cyberonveiligheid neemt naar verwachting toe en onze afhankelijkheid van digitale systemen groeit. De kosten voor effectieve maatregelen dreigen daardoor de pan uit te rijzen. We hebben een slimmere cybersecuritystrategie nodig, zegt Bernold Nieuwesteeg van Erasmus University Rotterdam.

tekst Lynsey Dubbeld

Een datalek is net als griep: iedereen krijgt er wel een keer mee te maken. Daarom kunnen we de meldingen van datalekken maar beter openbaar maken, zegt *Bernold Nieuwesteeg*, directeur van het Centre of the Law and Economics of Cyber Security van Erasmus University Rotterdam. “Bedrijven kunnen zelf open zijn over lekken, los van de meldplicht. Daarnaast werkt het systeem van de meldplicht datalekken nu niet goed. De meldingen komen binnen bij de Autoriteit Persoonsgegevens. Het is vreemd dat er verder geen onderzoek naar wordt gedaan. De informatie verdwijnt nu in een digitale bureaulade, terwijl de meldingen informatie opleveren over waar kwetsbaarheden liggen, welke trends zich voordoen en hoe veiligheidsmaatregelen werken.”

KENNIS VERSPREIDEN

Volgens Nieuwesteeg, die in 2018 promoveerde op het proefschrift *De rechtseconomie van cybersecurity*, is onderzoek naar effectieve maatregelen hard nodig. “Ik verbaasde me er tijdens mijn promotie-onderzoek over dat er bij de ontwikkeling van cyberwetgeving heel weinig wordt nagedacht over de effecten van juridische maatregelen en interventies. Je kunt wel iets op de tekentafel bedenken, zoals bij de Algemene Verordening Gegevensbescherming (AVG) is gebeurd, maar wat gebeurt er uiteindelijk in de praktijk met de regels?”

Ook in de cybersecurity-industrie wordt maar weinig aan effectmetingen gedaan, vindt Nieuwesteeg. “Neem maatregelen zoals een *awareness*-training of een penetratietest. Er is heel weinig kennis over wat die precies bereiken. De markt van dit soort diensten is vaak ook lastig te vatten. Na een hack schakelt een organisatie een beveiligingsbedrijf in om de schade op te lossen. Dan wordt er niet zo snel nagevraagd wat de oplossing voor de langere termijn betekent. Daarom is het slim om kennis over effectieve maatregelen breed te verspreiden.”

SLIM INVESTEREN

Door ontwikkelingen in bijvoorbeeld ransomware, DDoS-aanvallen en datalekken neemt de cyberonveiligheid in ons land naar verwachting alleen maar toe. Daarom is slim investeren een must, waarschuwt Nieuwesteeg. “Je ziet nu grofweg twee soorten houdingen. Aan de ene kant heb je de bijna apathische bedrijven en burgers die een lage *awareness* hebben en vrijwel niets doen aan security. Aan de andere kant van het spectrum staan bedrijven die – meestal nadat ze een hack hebben meegemaakt – uitzonderlijk veel maatregelen nemen. Het ideaal zou zijn dat we ergens in het midden tussen deze twee uitersten uitkomen.”

“Investeren in beveiliging is prima, maar vervolgens moeten we wel kritisch kijken naar de baten van maatregelen”, licht Nieuwesteeg toe. “Je kunt een euro

→

maar één keer uitgeven, dus wil je dat een investeringskeuze het juiste effect heeft. Dan is het zorgelijk dat niemand precies kan uitleggen wat bijvoorbeeld een penetratietest oplevert. Alleen al vanuit de theorie zijn er vraagtekens bij te zetten. Er zijn letterlijk honderden manieren om een bedrijf digitaal binnen te komen, dus hoeveel zegt een test over een of twee van die manieren dan precies over de concrete risico's?"

CYBERVERZEKERING

Nieuwesteeg beschrijft in zijn proefschrift oplossingsrichtingen om slimmere investeringen in cybersecurity mogelijk te maken. "De kernopgave is: hoe kunnen we tot een systeem komen waarmee organisaties zelf de effectiviteit van maatregelen beoordelen – en hoe kunnen we de kennis daarover delen met alle betrokken partijen?"

Nieuwesteeg noemt het voorbeeld van de cyberverzekering. "Verzekeraars hebben er baat bij om te weten welke maatregelen effectief zijn, zodat ze verzekerden kunnen aansporen om te investeren in de juiste preventie. Op het gebied van inbraken en branden weten we daar al veel over, maar cyberverzekeringen komen nog maar mondjesmaat van de grond. Een analyse van de meldingen van datalekken zou daarvoor bruikbare inzichten kunnen opleveren."

Nieuwesteeg ziet ook kansrijke juridische oplossingen om cybersecurity te verbeteren, zoals de AVG, die organisaties verplichtingen oplegt om risico's te analyseren en om passende organisatorische en technische beveiligingsmaatregelen te nemen. "De uitvoering van de vereisten van de AVG staat pas in de kinderschoenen – daar is nog veel winst te behalen. De komst van de verordening is een goede stap om het bewustzijn van risico's van datalekken te vergroten en inzicht te krijgen in maatregelen die werken. Maar we moeten daar echt van leren en zo nodig bijsturen. Je ziet nu al negatieve neveneffecten, zoals organisaties waarin een cultuur van afvinklijstjes ontstaat in plaats van dat er goed wordt nagedacht over wat veilig is."

SLIMME STRATEGIE

"Het hoofddoel van een slimme cyberstrategie is om ons te wapenen tegen cyberaanvallen", zegt Nieuwesteeg over de werkwijze die hij bepleit. "Maar we moeten ook nadenken over hoeveel sloten we eigenlijk op onze digitale deuren willen en tegen welke prijs. Vergelijk het met de gezondheidszorg: we vinden goede zorg superbelangrijk, maar er zijn toch grenzen aan wat we er als samenleving aan willen uitgeven."
Wat een goede investering is, is afhankelijk van het specifieke geval, geeft Nieuwesteeg toe. "Maar je zou misschien wel iedereen die met de meldplicht datalekken te maken heeft, een cursus stressmanagement moeten geven. We weten uit talloze onderzoeken dat mensen onder stress de verkeerde beslissingen nemen. Als je na een hack keuzes moet maken over nieuwe maatregelen, dan moet je oppassen dat je niet de volledige menukaart bestelt."

BASISNIVEAU

Bij het ontwikkelen van een slimme cyberstrategie ziet Nieuwesteeg een rol voor de overheid, het bedrijfsleven én de wetenschap. "De overheid kan kennis delen

Bernold Nieuwesteeg (links): "We moeten nadenken over hoeveel sloten we eigenlijk op onze digitale deuren willen en tegen welke prijs."

Een datalek is net als griep.

over effectieve maatregelen. Er wordt op dit moment nog niet echt geleerd van informatie over bijvoorbeeld hacks. De getroffen organisatie leert misschien van de ervaring, maar we zouden op grote schaal data moeten verzamelen over incidenten. Dan kan je uiteindelijk scenario's bedenken die organisaties helpen om te kiezen welke maatregelen in hun situatie het beste werken. Daarmee kan de organisatie bepalen wanneer het redelijke is gedaan om incidenten te voorkomen. Iedereen gaat onvermijdelijk een keer gehackt worden, maar dat vooruitzicht mag ons niet weerhouden om aan een basisniveau van beveiliging te werken."

RESTRISICO'S ACCEPTEREN

"Het einddoel is dat organisaties grosso modo weten wat ze nodig hebben om aan een basisniveau van cybersecurity te voldoen, en dat we die kennis delen met overheid, bedrijfsleven en wetenschap," zegt Nieuwesteeg over de samenwerking die hij voor de toekomst ziet. "Bij een complexe transactie zoals een huizenverkoop kan je een makelaar inschakelen, maar zo'n soort onafhankelijke partij ontbreekt in het domein van cybersecurity."

Nieuwesteeg waarschuwt dat cyberrisico's niet tegen alle kosten moeten worden bestreden. "Je gaat ook niet naar de huisarts en zegt: ik wil de komende tachtig jaar gezond blijven. Je wilt niet doodgaan, maar een griepje ga je zeker een keer krijgen. Bij cybersecurity zijn we geneigd om alle risico's te willen uitbannen. Maar dat lukt nooit. We zullen als samenleving een zeker restrisico moeten accepteren."

Nieuwesteeg ziet nog volop kansen voor nieuw, wetenschappelijk onderzoek naar cybersecurity. "We willen bijvoorbeeld de mechanismen bekijken die ten grondslag liggen aan *pooling*, het onderling delen van risico's. We kunnen dan ook nieuwe werkwijzen ontwikkelen en evalueren. Door de Europese Unie worden steeds vaker *impact assessments* uitgevoerd. Dat zijn positieve signalen, maar juist bij cybersecurity kan je naast veldwerk ook kwantitatief onderzoek doen. Daarmee kunnen we nieuwe inzichten opdoen over digitale dreigingen én over manieren om onze weerbaarheid daartegen te verbeteren." ■

Lynsey Dubbeld is communicatieadviseur, trendanalist, contentstrateeg en copywriter

'HET EINDDOEL IS DAT ORGANISATIES WETEN WAT ZE NODIG HEBBEN OM AAN EEN BASISNIVEAU VAN CYBERSECURITY TE VOLDOEN'