DOOR WOLTER PIETERS & BERNOLD NIEUWESTEEG

Verzekeringsprofessionals over de trends in hun vakgebied.

‘CYBERMARKT MOET GROEIEN OM MKB WEERBAARDER TE MAKEN’

CYBERVEILIGHEID STAAT STEEDS HOGER OP DE AGENDA VAN DE NEDERLANDSE OVERHEID EN HET BEDRIJFSLEVEN. ZO WAARSCHUWDE ONLANGS DE NATIONAAL COÖRDINATOR TERRORISMEBESTRIJDING EN VEILIGHEID DAT ER IN DE VADERLANDSE COMPUTERSYSTEMEN NOG TE VAAK ACHTERDEURTJES ZITTEN. EEN BEKEND VOORBEELD ZIJN DE CYBERAANVALLEN WANNACRY EN PETYA. VORIG JAAR ZOMER LIETEN DIE AANVALLEN ZIEN DAT CYBERCRIMINELEN SUBOPTIMALE VEILIGHEID AFSTRAFFEN MET GROTE (MAATSCHAPPELIJKE) SCHADE ALS GEVOLG.

Wolter Pieters is associate professor cyber risk aan de TU Delft

Bernold Nieuwesteeg is onderzoeker law & economics of cyber security aan de Erasmus Universiteit Rotterdam

De vraag welke cybersecurity-maatregelen je als organisatie zou moeten implementeren is volgens Wolter Pieters, cyberriskhoogleraar aan de TU Delft, geen gemakkelijke. “Waar de medische wereld werkt op basis van hard bewijs, kijken we in de beveiligingswereld toch vooral naar wat de buren doen. Zo zien we allemaal sterretjes als we onze wachtwoorden intypen, maar of het daadwerkelijk problemen voorkomt, weten we niet. Als we een vast budget hanteren kunnen we wel wat security-maatregelen bedenken die binnen dat budget passen, maar als we willen vaststellen hoe veel we eigenlijk zouden moeten investeren om ons risico tot een aanvaardbaar niveau te reduceren, dan zitten we met onze handen in het haar.

In deze context zou cyberinsurance een goed alternatief kunnen zijn. In plaats van zelf investeringsbeslissingen te nemen dek je je voor een vast bedrag in tegen de gevolgen van incidenten. Maar dezelfde vraag komt weer terug door de achterdeur: wanneer is het een goed idee om zo’n verzekering af te sluiten? En wanneer kan ik beter zelf maatregelen nemen? Of is een combinatie handig?

VOOROORDELEN

Er is nog te weinig bekend over hoe organisaties dit soort beslissingen nemen. We weten dat mensen gevoelig zijn voor allerlei soorten vooroordelen bij het nemen van beslissingen. Zo zijn we meer geneigd te ‘gokken’ als het over verlies gaat, en hebben we bij winst juist liever zekerheid. Maar in hoeverre geldt dit ook voor securityprofessionals?

Kennis over deze beslissingen is belangrijk om beleid te kunnen maken rond cyberinsurance. Als de beschikbaarheid van verzekeringen ertoe zou leiden dat niemand meer investeert in security, dan geven we cybercriminelen de vrije hand. Aan de andere kant kunnen verzekeraars juist ook bijdragen aan betere beveiliging door premies te koppelen aan beveiligingsniveaus, en door bepaalde zaken wel of niet te vergoeden. Ook kunnen ze advies geven op basis van de informatie die zij kunnen verzamelen over de effectiviteit van maatregelen.

GEDRAGSMODELLEN

Het CYBECO-project onderzoekt cyberinsurance vanuit het perspectief van gedragsmodellen. Hierbij kijken we naar het gedrag van verschillende partijen, en de invloed daarvan op de strategieën van anderen. Ten eerste bepaalt het gedrag van cyberaanvallers welke combinatie van maatregelen (inclusief insurance) voor een organisatie het beste is. Ten tweede bepaalt het investeringsgedrag van organisaties weer wat het beste

‘WE ZIJN MEER GENEIGD TE GOKKEN ALS HET OVER VERLIES GAAT EN WE HEBBEN BIJ WINST JUIST LIEVER ZEKERHEID’

‘GENOEG REDENEN VOOR CYBERVERZEKERAARS OM DE MARKT TE BETREDEN: ER ZIJN KANSEN VOOR NIEUWE BUSINESS EN MAATSCHAPPELIJKE BATEN’

beleid is voor beleidsmakers, als zij een betere beveiliging nastreven.”

ZWAKSTE SCHAKEL

Volgens Bernold Nieuwesteeg begint het cyberrisico voor veel organisaties al een dusdanige proportie aan te nemen dat een cyberverzekering een slimme keuze kan zijn. Hij promoveerde onlangs aan de Erasmus Universiteit op het onderwerp Law and Economics of Cybersecurity. “Met name voor grote organisaties is de markt voor cyberverzekeringen al relatief sterk ontwikkeld. Deze organisaties hebben vaak al de mogelijkheid om ‘op maat’ cyberverzekeringen aan te schaffen als onderdeel van hun intensieve relatie met verzekeraars. Er is echter nog een onvoldoende aantrekkelijk verzekeringsaanbod voor de markt voor cyberverzekeringen voor het midden- en kleinbedrijf (mkb).

Vanuit maatschappelijk oogpunt is het belangrijk dat mkb’ers hun cyberrisico goed managen en dat daar instrumenten, zoals een cyberverzekering, voor zijn. Cyberveiligheid wordt grotendeels bepaald door de zwakste schakel. En die zwakste schakel komt relatief vaak uit de hoek van het midden- en kleinbedrijf, omdat deze organisaties als vanzelfsprekend niet de personele capaciteit en middelen beschikbaar hebben om monitoring, detectie en beveiligingssystemen voor hun netwerk op maat te maken. Bovendien hebben mkb’ers soms onvoldoende inzicht in cybergerelateerde risico’s. Als klap op de vuurpijl kan een gehackte mkb-ondernemer ook gebruikt worden om bijvoorbeeld DDoS-aanvallen uit te voeren op burgers, overheden en grotere bedrijven.

TWIJFEL

Genoeg redenen dus voor de cyberverzekeraars om de markt te betreden: er zijn kansen voor nieuwe business en maatschappelijke baten. Uit onderzoek naar de markt voor cyberverzekeringen, blijkt echter dat verzekeraars lijken te twijfelen. Gaan zij voor marktaandeel of betreden ze de markt voorzichtiger om geen slachtoffer te worden van de potentieel sterk correlerende schadeclaims? Het is in ieder geval duidelijk dat op dit moment een kernfunctie van de cyberverzekeringsmarkt nog onvoldoende functioneert. Het schort aan informatie-overdracht van ‘best practices’ gerelateerd aan het rendement van cybersecurity-investeringen om weerbaarder te zijn tegen cyberaanvallen. Om het simpeler te zeggen: heel weinig cyberverzekeringen stellen daadwerkelijk eisen aan de verzekerde waarmee deze ‘gedwongen’ wordt zijn cyberveiligheid te verbeteren. Terwijl verzekeraars nou juist bij uitstek voor een soort van cybersecurity-APK zouden kunnen zorgen.

BASISCYBERVERZEKERING

Daarmee heeft de cyberverzekeringsmarkt haar volledige potentieel nog niet benut en dit rechtvaardigt verder onderzoek om groeimogelijkheden te verkennen. Een paar voorzetten. Men zou kunnen overwegen om de aanvraagprocedure te vereenvoudigen. Hierdoor kost het voor mkb’ers minder tijd en geld om verschillende offertes aan te vragen. Ten tweede zou een basiscyberverzekering overwogen kunnen worden, een initiatief waar nu al over nagedacht wordt. Ten derde zouden cyberverzekeraars meer kennis, zoals bijvoorbeeld claimdata, kunnen delen. Zo kunnen we een markt laten groeien en Nederland weerbaarder maken tegen cyberaanvallen.” ■

‘MAAK HET TASTBAAR’

Dit vakartikel schreven wetenschappers Wolter Pieters en Bernold Nieuwesteeg onder andere aan de hand van input van lezers van amweb. Op onze website riepen we u op mee te denken over de vraag waar een goede cyberverzekering aan moet voldoen en hoe zo’n polis aantrekkelijker kan worden voor het mkb. De belangrijkste reacties: “Als je als adviseur voorbeelden van cyberschade kunt laten zien, wordt de urgentie hoger”, aldus een inzender. “Het risico moet gaan leven”, bevestigt een ander. “Maak het tastbaar door het dichtbij te laten komen.”