Auteurs: Drs. M. (Marko) van Leeuwen en W. (Wouter) Wissink MSc. Marko van Leeuwen is senior beleidsadviseur bij het Verbond van Verzekeraars en Wouter Wissink is Senior Principal Cyber Engineer namens het Verbond van Verzekeraars.

Risicoklassenindeling digitale veiligheid gelanceerd

De coronacrisis heeft eens te meer duidelijk gemaakt dat verdere digitalisering van onze samenleving onvermijdelijk is. Ook is duidelijk dat het inschatten van cyberrisico's ingewikkeld is en het verzekeren ervan voor veel bedrijven en burgers niet vanzelfsprekend. Met de ontwikkeling van een 'risicomodel cyber' willen publieke en private partijen hierin gezamenlijk verandering brengen. Begin 2021 heeft het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) daarom de Risicoklassenindeling Digitale Veiligheid gelanceerd (1) , gebaseerd op de bij verzekeraars ingeburgerde 'VRKI-methodiek'.

Naast een objectief oordeel over het niveau van cyberrisico van een (mkb-)onderneming, biedt het instrument inzicht in de bijpassende beheersmaatregelen. Dit artikel schetst het belang en de werking van het instrument.

Particulieren en bedrijven ondervinden steeds meer hinder van cyberincidenten, een verzamelnaam voor falende systemen, maar ook vandalisme en criminaliteit zoals diefstal of afpersing. Cyberincidenten kunnen op verschillende manieren tot schade leiden. Systemen kunnen onbruikbaar worden en criminelen kunnen gegevens misbruiken voor geld of om te frauderen. Bedrijven lopen het risico dat hun operationele continuïteit in gevaar komt of dat ze klanten kwijtraken. Doordat ze bijvoorbeeld niet bereikbaar zijn of omdat gegevens op straat zijn komen te liggen. Steeds vaker ook worden systemen gegijzeld voor losgeld.

De toenemende digitalisering is ook zichtbaar in de criminaliteitscijfers; daar waar in algemene zin de offline criminaliteit gestaag daalt, neemt de online criminaliteit toe en is dit ook een vast onderdeel geworden in de opsporing door de politie. De politie roept daarom bedrijven op om altijd aangifte te doen (zie kader Melding of aangifte van incidenten).

Verzekeren van cyberrisico's niet vanzelfsprekend

Ook verzekeraars worstelen met cyberrisico's bij en cyberveiligheid van hun klanten. Het verzekeren van cyberrisico's is nog altijd verre van vanzelfsprekend. Voor een deel komt dit doordat het bewustzijn van deze risico's onder burgers en bedrijven wel toeneemt, maar nog altijd laag is, overheidscampagnes ten spijt. Ook komt het voor dat mensen of organisaties denken dat schade door cybercrime wordt gedekt door bestaande verzekeringen, de zogenaamde 'stille' cyberdekking, terwijl dat meestal niet of hooguit zeer beperkt het geval is. Tegelijkertijd is het aanbod van cyberverzekeringen nog relatief klein.

De modus operandi van criminelen en daarmee het risico verandert zeer snel en net als bij terrorisme en natuurrampen zijn cyberrisico's voor individuele verzekeraars en de verzekeringsbranche moeilijk in te schatten. De meeste 'traditionele' verzekeringsproducten bieden hooguit beperkte dekking voor de gevolgen van cyberrisico's. Verzekeraars willen hun (zakelijke) klanten ook oplossingen bieden voor cyberrisico's en bieden inmiddels cyberverzekeringen aan.

Het betreft hier vrijwel zonder uitzondering zogenaamde 'totaalpakketten', waarin verzekeraars vooraf risico's scannen, preventieve maatregelen adviseren, (technische, juridische, forensische) hulp bieden tijdens en na een incident en de financiële gevolgen van het restrisico verzekeren. Het Centrum voor Verzekeringsstatistiek van het Verbond van Verzekeraars becijfert het totale premievolume van cyberverzekeringen in Nederland in 2019 op 'slechts' 17 miljoen euro, tegen 2,3 miljard dollar in de Verenigde Staten. Hoewel het premievolume langzaam toeneemt en Nederland het in vergelijking met andere Europese landen zo slecht nog niet doet, blijven de absolute en relatieve aantallen klein. Zeker gezien de dichte IT-infrastructuur in ons land. Het Centraal Planbureau concludeert in het rapport *Risicorapportage cyberveiligheid economie 2019* (2) dat gebrek aan inzicht in kosten en baten van cyberveiligheid een belemmering is voor de ontwikkeling van een verzekeringsmarkt voor cyberrisico's.

Risicoklassenindeling

'Keurmerk voor een veilig internet is hard nodig', kopte het Financieele Dagblad in de zomer van 2017. Volgens Het FD werden er destijds wereldwijd per minuut tachtig apparaten aangesloten op het internet, maar kwamen deze onbeveiligd onze huiskamer of ons kantoor binnen. Nu, vijf jaar later is dit nauwelijks verbeterd. Ook onder verzekeraars en IT-beveiligingsbedrijven bestaat de behoefte aan een instrument om eenduidig en objectief de cyberrisico's van hun klanten te bepalen en te koppelen aan gepaste maatregelen. De Risicoklassenindeling helpt bedrijven om cybersecurityrisico's in te schatten en maatregelen te treffen.

Het instrument richt zich in eerste instantie op het midden- en kleinbedrijf (mkb), maar is ook voor andere bedrijven bruikbaar. Vertrekpunt is de impact van een cyberincident op de bedrijfscontinuïteit. Het gaat vervolgens om het vergroten van het bewustzijn en het op orde brengen van de basis van digitale beveiliging van ondernemingen.

Op basis van elf vragen, zoals vastgelegd in de *Scorekaart risico's digitale veiligheid*, wordt het risico van de mkb-onderneming op een cyberincident bepaald. De scores vertalen zich in vier risicoklassen en per risicoklasse is een set van beveiligingsmaatregelen opgesteld. Deze sluiten aan op de basisprincipes van het Digital Trust Center (3). Naast technische maatregelen gaat het ook om organisatorische maatregelen, want veel risico's ontstaan juist door menselijk handelen of falen. Net als in de fysieke wereld is een driesterrenslot immers alleen effectief als je dat bij het verlaten van het pand ook echt op slot doet. Datzelfde geldt voor de cyberwereld. Computers, tablets, telefoons en alle andere apparaten die inmiddels op het internet zijn aangesloten, zijn alleen goed beschermd als er een deugdelijke firewall is ingeschakeld en wachtwoorden goed zijn en ook goed kunnen en worden beheerd.

Door cyberrisico's objectief te koppelen aan beveiligingsmaatregelen kunnen bedrijven gericht hun IT-/securitybeleid aanpassen, medewerkers instrueren en eventueel samen met hun leveranciers gepaste beschermingsmaatregelen treffen. Dat laatste is belangrijk

omdat een goed en objectief gevalideerd handelingsperspectief veelal nog ontbreekt. Ondernemers die hun cyberrisico's willen beheersen moeten kunnen vertrouwen op bestaande (gecertificeerde) normen en procedures. Zij moeten hierin immers tijd en geld investeren.

Certificeringsregelingen

Cybersecuritydiensten zorgen voor een goede beveiliging van digitale systemen, die aansluiten op het risico van een cyberincident. Een onderneming die zich wil beschermen tegen cybercriminaliteit, wil dat dit goed gebeurt, met veilige producten en geïnstalleerd of uitgevoerd door een vakman. Voor een ondernemer is dit vaak moeilijk zelf goed in te schatten. Certificatieschema's van cybersecuritydiensten bieden hiervoor een goede oplossing. In het kader van de Risicoklassenindeling is als eerste een certificatieschema ontwikkeld voor pentesten. De komende periode wordt onderzocht voor welke andere instrumenten het wenselijk en haalbaar is om een certificatieschema te ontwikkelen.

Publiek-private samenwerking

De Risicoklassenindeling Digitale Veiligheid en de bijgaande certificeringsregeling zijn via publiek-private samenwerking tot stand gekomen, onder regie van het CCV. Gezien het maatschappelijk belang en de rol die met name het Digital Trust Center speelt, is de ontwikkeling van het instrumentarium door de overheid gefinancierd. De deelnemende organisaties en bedrijven (zie kader Publiek-private samenwerking) hebben belangrijke bijdrages geleverd. Samen vormden ze ook de stuurgroep van het project. Sinds 1 januari 2021 bemensen ze het College van Belanghebbenden, dat de uitvoering en de verdere ontwikkeling van het instrumentarium begeleidt. Naast het delen van kennis, biedt deze brede coalitie draagvlak en objectiviteit.

Conclusie

Met de Risicoklassenindeling Digitale Veiligheid is er voor verzekeraars, verzekeringsadviseurs, IT-/securityspecialisten en hun (mkb-) klanten een instrument beschikbaar gekomen om digitale risico's objectief in kaart te brengen en te koppelen aan gepaste beveiligingsmaatregelen. Dit vergroot de verzekerbaarheid van cyberrisico's.

Het digitale landschap verandert snel, waardoor onderhoud en mogelijk ook de ontwikkeling van een nieuwe certificeringsregeling nodig zal zijn. Ook voorziet het instrument vooralsnog niet in een mechanisme voor het controleren en aantoonbaar maken van hetgeen klanten invullen via de Scorekaart. Verzekeraars kunnen hieraan in hun eigen voorwaarden eisen stellen, bijvoorbeeld door te vragen om het formulier te ondertekenen of anderszins van waarborgen te voorzien.

Melding of aangifte van incidenten

Net als bij andere vormen van criminaliteit is het wenselijk dat ondernemers incidenten niet alleen melden bij hun IT-/security-adviseur en eventueel verzekeraar, maar dat ze ook aangifte doen. Hoewel opsporing bij cyberincidenten moeilijk is, ondersteunt het doen van aangifte het opsporingsproces meer in algemene zin. Minister Grapperhaus schrijft hierover (Tweede Kamer, vergaderjaar 2019–2020, 26 643, nr. 678): *'Door aangifte kunnen politie en justitie passende maatregelen nemen. Aangifte draagt daarnaast bij aan het brede inzicht in de aard en de omvang van deze vorm van criminaliteit waardoor ook op langere termijn een betere aanpak kan worden ontwikkeld en passende preventieve maatregelen kunnen worden genomen.'*

Publiek-private samenwerking

De ontwikkeling van de Risicoklassenindeling Digitale Veiligheid is een samenwerking tussen het CCV, het Verbond van Verzekeraars, VNO-NCW/MKB-Nederland, Cyberveilig Nederland, NLdigital, Politie, CIO Platform Nederland, Partnering Trust, het ministerie van Justitie en Veiligheid en het ministerie van Economische Zaken en Klimaat. Deze partijen vormen ook het College van Belanghebbenden. Het project is mogelijk gemaakt door de belangeloze medewerking van genoemde partijen en financiering door de ministeries. De Risicoklassenindeling Digitale Veiligheid is online beschikbaar op www.digitaltrustcenter.nl/risicoklasse.

Referenties

(1) https://hetccv.nl/nieuws/nieuw-instrument-gelanceerd-om-cyberweerbaarheid-ondernemers-te-vergroten
(2) https://www.cpb.nl/sites/default/files/omnidownload/cpb-notitie-risicorapportage-cyberveiligheid-2019.pdf.
(3) https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen