AUDIT
MAGAZINE

INTERVIEWS | 1 DECEMBER 2022

“HET TEKORT AAN MENSEN MET KENNIS VAN CYBERSECURITY IS EEN UITDAGING”

Auteur: Naeem Arif EMIA RO - Drs. Marc van der Veen RA RO CIA RMFI
Beeld: Adobe Stock
Leestijd: 6 min

De Inspectie Leefomgeving en Transport (ILT) houdt onder andere toezicht op de cybersecurity van bepaalde bedrijven die essentiële diensten leveren. De ILT is bezig om dit toezichtsthema in te bedden in haar bedrijfsvoering en processen, aldus Mineke de Lange en Peter Konings. Een kijkje in de keuken van de toezichthouder.

Wie zijn Mineke de Lange en Peter Konings?

Mineke de Lange (MdL): “Ik ben programmamanager cybersecurity binnen de ILT. Dit programma heeft als doel om cybersecurity een volwaardig onderdeel te maken van het toezichtsspectrum van de ILT. Hiervoor werkte ik bij het ministerie van Onderwijs, Cultuur en Wetenschappen.”

Peter Konings (PK): “Ik ben inspecteur op het gebied van cybersecurity en voer nu al meer dan een jaar cybersecurityinspecties uit bij onder toezicht staande organisaties van de ILT. Ik heb een achtergrond in cybersecurity en informatiebeveiliging.”

Wat is de primaire taak van ILT?

PK: “ILT staat voor Inspectie Leefomgeving en Transport en is een onderdeel van het ministerie van Infrastructuur en Waterstaat (IenW). De ILT houdt toezicht op diverse terreinen. Denk aan: waterkwaliteit, genetisch gemodificeerd voedsel, luchtvaart, personenvervoer, vervoer van gevaarlijke stoffen, et cetera. Sinds de introductie van de Wet beveiliging netwerk- en informatiesystemen (Wbni) is de ILT ook verantwoordelijk voor het toezicht op cybersecurity bij aanbieders van essentiële diensten.”

Mineke de lange, ILT: “Diverse incidenten hebben aangetoond dat het maatschappelijk belang van cybersecurity nauwelijks kan worden onderschat”

MdL: “De Wbni vormt dus de basis voor het toezicht op cybersecurity door de ILT. Het mandaat van de ILT vloeit vervolgens voort uit het Besluit beveiliging netwerk- en informatiesystemen (Bbni). In dit besluit wordt de toezichthouder ‘gekoppeld’ aan bepaalde sectoren waarop zij toezicht uitoefent. Daarnaast is er de ministeriële regeling (MR), deze regeling definieert het minimale niveau van beveiliging, inclusief een normenkader voor cybersecurity.”

Wat doet de ILT op het gebied van cybersecurity?

MdL: “Toezicht op cybersecurity is voor de ILT zoals gezegd een relatief nieuwe taak. Diverse incidenten hebben aangetoond dat het maatschappelijk belang van cybersecurity nauwelijks kan worden onderschat. Denk aan een brug die via internet bediend kan worden met bijvoorbeeld de naam van de brug als wachtwoord. Zo zijn er talloze voorbeelden te noemen die in potentie de maatschappij kunnen verlammen en waar toereikende beveiliging dus van essentieel belang is.”

MdL: “De Rijksoverheid heeft op basis van een rijksbrede risicoanalyse bepaalde sectoren aangewezen als vitaal. Voorbeelden van vitale sectoren zijn: drinkwater, luchtvaart, havens en onlangs zijn daar spoor- en wegvervoer bij gekomen. Bedrijven in deze sectoren zijn aanbieders van essentiële diensten en op hen wordt in het kader van de Wbni dus door de ILT toezicht gehouden.”

Peter Konings: “Criminelen en statelijke actoren als vreemde mogendheden vormen een bedreiging voor de aanbieders van essentiële diensten”

PK: “Er zijn verschillende actoren actief die belangen hebben om via het cyberdomein invloed bij organisaties uit te oefenen: cybercrime door criminelen en door statelijke actoren. Criminelen kunnen groepen of individuen zijn die primair uit zijn op financieel gewin. Statelijke actoren zijn vreemde mogendheden/overheden die door sabotage schade willen aanrichten of bepaalde innovatieve kennis willen stelen. Beide typen actoren hebben hun eigen dynamiek en drijfveren en vormen een bedreiging voor de aanbieders van essentiële diensten.”

Hoe bereidt ILT zich voor op deze nieuwe taak?

MdL: “Momenteel loopt er een programma bij de ILT dat als doel heeft om toezicht op cybersecurity volwaardig te verankeren in de bedrijfsvoering en processen van de ILT. Zo komt er een nieuwe afdeling Toezicht cybersecurity. Daarnaast worden collega’s op dit vakgebied opgeleid binnen de ILT en worden nieuwe collega’s geworven die als cybersecurityinspecteur aan de slag kunnen. Kortom, de ILT investeert momenteel om zich voor te bereiden op haar taak en deze ook professioneel uit te kunnen voeren.”

PK: “Bij de cybersecurityinspecties die nu al worden uitgevoerd vormen de Wbni en de MR dus de basis voor de uit te voeren werkzaamheden. Omdat deze wet en regeling niet hele concrete toetsbare normen aanreiken, hebben wij het afgelopen jaar, in samenwerking met het programma, een toezichtsvisie en een toetsingskader ontwikkeld en uitgerold. Dit kader wordt momenteel gebruikt om inspecties uit te voeren.”

Peter Konings, ILT: “Wij zijn inmiddels zover dat bedrijven intrinsiek gemotiveerd zijn om cybersecurity op orde te hebben en niet omdat de ILT langskomt”

Hanteert ILT in de praktijk de term cybersecurity of cyber resilience?

PK: “Mijns inziens is dat semantiek. Beide termen gaan uiteraard hand in hand. Vroeger noemden we het gewoon informatiebeveiliging, nu is hier wel de fysieke component aan toegevoegd. Hoe dan ook, het is van belang dat organisaties in het algemeen en voor de ILT de aanbieders van essentiële diensten in het bijzonder, kunnen aantonen

dat zij in staat zijn zich te wapenen tegen cyberaanvallen. Beveiliging vooraf en weerbaarheid achteraf spelen daarin een belangrijke rol."

Is cybersecurity in alle sectoren even belangrijk of is dit thema in bepaalde sectoren belangrijker?

PK: "Zoals gezegd is cybersecurity een maatschappelijk zeer relevant onderwerp. De risico's/dreigingen en dynamiek zijn per sector heel verschillend en de impact van een cyberaanval kan ook verschillend zijn, zowel per aanbieder van een essentiële dienst als per sector."

MdL: "Risicogestuurd toezicht helpt ons om met de huidige capaciteit gericht toezicht uit te kunnen oefenen op die sectoren of bij die organisaties waar de risico's het grootst zijn."

Welke risico's springen eruit op het gebied van cybersecurity?

PK: "Zonder twijfel ransomware. Dergelijke software kan zich nestelen in het systeem waardoor criminelen of statelijke actoren alle data kunnen gijzelen door het te versleutelen. En zoals de naam van de aanval al zegt, wordt bij dergelijke aanvallen losgeld gevraagd om de versleutelde data of informatiesystemen weer vrij te geven. De beheersing op dit vlak begint, zoals zo vaak, met bewustzijn bij de medewerkers. Daarnaast zullen organisaties ook technische en andere organisatorische maatregelen moeten treffen om zich te wapenen tegen ransomware-aanvallen."

Mineke de Lange: "Voorbeelden van vitale sectoren zijn drinkwater, luchtvaart, havens, spoor- en wegvervoer. Op bedrijven in deze sectoren houdt de ILT toezicht"

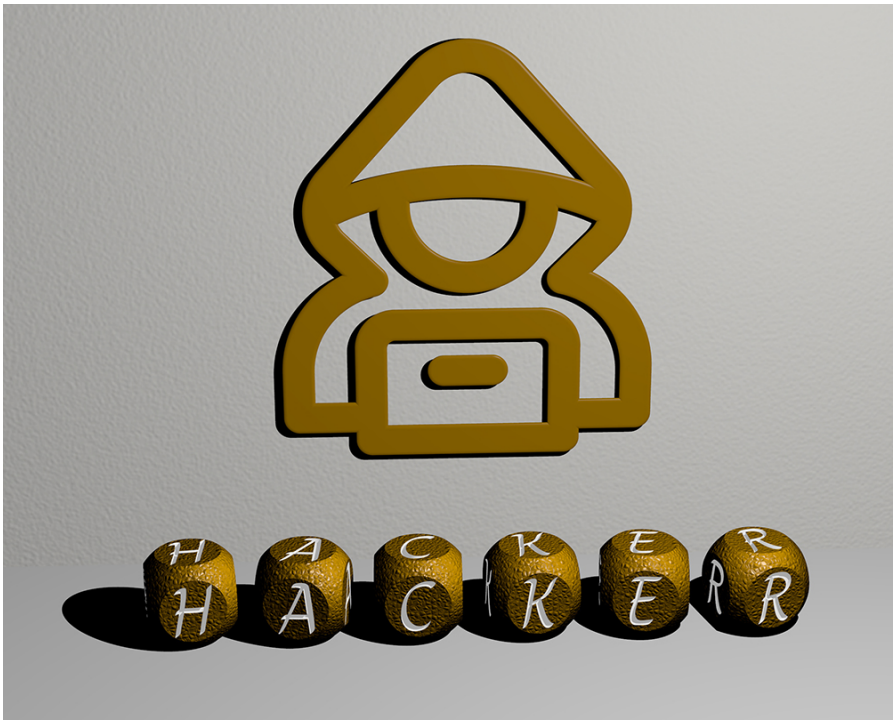
PK: "Verder zijn de risico's die voortvloeien uit de zogeheten supply chain belangrijk. Denk aan veiligheid van software van leveranciers die gebruikt wordt of in de samenwerking met andere ketenpartners. Met andere woorden, er moeten tevens eisen gesteld worden aan de leverancier van software om de risico's in de keten afdoende te kunnen beheersen."

MdL: "Awarenessprogramma's zijn inderdaad heel belangrijk. Dat geldt ook voor het draagvlak bij het topmanagement voor cybersecurity. Als de leiding het belang van de cybersecurity niet ziet of uitdraagt, dan uit dat zich doorgaans in matige beheersing van cyberrisico's. Kortom, de 'tone at the top' op het gebied van cybersecurity is van groot belang."

Hoe kunnen organisaties zich wapenen tegen dergelijke risico's/dreigingen?

PK: "De essentie is dat een organisatie een goed functionerend managementsysteem moet hebben voor cyberrisico's. Dat wil zeggen actuele risicoanalyses, geïmplementeerde beheersingsmaatregelen en periodiek toetsen of de getroffen maatregelen naar behoren werken. Zo niet, dan moet er een interventie volgen van het management. Kortweg, de organisatie moet in control zijn ten aanzien van cybersecurity en moet daar een terugkerende cyclus voor hanteren. Wij kunnen als toezichthouder vanuit onze taak vaststellen of het managementsysteem vervolgens naar behoren functioneert."

PK: "Wij zien onszelf als 'uitdager' op het gebied van cybersecurity. Wij zijn inmiddels zover dat bedrijven intrinsiek gemotiveerd zijn om cybersecurity op orde te hebben. Ze doen het niet omdat de ILT langskomt. Zij doen het omdat hun bedrijfsuitoefening en continuïteit hierbij gebaat is. We komen de houding tegen: wij hebben alles gedaan wat we konden bedenken, vertel maar wat we nog beter kunnen doen. Dat is een hele positieve en productieve grondhouding. Daarom zien we onszelf als 'uitdager' op het gebied van cybersecurity."



MdL: “Het tekort aan mensen met kennis van cybersecurity is wel een uitdaging voor veel onder toezicht staande organisaties. Die kennis is namelijk heel schaars. Dus er liggen volop kansen voor mensen die het domein van cybersecurity willen betreden, bij onze onder toezicht staande organisaties maar zeker ook bij de ILT.”

Welke actualiteiten of thema’s spelen er nog meer op dit moment?

PK: “Door de nieuwe Europese NIS2-wetgeving zien wij grote uitdagingen ontstaan, omdat het aantal onder toezicht staande organisaties enorm gaat stijgen. Daardoor zal ons toezicht breder en gerichter moeten worden. Naast dat we nu al weten dat de nieuwe afdeling in de nabije toekomst een flinke groei zal doormaken, zal ook onze aanpak en methodiek wellicht aangepast moeten worden zonder dat we aan kwaliteit inboeten.”

MdL: “Daarom zijn we nieuwe collega’s aan het werven en collega’s aan het opleiden zodat zij deze aanstaande uitdagingen aan kunnen. De ILT is wat dat betreft een hele interessante omgeving omdat we toezicht houden op zoveel verschillende sectoren en tegelijkertijd ons toezicht er echt toe doet, gelet op de organisaties waar wij toezicht op houden.”

Peter Konings: “Er is een dunne lijn tussen het uitvoeren van een inspectie en het doen van een audit. Immers, beide vormen een oordeel over het functioneren van het beheersingssysteem op een bepaald vlak”

Waar zien jullie overeenkomsten of verschillen tussen inspecties en het uitvoeren van audits?

PK: “Er is een dunne lijn tussen het uitvoeren van een inspectie en het doen van een audit. Immers, beide vormen een oordeel over het functioneren van het beheersingssysteem op een bepaald vlak. En net als auditors lopen wij zogeheten collisiegevaar; daarom mogen wij onder toezicht staande organisaties niet adviseren. Andere beleidsonderdelen van het ministerie mogen dat wel. Dergelijke beleidsafdelingen stimuleren bepaalde sectoren/bedrijven om cybersecurity goed

op orde te hebben. De ILT heeft uiteraard wel afstemming met deze beleidsonderdelen. Uiteraard zijn er ook verschillen want een inspecteur kan, afhankelijk van de geldende escalatieladder, sancties opleggen. Dat geldt voor een auditor niet."

Over
Mineke de Lange is programmanager cybersecurity bij ILT. Daarvoor werkte zij bij het ministerie van Onderwijs, Cultuur en Wetenschappen.

Peter Konings is cybersecurityinspecteur bij ILT. Hij heeft een achtergrond in cybersecurity en informatiebeveiliging.

Tags: Cyber resilience

Bron url: https://auditmagazine.nl/interviews/het-tekort-aan-mensen-met-kennis-van-cybersecurity-is-een-uitdaging/