CYBERSECURITY IN DE BOARDROOM

Voorbij de bits en de bytes in de Nederlandse ziekenhuizen

Cybersecurity en cybercrime worden steeds belangrijker in de ziekenhuissector. In de boardroom dient de samenstelling en het kennisniveau afgestemd te worden op de rol en de impact van ICT binnen de organisatie. De raden van bestuur en toezicht van de algemene ziekenhuizen in Nederland lijken dit nog onvoldoende te doen. De belangrijkste reden hiervoor is dat er een discrepantie bestaat tussen de werkvloer en de boardroom over de rol en de impact van ICT binnen de organisatie.

Mieke de Lepper en Marlies de Vries

De digitalisering van de maatschappij heeft vergaande gevolgen. Bijna alle organisaties zijn tegenwoordig geheel afhankelijk van een continue en betrouwbare gegevensverwerking van de netwerken en onderdelen die (vertrouwelijke) gegevens opslaan en transformeren. Gelijk met deze ontwikkelingen is een nieuwe vorm van criminaliteit ontstaan: cybercrime. Jaarlijks publiceert het Nationaal Cyber Security Centrum, onderdeel van de Nationaal Coördinator Terrorismebestrijding en Veiligheid van het ministerie van Veiligheid en Justitie, het Cybersecuritybeeld Nederland (CSBN). In het CSBN 2015 komt men tot de volgende definitie van cybersecurity: "Het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid in ICT opgeslagen informatie of schade aan de integriteit van die informatie." Deze definitie ligt in lijn met definities zoals deze gehanteerd worden in de wetenschappelijke literatuur en is daarmee een goede praktische, werkbare vertaling die verder als uitgangspunt kan worden genomen.

In lijn met de internationale ontwikkelingen (ondermeer binnen de EU, UK en US) creëert Nederland meer regelgeving op het gebied van cybersecurity. Een belangrijke aanname hierbij is dat de organisatorische inbedding van (toezicht op) de ICT functie op het hoogste niveau geregeld is. Onderzoek in bijvoorbeeld de UK laat zien dat ondanks alle inspanningen van de overheid de inbedding van het thema cybersecurity in het bedrijfsleven nog minimaal is (McLean, 2013).

Het huidige boardklimaat

In het najaar van 2015 startten de overheid, het bedrijfsleven en de wetenschap gezamenlijk de campagne Alert Online.[1] Het doel van deze campagne

ALS DE OPERATIEKAMER GEHACKT WORDT, IS DE RAVAGE NIET TE OVERZIEN

was om de kennis over online veiligheid een extra impuls te geven van jong naar oud en van werkvloer tot boardroom. Hieruit kan worden afgeleid dat cybersecurity niet meer alleen het domein is van de experts (Scully, 2011). Een breder bewustzijn en begrip is belangrijk binnen organisaties en is essentieel om de potentiële dreiging het hoofd te kunnen bieden. De communicatie tussen experts en niet-experts over dit onderwerp is lastig, omdat zij "elkaars taal" niet spreken.

Regelgeving lijkt gebaseerd te zijn op het uitgangspunt dat het toezicht op cyberrisico's op het hoogste niveau in de organisatie is verankerd. Een aanname die mogelijk niet terecht is. Immers, niet elke raad van bestuur en raad van toezicht heeft dit als een aparte verantwoordelijkheid gedefinieerd. Bovendien kan niet zomaar aangenomen worden dat er bij organisaties voldoende kennis "on board" is om effectief toezicht te kunnen houden op het cyberdomein. En natuurlijk is de daadwerkelijke inrichting van deze verantwoordelijkheid binnen het bestuur en het toezichthoudend orgaan afhankelijk van de complexiteit en afhankelijkheid van ICT.

De beheersing van ICT en de daarmee gepaard gaande beveiligingsvraagstukken is geen eenheidsworst: er bestaan meerdere alternatieven voor de beheersing van ICT. Centrale vragen bij de beheersing van ICT bij organisaties zijn bijvoorbeeld: "Hoe belangrijk is ICT voor de organisatie?" of "Wat zijn de belangrijkste ICT problemen waarmee de organisatie te kampen heeft?". En meer specifiek voor de aspecten control en governance: "Wat wordt er binnen de organisatie gedaan om ICT te beheersen?" en "Is de organisatie aantoonbaar in control over de ICT?".

Gekozen is om in dit artikel voorbij de bits en bytes te treden. Daarom zal er geen technische uiteenzetting van cybersecurity worden gegeven. In plaats daarvan zal de focus liggen op hoe er in organisaties mee omgegaan wordt door mensen en hoe de communicatie tussen de werkvloer en de board plaatsvindt. Dit wordt geïllustreerd aan de hand van de uitkomsten van een recent onderzoek uitgevoerd binnen Nyenrode Business Universiteit onder algemene ziekenhuizen in Nederland.

★★★★★★★★★★★★★★

BESTUURDERS EN DE TOEZICHTHOUDERS VINDEN DAT ZE OVER VOLDOENDE KENNIS BESCHIKKEN OVER CYBERSECURITY

Onderzoek algemene ziekenhuizen

In ziekenhuizen ligt enorm veel privacygevoelige informatie opgeslagen. Er zijn vrijwel geen hardcopy patiëntendossiers meer aanwezig. Alle gegevens liggen vast in digitale dossiers. Ook wordt er binnen ziekenhuizen veelvuldig gebruik gemaakt van high tech, digitale medische apparatuur. Deze ontwikkelingen vereisen veel op het gebied van cybersecurity. Dit is de aanleiding geweest voor het onderzoek van Van de Gevel (2015) naar de wijze waarop invulling wordt gegeven aan de communicatie over de bedreigingen uit hoofd van cybersecurity tussen de Information Security Officer (ISO), de bestuurders en het toezichthoudend orgaan binnen de algemene ziekenhuizen in Nederland. Onder de ISO wordt degene verstaan die binnen de organisatie verantwoordelijk is voor de communicatie inzake cybersecurity richting de raad van bestuur. Per ziekenhuis verschilt het bij welke functie deze verantwoordelijkheid belegd is. Over het algemeen is dat de ISO of het hoofd IT.

De wetgever is zich al langere tijd bewust van de cyberrisico's. In 2004 is reeds de eerste Nederlandse norm NEN 7510 Informatiebeveiliging in de zorg gepubliceerd. Deze norm biedt een algemeen kader voor de inrichting van informatiebeveiliging in de zorg. Daarnaast is het Nederlands Instituut voor Accreditatie in de Zorg (NIAZ) een belangrijke partij binnen de zorgsector. Eén van de normen waar zij op toetsen heeft betrekking op de kwaliteit van informatiebeveiliging binnen de zorg. De vraag is echter of deze normen het beoogde effect hebben. Het is niet voor niks dat er per 1 januari 2016 weer een nieuwe wet aan het normenkader is toegevoegd: de Wet meldplicht datalekken. In tegenstelling tot de eerder

HET VOLDOEN AAN HET NORMENKADER KAN DIENEN ALS MIDDEL OM CYBERSECURITY TE BEHEERSEN EN NIET ALS EINDDOEL OP ZICH

genoemde normen die op informatiebeveiliging in algemene zin inzoomen, gaat deze nieuwe norm specifiek in op het onderdeel "persoonsgegevens". De Wet meldplicht datalekken verplicht onder andere ziekenhuizen om beveiligingslekken te melden die leiden tot misbruik, diefstal of verlies van persoonsgegevens. Ook krijgt de Autoriteit Persoonsgegevens (AP) met de invoering van deze wet een uitgebreidere boetebevoegdheid bij het overtreden van de privacyregels. Het boetebedrag kan oplopen tot wel € 810.000 of, als dat hoger is, 10% van de jaaromzet van een organisatie. Dit wekt de indruk dat bij het ontstaan van nieuwe wet- en regelgeving sprake is van een repressieve aanpak.

Voor de algemene ziekenhuizen in Nederland geldt dat ze gedwongen worden om voldoende aandacht te besteden aan het normenkader. De maatschappij verwacht van ze dat ze hieraan voldoen. Echter zijn de meningen vanuit de ziekenhuizen wisselend over het nut van de normen. De één ziet het als echte dissatisfiers, iets waar je totaal geen beleid op moet maken, terwijl de ander het ziet als de basis voor het inrichten van de organisatie. Overall is het beeld dat de normen gezien moeten worden als een middel en niet als een doel. Opvallend is dat de toezichthouders de minste waarde hechten aan het normenkader, terwijl zij er juist toezicht op zouden moeten houden.

Kijkend naar het totaalplaatje binnen de algemene ziekenhuizen, blijken de bestuurders en de toezichthouders veelal tevreden te zijn over de wijze waarop invulling wordt gegeven aan de communicatie over cyberrisico's. Cybersecurity is een onderwerp dat zij bekijken vanuit de strategie en een risico-inventarisatie. Op basis van deze twee zaken zijn de bestuurders en de toezichthouders van mening dat ze over voldoende kennis beschikken over, voldoende aandacht hebben voor en zich voldoende bewust zijn van cybersecurity. Echter is het over het algemeen zo dat de ISO als zijnde de expert op het gebied van cybersecurity, de organisatie afhankelijker van ICT inschat dan de bestuurders en de toezichthouders. Zij delen hier dus niet dezelfde mening. Een gebrek aan kennis, aandacht en bewustzijn op het gebied van cybersecurity blijkt nog altijd een belangrijk knelpunt. De bestuurders steunen in grote mate op de expertise van de ISO. De communicatie tussen de ISO en de bestuurders blijkt veelal een eenzijdige informatieverstrekking te zijn en helemaal afhankelijk van wat de ISO inbrengt. Ook tussen de bestuurders en het toezichthoudend orgaan vormt cybersecurity niet een expliciet gespreksonderwerp. Bovendien dient er veelvuldig bezuinigd te worden binnen de ziekenhuissector en blijkt cybersecurity een onderwerp wat al vlug aan het kortste eind trekt. De prioriteit ligt bij het primaire proces.

De bevindingen uit het onderzoek samenvattend, kan geconcludeerd worden dat het allemaal teruggebracht kan worden naar een verschil in inzicht met betrekking tot de rol en de impact van ICT binnen een organisatie. Binnen de ziekenhuizen maakt iedere speler zijn eigen inschatting hiervan en hier blijkt vaak geen consensus over te bestaan.

Kan de theorie de praktijk helpen?

Kijkend naar de rol van het toezicht (RvB en RvT) binnen een organisatie en hoe deze ingericht moet worden, kan aansluiting gezocht worden bij de literatuur over ICT Governance. Leidraad in dit artikel is de IT Strategic Impact Grid van Nolan en McFarlan (2005). Dit model helpt bij de beoordeling van de impact van ICT binnen een organisatie en geeft richtlijnen die kunnen helpen bij de brede ICT governance, waar cyber deel van uitmaakt.

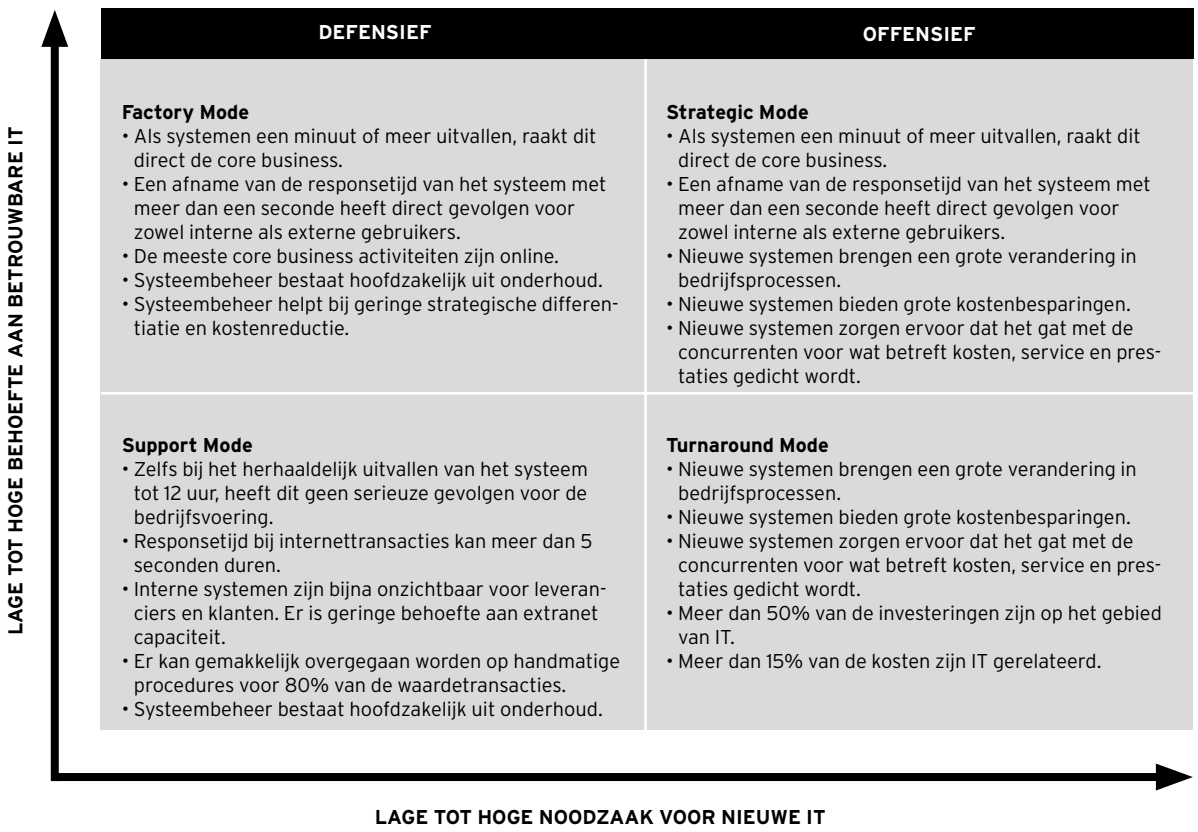
Vier configuraties als basis voor de beheersing van en toezicht op ICT

Ten aanzien van de ICT-strategie onderscheiden Nolan en McFarlan (2005) een viertal mogelijke benaderingen door de raad van bestuur / raad van toezicht op basis van twee belangrijke strategische vragen. De eerste vraag is in welke mate de organisatie afhankelijk is van efficiënte, permanent beschikbare en veilige ICT-systemen ("defensieve IT"). De tweede vraag is hoezeer de organisatie innovatieve ICT nodig heeft om te kunnen concurreren door middel van systemen die een toegevoegde waarde hebben voor diensten en producten of een hoge mate van klantbetrokkenheid genereren ("offensieve IT"). Het inzicht in de positie van de onderneming wordt weergegeven in de IT Strategic Impact Grid. Deze bepaalt in zekere mate hoe de ICT-governance ingevuld kan worden.

Defensieve IT gaat vooral over operationele betrouwbaarheid, de systemen draaiende houden en het verzorgen van een betrouwbare ondersteuning van bedrijfsprocessen en toereikende output. Offensieve IT heeft ook een strategisch aspect. Men wil de ICT optimaal benutten en daarmee strategische voordelen behalen. Betrouwbaarheid blijft belangrijk, strategische alignement wordt misschien nog wel belangrijker. ICT-projecten, die in deze categorie passen, zijn niet alleen ambitieus, maar ook riskant, omdat daarmee meestal een ingrijpende verandering in de organisatie (bedrijfsprocessen) in gang wordt gezet.

Dit leidt tot de volgende visuele weergave:

Figuur 1: IT Strategic Impact Grid - Nolan & McFarlan (2005)



Mogelijkheden voor toezicht op ICT
Wat bestuurders en toezichthouders over ICT moeten weten, hangt af van de strategische positie van de organisatie. Zodra de "mode" van de organisatie bepaald is, kunnen bestuurders en toezichthouders besluiten wat voor een soort ICT expertise ze nodig hebben binnen respectievelijk de Raad van Bestuur en de Raad van Toezicht. Zo kan bijvoorbeeld het onderwerp ICT bij ondernemingen in de support en factory mode behandeld worden door de audit commissie met hulp van een (externe) ICT expert. Organisaties in de turnaround mode en de strategic mode zullen een volledig ICT committee binnen de Raad nodig hebben om tot formulering te komen van de juiste vragen op het gebied van ICT en cybersecurity.

Slotoverwegingen

Het verhogen van het bewustzijn van werkvloer tot boardroom was één van de doelen van de Alert Online campagne. Op het niveau van de boardroom blijkt inderdaad nog werk aan de winkel. De eerste stap is dat geborgd dient te worden dat het kennisniveau van de bestuurders en de toezichthouders voldoende is om überhaupt een goede inschatting te kunnen maken over het belang van ICT voor de organisatie. Pas als dit goed geregeld is kan er een goede discussie plaatsvinden tussen de boardroom en de werkvloer. Uit deze discussie volgt dan een gedragen beeld over de rol en de impact van ICT binnen de organisatie op dit moment en voor de toekomst.

Zeker bij organisaties in de strategic mode en de turnaround mode is het van belang dat cybersecurity gezien wordt als onderdeel van het primaire proces. Dit vraagt om een structurele organisatorische inbedding op het hoogste niveau. Met andere woorden: de rol van ICT mag niet meer als een zij-traject gezien worden.

Specifiek voor de ziekenhuissector geldt dat er diverse normen op het gebied van cybersecurity van kracht zijn. Het gevaar is dat het normenkader gezien gaat worden als de graadmeter dat de organisatie "in control" is voor wat betreft cyberrisico's. Echter, het voldoen aan het normenkader kan dienen als een middel om cybersecurity te beheersen en niet als einddoel op zich. Het normenkader is de laatste jaren repressief tot stand gekomen. Maar, als er met enige pragmatiek mee omgegaan wordt, kan het meer sturend en als middel gezien worden voor de praktijk om het beleid te beheersen en er toezicht op te kunnen houden.

Noot

1. www. alertonline.nl

Literatuur

- Gevel, A.M.G. van de (2015). Cybersecurity in de boardroom: *Een uiteenzetting van de wijze waarop invulling wordt gegeven aan de communicatie over de bedreigingen uit hoofde van cybersecurity tussen de ISO, de bestuurders en het toezichthoudend orgaan binnen de algemene ziekenhuizen in Nederland*. Scriptie in het kader van de opleiding master Accountancy aan Nyenrode Business Universiteit.
- McLean, S. (2013). *Beware the Botnets: Cyber Security is a Board Level issue*. Intellectual Property & Technology Law Journal. Vol. 25: 12.
- Nationaal Cyber Security Centrum (2015). *Cybersecuritybeeld Nederland CSBN 2015*. https://www.nctv.nl/onderwerpen-a-z/cybersecuritybeeld-nederland.aspx.
- Nolan, R.L and McFarlan, F.W. (2005). *Information Technology and the Board of Directors*. Harvard Business Review, 83(10), 96-106.
- Scully, T. (2011). *The cyber threat, trophy information and the fortress mentality*. Journal of Business Continuity and Emergency Planning. Vol. 5: 3.

Over de auteurs

Mieke de Lepper - van de Gevel MSc is Internal Auditor bij Máxima Medisch Centrum.
Drs. Marlies de Vries RA is Assistent Professor Internal Control en PhD Onderzoeker aan Nyenrode Business Universiteit.

De auteurs zijn prof. dr. Lineke Sneller RC zeer erkentelijk voor de door haar gegeven commentaren op eerdere versies van dit artikel.