4.4 Leren van digitale voorvallen

Om de veiligheid te kunnen verbeteren is het belangrijk om te onderzoeken wat er gebeurde en welke factoren bijdroegen aan het ontstaan en de gevolgen van het voorval. Deze inzichten zijn belangrijk om toekomstige voorvallen te voorkomen of de gevolgen daarvan te beperken, in het bijzonder in een domein dat zo dynamisch is als digitale veiligheid.

In veel domeinen zijn grote voorvallen en publieke ophef een prikkel om te leren en de veiligheid te verbeteren. In Nederland wordt al meer dan honderd jaar onderzoek gedaan naar ongevallen en rampen, aanvankelijk alleen op transportgebied. Na de vuurwerkramp in Enschede en de cafébrand in Volendam werd in 2005 de Onderzoeksraad voor Veiligheid opgericht, omdat er behoefte was aan een permanent onderzoeksinstituut dat naast transport ook voorvallen in andere domeinen kon onderzoeken.[195] In de transportdomeinen kent dit onderzoek wereldwijd een lange traditie. Zo leidde een vliegtuigcrash met een populaire *football coach* in de VS in 1931 uiteindelijk tot de oprichting van de NTSB (Amerikaanse tegenhanger van de Onderzoeksraad voor Veiligheid).[196]

Het digitale domein is een relatief jong domein en de traditie om van voorvallen te leren is in dit domein beperkt en nog in opbouw. In deze paragraaf beschrijven we:

- hoe digitale voorvallen op dit moment worden gemeld en onderzocht;
- welke factoren beïnvloeden hoe van digitale voorvallen wordt geleerd. Daarbij gaat het zowel om keuzes en veronderstellingen die onderzoekers maken en hebben, als om de context waarbinnen de onderzoeken plaatsvinden.

4.4.1 De huidige praktijk van onderzoek naar digitale voorvallen

Er kunnen verschillende aanleidingen zijn om een voorval te onderzoeken. Allereerst vanuit de eigen behoefte van de betrokken organisatie, of dit nu de fabrikant van de software is of de organisatie die de software gebruikt: vanuit een intrinsieke behoefte om te leren en zo toekomstige voorvallen te voorkomen, niet alleen bij de organisatie zelf maar ook bij anderen. Daarnaast bestaan er verschillende wettelijke verplichtingen, die maken dat bepaalde voorvallen aan bepaalde instanties moeten worden gemeld (alhoewel gerapporteerde voorvallen dan niet altijd worden onderzocht). Partijen zoals politie en verzekeraars doen forensisch onderzoek naar voorvallen. Hierna gaan we in op wat we op dit moment in de praktijk waarnemen voor wat betreft het melden en onderzoeken van digitale voorvallen.

195 https://www.onderzoeksraad.nl/nl/page/12056/geschiedenis
196 Anderson, R., *Security Engineering*, 2020.

Melding en onderzoek op basis van wettelijke verplichting

Incidenten bij vitale aanbieders
De Europese *Network and Information Security* (NIS) *Directive*[197] bevat verplichtingen voor aanbieders van essentiële diensten in vitale sectoren en digitale dienstverleners. Nederland heeft de NIS geïmplementeerd in de Wet beveiliging netwerk- en informatiediensten (Wbni). Op grond van de Wbni moeten aanbieders van essentiële diensten ernstige incidenten melden bij het NCSC/sectorale CSIRT en hun sectorale toezichthouder. Voor energie en digitale infrastructuur is dit Agentschap Telecom, voor banken en betaalinfrastructuur DNB, vervoer en drinkwater ILT en gezondheidszorg IGJ.[198] Voor de telecomsector bestaat sinds 2012 een zorg- en meldplicht inclusief toezicht van AT op basis van de Telecommunicatiewet, ongeacht of een partij door EZK als vitaal is aangewezen. In de Wbni is aanvullend op deze sectorale wet- en regelgeving een meldplicht bij het NCSC opgenomen alleen voor de vitaal aangewezen telecompartijen.

Het betreffende vakdepartement stelt in samenspraak[199] met JenV drempelwaarden waarboven het incident moet worden gemeld. In de Wbni is bepaald dat als publieke bewustwording nodig is om een incident te voorkomen of te beheersen, de betreffende autoriteit het publiek kan informeren over het gemelde incident. Ook kan de autoriteit de vitale aanbieder verzoeken om zelf het publiek te informeren.[200]

Voor het leren is ook van belang dat andere organisaties de voor hen relevante lessen uit de onderzoeken eenvoudig tot zich kunnen nemen en op die manier kunnen leren van wat andere organisaties is overkomen. Incidenteel worden onderzoeken naar aanleiding van meldingen gepubliceerd op de website van de betreffende autoriteit of toezichthouder. Een voorbeeld hiervan zijn de onderzoeken van AT, JenV en IGJ naar de uitval van 112[201] en het onderzoek van ILT naar de cybersecurity bij Waternet naar aanleiding van een signaal in de media dat dit niet op orde zou zijn.[202] We hebben op de websites van NCSC, AT en andere sectorale toezichthouders geen overzicht kunnen vinden welke incidenten zijn onderzocht, of een geaggregeerd overzicht van het aantal incidenten, de factoren die tot de incidenten hebben geleid en de verschillende lessen die daaruit volgden. In theorie is het mogelijk dat de lessen uit incidenten impliciet zijn verwerkt in de adviezen en voorlichting van deze organisaties aan hun doelgroep. In de praktijk zijn toezichthouders op dit moment nog intern bezig met de vraag hoe zij hun

197 https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX%3A32016L1148&from=EN Krachtens de Wbni zijn als aanbieders van essentiële diensten aangewezen: als vitale aanbieder aangemerkte entiteiten die actief zijn in sectoren, genoemd in de bijlage bij de NIB-richtlijn (zie artikel 2 Bbni). Voor enkele categorieën andere vitale aanbieders geldt, los hiervan, ook een meldplicht bij het NCSC voor ernstige incidenten (zie artikel 3 Bbni), maar voor hen gelden niet de andere, uit de NIB-richtlijn voortvloeiende verplichtingen. Daarnaast: aanbieders van essentiële diensten dienen krachtens artikel 10 Wbni ernstige incidenten bij het NCSC en de sectorale toezichthouder te melden, maar niet ook (of in plaats daarvan) bij een "sectorale CSIRT". Overigens: voor entiteiten binnen de gezondheidszorg is wel al (in artikel 4 Wbni) de toezichthouder bepaald, maar binnen die sector zijn vooralsnog geen aanbieders van essentiële diensten aangewezen (waarop de verplichtingen vanuit de NIB-richtlijn van toepassing zouden zijn).
198 https://zoek.officielebekendmakingen.nl/stb-2018-387.html
199 Vanwege de vaak dubbele meldplicht aan zowel het vakdepartement als JenV (NCSC)
200 Artikel 23 Wbni artikel 20, lid 4, onder b, Wbni. Zie ook https://www.agentschaptelecom.nl/binaries/agentschap-telecom/documenten/publicaties/2020/januari/20/brochure-meldplicht-voor-aanbieders-van-essentiele-diensten/Brochure+Meldplicht+voor+aanbieders+van+essentiële+diensten.pdf
201 https://www.agentschaptelecom.nl/actueel/nieuws/2019/06/26/onderzoek-naar-storing-112
202 https://www.ilent.nl/documenten/rapporten/2021/4/2/onderzoeksrapport-stichting-waternet

eigen verantwoordelijkheid kunnen en moeten invullen. Zo schrijven toezichthouders in hun eerste gezamenlijke inspectiebeeld dat het toezicht nog in een opbouwende fase is en zij nog niet in staat zijn om samenhangende uitspraken te doen (rode draden te trekken) over hoe het op dit moment gaat met cybersecurity in vitale sectoren en processen.[203]

Onderzoek naar datalekken
Organisaties waarvan persoonsgegevens zijn gelekt zijn wettelijk verplicht om dit direct te melden aan de Autoriteit Persoonsgegevens (AP). Bij datalekken gaat het om 'toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie, zonder dat dit de bedoeling is van deze organisatie'.[204] De wettelijke plicht om datalekken te melden komt voort uit de Europese Algemene Verordening voor Gegevensbescherming (AVG) in de EU (in het Engels *General Data Protection Regulation* of GDPR). Omdat de AVG een verordening is, is deze Europese rechtsregel rechtstreeks van toepassing in de hele Europese Unie.

AP publiceert onderzoeks- en boeterapporten naar aanleiding van meldingen van datalekken en andere signalen.[205] De onderzoeken van AP zijn gericht op de mate waarin organisaties wettelijke verplichtingen hebben nageleefd, zoals het nemen van technische en organisatorische maatregelen om datalekken te voorkomen en het evalueren van datalekken. Wanneer een organisatie de wettelijke maatregelen niet heeft nageleefd kan AP een boete opleggen. Om deze reden zijn organisaties terughoudend in het melden van mogelijke datalekken. Het niet naleven van de wettelijke meldplicht kan echter ook leiden tot extra boetes, ongeacht de omvang van het oorspronkelijke datalek.

Een andere beperking is dat het bij de meldingen moet gaan om het lekken van persoonsgegevens en dat is slechts bij een deel van de voorvallen aan de orde. Verder gaan de onderzoeken van AP vooral in op het voldoen aan wet- en regelgeving. Om te kunnen leren is vooral de achterliggende vraag van het niet-naleven relevant: welke factoren er mogelijk toe hebben geleid dat organisaties de verplichtingen niet hebben nageleefd en wat kan daarvan worden geleerd?

AP publiceert jaarlijks een jaarverslag. In het jaarverslag over 2020 staat dat meeste van de in 2020 gemelde datalekken het gevolg zijn van het verkeerd versturen of afgeven van persoonsgegevens (66%). AP meldt dat bij 5% van de in 2020 gemelde datalekken een digitaal incident (*hacken, malware, phishing*) de oorzaak was en dat dit aandeel stijgt. In de rapportage gaat AP dieper in op de bijdrage die meerfactorauthenticatie (MFA) had kunnen hebben in het voorkomen en mitigeren van 249 datalekken, waarbij naar schatting minimaal 607.846 en maximaal 2.092.946 personen betrokken waren.[206]

Verdere inzichten biedt het AP op dit moment niet aan organisaties die software gebruiken. Om meer inzichten uit de datalekmeldingen te kunnen halen, en daarmee potentiele lessen voor andere organisaties, diende de Cyber Security Raad (CSR) in 2020 een onderzoeksvoorstel in bij de minister van Justitie en Veiligheid. Doel van dit

203 ANVS, DNB, IGJ, IJenV, ILT, *Samenhangend inspectiebeeld cybersecurity vitale processen 2020-2021*, juni 2021.
204 https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken
205 https://autoriteitpersoonsgegevens.nl/nl/onderzoeken
206 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_datalekken_2020.pdf

onderzoek is om te laten zien in hoeverre wetenschappelijk en/of statistisch onderzoek van datalekken het inzicht in de effectiviteit van veiligheidsmaatregelen (of het ontbreken daarvan) kan vergroten.[207]

Forensische onderzoeken

Er zijn verschillende organisaties die achteraf incidenten onderzoeken. Sommige van deze organisaties zijn erkend als digitaal forensisch opsporingsbureau. Deze erkenning betekent dat hun rapporten kunnen worden geaccepteerd als forensische onderbouwing in een rechtszaak. Forensische onderbouwing is primair gericht op het onderbouwen van juridische aansprakelijkheid, niet op het leren van het voorval om herhaling in de toekomst te voorkomen. In de meeste gevallen werken deze digitaal forensische opsporingsbureaus in opdracht van de getroffen organisatie en/of hun verzekeraar. Deze onderzoeken blijven doorgaans vertrouwelijk binnen de eigen organisatie (tenzij de opdrachtgever het uit eigen beweging publiceert, zie volgende paragraaf). Andere organisaties krijgen daardoor geen inzicht in de getrokken lessen en ze dragen niet bij aan een geaggregeerd beeld van factoren en effectiviteit van maatregelen; hooguit binnen een betrokken verzekeraar (silo's tussen verzekeraars).

Daarnaast wordt forensisch onderzoek gedaan door de politie (waaronder het *Team HighTech Crime* en regionale *cybercrimeteams*) en door het NFI. Voor deze organisaties geldt in grote lijnen hetzelfde als voor de opsporingsbureaus voor wat betreft de mogelijkheid om van hun onderzoeken te kunnen leren. Als er een rechtszaak is, kan het zijn dat een deel van deze informatie via media en de gerechtelijke uitspraak openbaar bekend wordt. De informatie is echter niet voor organisaties doorzoekbaar zoals bijvoorbeeld wel het geval is bij verkeersongevallen die worden geregistreerd in een verkeersongevallenregistratie die onder meer wordt gebruikt voor wetenschappelijk onderzoek (onder andere door SWOV) en voor beleidsondersteuning.

Uit eigen beweging onderzoek doen en publiceren

Een aantal organisaties heeft ervoor gekozen om in het publiek belang en ter verantwoording aan zijn eigen achterban (burgers, studenten) de resultaten van forensische of andere onderzoeken, openbaar te maken.

207 https://www.cybersecurityraad.nl/documenten/adviezen/2020/02/11/csr-advies-beschikbaar-stellen-datalekmeldingen-voor-onderzoeksdoeleinden---csr-advies-2020-nr.-1

Onderzoek naar cyberongevallen in de openbaarheid
In juni 2019 informeerde de politie de gemeente Lochem dat aanvallers het digitale systeem van de gemeente mogelijk was binnengedrongen. Sindsdien ziet de burgemeester van Lochem voor zichzelf een missie om gemeenten en andere overheden te waarschuwen voor dit risico en het belang van digitale weerbaarheid te onderstrepen.[208]

Op 23 december 2019 werd de Universiteit Maastricht getroffen door een cyberaanval. De universiteit liet het voorval onderzoeken en hield medewerkers en studenten op de hoogte van de gebeurtenissen. Tijdens een symposium op 5 februari 2020 presenteerden zij de resultaten en legde de universiteit uit hoe het ongeval kon gebeuren en welke lessen ze eruit trokken.[209] Ook de Onderwijsinspectie onderzocht het ongeval.[210]

In december 2020 werd de gemeente Hof van Twente binnengedrongen. Het gevolg was dat de gemeente zijn dienstverlening aan inwoners een aantal weken (paspoorten, rijbewijzen en uittreksels) tot maanden (gemeentelijke belasting) moest stilleggen, konden facturen niet worden betaald en kon de gemeente niet veilig samenwerken met andere organisaties. Ook moest de gemeente zijn digitale systeem opnieuw opbouwen. Net als de Universiteit Maastricht hield de gemeente Hof van Twente haar inwoners op de hoogte met regelmatige updates. Ook liet zij het voorval onderzoeken en publiceerde de resultaten daarvan aan het publiek.[211]

In februari 2021 werden de Universiteit Amsterdam en de Hogeschool van Amsterdam getroffen door een cyberaanval. Ook zij lieten het voorval onderzoeken en publiceerden daarvan de resultaten.[212]

De traditie om van voorvallen te leren is in het digitale domein nog in ontwikkeling. Voorvallen moeten worden gemeld, maar worden niet systematisch onderzocht. Een "infrastructuur" voor gezamenlijk leren door fabrikanten, organisaties die software gebruiken en andere relevante publieke en private partijen ontbreekt.

208 https://ibestuur.nl/magazine/cyberaanval-lochem-gaat-de-hele-overheid-aan
209 https://www.maastrichtuniversity.nl/nl/updates-cyberaanval
210 https://www.onderwijsinspectie.nl/documenten/rapporten/2020/06/12/rapport-cyberaanval-universiteit-maastricht
211 https://www.hofvantwente.nl/actueel/nieuws-en-persberichten/nieuwsbericht/archief/2021/03/artikel/hof-van-twente-cyber-hack-stevige-les-voor-ons-1872
212 https://www.uva.nl/content/nieuws/nieuwsberichten/2021/07/evaluatie-cyberaanval.html

4.4.2 Belemmeringen om van (onderzoeken naar) digitale voorvallen te leren

In de vorige paragraaf werden de verschillende manieren beschreven waarop op dit moment digitale voorvallen worden gemeld en onderzocht. En op welke manier de resultaten van deze meldingen en onderzoeken worden gebruikt om organisaties meer inzicht te geven in wat zij kunnen doen om toekomstige voorvallen te voorkomen. Over het geheel genomen laat de huidige werkwijze zien dat het leren van digitale ongevallen door een aantal factoren wordt belemmerd.

Melden en in de openbaarheid komen

De gemeenten Lochem en Hof van Twente, evenals onderwijsinstellingen Universiteit Maastricht en Universiteit van Amsterdam/Hogeschool van Amsterdam kunnen worden gezien als uitzonderingen op de regel dat organisaties niet geneigd zijn om in het openbaar te delen dat zij een digitaal voorval hebben meegemaakt en wat zij daarvan hebben geleerd. In de gesprekken die de Onderzoeksraad heeft gevoerd met verschillende organisaties en met partijen die deze organisaties bijstaan, worden meerdere redenen genoemd, waarvan er hier drie worden besproken.

Ten eerste is dat angst voor reputatieschade en afnemend vertrouwen van partijen waar de organisatie mee samenwerkt. Een digitaal voorval zoals een *ransomware* aanval kan in de buitenwereld worden gezien als een teken dat de organisatie de informatiebeveiliging niet op orde heeft. Dit kan ervoor zorgen dat het vertrouwen in de betreffende organisatie afneemt. Dit effect is moeilijk meetbaar. Tot nu toe zijn er geen signalen dat datalekken per definitie leiden tot een waardedaling van het bedrijf. Daarnaast zijn er in andere domeinen zoals de voedselsector aanwijzingen dat organisaties juist het vertrouwen kunnen behouden of versterken als zij vrijwillig naar buiten komen met een veiligheidsprobleem en dit ook daadkrachtig aanpakken.[213] Een ander psychologisch effect is schaamte. Bij cybervoorvallen is dit effect sterker dan bij andere voorvallen zoals een auto-ongeluk. Dat komt onder meer doordat betrokkenen bij een cyberaanval zoals een *ransomware* aanval het gevoel hebben opgelicht te zijn, ergens ingetuind te zijn en gefaald te hebben. Naast verlies van een gevoel van veiligheid leidt dit ook tot een verlies van status.[214]

Een tweede belemmering om met een voorval naar buiten te komen, is dat dit juridische consequenties kan hebben. Als het digitale voorval gepaard is gegaan met het overtreden van wettelijke regels (bijvoorbeeld als er data is gelekt of een zorgplicht niet is nagekomen), dan kunnen toezichthouders handhavend optreden. Andere partijen (consumenten, afnemers, leveranciers, aandeelhouders) kunnen zich aangetast voelen in hun rechten en de organisatie daarvoor aansprakelijk stellen. Zo heeft één van de software fabrikanten die we spraken lessen uit het voorval getrokken, maatregelen genomen en die gedeeld via hun website, maar deze lessen niet actief gedeeld met andere fabrikanten andere betrokken organisaties of het publiek. Als de software industrie onderling en publiekelijk gesloten blijft over hoe fouten ontstaan kan er geen gezamenlijk leerproces plaatsvinden.[215]

213 Zie bijvoorbeeld https://doi.org/10.15728/bbr.2017.14.2.4
214 Goffman, E., On Cooling the Mark Out, 1952, *Psychiatry*, 15:4, 451-463, DOI: 10.1080/00332747.1952.11022896.
215 Zie ook Tjong Tjin Tai, E., en Knoops, B., *Zorplichten tegen cybercrime* (NJb), 2015.

Als derde belemmering wordt genoemd dat de organisatie vreest dat het risico op aanvallen toeneemt zodra bekend wordt dat de organisatie al een keer (succesvol) is aangevallen.

De wijze waarop digitale voorvallen worden onderzocht
Een beletsel voor het leren die samenhangt met de vorige belemmeringen is hoe er in de rapporten wordt geschreven over de factoren die bijdroegen aan het ontstaan van het voorval. Zoals we hiervoor schreven is reputatieschade een reden om voorvallen niet te melden. Schaamte (zelfstigma) speelt daarbij ook een rol. Evaluaties die opsommen welke fouten een organisatie heeft gemaakt, zonder daarbij te onderzoeken hoe het begrijpelijk kan zijn voor een organisatie dat hij zich in deze situatie bevond, kunnen dit (zelf)stigma vergroten en dragen niet bij aan de bereidheid van organisaties om naar buiten te treden met wat ze hebben meegemaakt, zodat anderen ervan kunnen leren.

Veel van de evaluaties zijn gericht op wat de organisatie in kwestie zelf zou moeten doen, en gaan niet in op de systeemvraag die wegkomt achter de vraag hoe het komt dat het voor organisaties moeilijk is om te voorkomen dat ze worden aangevallen en om aanvallen succesvol te kunnen weerstaan. In de evaluaties ligt de focus op *security* (beveiliging) en minder op het inrichten van een veilig digitaal systeem dat weerstand kan bieden tegen allerlei mogelijke bedreigingen.

Willen begrijpen hoe dingen konden gebeuren is cruciaal bij alle onderzoeken naar voorvallen, ook bij het voorliggende onderzoek. Om van ongevallen te leren is dan ook van belang hoe het ongevalsonderzoek is ingericht: dat het ongevalsonderzoek erop is gericht om het ongeval te kunnen verklaren. Daarvoor moet het onderzoek verder gaan dan toetsen aan normen en standaarden (eerste orde leren), het moet ook reflecteren op gehanteerde uitgangspunten (tweede orde leren). Zeker in een domein waar het leren van voorvallen in ontwikkeling is, is belangrijk om ook te reflecteren op de wijze waarop we leren (derde leren of deuteroleren). De meeste evaluaties die de Onderzoeksraad bekeek waren beperkt tot eerste orde leren. De evaluaties bestonden voornamelijk uit constateringen dat de betreffende organisatie niet alle voorgeschreven of verwachte basismaatregelen had geïmplementeerd en dat dit factoren waren die tot het voorval hadden geleid. Of er waren evaluaties die weliswaar de aanpak en het beleid analyseren, maar waaruit niet duidelijk werd welke factoren bijdroegen aan het ontstaan van het voorval.

De evaluatie van de Onderwijsinspectie van de *ransomware* aanval op de Universiteit Maastricht laat zien dat een reflectieve insteek van een voorvalonderzoek mogelijk en zinvol is. Zo is in dat onderzoek gezocht naar een verklaring voor het feit dat de informatiebeveiliging niet aan de beschikbare normen en standaarden voldeed. Eén van deze verklaringen was dat het op universiteiten en hogescholen vanwege de bestuurlijke gelaagdheid moeilijk is voor het bestuur om zicht te hebben op de staat van de informatiebeveiliging. Dit inzicht is van belang, omdat een dergelijke bestuurlijke gelaagdheid bij alle universiteiten en hogescholen aanwezig is en mogelijk bij meer hoger onderwijsinstellingen het zicht van het bestuur op de informatiebeveiliging belemmert.

Het verspreiden van inzichten naar degenen die deze inzichten nodig hebben
In de voorgaande subparagraaf worden verschillende soorten onderzoeken naar voorvallen benoemd. De informatie die deze onderzoeken oplevert wordt in een beperkt aantal gevallen openbaar gemaakt: wanneer de organisatie daar bij uitzondering voor kiest of daartoe wordt bewogen door de toezichthouder. In de vorige subparagraaf worden als voorbeeld de universiteit van Maastricht, Universiteit/Hogeschool van Amsterdam, gemeente Lochem en gemeente Hof van Twente genoemd. Ook wordt beschreven dat de meeste onderzoeken naar voorvallen niet worden gepubliceerd, of alleen in besloten kring. Vaak is de informatie alleen begrijpelijk voor een beperkte kring van experts en lijkt het een abstracte technische gebeurtenis. Daarom is het belangrijk om bij het delen van inzichten uit cyberaanvallen, deze te demystificeren en de menselijke gevolgen ervan te benadrukken.[216]

Ook is er nog geen entiteit die informatie uit onderzoeken en meldingen verzamelt ten behoeve van wetenschappelijk en/of statistisch onderzoek. In het cyberdomein, dat een relatief nieuwe traditie heeft als het gaat om incidentenonderzoek, is behoefte aan een platform waar kennis wordt gedeeld, vastgehouden en waar organisaties op zoek kunnen naar relevante inzichten om hun informatiebeveiligingsbeleid beter te kunnen onderbouwen (*historic capture*). Overigens sluit dit aan bij de missie van het NCSC als Nationaal Cyber Security Centrum: begrijpen en duiden wat er gebeurt, het verbinden van partijen, kennis en ervaring met als doel om herhaling te voorkomen.[217]

In de huidige praktijk komen veel organisaties er niet voor uit dat ze zijn aangevallen. De onderzoeken bieden niet de verklaringen die nodig zijn om het systeem te verbeteren. Betrokken organisaties verspreiden lessen uit voorvallen meestal niet buiten de eigen organisatie of gemeenschap.

4.5 Beleid en internationale context

Op Europees niveau is er verschillende regelgeving op het gebied van cybersecurity, en zijn ook een aantal initiatieven in ontwikkeling. Deze regelgeving en initiatieven hebben ieder een verschillend doel en doelgroep. In de tabel hieronder zijn enkele kenmerken van de regelgeving opgenomen.

216 Schaake, M., *The Lawless Realm, Countering the Real Cyberthreat*. 2020. https://www.foreignaffairs.com/articles/world/2020-10-13/lawless-realm
217 https://www.ncsc.nl/over-ncsc, geraadpleegd op 13 september 2021.