4.2 De aanschaf en ingebruikname van software door organisaties

Steeds meer processen in onze maatschappij en binnen organisaties vinden digitaal plaats. Hiermee neemt de afhankelijkheid van digitale systemen, en de software die deze systemen bevatten, toe voor zowel organisaties als voor de gehele samenleving. Omdat software altijd kwetsbaarheden zal bevatten, is het voor organisaties van belang om rekening te houden met de risico's die dit met zich meebrengt bij de aanschaf en het gebruik van software. De vragen die hier worden behandeld zijn: hoe gaan organisaties die software aanschaffen en gebruiken (we noemen dit verder 'afnemers'), zoals gemeenten, ziekenhuizen en bedrijven, om met de risico's bij de aanschaf en ingebruikname van software? Welke dilemma's en belemmeringen spelen hierbij een rol?

4.2.1 De verhoudingen op de softwaremarkt

Een aantal factoren belemmert de mate van risicobeheersing bij het aanschaffen van software met kwetsbaarheden. Dat blijkt uit interviews met organisaties. Eén van deze factoren is de verhouding tussen fabrikanten en afnemers op de softwaremarkt. Op de softwaremarkt is sprake van informatieasymmetrie.[151] Softwarefabrikanten hebben meer informatie over de samenstelling van producten dan afnemers. Voor een afnemer is de samenstelling en kwaliteit van software vaak niet te achterhalen. Dit komt doordat fabrikanten over het algemeen weinig transparant zijn over de opbouw van hun producten. Daarnaast hebben veel organisaties niet de juiste kennis en capaciteit om de informatie te kunnen beoordelen wanneer een fabrikant dit inzicht wel biedt.

Door deze informatieasymmetrie is het voor afnemers moeilijk om de kwaliteit en veiligheid van software te beoordelen. Hierdoor beoordelen afnemers producten voornamelijk op de elementen die zij wel kunnen controleren zoals prijs, functionaliteit en gebruiksgemak. Het gevolg hiervan is dat fabrikanten met elkaar concurreren op deze elementen, en dat het voor fabrikanten niet loont om te investeren in de veiligheid van hun producten. Er zijn geen wettelijke bepalingen die deze informatieasymmetrie compenseren door de aansprakelijkheid te verleggen van afnemer naar fabrikant.

Op de softwaremarkt zijn er enkele grote fabrikanten die de markt beheersen. Door de marktmacht van een aantal fabrikanten zijn er voor bepaalde functionaliteiten maar enkele producten beschikbaar van een selecte groep leveranciers, bijvoorbeeld bij besturingssystemen als Windows en macOS of kantoorsoftwarepakketten als Microsoft Office. Fabrikanten bieden veelal standaard pakketten aan en afnemers hebben weinig mogelijkheden om deze op eigen wensen of eisen af te stemmen. Dit komt doordat de softwaremarkt een wereldwijde markt is, waarbij het voor afnemers in Nederland alleen lastig is om hier invloed op uit te oefenen. Daar is een groter machtsblok voor nodig, bijvoorbeeld op EU of VN niveau of door gezamenlijke inspanning van afnemers.

Wanneer kwetsbaarheden worden ontdekt in softwareproducten, gaat de fabrikant aan de slag met het ontwikkelen van een patch voor de kwetsbaarheden. Dit kost de fabrikant middelen. Veel van de kosten en de risico's bij kwetsbaarheden worden gedragen door de afnemer van de software. De afnemer maakt kosten om systemen te mitigeren en te patchen. Bovendien maakt de afnemer ook kosten bij eventuele stilstand van de

151 Anderson, R. and Moore, T., The Economics of Information Security, *Science* 314, oktober 2006.

bedrijfsvoering bijvoorbeeld bij een aanval. Indien de afnemer verzekerd is voor cyberincidenten, vergoedt de verzekeraar in sommige gevallen een deel van de kosten die een afnemer maakt. Over het algemeen worden de risico's op schade door kwetsbaarheden in software hoofdzakelijk door de afnemer gedragen. Deze factoren samen maken dat de markt voor software door experts wordt gekenmerkt door de asymmetrische relatie tussen fabrikant en afnemer.[152]

4.2.2 De aanschaf van software

Een afnemer schaft software aan vanuit een functionele behoefte om werkzaamheden of processen op een digitale manier te kunnen afhandelen. Na het identificeren van deze functionele behoefte kijkt een afnemer welke mogelijkheden er allemaal in de markt zijn om in zijn behoefte te voorzien. Bij het selecteren van een product spelen verschillende wensen en eisen een rol, zoals de functionaliteiten van de software, gebruikersgemak, prijs en beveiliging.

Veiligheidseisen formuleren en daarop controleren

Zoals in paragraaf 4.1 besproken zijn er momenteel weinig manieren om fabrikanten te verplichten cybersecurity te borgen in hun producten. Dit legt een extra belasting bij de afnemers om bij de aanschaf van software op veiligheid te toetsen. Omdat er sprake is van informatieasymmetrie op de softwaremarkt (zie 4.2.1), schaffen afnemers software veelal aan op basis van een functionele behoefte, en spelen veiligheidsaspecten een kleinere rol.

Om de juiste veiligheidseisen te kunnen formuleren heeft de afnemer kennis nodig van wat relevante eisen zijn voor zijn situatie. Daarnaast heeft de afnemer ook informatie nodig over het product om te kunnen beoordelen in hoeverre het product aan die eisen voldoet en hoe dit te duiden voor zijn situatie. Wanneer een organisatie wel de juiste eisen kan stellen, maar deze niet kan controleren, is het immers niet mogelijk voor de organisatie om te beoordelen of de software daadwerkelijk aan de veiligheidseisen voldoet.

Er zijn veel verschillen te zien in de mate waarin organisaties veiligheidseisen stellen aan de softwareproducten die zij aanschaffen. Sommige, veelal grotere, organisaties hebben de juiste kennis in huis om eisen te stellen en deze ook te controleren. Een veel gestelde veiligheidseis is het mogen uitvoeren van penetratietesten.[153] Andere, meestal kleinere, organisaties lukt het niet om de juiste veiligheidseisen te stellen omdat zij de kennis en middelen hiervoor niet beschikbaar hebben, of het belang hiervan niet inzien. Fabrikanten laten ook niet altijd toe dat hun producten gepentest worden, omdat er ook risico's bij komen kijken. Wanneer penetratietesten bijvoorbeeld worden uitgevoerd op een cloud omgeving, bestaat het risico dat de test schade aanricht en de beschikbaarheid van de omgeving in het geding komt. Daarnaast is het bij het uitvoeren van penetratietesten of *reverse engineering*[154] mogelijk om erachter te komen hoe een softwareproduct opgebouwd is, en bijvoorbeeld details over een bepaald algoritme te achterhalen.

152 Anderson, R., *Security Engineering*, 2020.
153 Een pentest is een beveiligingscontrole waarbij er van buitenaf wordt getoetst op kwetsbaarheden en er vervolgens wordt geprobeerd om via deze kwetsbaarheden in te breken in het systeem. Zie hoofdstuk 2.
154 Reverse engineering is het onderzoeken van een product om de werking en opbouw hiervan af te leiden.

Vanwege de concurrentie op de markt geven fabrikanten deze informatie niet graag prijs. Fabrikanten stellen daarom vaak voorwaarden en beperkingen aan penetratietesten.

Het is dus niet vanzelfsprekend dat afnemers penetratietesten mogen uitvoeren op de software die zij gebruiken. Een manier waarop afnemers zeker kunnen stellen dat ze penetratietesten wel mogen uitvoeren, is door dit expliciet als eis op te nemen in het contract met de leverancier. Enkele organisaties gaven in interviews aan dat ze penetratietesten weliswaar als standaardeis in contracten opnemen, maar dat het soms overtuigingskracht kost in de onderhandelingen met leveranciers van producten. Grotere organisaties met een hogere cybervolwassenheid laten over het algemeen wel penetratietesten uitvoeren op hun systemen. Er zijn ook organisaties die bij het vinden van een kwetsbaarheid in software die in hun branche veel gebruikt wordt, deze kwetsbaarheid doorgeven aan de brancheorganisatie zodat deze de kwetsbaarheid namens alle aangesloten organisaties kan aankaarten bij de fabrikant van het product.

Hoewel het stellen van veiligheidseisen en het controleren hiervan dus niet standaard gebeurt, zijn er wel voorbeelden van bepaalde sectoren waarin afnemers verplichte veiligheidseisen stellen aan softwareproducten en leveranciers. Het ministerie van Defensie stelt bijvoorbeeld strenge veiligheidseisen aan leveranciers die opdrachten voor het ministerie uitvoeren. Deze eisen zijn vastgelegd in de Algemene Beveiligingseisen voor Defensieopdrachten (ABDO) regeling. De MIVD controleert of een leverancier voldoet aan deze regeling. Daarnaast stellen financiële instellingen ook strenge veiligheidseisen aan de producten die zij in gebruik nemen. Ook de Rijksoverheid wil door middel van inkoopbeleid digitale veiligheid van software bevorderen. Om overheidsorganisaties te helpen bij het formuleren van veiligheidseisen is de Inkoopeisen Cybersecurity Overheid (ICO) wizard ontwikkeld. De ICO-wizard is een hulpmiddel voor overheidsorganisaties, maar het is niet verplicht om deze te gebruiken en het geeft geen handvatten hoe afnemers de gestelde eisen kunnen controleren. Bovendien geeft de ICO-wizard alleen een groslijst aan eisen waar organisaties uit kunnen putten. Een organisatie moet zelf de juiste selectie maken, daar is expertise voor nodig die niet elke organisatie tot zijn beschikking heeft. Daarnaast moet de organisatie ook zelf het product beoordelen, waar ook kennis voor nodig is en medewerking van de fabrikant.[155]

155 Ministerie van Defensie, *Algemene Beveiligingseisen Defensieopdrachten 2019*, februari 2020. Ministerie van Economische Zaken en Klimaat en Ministerie van Justitie en Veiligheid, *Roadmap Digitaal Veilige Hard- en Software*, april 2018. De ICO wizard is een tool ontwikkeld voor overheidsorganisaties op basis van de Baseline Informatiebeveiliging Overheid (BIO), om de vraag naar digitaal veilige software te stimuleren en een prikkel voor fabrikanten te creëren om digitaal veilige producten op de markt te brengen. Organisaties kunnen in de ICO-wizard zelf de eisen selecteren die bij hen van toepassing zijn bij de inkoop van software, zie: https://www.bio-overheid.nl/ico-producten/

Inkoopeisen door overheden in het buitenland: US Executive Order
In de Verenigde Staten is in mei 2021 een *Executive Order*[156] uitgebracht, waarin verschillende maatregelen worden genomen met als doel het verbeteren van de nationale cybersecurity.[157] Naast een aantal maatregelen met betrekking tot informatiedeling, het versterken van capaciteit bij incidentbestrijding en leren van incidenten, is de *Executive Order* ook gericht op het veiliger maken van software.

Een van de maatregelen die in de *Executive Order* is opgenomen is het stellen van standaarden aan software die gebruikt wordt door de federale overheden. In het *Executive Order* worden federale overheden verplicht om veiligheidseisen te stellen aan softwareleveranciers. Indien partijen niet aan deze gestelde eisen voldoen, zullen zij geen software meer mogen leveren aan Amerikaanse federale overheids-organisaties.

In het algemeen is het stellen van veiligheidseisen en controle hierop door organisaties aan fabrikanten vrijblijvend. Hier is geen regelgeving voor. De mate waarin dit gebeurt is dus afhankelijk van de organisaties zelf. Niet iedere organisatie heeft de expertise om de juiste eisen te stellen aan software, en om vervolgens te controleren of producten aan de eisen voldoen. Er zijn geen waarborgen in het systeem om af te dwingen dat producten aan bepaalde eisen voldoen.

4.2.3 Gebruiks- en onderhoudsfase van software binnen organisaties

Zoals in hoofdstuk 2 is beschreven is er een aantal maatregelen die organisaties kunnen nemen om hun bedrijfssystemen te beveiligen en zich voor te bereiden op incidenten. Het NCSC beveelt een aantal basismaatregelen aan, die organisaties kunnen treffen om cyberaanvallen tegen te gaan. Voorbeelden daarvan zijn het patchen van systemen, het gebruik van *firewalls*, netwerksegmentatie en detectiemogelijkheden. In het Cybersecuritybeeld Nederland 2021 en de tien jaren ervoor concludeert de NCTV dat hoewel de weerbaarheid van organisaties zich ontwikkelt, deze nog niet voldoende is. Niet alle organisaties hebben de basismaatregelen getroffen.[158] Hoe kunnen we begrijpen dat organisaties deze basismaatregelen niet altijd nemen? Dit heeft deels te maken met het vermogen om maatregelen te nemen en deels met *biases* in de manier waarop mensen in organisaties naar het risico van cyberaanvallen kijken.[159] Hieronder gaan we in op de belemmeringen en dilemma's die bij deze maatregelen komen kijken.

Omgaan met de afhankelijkheid van software

Bij het gebruik van software en de afhankelijkheid hiervan komen altijd risico's kijken. Het is voor afnemers onmogelijk om een risico volledig te mitigeren, maar wel van belang om allereerst de risico's in beeld te hebben en af te wegen. Het dubbel uitvoeren van een systeem door twee softwareproducten van verschillende fabrikanten te gebruiken is een manier om de afhankelijkheid van een product te verminderen. Het is echter niet

156 Een *Executive Order* is een decreet uitgegeven door de president, met dezelfde kracht als een wet.
157 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/, geraadpleegd op 14 juli 2021.
158 Nationaal Coördinator Terrorismebestrijding en Veiligheid, *Cybersecuritybeeld Nederland 2021*, juni 2021. https://www.security.nl/posting/710981/Cybersecuritybeeld+Nederland%3A+al+tien+jaar+lang+de+basis+niet+op+orde
159 Meyer, R. en Kunreuther, H., *The Ostrich Paradox: Why we underprepare for disasters*, 2017.

realistisch voor iedere organisatie om alle systemen redundant uit te voeren omdat dit extra middelen kost. Daarnaast kan het ook zo zijn dat wanneer een afnemer verschillende systemen heeft van verschillende leveranciers, systemen niet goed samen kunnen werken (compatibiliteitsproblemen). In sommige gevallen kiezen afnemers er wel uitdrukkelijk voor om systemen redundant uit te voeren, bijvoorbeeld wanneer het gaat om vitale systemen die cruciale processen mogelijk maken en wanneer er grote gevolgen zijn wanneer de beschikbaarheid wegvalt.[160] Wat betreft de systeemafhankelijkheden van een bepaald product in een netwerk, zijn veel verschillen te zien in hoe organisaties netwerken hebben ingericht. Een organisatie gaf in een interview aan zijn systemen zo ingericht te hebben dat er geen *single point of failure* is, zodat wanneer een systeem wegvalt, andere systemen en processen wel door kunnen gaan. Een andere organisatie gaf aan dat in zijn netwerk een aantal producten zit waar veel processen van afhankelijk zijn. Wanneer een systeem in dat geval wegvalt, kunnen veel processen in die organisatie niet meer doorgaan.

Bij het omgaan met de afhankelijkheid van software is het van belang om inzicht te krijgen in de risico's die komen kijken bij het gebruik van een bepaald product en de systeemafhankelijkheden. Wanneer een organisatie zich bewust is van zijn kritieke systemen en de afhankelijkheid hiervan goed in beeld heeft, is het beter mogelijk om een risicoafweging te maken van de maatregelen die genomen moeten worden bij een incident en in voorbereiding op een incident. In het algemeen is een groot verschil te zien tussen organisaties in de mate waarin zij hun systemen in beeld hebben. Voornamelijk de grote organisaties hebben vaak een (redelijk) goed beeld welke systemen ze hebben, en welke versies er draaien. Dit leggen ze bijvoorbeeld vast in een *Configuration Management Database* (CMDB). Wanneer er een kwetsbaarheid wordt gepubliceerd, kunnen zij in deze database zien of de kwetsbaarheid van toepassing is op de organisatie, en of ze dus moeten patchen. Ook kunnen ze, doordat ze systemen en afhankelijkheden in beeld hebben, makkelijker en accurater een risicoanalyse maken wat er zou gebeuren als het systeem bijvoorbeeld uitgeschakeld moet worden. Bij andere (veelal kleinere) organisaties is te zien dat ze niet altijd een compleet beeld hebben van de systemen die ze hebben. Het risico hierbij is dat wanneer er een belangrijke kwetsbaarheid aan het licht komt, deze organisaties niet (op tijd) actie op ondernemen en gecompromitteerd kunnen worden. Bovendien kunnen deze organisaties ook geen complete risicoanalyse maken wat de impact is wanneer een systeem uitgezet moet worden.

Het in beeld brengen en houden van de systemen en de systeemafhankelijkheden kost capaciteit en het belang van het up-to-date houden van dit overzicht moet door de hele organisatie gezien worden. Voor organisaties met weinig capaciteit kan het hierdoor een uitdaging zijn om een compleet beeld te krijgen van alle systemen en de afhankelijkheid tussen deze systemen. Ook de organisatiestructuur kan het lastiger maken om een compleet beeld te krijgen van alle systemen. De Inspectie van het Onderwijs stipt dit, na de aanval met gijzelsoftware bij de Universiteit Maastricht, aan als een van de bepalende factoren.[161] Universiteiten kennen een gelaagde bestuursstructuur met verschillende bestuursorganen, die ieder hun eigen informatiebeveiliging regelen. Dit maakt het een

160 Jacobs, D., *7 factors to consider in network redundancy design*, https://searchnetworking.techtarget.com/tip/7-factors-to-consider-in-network-redundancy-design, geraadpleegd op 16 juli 2021.
161 Inspectie van het Onderwijs, *Cyberaanval Universiteit Maastricht*, mei 2020.

uitdaging om zicht te hebben op de complete netwerk van ICT-systemen. Daarnaast kunnen ketenafhankelijkheden het lastig maken om een beeld te hebben van het complete systeem en de afhankelijkheden. Veel organisaties werken samen met externe leveranciers of ketenpartners. Processen van een organisatie kunnen hierdoor ook (deels) afhankelijk zijn van de systemen die externe partijen in gebruik hebben, zoals bijvoorbeeld het geval was bij het Kaseya voorval (zie 3.3.5).

Patchen

Software is meestal geen statisch product, maar blijft ook na de aanschaf in ontwikkeling. Ook het dreigingslandschap is niet statisch en continu in beweging. Wanneer kwetsbaarheden in software worden gevonden, ontwikkelen fabrikanten patches om deze te verhelpen (zie paragraaf 4.1). Het is op dit moment voornamelijk aan de afnemer om deze patches door te voeren om de kwetsbaarheden op zijn systemen op te lossen. Patchen brengt echter ook risico's en afwegingen met zich mee. Vanwege het grote aantal patches dat jaarlijks verschijnt (sommige organisaties moeten wel 100 duizend patches per jaar toepassen) is het voor een organisatie niet altijd mogelijk om patches op tijd te installeren. Door de grote hoeveelheid jaarlijkse patches hebben organisaties moeite om een volledig en *up-to-date* overzicht te hebben van kwetsbaarheden in hun systemen. Om dit te vereenvoudigen kunnen bedrijven een scanningdienst afnemen. Deze scanningdiensten scannen op bekende kwetsbaarheden. Maar niet alle kwetsbaarheden zijn te scannen en de lijst waarop wordt gescand is vaak incompleet. Kleinere organisaties hebben daarnaast meestal niet de middelen om dergelijke scanningdiensten af te nemen. Zij baseren zich vaak alleen op adviezen van het NCSC. Organisaties kunnen in deze omstandigheden niet alles tijdig patchen. Het is daarom onvermijdelijk dat bekende kwetsbaarheden, ook kritieke, niet worden gepatcht.

Het grote aantal kwetsbaarheden zorgt voor een grote druk op organisaties om het patchproces op gewenste wijze te organiseren en af te wegen bij welke kwetsbaarheden direct actie moet worden ondernomen. Het onvermogen van organisaties om beveiligingslekken tijdig te patchen maakt het volgens penetratietesters van *Positive Technologies* makkelijker voor aanvallers om bedrijfsnetwerken binnen te dringen. Patchen vergt kennis van systemen en capaciteit van medewerkers in organisaties. ICT medewerkers hebben naast het patchen van systemen nog vele andere werkzaamheden die ook uitgevoerd moeten worden. Voor iedere organisatie is het een afweging tussen het door laten gaan van dagelijkse werkzaamheden of het direct patchen van de systemen. Afnemers zijn soms terughoudend om patches direct uit te voeren omdat het risico bestaat dat na de patch systemen niet meer goed werken of uitvallen, wat gevolgen heeft voor de bedrijfsvoering van een organisatie. Daarnaast kan het zijn dat een patch de kwetsbaarheid niet of maar deels verhelpt.[162] Uit interviews blijkt dat deze afweging voornamelijk voor kleinere organisaties lastig is, omdat zij beperkte middelen hebben om extra capaciteit in te zetten voor het patchen van systemen.

Omdat het zoals hierboven besproken voor organisaties een uitdaging kan zijn om een compleet beeld te hebben van alle systemen die in gebruik zijn, kan het ook zijn dat een

162 Nichols, S., You weren't hacked because you lacked space-age network defenses. Nor because cyber-gurus picked on you. It's far simpler than that, *The Register*, augustus 2020. 'The Nightmares of Patch Management: the Status Quo and Beyond', *Trend Micro*, https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-nightmares-of-patch-management-the-status-quo-and-beyond, geraadpleegd op 14 juli 2021.

afnemer een kwetsbaarheid niet patcht omdat deze geen *up-to-date* overzicht heeft van welke software waar draait, welke versie het betreft en of een patch al dan niet nodig is om de veiligheid van de systemen te kunnen garanderen. Ook is voor afnemers niet altijd duidelijk uit welke componenten de door hen gebruikte software precies bestaat omdat deze veelal *closed source* is. Dat wil zeggen dat de broncode niet inzichtelijk is voor de afnemer en de fabrikant ook weinig loslaat over de architectuur van de software. Daarnaast is veel software gebaseerd op open source componenten die kritieke lekken bevatten, zonder dat dit bekend is bij afnemers.[163] Hierdoor kunnen afnemers zonder dat ze het zelf weten kwetsbaar zijn.

Ook moet de gehele organisatie het belang en de urgentie van patchen onderkennen. Voor organisaties is niet altijd duidelijk dat ze aangevallen kunnen worden zonder dat een aanvaller het specifiek op ze voorzien heeft. Een kwetsbaarheid in software op een server die met het internet verbonden is trekt aanvallers als het ware aan. Deze aanvallers scannen automatisch op alle servers die kwetsbare software bevatten, in de hoop dat daar servers bij zijn waarlangs ze het digitale systeem van organisaties kunnen binnendringen. Uit onderzoek blijkt dat afnemers hun acties vaak baseren op eerdere ervaringen die zij hebben gehad met updates.[164] Veel gepubliceerde kwetsbaarheden worden niet actief misbruikt door aanvallers. Wanneer afnemers wachten met patchen van kwetsbaarheden die niet worden gebruikt voor aanvallen, heeft dat geen gevolgen voor de organisatie. Dit zorgt ervoor dat afnemers het belang van een snelle reactie wellicht minder hoog inschatten bij volgende kwetsbaarheden.

Volgens fabrikanten en experts kan het verplaatsen van software naar de *cloud* een oplossing zijn om ervoor te zorgen dat systemen op tijd gepatcht kunnen worden. Dit wordt een *Software as a Service* (SaaS) oplossing genoemd.[165] Omdat de software dan wordt beheerd door de fabrikant, is het voordeel van SaaS dat patches sneller getest en toegepast kunnen worden. Er zit dan namelijk geen tijd tussen het uitkomen van een patch en het toepassen hiervan, waardoor afnemers altijd snel de laatste patches hebben. Bij SaaS wordt het toepassen van patches de verantwoordelijkheid van de fabrikant in plaats van de afnemer. Het verplaatsen van software naar de *cloud* gaat echter ook gepaard met afwegingen en risico's voor een organisatie. Het nadeel van SaaS oplossingen is dat in het geval van een kwetsbaarheid alle servers kwetsbaar zijn, aangezien deze allemaal op dezelfde versie draaien. Daar kan dan alleen door de fabrikant iets aan gedaan worden, de afnemer speelt daar geen rol in.

Wanneer afnemers systemen in eigen beheer hebben, kunnen ze zelf patchen, mitigeren of de systemen afsluiten. Bovendien hebben organisaties bij het afnemen van een clouddienst geen zicht op wat het product inhoudt. Daarnaast is een organisatie dan ook minder flexibel, het aanpassen van software is nog maar beperkt mogelijk. Ook kunnen automatische updates - bij SaaS oplossingen - de continuïteit van systemen bedreigen of nieuwe kwetsbaarheden introduceren. Afnemers hebben daar dan helemaal geen

163 'Veel kritieke lekken door open source in standaard apps', *AG Connect*, https://www.agconnect.nl/artikel/veel-kritieke-lekken-door-open-source-standaard-apps, 5 augustus 2021.
164 Rajivan et al., Update now or later? Effects of experience, cost, and risk preference on update decisions, *Journal of Cybersecurity*, 2020.
165 Bij SaaS wordt software als een online dienst aangeboden. De afnemer krijgt via internet of via een VPN toegang tot de software die bij de aanbieder beheerd wordt.

controle meer over. Een andere overweging voor een afnemer is dat bij een incident de systemen bij de fabrikant staan. Een fabrikant weet het meeste van het product en is daarmee de aangewezen partij om bij een incident zijn software te kunnen analyseren. De fabrikant kan dan de afnemer helpen om te onderzoeken of deze getroffen is, en het probleem op te lossen. Soms willen afnemers echter geen informatie delen met externe partijen, bijvoorbeeld omdat het niet mag, of omdat ze geen risico willen lopen dat informatie buiten de organisatie belandt. Ook kan het vanwege de aard van het systeem zo zijn dat een afnemer deze niet wil verbinden met het internet. In dat geval is SaaS geen oplossing en moet een afnemer (een deel van) zijn systemen fysiek in beheer hebben.

Het veelvuldig patchen van software introduceert nieuwe problemen. Wanneer een afnemer niet patcht heeft deze mogelijk een beveiligingslek dat van buitenaf automatisch op te sporen is. Vanwege de grote en toenemende hoeveelheid patches is het patchen van alle kwetsbaarheden niet behapbaar voor organisaties. Bovendien is voor afnemers de noodzaak van (snel) patchen niet altijd duidelijk. Het aanbieden van software vanuit de *cloud* verplaatst de verantwoordelijkheid om te patchen naar de fabrikant, maar gaat ook gepaard met risico's voor afnemers.

Preventie en detectie

Naast patchen is er ook nog een aantal andere preventieve en detectiemaatregelen die een organisatie kan nemen om zijn netwerk te beschermen, zoals het instellen van een *firewall*, netwerksegmentatie en de monitoring van systemen. Deze maatregelen gaan ieder gepaard met risico's en afwegingen voor een organisatie.

Een maatregel om toegang van buitenaf tot de systemen van een organisatie te beperken is het instellen van een *firewall*.[166] De uitdaging bij *firewalls* is dat deze zo ingesteld moeten worden dat ongewenste activiteit wordt tegengehouden, maar dat gewenste activiteit niet onterecht ook tegen wordt gehouden. Daarnaast moeten de juiste regels en beleid ingesteld worden, en is het van belang deze periodiek te checken en updaten. Dit vraagt kennis en capaciteit van een organisatie. Een *firewall* brengt ook risico's met zich mee wanneer een organisatie niet de juiste kennis heeft over wat de firewall precies doet. Hierdoor heeft een organisatie geen zicht op of er systemen onnodig openstaan voor verkeer.[167]

Om de impact van een mogelijk incident te beperken kan een organisatie zijn netwerk segmenteren. Het risico bij segmentatie is dat wanneer een netwerk uit veel segmenten bestaat, het erg veel tijd en geld kost om het netwerk te beheren.[168] Het implementeren van segmentatie in een netwerk is een proces dat veel aanpassingen vergt, kostbaar is en verstorend kan zijn voor het primaire proces van een organisatie. Voor organisaties is

166 Een firewall is een machine die tussen een netwerk en het internet in staat, verkeer monitort, en mogelijk schadelijk verkeer tegenhoudt.

167 https://www.insightsforprofessionals.com/it/security/firewall-management-challenges-how-solve-them, geraadpleegd op 22 juli 2021. AlgoSec, *Firewall Management: 5 challenges every company must address – an AlgoSec Whitepaper,* 2015.

168 *'Hazardous Network Segmentation: when more isn't better'*, AlgoSec, https://www.algosec.com/blog/hazardous-network-segmentation-when-more-isnt-better, geraadpleegd op 22 juli 2021.

het daarnaast moeilijk om medewerkers te vinden met de noodzakelijke vaardigheden en expertise.[169]

Naast meer preventieve maatregelen als *firewalls* en segmentatie investeren organisaties ook in detectiemogelijkheden en de monitoring van systemen. Hierbij kan een organisatie verdachte activiteit detecteren wanneer deze plaatsvindt. De uitdaging hierbij voor organisaties is dat het van belang is dat de detectie goed ingesteld is. Wanneer dit niet het geval is kan verdachte activiteit niet opgemerkt worden, of kan activiteit ten onrechte gedetecteerd worden als verdacht (*false positives*). Het hebben van detectiemogelijkheden garandeert dus niet dat alle verdachte activiteit opgemerkt wordt. Daarnaast moeten organisaties de kennis hebben om de activiteiten te kunnen duiden, en weten hoe ze moeten reageren wanneer ze activiteit van een aanvaller detecteren. Dit vraagt capaciteit en expertise van een organisatie. Voor vitale en rijksoverheidsorganisaties is het mogelijk om zich aan te sluiten bij het Nationaal Detectie Netwerk (NDN). Het NCSC geeft indicatoren door aan de deelnemers van het NDN om een potentiële aanval te kunnen herkennen. Voor deelname aan het NDN is het een vereiste dat organisaties zelf hun monitoringproces al ingericht hebben. Alleen de rijksoverheid en vitale organisaties kunnen zich direct aansluiten bij het NDN.[170]

Een tendens die in de cybersecuritywereld opgemerkt wordt is dat er steeds meer wordt geïnvesteerd in detectiemogelijkheden ten opzichte van preventie.[171] In de beveiligingswereld wordt vaak benadrukt dat het niet mogelijk is alle aanvallen te voorkomen, dus dat het loont om vooral te investeren in detectie en respons. Dit was ook zichtbaar bij enkele organisaties die we hebben gesproken, die voornamelijk in detectie en respons hadden geïnvesteerd. Investeren in detectie biedt echter niet altijd garanties, zoals hierboven ook besproken. Bij één van de geïnterviewde organisaties detecteerde het systeem de aanval via de software kwetsbaarheid niet, met als gevolg dat de organisatie alsnog werd gecompromitteerd. Voor een zo veilig mogelijk systeem zijn dus meerdere lagen van veiligheid en beveiliging nodig, zowel preventie als detectie en respons.

4.2.4 Besturen van digitale veiligheid in organisaties

Capaciteit en expertise

Alle hierboven genoemde maatregelen vragen capaciteit en kennis van organisaties. De mate waarin een organisatie deze capaciteit en kennis tot zijn beschikking heeft hangt af van de grootte van een organisatie en de volwassenheid op cybersecuritygebied. Kleinere organisaties hebben weinig capaciteit en kennis op het gebied van informatiebeveiliging. In het algemeen zagen we in dit onderzoek grote verschillen in de mate waarin organisaties maatregelen nemen om incidenten te voorkomen en de mate waarin zij voorbereid zijn op incidenten.

169 Holt, M., Security Think Tank: Benefits and challenges of security segmentation, *Computer Weekly*, https://www.computerweekly.com/opinion/Security-Think-Tank-Security-segmentation-benefits-and-challenges, geraadpleegd op 15 juli 2021.

170 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en ministerie van Veiligheid en Justitie, *Handreiking voor implementatie van detectie-oplossingen*, oktober 2015. Bepaalde organisaties als zorginstellingen, gemeenten, onderwijsinstellingen en waterschappen kunnen zich indirect aansluiten op het NDN via de sectorale CERTs. Zie: https://www.ncsc.nl/actueel/weblog/weblog/2020/het-nationaal-detectie-netwerk-voor-een-private-organisatie.

171 https://www.youtube.com/watch?v=3IDiqYil2lQ, geraadpleegd op 16 juli 2021.

Een gemeente met een beperkt budget heeft bijvoorbeeld weinig capaciteit op het gebied van informatiebeveiliging en ICT in het algemeen. De CISO is daar de enige medewerker die zich bezig houdt met informatiebeveiliging. Door de beperkte capaciteit heeft de ICT afdeling onder andere moeite met het op orde krijgen van de CMDB van de organisatie en het op tijd uitvoeren van alle benodigde patches. Daartegenover staan bijvoorbeeld financiële instellingen die honderden cybersecurityprofessionals in dienst hebben. Zij hebben de capaciteit en expertise om de basis op orde te hebben en te anticiperen en reageren op incidenten.

Er zijn veel verschillen zichtbaar tussen organisaties in de mate waarin zij ICT werkzaamheden zelf uitvoeren of uitbesteden. Organisaties besteden werkzaamheden uit omdat zij niet voldoende expertise en capaciteit in huis hebben om het zelf uit te voeren. Door dit gebrek aan expertise en capaciteit hebben zij echter ook niet altijd de kennis om goed te kunnen beoordelen of de partij waar zij werkzaamheden aan hebben uitbesteed goed werk levert.

In het algemeen is er sprake van een tekort aan expertise in de cybersecurity markt. Dit is een jarenlang probleem dat niet af lijkt te nemen. In de gehele IT-sector is sprake van een krappe arbeidsmarkt, zo was in juli 2021 dertig procent van de vacatures voor IT-programmeurs en IT-ontwikkelaars onvervulbaar. Een van de oorzaken van het tekort aan expertise is dat professionals zich ondergewaardeerd voelen, en het moeilijk is in het cybersecurity domein te starten. Door toenemende hoeveelheid en complexiteit van aanvallen ervaren veel professionals daarnaast stress en burn-out klachten.[172]

Het risico hierbij is dat het capaciteitstekort op de markt alleen maar gaat toenemen. Tijdens het Citrix voorval was ook te zien dat er meer vraag naar cybersecurity professionals was dan aanbod, waardoor beveiligingsbedrijven geen capaciteit hadden om iedere organisatie die expertise nodig had te helpen. De capaciteit op het gebied van incidentbestrijding is gefragmenteerd via sectorale CERTs en voor preventieve maatregelen moet elke organisatie zelf capaciteit en expertise inzetten. Expertise wordt niet of weinig gebundeld en is hierdoor versnipperd.

Urgentie

Ook de mate waarin een organisatie het belang en de urgentie van het nemen van maatregelen inziet, en daar ook middelen voor in kan en wil zetten, speelt een rol bij de weerbaarheid van een organisatie. Bij overheden zoals gemeenten kan het bestuur niet zelf bepalen hoe middelen worden besteed, zoals bij private organisaties. Zij leggen daarvoor verantwoording af aan de gemeenteraad, die naast cybersecurity veel andere belangen heeft die ze moeten meewegen en ook veel gemeentelijke taken erbij hebben gekregen waar middelen voor moeten worden ingezet. Daar komt bij dat ICT vaak als vanzelfsprekend wordt beschouwd door bestuurders of volksvertegenwoordigers, zonder dat zij weten wat daar allemaal bij komt kijken. Het is vaak aantrekkelijker om geld uit te geven aan zaken die een tastbaar resultaat opleveren dan aan het voorkomen van problemen. Wanneer problemen worden voorkomen, is het resultaat namelijk niet zichtbaar.

172 ESG & ISSA, *The Life and Times of Cybersecurity Professionals 2021 – Volume V*, juli 2021. ABN Amro, *Stand van TMT*, september 2021. VMware, *Global Incident Response Threat Report*, 2021.

Uit interviews is daarnaast gebleken dat in sommige organisaties de positie van de CISO in de organisatie ten tijde van het voorval zwak was, waardoor deze niet bij kon dragen aan een goed verloop van het incident. Bij een van de gesproken organisaties lukte het de CISO tijdens het voorval niet om het besluit om te mitigeren erdoorheen te krijgen bij de ICT afdeling, waardoor de organisatie gecompromitteerd werd. Naar aanleiding van dit incident is de positie van de CISO in de organisatie veranderd en versterkt, waardoor deze incidenten in de toekomst makkelijker aan kan kaarten bij het bestuur. Bij veel van de gesproken organisaties is te zien dat het gevoel van urgentie om te investeren in digitale veiligheid toeneemt na een dergelijk incident.

Individueel risico

Risico's die komen kijken bij kwetsbaarheden in software worden nu voornamelijk gezien als individuele risico's die iedere organisatie zelf moet beheersen. Het uitgangspunt in het Nederlandse stelsel is namelijk dat elke publieke en private organisatie zelf verantwoordelijk zijn voor zijn digitale weerbaarheid. De meeste organisaties hoeven hier geen verantwoording voor af te leggen. (Middel)grote bedrijven en organisaties moeten jaarlijks een accountantscontrole laten uitvoeren op de jaarrekening, om de getrouwheid hiervan aan te tonen. Een IT-verklaring maakt momenteel geen deel uit van deze accountantsverklaring, terwijl het op orde hebben van IT-beveiliging wel van belang is voor de continuïteit van een organisatie. De beroepsvereniging van IT-auditors heeft onlangs voorgesteld om een IT-verslag een vast onderdeel te maken van de accountantsverklaring.[173]

Wanneer incidenten als gevolg van kwetsbaarheden in software plaatsvinden, hebben deze impact op vele organisaties en burgers. Kwetsbaarheden vormen hierdoor een collectief risico voor de samenleving als geheel. Individuele organisaties hebben maar beperkte mogelijkheden om zelf de risico's te beheersen, afhankelijk van de capaciteit en expertise die ze in huis hebben. De kosten van cyberaanvallen stijgen jaarlijks. Steeds meer organisaties sluiten een cyberverzekering af om zich te verzekeren tegen schade bij incidenten. Toch is nog maar een klein deel van MKB bedrijven verzekerd tegen cyberincidenten.[174] Doordat de kosten van cyberincidenten oplopen, stijgt de premie voor cyberverzekeringen op dit moment ook. Wanneer er een incident plaatsvindt met een kwetsbaarheid in software die door vele organisaties wordt gebruikt, zullen de collectieve kosten van een incident echter dusdanig hoog zijn dat deze ook niet meer te dragen zijn door verzekeraars.

Van verzekeraars wordt verwacht dat ze een positieve rol kunnen spelen in het bevorderen van de cyberhygiëne van organisaties. Dit door eisen te stellen aan de maatregelen die organisaties genomen moeten hebben om gedekt te zijn voor cyberincidenten. Tegelijkertijd is er ook kritiek op de rol van verzekeraars, en staat ter discussie of zij een goede cyberhygiëne stimuleren, omdat verzekeraars *ransomware* betalingen dekken en omdat door organisaties genomen beveiligingsmaatregelen niet worden gecontroleerd.

173 NCTV, *Nederlandse Cybersecurity Agenda*, april 2018. Van Gils en Van Wijnen, 'Nieuwe IT-check kan voorwaarde worden voor krediet', *FD*, 11 augustus 2021.

174 Hiscox, *Hiscox Cyber Readiness Report 2020*, 2020; https://www.trouw.nl/economie/het-aantal-cyberaanvallen-groeit-explosief-maar-echt-ongerust-zijn-bedrijven-niet~b332e73e, geraadpleegd op 29 juli 2021. https://www.rtlnieuws.nl/tech/artikel/5000096/cyberverzekering-hacken-ransomware-gijzelsoftware-ddos-citrix, geraadpleegd op 29 juli 2021. Modderkolk, 'Vooraanstaande ict-beveiligers: 'Ransomware gaat richting nationale crisis, overheid moet meer doen', *De Volkskrant*, augustus 2021.

Recent is hier verandering in gekomen, en worden *ransomware* betalingen niet altijd meer gedekt door verzekeraars.[175]

Er is momenteel geen collectieve basis om organisaties te helpen hun weerbaarheid te vergroten. Elke organisatie moet zelf zijn basis opbouwen met de kennis en capaciteit die ze hebben.

Door de asymmetrische relatie tussen fabrikant en afnemer op het gebied van softwareveiligheid zijn afnemers doorgaans niet in staat zelf veiligheidseisen stellen bij de aanschaf van software en de juiste afwegingen maken. Er zijn wel mogelijkheden voor afnemers om bewust om te gaan met risico's van software, maar niet elke afnemer heeft de kennis en capaciteit om de juiste eisen te stellen en deze te controleren. Er bestaat geen algemene regelgeving omtrent de controle van software die fabrikanten verplicht aan bepaalde veiligheidseisen te voldoen.

Wat betreft preventie en voorbereiding op incidenten is er veel verschil in de weerbaarheid van organisaties. Veel maatregelen vergen een afweging van risico's. Niet alle organisaties hebben de expertise en capaciteit om maatregelen voldoende uit te voeren, of onderkennen de urgentie om hier capaciteit op in te zetten niet. Iedere organisatie is zelf verantwoordelijk voor zijn digitale weerbaarheid. Er is geen collectief fundament dat geboden wordt om organisaties te helpen de digitale weerbaarheid te vergroten.

4.3 Incidentbestrijding (respons)

De voorvallen die we in hoofdstuk 3 beschrijven laten zien dat de tijd tussen dat een kwetsbaarheid in software wordt gemeld en dat organisaties die kwetsbaar zijn worden aangevallen beperkt is: variërend van een maand tot enkele dagen of geen (*zero day*). In de vorige paragrafen beschreven we welke factoren van invloed zijn op de wijze waarop fabrikanten kwetsbaarheden in software voorkomen en reageren op kwetsbaarheden en wat organisaties die software gebruiken doen om te voorkomen dat hun digitale systeem daardoor beveiligingslekken kan hebben. In deze paragraaf gaan we in op de factoren die beïnvloeden hoe betrokken partijen, zoals fabrikant, organisatie en publieke en private incidentbestrijders het incident bestrijden om de gevolgen te beperken.

4.3.1 Informatiestroom

Na het bekend worden van een kwetsbaarheid is van cruciaal belang dat de relevante organisaties zo direct en zo snel mogelijk worden geïnformeerd. Organisaties die de software gebruiken hebben zo betrouwbaar en toegesneden mogelijke informatie nodig om in korte tijd een eigen afweging te maken hoe te handelen om de risico's te kunnen beheersen. Organisaties die niet in staat zijn om een eigen afweging te maken hebben behoefte aan een advies dat ze kunnen volgen. Fabrikanten en incidentbestrijders willen

175 Verzekeraars deinzen terug voor ransomware', *AG Connect*, https://www.agconnect.nl/artikel/verzekeraars-deinzen-terug-voor-ransomware, 25 mei 2021.