AUDIT
MAGAZINE

INTERVIEWS | 1 NOVEMBER 2022

UITBESTEDING: VERGEET DE CYBER RISKS NIET!

Auteur: Sierd Stapersma RO EMITA - Raymond Wondergem MSc RO
Beeld: Adobe Stock - Pexels
Leestijd: 7 min

Cybersecurity en uitbesteding van operationele activiteiten zijn twee domeinen die steeds prominenter aanwezig zijn in het auditwerkveld. René Ewals, managing partner bij ACS, geeft zijn visie op beide en hoe deze fenomenen elkaar kunnen versterken of juist verzwakken.

Wie zit er digitaal tegenover ons?

“Dat is René Ewals. Sinds 2010 ben ik een van de partners/eigenaren van ACS. ACS is gespecialiseerd in gedragsonderzoek alsmede in audit en assurance, voert opdrachten uit voor zowel het bedrijfsleven als de overheid en geeft opleidingen en trainingen. Mijn professionele achtergrond ligt met name in de bestuurlijke informatiekunde en de IT-audit. Ik heb bij drie van de vier Big-4-kantoren gewerkt (KPMG, PwC en Deloitte), nagenoeg altijd IT-audit en assurance gerelateerd. Tussendoor ben ik de CAE geweest bij een pensioenuitvoerder. Qua nevenfuncties ben ik voorzitter van de Commissie Beroepsregels van NOREA, geef ik af en toe colleges en heb ik meegeholpen in de ontwikkeling van de ISAE 3402 standaard. Deze standaard heeft als doel een antwoord te geven op de risico’s en de uitdagingen die gerelateerd zijn aan outsourcing door assurance over risicomanagement en interne beheersing te verstrekken.”

Uitbesteding, hoe moeten we dat voor ons zien?

“Uitbesteding vindt in veel sectoren plaats. Voorbeelden van ondersteunende processen die veelvuldig worden uitbesteed zijn de loonadministratie en het IT-beheer. Kijk naar pensioenfondsen die het beheer van primaire processen uitbesteden, namelijk de beleggingen en de administratie van haar pensioenverplichtingen aan pensioenuitvoerders en vermogensbeheerders. Bij uitbesteding is altijd sprake van een relatie tussen de gebruikers- en de serviceorganisatie. De gebruikersorganisatie besteedt werkzaamheden uit aan de serviceorganisatie, deze worden (vooraf) contractueel vastgelegd.”

Als u aan cyberrisico’s denkt wat komt er dan meteen bij u op?

“Het cybersecurity en -resiliencesysteemrisico bij uitbesteding.”

René Ewals, ACS: “Internal audit moet de discussie aanslingeren als IT en cybersecurity niet goed geregeld zijn, met als doel dat een organisatie serieus investeert in cybersecurity”

Vertel

“Een groot deel van de uitbestedingsmarkt op IT-gebied is belegd bij een paar conglomeraten. Denk aan partijen als Amazon, Google en Microsoft. Dit concentratierisico heeft tot gevolg dat de impact van een cyberaanval op een van deze partijen enorm kan zijn. Dat kan zelfs maatschappijontwrichtend werken. Maar dat is niet het enige, een grote stroomonderbreking kan ook voor veel problemen zorgen. Zo is Nederland een belangrijk internetknooppunt waar veel IT-infrastructuur voor nodig is (en veel energieconsumptie). Als dat internetknooppunt (tijdelijk) niet beschikbaar is, heeft dat een verlammende werking op mensen, ondernemingen en overheden. Als maatschappij hebben we een paar ‘single points of failure’. Actueel is bijvoorbeeld de grote afhankelijkheid van Russisch gas. We moeten hier dus echt werk van (gaan) maken. Daarnaast kan het concentratierisico een kettingreactie op gang brengen als gevolg van de verwevenheid tussen de vele kleine(re) uitbesteders en de grote serviceorganisaties en de kleine(re) uitbesteders onderling.”

Is dat weleens voorgekomen?

“Ja, ongeveer een jaar geleden. Facebook werkte op dat moment niet (goed) waardoor veel organisaties geen orders

konden ontvangen (klantgegevens van Facebook konden niet gebruikt worden).”

Waar moet een internal auditor vooral op letten?

“Als ik deze vraag betrek op cybersecurity dan ontbreekt het bij (gedeeltelijke) uitbesteding van het beheer van de IT-omgeving vaak aan (harde) eisen die gesteld worden door de gebruikersorganisatie aan de (kwaliteit van de) serviceorganisatie. Ook op het gebied van cybersecurity en -resilience. Wat ik regelmatig zie, is dat er bijvoorbeeld geen duidelijke eisen afgesproken zijn over ‘patching’. Een patch is een installatiebestand dat een kwetsbaarheid of fout in een programma herstelt. Cybercriminelen maken namelijk veelvuldig gebruik van ontdekte ‘gaten’ in software. Als gebruikersorganisatie moet je dus een duidelijk beeld hebben wat je hebt uitbesteed, welke eisen je hebt gesteld aan de serviceorganisatie en welke activiteiten je ‘in-house’ wil blijven doen.”

“Het ontbreekt bij (gedeeltelijke) uitbesteding van het beheer van de IT-omgeving vaak aan (harde) eisen die gesteld worden door de gebruikersorganisatie aan de (kwaliteit van de) serviceorganisatie”

Er bestaan veel cybersecurity frameworks, wat zijn de belangrijkste verschillen?

“Dat klopt. Laten we onderscheid maken tussen op IT gerichte raamwerken en de assurancestandaarden die hiervoor kunnen worden gebruikt. De meest voorkomende assurancestandaarden zijn de ISAE 3000-standaard, het ‘SOC for CyberSecurity’-raamwerk en de ISAE 3402. Belangrijke op IT en security gerichte raamwerken zijn NIST en het CIS-raamwerk van SANS. Daarnaast hebben verschillende regelgevers zo hun eigen eisen op het gebied van cybersecurity opgesteld, waaronder rapportageverplichtingen. Voorbeelden daarvan zijn de EBA, die cyber heeft opgenomen in haar EBA Guidelines on ICT and security risk management en de SEC, die medio 2022 publieke organisaties heeft verplicht CyberSecurity incidenten publiek te maken.”

Licht eens toe

“Het SOC for Cybersecurity-raamwerk is ontwikkeld door de AICPA (American Institute of Certified Public Accountants) en gaat specifiek in op het cybersecurity risk-managementprogramma van een organisatie. Dit raamwerk bevat veel (technische) IT-elementen en stelt organisaties in staat om relevante en waardevolle informatie over de effectiviteit van haar cybersecurity risk-managementprogramma’s te communiceren. Hierdoor creëert een organisatie een duidelijker beeld van de (genomen) cybersecuritymaatregelen, zowel intern als naar buiten toe. Ik zie dit raamwerk overigens (nog) niet veel in Nederland gebruikt worden.”

“ISO/ IEC 27001 is een internationale standaard die richtlijnen geeft hoe je de sturing en beheersing van information security moet inrichten. Dit is een goed gestructureerde certificering, alleen voor de toetsing is geen RA of RE nodig. De verplichtingen voor de onderbouwing van de certificering zijn daarnaast minder stringent. Voorts is het toekomstgericht, hetgeen we met assurance niet kunnen bewerkstelligen. Een externe auditor mag ook niet steunen op een ISO 27001.”

Waar moet je als organisatie nog meer op letten?

“Bij een ISAE-rapport moet je kijken naar of het een type 1- of een type 2-rapport is. Een type 1-rapport geeft één momentopname, als het ware een foto van de situatie op dat moment. Daarentegen geeft een type 2-rapport inzicht over een langere periode met meerdere toetsmomenten in die periode. Meestal beslaat een type 2-rapport een periode van (ongeveer) een jaar. Daarnaast is een formaliteit – maar niet onbelangrijk – te kijken naar wie het rapport formeel heeft ondertekend en of deze persoon de juiste beroepstitel heeft om te mogen ondertekenen.”

En inhoudelijk?

“De reikwijdte van de werkzaamheden moeten aansluiten bij datgene wat je hebt uitbesteed. Ten tweede moet duidelijk worden met welke diepgang de auditor van de serviceorganisatie werkzaamheden heeft verricht. Verder moet de rapportage inzicht geven in hoeverre aan de gestelde eisen is voldaan gedurende de rapportageperiode. Als je kijkt naar de beheersmaatregelen van de serviceorganisatie, dan moeten die natuurlijk aan de verwachtingen voldoen (vereist of niet). In deze assurancerapportages is altijd zichtbaar welke beheersmaatregel effectief is of niet.”

“Inzoomend op cybersecurity zie je vaak niet terug in de rapporten hoeveel cyberaanvallen aantoonbaar succesvol zijn afgeslagen. Of waarvan de impact gering is geweest door snelle detectie en de juiste respons. Dit is namelijk hét bewijs dat de getroffen cybersecurity- en resiliencemaatregelen hebben gewerkt. Natuurlijk zie je steeds meer dat aanvallen worden nagebootst door bepaalde tests uit te (laten) voeren, zoals ‘pentesten’ en ‘red teaming’. Grotere ondernemingen hebben ook security operations centers (SOC) die al het (interne en externe) netwerkverkeer monitoren. Desalniettemin, je weet nooit wanneer, waar en hoe een echte aanval gaat plaatsvinden.”

“Het ene ISAE-rapport is het andere niet, voornamelijk als je kijkt naar de diepgang, de technische beschrijvingen en de (onderliggende) werkzaamheden van de auditor”

Is het lezen van een ISAE-rapport voldoende?

“De gebruikersorganisatie en haar auditors moeten het rapport in detail tot zich nemen en eruit halen wat voor hen van belang is. Een externe auditor kijkt met name vanuit het perspectief van de jaarrekeningcontrole. De

gebruikersorganisatie en internal auditor gebruiken de rapportage als onderdeel van hun toezicht op de serviceorganisatie en hebben daarnaast wellicht andere inzichten nodig om bij te dragen aan de organisatiedoelen."

"Het ene ISAE-rapport is overigens het andere niet, voornamelijk als je kijkt naar de diepgang, de technische beschrijvingen en de (onderliggende) werkzaamheden van de auditor. Het kan dus verstandig zijn om na het lezen van het rapport met de betreffende auditor te spreken (wel langs de lijnen van de serviceorganisatie). En dat gebeurt lang niet altijd! Grotere serviceorganisaties stellen soms maar één ISAE-rapportage op ten behoeve van al haar afnemers. Deze rapportage bevat vaak generieke beschrijvingen, zodat het de meerderheid van de uitbestede werkzaamheden van alle afnemers dekt, maar net niet die, die voor jou relevant zijn. Door aanvullende toelichting te vragen, kom je sneller tot de kern die er voor jouw onderneming echt toe doet."

Voorkomen (preventie) is beter dan genezen (detectie), geldt dat ook voor cyberrisico's?

"Ja, alleen zijn preventieve maatregelen soms erg duur en wil het management daaraan mogelijk geen geld uitgeven. Daar staat tegenover dat als je als organisatie gehackt wordt of slachtoffer wordt van ransomeware de kosten van repareren hoog zijn. Bovendien loop je als organisatie reputatierisico. Daarnaast moet een organisatie detectie- en responsmaatregelen nemen om te kunnen reageren als een cyberrisico zich voordoet."

René Ewals, ACS: "Een grote stroomonderbreking kan voor veel problemen zorgen. Nederland is een belangrijk internetknooppunt. Als dat internetknooppunt niet beschikbaar is, heeft dat een verlammende werking op mensen, ondernemingen en overheden"

Is er voldoende awareness bij raad van besturen?

"Schoorvoetend reserveren RvC's steeds vaker geld voor cybersecurity. Aarzelingen komen vaak door het gebrek aan kennis op het gebied van IT. Daarnaast geven ze geld uit om iets niet te laten gebeuren. Investeren in cybersecurity heeft geen directe opbrengst en de effectiviteit is lastig te monitoren. Als een cybersecurityrisico zich niet voordoet merkt niemand er wat van."

Wat is de rol van internal audit?

“Internal audit heeft een signalerende functie. Zij moeten de discussie aanslingeren als IT en cybersecurity niet goed geregeld zijn, met als doel dat een organisatie serieus investeert in cybersecurity. Daarnaast heeft internal audit een rol in het aantonen van de effectiviteit van de genomen maatregelen. Enerzijds om aan te geven dat de maatregelen werken en anderzijds om inzicht te geven in de huidige risico’s. Eén ding is namelijk zeker: cybersecurityrisico’s gaan niet meer weg.”

Is er nog een onderwerp om te bespreken?

“Ja, ‘air gapping’. Het is belangrijk dat bepaalde onderdelen van het netwerk, zeker de back-ups, disconnected zijn van internet. Daarnaast moet je bewaken en bij voorkeur controleren of de back-ups niet besmet zijn met ransomware en/of andere malware. Deze back-ups zijn nodig om het netwerk opnieuw op te bouwen indien de organisatie wordt geraakt door een ransomware-aanval.”

Over
René Ewals is een van de managing partners van ACS. ACS is gespecialiseerd in audit en assurance alsmede gedragsonderzoek. Ewals heeft mede de ISAE3402-standaard ontwikkeld en deed eerder ervaring op bij onder andere KPMG, PwC en Deloitte.

Tags: Cyber resilience, informatiebeveiliging

Bron url: https://auditmagazine.nl/interviews/uitbesteding-vergeet-de-cyber-risks-niet/