NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Manifest

Op naar een digitaal weerbare samenleving

maart 2023

Deze pdf is klikbaar. Gebruik de tabbladen en de knoppen om te navigeren.

©2023 – NOREA Manifest

Voorwoord

Deze publicatie bevat de bijdrage van de IT-audit community aan het streven naar een digitaal weerbare samenleving, naar aanleiding van het 6e lustrum van NOREA, de beroepsorganisatie van geregistreerde IT-auditors. We geven vier adviezen die we in dit document onderbouwen.

Vier adviezen om de digitale weerbaarheid te verbeteren

- Positioneer digitale weerbaarheid als een zaak voor iedereen in de organisatie. (Cyber) security is geen afdeling maar is van iedereen, van bestuurders tot operationeel medewerkers.
- Leg externe verantwoording af over de IT-beheersing binnen een organisatie en geef daarmee een impuls aan deze verantwoordelijkheid.
- Breng de digitale samenwerking binnen ketens en sectoren naar een hoger niveau. Deze samenwerking gaat over kennisuitwisseling, gezamenlijk testen, een collectief zicht op dreigingen, uitwisseling van waarschuwingen en leren van elkaars aanpak. Dit is organisatie-overstijgend en juist daarom kunnen toezichthouders en regelgevers hier het initiatief nemen.
- Breng het vakmanschap van IT-professionals omhoog. Geef het thema beheersing van IT al een plek op de basisschool, en zet in op normering van opleiding, kennis en ervaring van IT-professionals.

Mission Possible: samenwerken aan digitale weerbaarheid

Digitaal is het nieuwe normaal. Al enige tijd. Digitale technologie is de backbone van vrijwel alles wat we doen, van het sturen van een simpel app-bericht tot de ingewikkelde logistiek op een luchthaven.

Digitale technologie biedt grote voordelen op het vlak van efficiency en levert al jaren een niet aflatende stroom toepassingen op waar we twintig jaar geleden alleen maar van konden dromen. Het maakt ons leven gemakkelijker en vaak ook leuker. Naast deze mooie kant is er echter ook een lelijke kant.

Systemen kunnen bijvoorbeeld worden platgelegd door kwaadwillenden; (persoonlijke) data kan op straat komen te liggen na een hack; intellectueel eigendom kan (on-gemerkt) worden gestolen; en zelfs de democratie kan op het spel komen te staan door digitale beïnvloeding van besluitvorming.

De maatschappelijke uitdaging is dan ook duidelijk: we willen ruim baan geven aan de mooie kant en tegelijkertijd de lelijke kant temmen. Oftewel: zorgen dat we digitaal weerbaar zijn. Als maatschappij, maar ook op het niveau van individuele organisaties.

Het vakgebied IT-audit speelt daarin een centrale rol. IT-auditors werken elke dag aan veilige en betrouwbare informatietechnologie, in een adviserende en controlerende rol. Het is een rol die hen vanuit hun kennisgebied op het lijf geschreven is. Het is echter ook een rol die continu moet

©2023 - NOREA Manifest

Voorwoord (vervolg)

doorontwikkelen, omdat ook de uitdaging zelf zich door-ontwikkelt. Er komen bijvoorbeeld voortdurend innovaties op die gevolgen hebben voor onze digitale weerbaarheid. Denk aan het gebruik van algoritmes die menselijke besluitvorming overnemen of ondersteunen; of wat verder weg in de tijd, denk aan de opkomst van quantum computing dat grote gevolgen heeft voor informatiebeveiliging.

Ook de afhankelijkheid van digitale technologie neemt toe in een maatschappij waar vrijwel alles via internet met

elkaar verknoopt is. Daarbij gaat het nadrukkelijk ook om de kwetsbaarheid van de fysieke wereld: een digitale aanval of een computerstoring kunnen ervoor zorgen dat winkels niet meer worden bevoorraad, snelwegen moeten worden afgesloten, treinen en (lucht)havens tot stilstand komen of fabrieken stilvallen.

Tot slot ontwikkelt ook het karakter van de digitale dreigingen zich. In de begindagen ging het nog vooral om individueel opererende 'script kiddies' of storingen in hardware; nu is er sprake van professioneel georganiseerde criminele groepen (en soms ook statelijke actoren) met duidelijke strategieën die vaak ook goed gefinancierd zijn. En de explosieve toename van clouddiensten maakt de leveranciers hiervan tot een 'nieuwe' achilleshiel van onze maatschappij.

De uitdaging evolueert dus voortdurend en we moeten daarom blijven werken aan digitale weerbaarheid. Wie berichten in de media tot zich neemt zou wat moedeloos kunnen worden vanwege de veelheid aan (ingrijpende) incidenten. Ten onrechte. We hebben de middelen, de kennis en de infrastructuur om de genoemde lelijke kant te temmen. Maar dan moet er wel wat gebeuren, zoals anticiperen in plaats van reageren en de handen meer ineenslaan. We moeten burgers aantonen dat ze digitale technologie kunnen (blijven) vertrouwen. En de volgende stap zetten in transparantie over (de betrouwbaarheid van) IT.

Dat we als maatschappij sneller stappen moeten gaan zetten werd ook duidelijk tijdens het lustrum dat NOREA organiseerde op 19 mei 2022. De sessies leverden een schat aan inzichten op vanuit het IT-auditvak – een belangrijke community bij het borgen van digitale weerbaarheid. De belangrijkste bevindingen leest u hierna in dit manifest in de vorm van 6 thema's die als rode draad naar voren kwamen.

Een ding staat vast: investeren in digitale weerbaarheid is geen luxe. Er staat veel op het spel. Als digitaal het nieuwe normaal is, dan moet digitale weerbaarheid dat ook worden. En het rapporteren daarover ook. En dat alles is zeker niet onmogelijk. Het is een mission possible.

Namens de beroepsorganisatie van IT-auditors,

Bestuur NOREA
maart 2023

©2023 – NOREA Manifest

Een sterke keten ontstaat alleen als elke bestuurder verantwoordelijkheid neemt

Digitale weerbaarheid is een verantwoordelijkheid van ons allemaal; daarom moet het *chefsache* worden voor bestuurders, zeker in een digitaal verknoopte wereld. Zij moeten het belang actief uitdragen en kunnen dit niet wegdelegeren. Dit is niet langer vrijblijvend, men moet zich naar stakeholders kunnen verantwoorden.

Hoe zorg je dat je de hoogste kwaliteit producten levert? Door het inrichten van een afdeling kwaliteit met gespecialiseerde professionals en hoogwaardige tools? Nee. Kwaliteit ontstaat alleen als de hele organisatie ervan overtuigd is waarom kwaliteit belangrijk is. Kwaliteit is geen afdeling.

Dit is gesneden koek voor elke bestuurder.

Precies hetzelfde geldt echter voor digitale weerbaarheid en de daarvoor benodigde cybersecurity. Ook dat is geen afdeling maar een verantwoordelijkheid van iedereen. Het thema overlaten aan specialisten doet geen recht aan de grote maatschappelijke uitdaging en kan bovendien schijn-zekerheden opleveren. Want dan zullen niet-specialisten het niet als hun probleem zien en zodra er dan incidenten optreden zal er vooral worden geïnvesteerd in verdere versterking van de specialistische afdeling. Een heilloze weg.

Bestuurders binnen overheid en bedrijfsleven moeten dan ook hun verantwoordelijkheid nemen door digitale weerbaarheid als een *chefsache* te beschouwen en dat ook te laten zien in woord en daad. Ze kunnen deze verantwoordelijkheid niet delegeren aan specialisten.

Dat vraagt onder andere om hun besef dat het bij dit thema om meer gaat dan het gebruik van geavanceerde technologie om risico's te beheersen. Digitale weerbaarheid gaat over techniek én over mensen. Het is onvermijdelijk dat organisaties te maken krijgen met zwaktes, lekken of gaten in de systemen die ze gebruiken en dus is het ook van groot belang om die technische kant goed te beheersen. Maar de mens is en blijft vaak de zwakste schakel en investeren in de allerbeste tools is dan ook alleen maar zinvol als mensen hun verantwoordelijkheden op dit punt begrijpen. Social engineering – waarbij hackers het vertrouwen winnen van mensen met slim sociaal gedrag en zich daarmee toegang verschaffen tot systemen – blijft een van de belangrijkste risico's en de praktijk laat zien dat ook CEO's hier kwetsbaar voor zijn.

©2023 – NOREA Manifest

Een sterke keten ontstaat alleen als elke bestuurder verantwoordelijkheid neemt (vervolg)

Het creëren van dit besef is overigens geen vanzelfsprekendheid in een wereld waarin leveranciers en hun proposities een dominante rol spelen. Bovendien is het een wereld die wat ongrijpbaar is voor generalisten vanwege het technisch jargon en het gespecialiseerde karakter.

De echte uitdaging zit erin om aandacht voor digitale weerbaarheid te integreren in alle aspecten van een organisatie. Het betekent bijvoorbeeld dat het digitale bewustzijn onderdeel moet worden van het HR-beleid, maar ook dat het een centrale plaats moet krijgen bij de ontwikkeling van nieuwe IT-systemen. En dus niet, zoals vaak gebeurt, op het einde van zo'n project pas gaan nadenken over de veiligheid, privacy, robuustheid, etc.

Dit verhaal moet onophoudelijk worden verteld door bestuurders. En duidelijker dan het nu gebeurt want er staat veel op het spel. Het gaat over continuïteit van onze maatschappij en de huidige vrijblijvendheid moet eruit. Het onderwerp moet continu op de bestuurstafel geagendeerd en actief bestuurd worden. Het afleggen van externe verantwoording erover draagt eraan bij dat het onderwerp hoog op de agenda blijft. Ook persoonlijk voorbeeldgedrag door deze bestuurders is een belangrijk punt.

Het gaat hier om het doorvoeren van een majeure verandering in onze manier van denken. Niet alleen voor het MKB (daar heeft het wel de grootste impact waarschijnlijk) maar ook voor (semi-)Overheid en Toezichthouders.

Handelingsperspectief:

- Iedere CEO of bestuursvoorzitter moet digitale weerbaarheid vol overtuiging in portefeuille nemen en pro-actief uitdragen.
- Digitale weerbaarheid wordt gepositioneerd als een zaak voor iedereen in de organisatie.
- Het afleggen van externe verantwoording geeft een impuls aan deze verantwoordelijkheid.

©2023 - NOREA Manifest

Als inbraken toch vrijwel zeker zijn is het ook zaak om de schade te beperken

Cybersecurity is business as usual geworden; een goed beleid gaat niet alleen over sterke muren en dijken maar ook over maatregelen om de impact van incidenten te beperken. Preventie is goed. Preventie in combinatie met een goede response nog beter.

Het is niet de vraag óf een organisatie wordt aangevallen door hackers, maar wanneer. Bovendien is de kans ook groot dat zo'n aanval een keer succesvol is. Een 100% bescherming is dan ook simpelweg onmogelijk. Vaak is het ook onwenselijk omdat het streven naar 100% tot een onwerkbare (of zeer kostbare) situatie zou leiden.

Deze redenering wordt door velen onderschreven. Cybersecurity is in feite 'business as usual' geworden. Maar de redenering wordt maar beperkt vertaald naar een uitgebalanceerd beleid voor cybersecurity. Daarom is het nodig om het thema vanuit het perspectief van risicomanagement te bekijken. Dat vraagt om inzicht in risico´s vanuit het perspectief van de organisatie én vanuit de crimineel. De organisatie moet nadenken over de zaken die bescherming verdienen (de 'kroonjuwelen') en ook in de huid kruipen van indringers om hun denk- en handelwijze te doorgronden. Op basis hiervan wordt geïnvesteerd in preventie. Daarnaast gaat het om het signaleren van verdachte activiteiten (detectie) en het nemen van maatregelen om incidenten direct op te pakken (respons). De huidige praktijk leert dat de nadruk nu ligt op preventie (het opwerpen van stevige dijken die indringers moeten tegenhouden).

Wie echter doordrongen is van het feit dat cybersecurity 'business as usual' is – begrijpt direct het belang van een adequate respons. Organisaties moeten na een incident – variërend van diefstal van intellectuele eigendom of persoonlijke data tot een ontwrichting van kernsystemen – snel zaken op orde kunnen krijgen. Want als een inbreker zich toegang heeft verschaft is er nog geen of maar beperkte schade aangericht. Op dat moment gaat het om snel handelen om vervolgschade te voorkomen of te beperken.

Dat is niet eenvoudig. Extern vraagt het om het in de gaten houden van dreigingen: welke beweging zien we in het gedrag van malafide partijen en welke kwetsbaarheden willen ze misbruiken. De daaruit voortvloeiende zwakheden kunnen op basis daarvan worden aangepakt (bijvoorbeeld door patching). Ook intern vraagt het om een continue monitoring om in staat te zijn adequaat te reageren op

©2023 – NOREA Manifest

Als inbraken toch vrijwel zeker zijn is het ook zaak om de schade te beperken (vervolg)

incidenten. Tot slot is het ook zaak om voortdurend te testen of de maatregelen ook daadwerkelijk werken als dat nodig is.

Het hanteren van het perspectief van risicomanagement vraagt ook om een rationele kijk op de zaak. ‘de hacker is een wekker’, zo wordt wel eens gezegd om aan te geven dat incidenten de angst aanwakkeren om slachtoffer te worden en daarmee een impuls geven aan investeringen in cybersecurity. Angst is echter een slechte raadgever om dit thema goed aan te pakken. Een goede aanpak vraagt zoals gezegd niet alleen om kennis van je vijand maar vooral ook om kennis van wat de waardevolste dingen te verdedigen zijn (de kroonjuwelen). Simpel gesteld: de impact van een gehackt zaalreserveringssysteem is van een andere orde dan malware in kernsystemen van een netbeheerder. Het is dan ook van het grootste belang om te weten wat de kritieke processen zijn inclusief bijbehorende assets. Het gaat hierbij niet alleen om interne assets, maar in een sterk genetwerkte wereld ook om de interfaces met externe partijen in het ecosysteem.

Handelingsperspectief:

- Beschouw cybersecurity als business as usual: het hoort er gewoon bij en het vraagt net als bij andere risico’s om een goede voorbereiding, analyse van scenario’s en voldoende oefenen daarvan.
- Digitale weerbaarheid vraagt niet alleen om een sterke verdediging maar ook om maatregelen om de impact van incidenten snel in te perken.

©2023 – NOREA Manifest

Spelregels zijn nodig om vertrouwen in nieuwe technologie te behouden

Om het vertrouwen van de maatschappij in digitale technologie te behouden is een nieuwe modus in toezicht op samenwerking mens-machine nodig, ook al omdat veel organisaties nog een onvolwassen beleid hebben op dit punt.

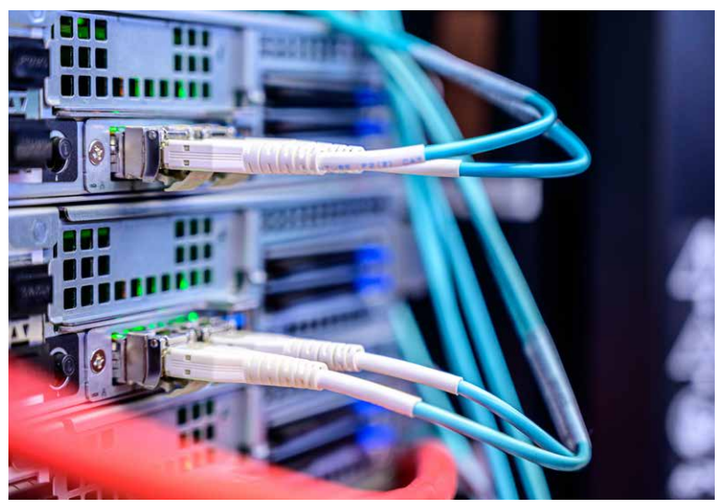
Digitale technologie speelt een centrale rol in ons leven, ook in de beslissingen die we nemen. Geautomatiseerde modellen (algoritmes, al dan niet gebaseerd op kunstmatige intelligentie) helpen ons beslissingen te nemen op basis van de informatie die we erin stoppen. Huisartsen stellen bijvoorbeeld diagnoses met behulp van deze technologie. Nieuwsmedia schotelen ons een gepersonaliseerde newsfeed voor op basis van wat ze van ons weten. En zo kunnen we nog wel even doorgaan. Technologie 'gidst' ons door het leven.

Nieuwe technologie brengt ons kortom veel innovatie. Ook de nieuwe vraagstukken die daarmee ontstaan vragen om innovatie, onder meer op het vlak van het omgaan met nieuwe risico's.

Als gevolg van de dominante rol van technologie komt bijvoorbeeld steeds vaker de vraag op – mede naar aanleiding van incidenten – of die technologie wel deugt. Daarbij gaat het niet alleen om de in de media veel voorkomende vraag of algoritmes geen vooroordelen hanteren over bepaalde groepen op basis van de gebruikte datasets. Het gaat in bredere zin over de vraag of de technologie onder de motorkap wel goed is opgezet en de juiste afwegingen maakt. Bovendien gaat het niet alleen om de 'technische' afwegingen onder de motorkap maar ook over de vraag of de organisatie de uitkomsten wel goed begrijpt en deze op een (ethisch) verantwoorde manier toepast.

Er staat veel op het spel: als het mis gaat is het vertrouwen weg, en wordt daarmee ook het fundament onder de technologie weggeslagen. Precies daarom is het zaak om toe te zien op een deugdelijke ontwikkeling van deze toepassingen (kwaliteit en betrouwbaarheid). Politici, wetgevers en toezichthouders zijn nog zoekende naar hoe dat precies moet. Ze benadrukken het belang van uitlegbaarheid en controleerbaarheid (Explainable AI, XAI) maar realiseren zich ook steeds meer dat daar grenzen aan zitten.

Het is dan ook zaak om op zoek te gaan naar hoe mens en machine op een verantwoorde manier kunnen samenwerken.



©2023 – NOREA Manifest

Spelregels zijn nodig om vertrouwen in nieuwe technologie te behouden (vervolg)

Vragen die daarbij spelen zijn: Welk typen toepassingen zijn er? Welke snelheid van beslissen is nodig? Welke risico's spelen een rol? Hoe ingewikkeld is de besluitvorming onder de motorkap? Is de beschikbare data wel geschikt om tot betrouwbare uitkomsten te komen? Welke belangen worden gediend met de toepassingen? Afhankelijk van de antwoorden kan dan worden bepaald welke rol een mens moet (blijven) spelen en waar een machine een dominante rol kan hebben.

In dat kader hebben toezichthouders al risicoprofielen gedefinieerd. Bepaalde typen kunstmatige intelligentie zijn verboden – denk aan subliminal techniques (mensen misleiden), misbruik van kwetsbare mensen, social scoring (mensen sturen naar een bepaald gedrag. Voor toepassingen met een hoger risico – toegang tot financiering, overheidssteun, onderwijs basisschool selectie, Artificial Intelligence in cruciale infrastructuur – zijn regels gedefinieerd.

Het gaat hier echter voor een groot deel nog om onontgonnen gebied, waar meer handvatten zeer wenselijk zijn. Meer duidelijkheid is nodig, juist omdat het maatschappelijk vertrouwen hier op het spel staat. Tegelijkertijd kunnen nieuwe regels ook ongewenste effecten hebben. Ervaring op andere gebieden leert dat een te strikt keurslijf vooruitgang

in de weg kan staan. Dat kan (deels) worden voorkomen door nauwe samenwerking tussen gebruikers en regelgevers.

Hoe dan ook gaat het om een thema dat bestuurders van organisaties zich ter harte moeten nemen. In het geval van ondeugdelijke algoritmes lopen deze organisaties grote (reputatie)risico's. Op dit domein kennen veel organisaties nog geen volwassen methodes voor het beheersen van risico's.

Handelingsperspectief:

- Organisaties moeten (beter) beleid ontwikkelen over hoe ze komen tot verantwoord gebruik van nieuwe digitale technologie (zoals AI).
- De behoefte aan duidelijke spelregels op dit punt moet worden ingevuld in nauwe samenwerking tussen gebruikers en regelgevers.

©2023 – NOREA Manifest

Digitale samenwerking is noodzakelijk voor sterke ketens

Een keten is zo sterk als de zwakste schakel; meer samenwerking biedt potentieel voor hogere weerbaarheid. Partijen zijn van elkaar afhankelijk en kunnen alleen samen een krachtige vuist maken. Dit vraagt om voortbouwen op en doorontwikkeling van bestaande initiatieven.

Digitale technologie knoopt organisaties steeds nauwer aan elkaar vast. Organisaties stellen hun IT-landschap bijvoorbeeld open voor een breed scala van toepassingen via alle denkbare mobiele apparaten en zijn daarmee voor de veiligheid mede afhankelijk van andere organisaties. Bovendien is de continuïteit van kernprocessen – zowel maatschappelijk als binnen bedrijven, zowel fysiek als digitaal – steeds meer afhankelijk van IT. Een verstoring ervan – al dan niet door moedwillige inbraak van buiten – kan dan ook een grote impact hebben. Ook de achterliggende IT-infrastructuren (zoals clouds) zijn relevant. Als iedereen dezelfde cloud gebruikt wordt dat immers een risico op zich.

Er ligt een duidelijke kans om de digitale weerbaarheid te vergroten door minder geïsoleerd maatregelen te nemen en in plaats daarvan partijen te betrekken waarmee wordt samengewerkt, de zogeheten ketenafhankelijkheden. In de financiële sector zijn goede ervaringen opgedaan met de zogenaamde TIBER[1] testen. Deze helpen organisaties te doorgronden of hun verdediging op niveau is. Het unieke is dat het hierbij feitelijk niet alleen om een IT-audit gaat maar om een ecosysteem audit: er wordt gekeken naar de hele keten van diensten, ook naar leveranciers.

De weerbaarheid komt op een hoger niveau als iedereen in de keten zijn verantwoordelijkheid neemt en op zijn minst het eigen ecosysteem goed kent. Er zijn al diverse samenwerkingen (zoals tussen grootbanken, binnen interpol/europol, tussen CISO's van grote organisaties, digital trust centers, NCSC) maar er is ook nog een wereld te winnen. De basis is werken vanuit vertrouwen en op basis daarvan actief informatie uitwisselen (bijvoorbeeld over actuele dreigingen).

Deze samenwerking is niet alleen relevant voor de verdediging maar ook voor een goede omgang met incidenten. Organisaties hebben de neiging om gesloten te zijn over zaken die fout gaan, maar ervaringen uit bijvoorbeeld de luchtvaart leren dat het delen van lessons learnt naar aanleiding van fouten of incidenten waardevol is. Ook dat vraagt om vertrouwen en om de juiste houding: met 'victim shaming' schiet niemand iets op.

[1] TIBER staat voor 'Threat Intelligence-based Ethical Red teaming'. Voor meer informatie zie www.dnb.nl

Handelingsperspectief

- De samenwerking binnen ketens en sectoren kan naar een hoger niveau en toezichthouders en regelgevers kunnen hier initiatief nemen.
- Deze samenwerking gaat over kennisuitwisseling, gezamenlijk testen, een collectief zicht op dreigingen, uitwisseling van waarschuwingen en leren van elkaars aanpak.

©2023 – NOREA Manifest

Versterking vakmanschap van IT-professionals

Methoden en technieken ontwikkelen snel en daarbij past dat we hogere eisen moeten stellen aan het vakmanschap van IT-professionals. Meer nadruk op ontwikkeling van hun vakmanschap versterkt hun positie.

Bij de ontwikkeling van systemen is veel aandacht nodig voor veiligheid en betrouwbaarheid. ‘Trust by design’ is daarbij een populair mantra maar komt vaak onvoldoende uit de verf, of pas in een te laat stadium.

Bovendien verandert de professionele uitdaging voortdurend doordat de technologie zelf zich ontwikkelt. Denk bijvoorbeeld aan de impact van quantum computing die op termijn een nieuw paradigma in beveiliging (cryptografie) met zich meebrengt. Maar denk ook aan de opkomst (en impact) van kunstmatige intelligentie.

Ontwikkelaars van systemen hebben in de huidige tijd meer dan ooit een grote verantwoordelijkheid voor het goed functioneren van organisaties en de maatschappij. Ze bepalen feitelijk hoe processen lopen, hoe we samenwerken en in toenemende mate hoe beslissingen worden genomen.

Daarbij hoort ook dat we de allerhoogste eisen mogen stellen aan de technische deskundigheid van deze professionals. Organisaties hebben vaak als eerste prioriteit

het van de grond krijgen van innovatie en stellen pas op de tweede plaats eisen aan de training en opleiding van de professionals die deze innovaties realiseren. Dit zou eigenlijk omgekeerd moeten zijn: ‘eerst een rijbewijs halen en dan pas kun je verder’.

Hierbij bestaat een analogie met NOREA als beroepsorganisatie van gekwalificeerde professionals. Kwalificatie vindt plaats door inschrijving in het NOREA-register als je de (post-master) opleiding IT-auditing hebt afgerond en voldoende praktijkervaring hebt opgedaan en deze blijvend onderhoudt. Zoiets zou ook voor IT professionals moeten gelden (beginner – proficient – expert, in combinatie met meester/gezel principe). Inhoudelijke deskundigheid zou belangrijker moeten zijn dan het vervullen van managementrollen.

Handelingsperspectief:

- Normering van opleiding, kennis en ervaring kan helpen bij het juist waarderen van vakmanschap van IT professionals. NOREA kan hierbij als een voorbeeld worden gesteld.
- Maak praktijkervaring meer onderdeel van de weg tot certificering, niet alleen theorie maar ook proeve van bekwaamheid in de praktijk.

©2023 – NOREA Manifest

Als digitaal het nieuwe normaal is, geldt dat ook voor verantwoording daarover

IT is de backbone van bijna alles en moet het vertrouwen krijgen van stakeholders. Betere verantwoording draagt daaraan bij mits het niet gaat om een afvinkexercitie. 'Niet omdat het moet maar omdat het ertoe doet'.

De meeste organisaties zijn zoals gezegd zeer afhankelijk van hun IT en van de IT van andere partijen (in de ketens). Daarbij zou het eigenlijk de normaalste zaak van de wereld moeten zijn dat zij beschikken over een moderne verantwoording – een (gestandaardiseerd) IT-verslag – over hoe zij de beheersing van IT inrichten. De stakeholders hebben daar simpelweg recht op.

Organisaties leggen al sinds jaar en dag verantwoording af over hun financiële performance in een jaarverslag en ook steeds meer over hun maatschappelijke impact. Op soortgelijke wijze kunnen ze ook – toegespitst op de behoeften van hun stakeholders – een verslag over hun IT uitbrengen. De IT-auditor kan vervolgens assurance geven bij dit verslag.

De voordelen hiervan zijn talrijk. Het verslag speelt niet alleen in op de moderne eisen aan transparantie vanuit de maatschappij maar stimuleert ook bewustzijn binnen organisaties – en bij partners in het ecosysteem – over de verantwoordelijkheden. Het legt de verantwoordelijkheid

voor deze onderwerpen waar deze hoort, bij de hoogste leiding (chefsache).

Essentieel is dat het IT-verslag geen 'afvinkexercitie' wordt. Het moet substantie hebben en inzicht geven in de echt relevante IT gerelateerde thema's voor de organisatie. En inzicht geven in de digitale fitheid van de organisatie, niet alleen op gebied van digitale weerbaarheid maar ook over de innovatieve kracht en invulling van de ethische kant van haar IT toepassingen. Het verslag kijkt niet alleen terug in de tijd maar heeft ook een vooruitkijkend karakter en kan over die toekomst uiteraard geen harde zekerheid bieden. Het geeft niettemin goed inzicht in hoe de organisatie haar IT toepast en organiseert richting de toekomst. Het verslag is een momentopname waarin het management een helder statement maakt en waarbij de auditor nagaat of dat statement een getrouwe weergave is.

Door het IT-verslag te laten certificeren (IT-auditverklaring) ontstaat een level playing field (want de verslagen komen volgens dezelfde standaard tot stand) tussen organisaties, sectoren en door vitale ketens.

Handelingsperspectief:

- Het opstellen van een IT-verslag is een kans om stakeholders inzicht te geven in de kwaliteit van de IT en daarmee ook een essentieel onderdeel om de digitale weerbaarheid te laten zien.
- Het IT-verslag draagt bij aan de volwassenheid van het thema digitale weerbaarheid en borgt dat dit een permanente plaats op de bestuursagenda heeft.
- Het toevoegen van IT-auditverklaring bij het verslag verschaft meerwaarde.

©2023 – NOREA Manifest

Tot slot

Het voorgaande maakt duidelijk dat IT zo'n cruciale en onmisbare rol speelt in de samenleving dat digitale weerbaarheid continu aandacht vereist. Dat moet ook te zien zijn in ons collectieve denken en doen en afgaande op de praktijk van alledag is dat (nog) geen vanzelfsprekendheid. We zien nog vaak in een dwarsdoorsnede van de samenleving dat digitale weerbaarheid niet top of mind is en dat er soms zelfs sprake is van naïviteit. Daarom zou het goed zijn om (1) het onderwerp ook meer aandacht te geven in het onderwijs (startend met digitale basisvaardigheden in het basisonderwijs) en (2) niet alleen te werken aan veilige oplossingen, maar vooral ook aan gebruiksvriendelijke veilige oplossingen (bijvoorbeeld makkelijk hanteerbare manieren voor het identificeren en authentiseren van gebruikers en voor het beschermen van privacy-gevoelige gegevens). Op deze onderwerpen is nog veel verbetering mogelijk.

NOREA maakt zich hard voor het verbeteren van de digitale weerbaarheid van Nederland en in dit manifest zetten we daartoe een aantal lijnen uit die volgens ons de kern vormen van die verbetering. We zijn ervan overtuigd dat professionalisering – in de aanpak van cybersecurity, in het vakmanschap van IT, in de wet- en regelgeving, in de communicatie en het afleggen van verantwoording – Nederland naar het volgende niveau kan brengen. Maar we zijn er vooral ook van overtuigd dat er een flinke sprong mogelijk is door dit alles in nauwe samenwerking tussen alle betrokken partijen te doen.

Want digitale weerbaarheid is geen afdeling. Het is van ons allemaal.

We gaan graag nader het gesprek aan met beleidsbepalers, regelgevers en andere stakeholders om de geschetste opties van de tekentafel naar de praktijk te brengen.

Namens de beroepsorganisatie van IT-auditors,

Bestuur NOREA
maart 2023

©2023 – NOREA Manifest

Inhoud

Inleiding

Ter gelegenheid van het 6e lustrum van NOREA werd op 19 mei 2022 een congrestival gehouden met als thema het bevorderen van de digitale weerbaarheid van onze maatschappij. Nicole Stolk, Board Member van de Nederlandsche Bank, daagde de beroepsgroep uit om met voorstellen te komen om de digitale weerbaarheid van ons land te versterken. Staatssecretaris Digitalisering, Alexandra van Huffelen, feliciteerde de beroepsorganisatie van IT-auditors door middel van een videoboodschap waarbij ze eveneens 'deze enorm krachtige denktank' opriep om onze digitale kwetsbaarheid te blijven beheersen. Zie hierbij het programma en een sfeerimpressie. De volgende pagina's bevatten korte samenvattingen van de verschillende sessies.

©2023 – NOREA Manifest – Bijlage

Sessie 1.1 De hardware van Nederland

De meeste mensen hebben geen concreet beeld bij 'de cloud'. In de praktijk zijn het gewoon kabels en kasten met apparatuur. De openheid en verbondenheid maken het bijzonder. Om de cloud te laten werken is een netwerk van partijen actief. Het publiek verwacht van de cloud dat ze goed werkt. Indirect betekent dat allerlei verwachtingen van deze partijen op gebied van veiligheid, continuïteit en netjes handelen.

Hoe weten we of de IT waar we zo afhankelijk van zijn betrouwbaar genoeg is? Het gaat hierbij om de totale keten. Het staat en valt met samenwerking. Maatschappelijk belang vs individueel belang balanceren.

Normstelling is wel nodig, en ook controle op de naleving. Om dit zeker te stellen zou de overheid wet(ten) kunnen maken. Maar dat werkt niet altijd zo goed, is ook lastig want in EU verband heb je veel lidstaten nodig en krijg je te maken met politiek tussen landen. En veranderingen gaan snel, en het kiezen van het juiste detailniveau voor wetgeving is vaak moeilijk. De overheid kan een aantal zaken het beste aan de sector zelf overlaten. Denk aan of zelfregulering, certificering, of transparantie, via rapportage volgens een standaard. En aan het organiseren van 'Circles of trust'. In NL hebben we een stelsel van elkaar aanvullende maatregelen, ieder met hun eigen

mogelijkheden. Dit stelsel zou nog beter uitgebalanceerd kunnen worden. Internationaal is NL een van de grote landen – die rol moeten we ook pakken.

Het organiseren van adequate beveiliging is een proces van een aantal jaar waar je als organisatie doorheen moet; het gaat over beleid, plannen, detectie, respons, hebben van backups, gebruikersbewustzijn.

De IT-auditor kan aan vele kanten een nuttige rol spelen rond het vraagstuk "waar moet cloud aan voldoen?"

1 Criteria – opschrijven.
2 Naleving nagaan (onafhankelijk).
3 Transparantie – rapporteren – conform de geldende standaard.

Samengevat

- Het belang – criteria nodig wat goed genoeg is.
- Samenwerken – binnen ecosystemen.
- Rapport moet voldoen aan onze eisen (kans aan IT-auditors) – bestuurlijk / technologische kloof – IT-auditors kunnen helpen om kloof kleiner te maken (begrijpelijk uitleggen).
- Rol overheid niet te afwachtend maar niet dichtreguleren.

Sessie 1.2 Keeping us safe

Cybersecurity wordt ook in de transport/logistieke sector steeds belangrijker. Het is een vitale sector die moet blijven draaien. Maar ketens kunnen lamgelegd worden, met direct grote gevolgen. Het niveau van beveiliging in de sector is achter gebleven.

Cyberbeveiliging van de sector kunnen we niet alleen aan de IT afdelingen overlaten, het gaat over continuïteit van onze maatschappij. De huidige vrijblijvendheid moet eruit. Het onderwerp moet daarom op de bestuurstafel geagendeerd en actief bestuurd worden. En hierop is toezicht nodig.

Er is sectorbreed te weinig bewustzijn dat iedere schakel in de ketens doelwit van aanvallen kan zijn. Inzicht in de risico's in de ketens is nodig. Over ketens heen zijn afspraken nodig over inrichten van beveiliging en uitwisselen van informatie over dreigingen en incidenten.

Het idee dat je een muur om een organisatie kunt bouwen is achterhaald. De deur op slot doen voor cyberaanvallen kan niet. Want de gaten waardoor je gehackt gaat worden zijn nog niet bekend. Dus je gaat gehackt worden, en de inbrekers komen binnen. De belangrijkste vraag is: Wat ga je doen als er iets gebeurd? Om de impact te beperken, om de continuïteit te waarborgen, om anderen te waarschuwen waar nodig.

Het organiseren van adequate beveiliging is een proces van een aantal jaar waar je als organisatie doorheen moet; het gaat over beleid, plannen, detectie, respons, hebben van backups, gebruikers bewustzijn. Investeer in digitale vaardigheden van je medewerkers (herkennen en melden).

Focus niet alleen op eigen organisatie, maar ook naar partijen waar je nauw mee samen werkt. Ook de achterliggende IT infrastructuren (zoals clouds) zijn relevant, als iedereen dezelfde cloud gebruikt wordt dat vanzelf een risico op zich.

De rol van de IT-auditor is de juiste vragen stellen, kennis van zaken hebben. Zich echt verdiepen in risico's voor de organisatie (niet alleen lijstjes afvinken).

Samengevat

- Voor alles wat vitaal is voor de samenleving moet een basisniveau worden gehanteerd. De huidige vrijblijvendheid moet eruit. Door ketens heen. Toezicht nodig. Dit mag niet versnipperd worden. Hier is nog een wereld te winnen.
- Versimpeling nodig. Rijksinspecties nog beter laten samenwerken.
- Leer van de ervaring van de verzekeraars. Focus op MKB hier zit het grootste probleem, onze maatschappij drijft hier op.
- Overheid geef het goede voorbeeld (voorbeelden bewindspersonen).
- Bewustzijn op het hoogste niveau (chefsache) is heel belangrijk.

©2023 – NOREA Manifest – Bijlage

Sessie 1.3 Digitale weerbaarheid van de Financiële Sector

De sector heeft duidelijke (en hoge) normen voor IT veiligheid en weerbaarheid nodig, maar moet deze wel proportioneel toepassen, met name voor kleinere organisaties, anders is innovatie niet meer goed mogelijk. Waarbij het doel van de normering wel overeind moet blijven. Regelgeving zoals DORA voorziet hierin.

Daarbij is de vraag of bij normering niet ook veel meer naar de vakbekwaamheid van de IT professionals moet worden gekeken. IT toepassingen worden steeds complexer om te maken, beheren en controleren, maar de vakbekwaamheid van de mensen die eraan werken is niet genormeerd. De vraag is of we kwaliteit van mensen moeten gaan auditen, om ze bewust onbekwaam te maken. En IT vakmanschap belangrijker maken, ook in waardering en beloning, belangrijker dan managementtaken.

Ook is het goed om verschillen in normering tussen sectoren los te laten. De financiële sector raakt steeds meer vervlochten in andere sectoren. En de IT-beheersingsproblematiek verschilt niet wezenlijk tussen sectoren. De digitale sector moet aan dezelfde strenge normen voldoen als de financiële sector. Harmonisatie van regels, internationaal en over sectoren heen is wenselijk.

We leven in een tijd waarin geopolitiek belangrijk is, ook op IT gebied. De financiële wereld is deels een warzone, met uitvoering van sancties en een (soms) vijandige buitenwereld. En met geopolitieke afhankelijkheden, bijvoorbeeld op gebied van authenticatie en cloud infrastructuren.

Een Europese cloud is een mooi idee, maar zal moeilijk te realiseren zijn. Dus samenwerking met grote US cloud-providers nodig. Hierbij de normen op gebied van authenticatie, trust, privacy, ethiek, etc. in eigen hand houden. Ook voor ogen houden dat de weerbaarheid van de financiële sector komt uit kleine nieuwe organisaties waar slimme mensen met goede ideeën oplossingen voor complexe problemen bedenken. Hiervoor is goede opleiding nodig, en regelgeving die dit faciliteert en geen drempels opwerpt.

Samengevat

- Duidelijke (en hoge) normen voor IT veiligheid en weerbaarheid zijn nodig, maar deze wel proportioneel toepassen, anders is innovatie niet meer goed mogelijk. Waarbij het doel van de normering wel overeind moet blijven.
- Maak IT vakmanschap belangrijker, en maak dit aantoonbaar.
- Stop met generieke digitale vraagstukken per sector verschillend aan te pakken. Dat leidt tot inefficiëntie en uiteindelijk in-effectiviteit.

©2023 - NOREA Manifest - Bijlage

Sessie 1.4 Naar een digitaal weerbare Overheid

Cyberweerbaarheid en privacy bescherming zijn chef sache: de hoogte baas van een organisatie, als bestuurder, algemeen directeur moet er over gaan. Deze moet snappen waarom het belangrijk is om cyberweerbaar te zijn.

Elke organisatie zou de volgende stappen moeten doorlopen:

- wat zijn de kritieke processen inclusief bijbehorende assets (kroonjuwelen). Niet alleen interne assets, maar eveneens naar koppeling met stakeholders (ketenafhankelijkheden)?
- wat zijn de kwetsbaarheden voor deze assets en ketenafhankelijkheden?
- Voer testen uit op de getroffen maatregelen.
- In de praktijk blijkt steeds dat hier nog veel werk aan de winkel is.

Voor de zogenoemde ketenafhankelijkheden zijn ook de achterliggende IT infrastructuren (zoals clouds) relevant. Want als iedereen bijvoorbeeld dezelfde cloud gebruikt wordt deze cloud vanzelf een risico op zich. Voor wat betreft maatregelen:

- Zorg ervoor dat je organisatie de beveiliging op orde heeft (zie NCSC maatregelen).
- Zorg voor op tijd detecteren en responderen; het beperken van impact van incidenten.
- Test!
- Leer van elkaar. Heb je getest en heb je bevindingen, deel deze, ook met andere organisaties.
- Wees bewust van interne fraude en van de gevaren via social engineering.
- Denk ook aan awareness.

The “war on talent”: overheidsdiensten moeten elkaar niet gaan beconcurreren op de arbeidsmarkt, het is veel beter om samen te werken, mooie uitdagende carrière paden te bieden aan hun IT professionals en te kijken naar de mogelijkheden van het uitwisselen van expertise. De overheid moeten af van het stereotype “ambtenaar” en dient de positieve kanten van werken bij de overheid beter te benadrukken.

Het IT Verslag inclusief IT-auditverklaring mag geen ‘compliance vinkje’ worden (moet echt substantie hebben). Een verslag voor op de bestuurstafel vanuit organisatie zo staan we ervoor, dit gaan we eraan doen en IT-auditor zegt “klopt” / geeft er assurance bij. De cyberwereld is dynamisch; een rapportage blijft een momentopname, het is van belang het management hier bewust van te maken.

Samengevat

- Digitale veiligheid is net zo belangrijk als financiële verantwoording. Cyberweerbaarheid en privacy bescherming is dan ook chef sache. Kijk naar de mogelijkheden om de hoogte baas van een organisatie nadrukkelijker in zijn rol te zetten met betrekking tot deze onderwerpen.
- Kijk naar hoe het “victim shaming” (binnen het cyberdomein) er vanaf gehaald kan worden en hoe lessen vanuit cyberincidenten breder gedeeld kunnen worden.
- Kijk naar de mogelijkheden van de IT-auditverklaring; dit is een goed initiatief.

©2023 - NOREA Manifest - Bijlage

Sessie 2.1 Nieuwe cybercrime trends

Combineren van twee gebieden waar NL goed in is: cybersecurity en verzekeren. Cybersecurity is een probleem voor onze maatschappij. Beschikbare oplossingen werken niet. Daardoor is het een moeilijk verzekerbaar risico, met alle gevolgen van dien. In oplossingen wordt momenteel veelal gekeken van de buitenkant of er kwetsbaar zijn (via penetratietesten); niks real-time en dit zegt dan ook niks over morgen / overmorgen: allemaal puur gericht op kansreductie.

Cybersecurity goed doorvoeren is complex en de aanvallers hebben een hoog technisch niveau. Succesvolle aanvallen gebeuren bijna altijd via gaten in software die je zelf hebt aangeschaft en geïnstalleerd of door gebruik te maken van (normaal) menselijk gedrag. Je kunt aanvallers niet buiten houden. Kunnen leren van ervaringen in andere sectoren om cyber risico's in te dammen – bv verzekeringssector: in alle gevallen waar risico's te hoog werden is de switch gemaakt van kansreductie naar impactreductie.

Ook voor cybersecurity gaat het er vooral om de impact te reduceren – hier is nog heel veel te bereiken. Dit doe je door goede maatregelen te treffen voor monitoring, detectie en snelle respons als er iets geks aan de hand is. Daar is best wat voor nodig. Enerzijds in de buitenwereld, maar ook binnen de organisatie:

- Extern: Advanced Persistent Threats (APT's) in de gaten houden – waar ze bewegen, welke kwetsbaarheden ze weaponizen (actief gaan misbruiken). Deze vulnerabilities vervolgens proactief (laten) patchen.
- Intern: Naast de aandacht voor een goede inrichting moet je constant blijven kijken en in staat zijn om te reageren op incidenten. Hiervoor is nodig:
  - Data over alles wat binnen komt (monitoren).
  - Risico constant kunnen duiden (detecteren).
  - Iemand hebben die meteen kan ingrijpen als er iets geks gebeurt (response).

Samengevat

- Kijk naar de rol van de verzekeraars, zijn de enigen die de pijn direct voelen, welke sturingsmechanismes kunnen we via hen doen. Als oplossingen goed werken zullen verzekeraars ze gaan omarmen.
- Kijk naar impactreductie in plaats van kansreductie.
- Vergeet het MKB niet, hier zit het grootste probleem (stille ellende – staan er alleen voor – weten niet wat ze moeten doen – laten we zorgen dat die groep een stuk weerbaarder wordt).

©2023 – NOREA Manifest – Bijlage

Sessie 2.2 Klaar zijn voor een cyberaanval

Ken jezelf en ken de ander (je vijand) en test jezelf; Bereid je voor, want je gaat aangevallen worden. Ga uit van bedreigingen analyse: Weet wat je in huis hebt en wat waardevol is voor een ander. Kroonjuwelen zijn niet alleen je systemen, maar ook je gegevens.

We zien nog (te) vaak dat organisaties denken vanuit interne risico's. Terwijl ook het perspectief en de motieven van de aanvaller heel relevant zijn. Begrijpen hoe gemotiveerd de mensen zijn die je aan willen vallen. En welke technieken ze daarbij willen en kunnen gebruiken. En op moment dat iemand bij je binnenkomt, wat kun je er dan aan doen?

Tiber testen helpt om te begrijpen of je op niveau bent en te (blijven) bouwen aan je verdediging. Het is een continu proces (identify en protect) waarbij zowel technische als niet technische aspecten (communicatie, stakeholders, sentiment/reputatie) van belang zijn. Grote organisaties hebben meer resources en mogelijkheden om dit te organiseren, maar binnen kleine organisaties sta je dichter bij elkaar en kun je sneller opereren.

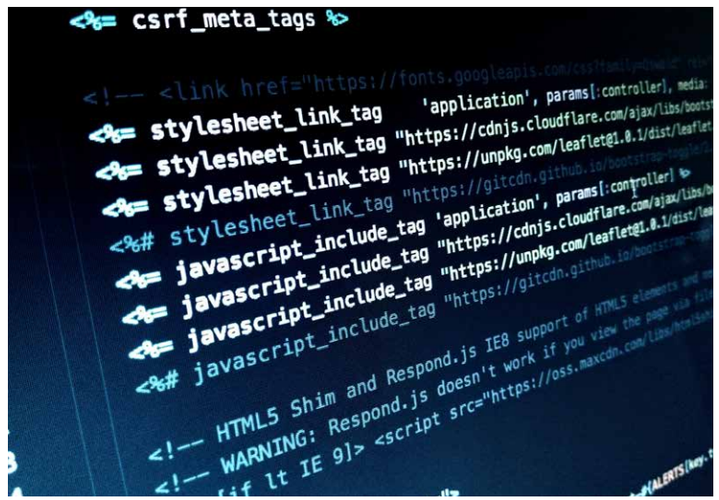
Het is feitelijk geen IT-audit maar een eco-systeem audit, je kijkt naar de hele keten van diensten, ook door leveranciers. Iedereen in de keten moet zijn verantwoordelijkheid pakken.

In contracten met leveranciers moet je afspraken over uitvoeren hacktests opnemen. Assurance rapporten helpen, maar je moet wel een tandje meer doen. Je zult echt met elkaar moeten gaan testen. Testen niet alleen jaarlijks uitvoeren in kader van assurance, maar embedden in je eigen bedrijfsvoering, en niet alleen vanuit tweede of derde lijn of een extern partij. Dit helpt je om klaar te zijn voor een aanval en om te kunnen reageren.

De meeste organisaties willen niet concurreren op veiligheid, dus samenwerken tegen de gemeenschappelijke vijand is goed en nodig.

Samengevat

- Concluderend: Ken jezelf, ken je vijand en test jezelf!
- Oefen realistisch: intelligence based hacktesten en gebruik de scenario's ook voor realistische oefeningen van je crisismanagement structuur.
- Stilstaan is geen optie!



Sessie 2.3 Opkomst van crypto's & digital currencies

Betaalmiddelen hebben een lange historie; van schelpen, naar zilver/gulden, naar roebel/euro en de actueelste opkomst betreft crypto's en digital money. Er is steeds meer sprake van online betalingen en cash betalingen lopen terug en gaan mogelijk op termijn verdwijnen. Digital money/currency is geen crypto valuta. Digital money/currency is een betaalmiddel waarvan de centrale bank zegt dat het echt geld is (liability op de central bank).

Digital currency zal naast crypto blijven bestaan. Crypto is afhankelijk van waarde (vraag en aanbod), maar er zijn "andere" online werelden waar crypto's meer geschikt zijn dan een digital currency. Denk aan metaverse, gaming, developers, etc.

Europese Centrale Bank (ECB) is twee jaar geleden begonnen met een onderzoek naar de mogelijkheid om naast eurobiljetten en -munten ook een digitale euro uit te geven. Een digitale euro komt neer op een elektronische vorm van centralebankgeld, een zogenoemde "central bank digital currency (CBDC)". Dit geld komt voor alle burgers en bedrijven toegankelijk en is vergelijkbaar met bankbiljetten, maar dan in digitale vorm. Plan is najaar 2023 naar governing counsel ECB het resultaat van het onderzoek op te leveren met een advies wel of niet issuen van een digital currency. Ook andere Centrale Banken kijken naar CBDC's. Een Pan-

europese oplossing voor retail betalingen is er nu niet en deze moet er wel komen.

Uitgifte en beheer van digitale currencies vereist een assurance verklaring als het als betaalmiddel gebruikt wordt. Op dit moment zijn er weinig mensen die dit kunnen. IT-auditors voelen zich nu niet voldoende toegerust om crypto's te auditen. Daarnaast zijn de frameworks om te auditen er nog niet helemaal (sluiten nog niet helemaal aan). Hier moet nog veel gebeuren, want het is allemaal nog jong en volop in beweging, maar gaat allemaal wel gebeuren.

IT-auditors: Laat je niet bang maken door het geneuzel over hoge risico's. Het is een fintech als alle anderen. Het is een fascinerende markt voor de toekomst.

Samengevat

- De digital currency gaat een prominentere rol kijken in de toekomst van het betalingsverkeer. Het is van belang dat er voldoende mensen zijn die kennis van zaken hebben omtrent dit onderwerp.

Sessie 2.4 Digitaal Boeven Vangen

Via het samenwerkingsverband FEC (Financieel Expertise Centrum) werken diverse diensten waaronder Politie en FIOD samen in het bestrijden van digitale misdaad.

In de sessie zijn diverse vormen van digitale misdaad aan de orde gekomen. Wat opvalt is dat digitale criminelen hun misdaden steeds meer als een businessmodel benaderen. Taken worden verdeeld over verschillende teams, delen worden uitbesteed, en IT is steevast onderliggend aan de diverse onderdelen van de organisatie. Dit gaat zo ver dat op voor criminelen geliefde kanalen als telegram en het dark web recensies te vinden zijn over de aanbieders van criminele tools en diensten. En waarschuwingen voor oplichters…

De resultaten van de (ethische) hackactiviteiten die het FEC/Politie/FIOD team op het congrestival uitvoerden tonen aan dat de IT-audit beroepsgroep zich op gebied persoonlijke digitale weerbaarheid nog kan verbeteren. Meer dan honderd bezoekers scande een QR code onder het mom van ‘win een ipad’, de gegevens van honderden wifi netwerken werden uitgelezen van de telefoons (en een aantal daarvan gesimuleerd) en telefoons die bekend bleken met hotspots (zoals wifi in de trein) werden actief benaderd.

Omdat digitale criminele businessmodellen vaak internationaal en zelfs mondiaal (buiten EU) zijn opgezet is handhaven naar de daders vaak lastig. Daarom richten de diensten zich op de voorkant van deze modellen, door de burger weerbaarder te maken. En werken ze samen met bedrijven en andere organisaties (uitwisselen gegevens van gehackte accounts om misbruik elders te voorkomen) en zetten ze in op bewustwording bij het publiek, bijvoorbeeld via het (basis)onderwijs.

Via het FEC samenwerkingsverband worden gegevens uitgewisseld voor projecten, task forces (voor serious crime) en steeds meer via publiek-private samenwerking. Het doel is het verstevigen van elkaars informatiepositie, binnen de geldende regels zoals AVG en elkaars rol respecterend. Waardoor bestrijden van digitale criminaliteit beter vorm gegeven kan worden.

Samengevat

- Integreer IT security binnen het onderwijs (vanaf lagere school) en andere opleidingen.
- Zorg voor een gebruikersvriendelijke gebruikers-ervaring van IT (investeer in gebruikerservaringen in plaats van technische oplossingen).

2.5 Gebruik en misbruik van algoritmes

Als onderdeel van hun digitale transformatie maken organisaties in toenemende mate gebruik van kunstmatig intelligente algoritmische systemen (hierna: "AI-systemen"). AI-systemen worden gedefinieerd als geautomatiseerde wiskundige modellen die in besluitvormingsprocessen worden gebruikt en worden gekenmerkt door hun autonome gevolgtrekkingen ("leren") uit enorme hoeveelheden uiteenlopende gegevensreeksen. De toenemende rol die deze systemen spelen in de besluitvorming, met aanzienlijke potentiële gevolgen voor het menselijk welzijn (d.w.z. voor werknemers, consumenten, burgers, patiënten enz.), heeft geleid tot de roep om een grotere verantwoordingsplicht bij het ontwerp, de uitvoering en de werking van algoritmen.

We zien in de praktijk van AI al veel toepassingen voor het nemen van geautomatiseerde beslissingen maar ook voorbeelden van onrechtmatige uitkomsten.

Ook staan bij bijna alle maatschappelijke discussies (klimaatverandering, stikstof, pfas, coronamaatregelen) de uitkomsten van modellen centraal (dit zijn ook algoritmes). Terugdraaien van gebruik van algoritmes lijkt geen optie. Wat zou gedaan moeten worden om de uitkomsten van algoritmes beter te kunnen vertrouwen? Spelregels? Keurmerken? Vanuit EU-perspectief zien we veel initiatieven om AI te reguleren. De EU AI-act introduceert AI-assessment. De invalshoeken daarbij zijn:

- Data protection and security.
- Accountability.
- Governance and Ethics.
- Bias (unrepresentative, incomplete or incorrect data).
- Explainability.

Door TNO wordt een ontwikkelmethodiek voor 'Trustworthy AI beproefd in het 'AI Oversight Lab':

- Regulatory and policy context and components to evaluate.
- Best Practices and requirements to use and develop.
- Methods and Tools to evaluate.

Voor auditors zijn standaarden en handreikingen nodig en in ontwikkeling. Door de NOREA is een eerste voorzet gepubliceerd van Guiding Principles Trustworthy AI Investigations op basis van ISO/IEC JTC 1/SC 42.
Bij het verrichten van onderzoek naar AI-systemen en het toepassen van deze leidende beginselen moeten IT-auditors met een aantal overwegingen rekening houden:

- De Guiding Principles zien ook toe op uitbestede (deel) procesgang die relevant is voor het ontwerp, de implementatie en de werking van AI-systemen.
- Zowel de ontwikkeling als de controle van AI-systemen zijn van nature zeer multidisciplinair. Dit betekent dat het zeer waarschijnlijk is dat IT-auditors bij de uitvoering van hun onderzoek deskundigen (bijv. gegevenswetenschappers, gegevensingenieurs, bedrijfsethici, juristen/privacydeskundigen, gegevensbeschermingsfunctionarissen, deskundigen op het gebied van cyberbeveiliging) zullen (moeten) betrekken. De IT-auditor moet echter voldoende deskundig zijn met betrekking tot het onderwerp en de meting daarvan om de algehele verantwoordelijkheid voor het onderzoek en de bijdrage van die deskundigen te aanvaarden.
- Indien de leidende beginselen worden gebruikt als input voor de ontwikkeling van controlekaders voor algoritmen, moedigen wij aan de bestaande risicobeheersingsmethoden zoals COSO of COBIT te volgen.

Samengevat

- Artificial Intelligence (AI) is een belangrijk aandachtsgebied voor IT-auditors vanwege de risico's en bedreigingen.
- Voor het begrip van en onderzoek naar betrouwbare AI-toepassingen zijn de eerste uitgangspunten en beginselen beschikbaar, die in combinatie met de bestaande risicobeheersingsmethoden, zoals COSO en COBIT kunnen worden gehanteerd.

©2023 - NOREA Manifest - Bijlage

Sessie 3.1 IT verslag en IT-auditverklaring

Het IT verslag en bijbehorende IT-auditverklaring zijn een initiatief van NOREA. Het IT verslag is gebaseerd op het GRI initiatief. Norea sluit hiermee aan op ontwikkelingen rond sustainability reporting.

Het is geen control framework of audit standaard of aanpak, het is een verslagleggingsstandaard, hulpmiddel voor management (of toezichthouders of RvC's) om verantwoording af te leggen over de kwaliteit van IT van een organisatie. De control frameworks blijven wat ze al waren, en kunnen heel specifiek zijn (bijv per sector).

Wat NOREA oplevert is het volgende:

- Verslaggevingsstandaard (opgezet conform GRI).
- IT-auditverklaring.
- Handreiking aan de leden.

Rapportage is dus altijd gericht op behoefte stakeholders. Dat moet je eerst in kaart hebben, daar de rapportage op inrichten. De stakeholder behoefteanalyse moet je eerst maken en in het verslag moet je ook aantoonbaar maken dat je van buiten naar binnen redeneert.

Het IT verslag is voor een deel terugkijken en voor een deel vooruitkijken. Daarom geeft de verklaring limited assurance (geen reasonable assurance).

Wie mag IT-auditverklaring afgeven? De RE, dit mag ook een RE van Internal Audit zijn.

Het IT verslag en IT-auditverklaring zijn voor iedereen maar we verwachten dat OOB's deze het meest zullen omarmen. Maar ook kleine innovatieve IT bedrijven. De overheid denkt erover na.

NOREA voorziet proces van ingroeien. Voetje voor voetje, en op gegeven moment is iedereen eraan gewend en kun je niet meer zonder. Timing is goed DORA komt eraan, een reporting tool hiervoor maken is prima. En denk ook aan CSRD (Corporate Sustainability Reporting Directive). Stakeholders zoals beleggers willen weten dat een organisatie resilient is.

Samengevat

- Het IT verslag is verslagleggingsstandaard verantwoording af te leggen over de kwaliteit van IT van een organisatie.
- Het is een initiatief van NOREA en sluit aan bij GRI dat we kennen van sustainability reporting.
- De RE mag een verklaring afgeven bij het verslag.

©2023 - NOREA Manifest - Bijlage

Sprekers

NAAM	FUNCTIE	BEDRIJF
Mathijs Aler	CEO	Ohpen
Marjolein Baart	Onderzoeker	Onderzoeksraad voor de Veiligheid
Britt van den Berg	CIO	SVB
Rogier Besemer	CIO	TIBER team DNB
Mona de Boer	Partner	PWC
Michiel le Comte	Head of Section IT & Operational risk	de Nederlandsche Bank
Martijn Dekker	CISO	ABN AMRO
Erwin Dijkstra	Expert financieel economische integriteit	FEC
Rudrani Djwalapersad	Partner	EY
Arco van Emous	Manager Digitale Weerbaarheid	Agentschap Telecom
Barend Frans	Publiek Private Samenwerking bij Politie Nederland	Politie
Wouter Goudswaard	Chief Commercial Officer	EYE Security
Alexandra van Huffelen	Staatssecretaris Digitalisering	BZK (videoboodschap)

NAAM	FUNCTIE	BEDRIJF
Joep Jansen	Lead IT-auditor	Verdonck, Klooster & Associates
Bart de Jongh	Directeur Kennis en Ontwikkeling	Auditdienst Rijk - (Scheidsrechter)
Adrie Kerkvliet	Algemeen Directeur	Auditdienst Rijk
Ruud Kerssens	Expert member AI	NEN
Maurice Koetsier	Senior Manager IT Risk Assurance	BDO (Scheidsrechter)
Hans Koster	Auditor business and IT	ABN AMRO
Job Kuijpers	CEO	EYE Security
Thijs Laarhoven	Onderzoeker	TNO
Simon Lelieveldt	Regulatory and Compliance Consultant	
Jan Matto	Partner	IT-audit Mazars
René Putters	Afdelingshoofd	Inspectie Leefomgeving en Tranport Rijkswaterstaat
Merijn van Schoote	CISO	Port of Rotterdam
Paul Slootmaker	Hoofd Taskforce Monitoring and Reporting	KPN

NAAM	FUNCTIE	BEDRIJF
Nicole Stolk	Directielid	de Nederlandsche Bank
Tjerk Timan	Beleidswetenschapper	TNO
Steven Vethman	Onderzoeker en Data Scientist	TNO
Tom van de Ven	Manager Operational & IT Risk	Autoriteit Financiële Markten
Kees Verhoeven	Adviseur	Bureau Digitale Zaken
Kees Verkade	Senior Advisor	NCSC
Frank Versleijen	Director Digital Trust	PWC (Scheidsrechter)
Lieke Verstegen	Partner	EY (scheidsrechter)
Rob Visser	Group CIO	NN Group
Arie Vooijs	IT-auditor	FIOD
Marc Welters	Partner	IT-audit EY
Evelien Witlox	Program Director Digital Euro	ECB
Ing Yan Ong	Global CIO	Heineken

©2023 - NOREA Manifest - Bijlage

Sfeerimpressie

©2023 – NOREA Manifest – Bijlage

Sfeerimpressie