Huisartsen en cyberverzekeringen. Niet zo simpele materie als het lijkt

Op 18 december 2020 vroeg de Landelijke Huisartsen Vereniging(LHV) in een ledenbrief per email aandacht voor cyberverzekeringen. Daarmee reactiveerde men een artikel op de website van de LHV van 30 september 2020 met de kop: "Beveiligingsrisico's verminderen en verzekeren". Met het toenemende aantal hacks en door ransomware gegijzelde ICT-systemen zullen cyber-calamiteiten bij huisartsen geen uitzonderingen gaan vormen. Problematisch is daarbij dat in de huisartspraktijken in Nederland er niet sprake is van een eenduidige inrichting van ICT-zaken, met een veelvoud van manieren om uiteindelijk allemaal hetzelfde te doen. Dat is zorg leveren aan de patiënt op een bedrijfsmatige manier. Bij uitval door een cyberincident is er sprake van een organisatorische en praktische ramp die zo spoedig mogelijk verholpen moet worden. Uiteraard met inschakeling van specialisten. Bij uitval kan men terugvallen op ouderwets pen en papier, maar een cyberverzekering kan behulpzaam zijn bij het snel verhelpen van de blokkade.

Ingewikkeld ICT-landschap

In de huisartsenzorg is er geen eenduidig ICT-landschap. Niet alleen zijn er acht verschillende huisarts informatiesystemen(HIS-sen). Ook de manier waarop men met die systemen werkt kent meerdere vormen. Zo hebben sommige praktijken een eigen server. Soms werken meerdere praktijken op een lokale/regionale server in eigen beheer. Daarnaast zijn er praktijken die het HIS via een ASP-verbinding bij een ICT-leverancier hebben draaien. Tenslotte bestaat ook de

mogelijkheid van het werken met Software As A System(SAAS). In die constructie is er software die als een online dienst wordt aangeboden. De klant hoeft de software niet aan te schaffen, maar sluit bijvoorbeeld een contract per maand per gebruiker af, eventueel in combinatie met andere parameters. Door al deze variabelen is er ook sprake van verschillen in verantwoordelijkheden van partijen waar de huisarts voor de ICT van afhankelijk is. Bij afname van een ASP/SAAS-constructie is de verantwoordelijkheid een gedeelde van praktijkhouder en leverancier.

Waaraan denken bij cyberverzekering?

Een cyberverzekering beschermt tegen de gevolgen van hacking, systeeminbraak, verloren data, gegevensdiefstal en andere vormen van cybercriminaliteit. Inclusief 24/7 hulp bij cyberincidenten. Verschillende markpartijen zijn actief op dit vlak. Opvallend is dat daarbij de naam Hiscox direct of indirect valt. Zo biedt Nationale Nederlanden een dergelijke verzekering aan die ze bij doorlezen van Hiscox blijken te betrekken. Ook MKB-bedrijfsverzekeringen blijkt gebruik te maken van Hiscox. De polisvoorwaarden zijn op het internet ook te vinden. Het is zinvol die een keer van A tot Z door te lezen.

Voorwaarden

Een cyberverzekering kent nogal wat bepalingen. De polis van Hiscox is 24 pagina’s lang. Men betaalt premie maar er bestaat ook een fors eigen risico. Daarnaast geldt een retentietijd. Dat is het aantal uren zoals vermeld in de polis dat voor uw eigen rekening blijft wanneer uw internetactiviteiten waarmee u uw inkomsten genereert, voortdurend worden onderbroken of ernstig worden belemmerd. De retentietijd begint pas als melding van de onderbreking of de belemmering aan de verzekeraar. In het geval van MKB-bedrijfsverzekeringen zijn dat tien uren. Dat betekent dat als de verzekeraar in staat is

de problemen binnen die tijd op te lossen er geen uitkering plaats vindt.

Bereddingsplicht

Daarnaast staat in zo'n polis een zeer belangrijk, maar wel kort vermeld item over de eigen bereddingsplicht van de verzekerde. Die dient alle maatregelen te nemen ter voorkoming of vermindering van schade of dreigende schade als bedoeld in artikel 7:957 BW (bereddingsplicht). Dat houdt in dat als de bedrijfsonderbreking door een cyberincident het gevolg is van het zelf niet nemen van goede voorzorgen er geen uitkering zal volgen. Daarbij moet je denken aan het hebben van een goede firewall, goede antivirusmaatregelen, vastgelegde instructies aan personeel ter voorkomen van openen van phishing mail etc. Onder de bereddingsplicht valt ook het tijdig installeren van updates van besturingssystemen en functionerende bedrijfssoftware. Het niet tijdig installeren kan leiden tot kwetsbaarheden die buitenstaanders genadeloos kunnen afstraffen. Over de bereddingsplicht schreef ik eerder een artikel op 3 september 2019. Daarin een zeer interessant artikel van mr. Nynke Brouwer over "eigen schuld en beredding".

Tijdsduur

Ook is het goed te weten dat de verzekeraar soms een ander eindpunt van de verstoring op het oog heeft dan de verzekerde. Zo staat in de Hiscox-polis: "Onze vergoedingsplicht eindigt met ingang van het uur nadat uw internetactiviteiten **niet meer voortdurend onderbroken** of **ernstig belemmerd** zijn."(vet gedrukt door WJJ). Dit kan betekenen dat de verstoring niet volledig voorbij is(niet meer voortdurend onderbroken), maar toch uitermate hinderlijk kan zijn voor de bedrijfsvoering binnen een huisartsenpraktijk. Het kan betekenen dat de verbinding met een loco/regionale server, dan wel met ASP-server of SAAS-systeem haperend kan zijn terwijl de

verzekeraar dat normaal vindt.

Noodzaak

Los van de genoemde zaken in de “kleine letters” van de polis kan het toch uitermate verstandig zijn een cyberverzekering af te sluiten. Vaak is bij of via de verzekeraar expertise voorhanden waarover men zelf niet beschikt of die men zelf niet weet te vinden. Belangrijk is je niet rijk te rekenen als er in verzekerde toestand een cyberincident zich voordoet. Het zal altijd geld kosten, veel geld. En een hoop frustratie door de werkverstoring.

W.J. Jongejan, 31 december 2020

Afbeelding van Gerd Altmann via Pixabay