FABRIC FOR CYBER RESILIENCE

EEN GEZAMENLIJKE AANPAK
VOOR ABUSE BESTRIJDING

TABLE OF CONTENTS

OVER HET FABRIC FOR CYBER RESILIENCE

Onrechtmatigheid op internet groeit zowel in volume als in diversiteit. Nog niet eens zo lang geleden waren termen als spam of DDoS alleen bekend bij internet experts. Inmiddels heeft vrijwel iedere Nederlander wel eens gehoord van phishing, ransomware, malware of sextortion. Het bestrijden ervan is een lastige opgave. De klassieke aanpak van handhaving is niet altijd effectief. Een andere, bottom-up aanpak is nodig. De online sector, justitie, politie, meldpunten, collectieve initiatieven en andere partijen uit overheid, bedrijfsleven en het maatschappelijk middenveld moeten intensiever gaan samenwerken. Zodat we abuse beter kunnen bestrijden en ook toekomstige vormen van abuse het hoofd kunnen bieden. Kortom, we hebben een ‘Fabric for Cyber Resilience’ nodig.

DEEL I : WAT IS ABUSE, EN HOE WERKT HET?

OOK CYBERCRIMINELEN INNOVEREN

Op het internet is het gemakkelijk om iets nieuws te bedenken. Alles wat je nodig hebt is met enkele muisklikken te vinden. Zonder investeringen of vergunningen kun je beginnen en de wereld bereiken. Door bestaande digitale diensten te combineren in nieuwe toepassingen ontstaan zelfs compleet nieuwe business modellen. Dat is de kern van het “permissionless innovation paradigma”. Die term werd al in de tachtiger jaren gebruikt door Vint Cerf, één van de grondleggers van het internet. Het verklaart de razendsnelle ontwikkeling van online diensten, de kansen voor de economie en de grote impact van digitalisering op de samenleving.

Permissionless innovation biedt niet alleen voordelen. Ook voor kwaadwillenden is het eenvoudig om nieuwe, onrechtmatige activiteiten te ontplooien. Zij maken daarbij gebruik van dezelfde voorzieningen of diensten die essentieel zijn voor innovatie, bescherming van de vrijheid van meningsuiting of communicatie.

ABUSE BESTRIJDEN IS LASTIG

De internationaal geaccepteerde verzamelnaam voor onrechtmatigheid op het internet is “abuse”[1].In de technische context wordt soms de term “badness” gebruikt. Abuse kent veel verschijningsvormen en er komen steeds nieuwe bij. Het kan gaan om schendingen van auteursrechten, verspreiden van malware, CAM[2], versturen van phishing mails of spam, een frauduleuze website, botnets en meer. Voor hun praktijken maken de veroorzakers soms gebruik van gaten in de beveiliging van bestaande voorzieningen. Of gebruiken “normale“ voorzieningen. En maken daarbij dan vaak gebruik van de mogelijkheden om op het internet anoniem te blijven.

Het aanpakken van abuse is daardoor niet eenvoudig. Het is in de eerste plaats vaak moeilijk om de daders te lokaliseren omdat ze anoniem zijn en zich letterlijk overal ter wereld kunnen bevinden. Hun IP-adres kan ook dat van een proxy zijn waardoor de werkelijke locatie van de dader niet te achterhalen valt. Ten tweede is het niet altijd mogelijk om op basis van de technologie het gebruik voor rechtmatige dan wel onrechtmatige doeleinden te onderscheiden. Goed en fout gebruik van digitale infrastructuur lopen door elkaar en zien er vaak hetzelfde uit. Het eenvoudig en snel kunnen aanmaken van een server, opslag, domeinnaam of website is belangrijk voor innovatie maar is ook handig voor iemand die een phishing site wil maken. En ten derde is het ineffectief om voor elk probleem een specifieke aanpak te ontwikkelen. Dat leidt tot versnippering en dubbel werk, omdat de vele vormen van abuse ook veel overeenkomsten hebben.

1 Zie de definitie van abuse op de home page van de m3aawg, de anti-abuse coalitie

2 Child Abuse Material, in Nederland wordt meestal de term kinderporno gebruikt

ABUSE BESTRIJDEN MET EEN GENERIEKE AANPAK

Een mogelijkheid om versnippering te voorkomen is het gericht inzetten op de gemeenschappelijke kenmerken. Wat hebben alle vormen van abuse gemeen? Welke mechanismen werken er “onder de motorkap”? Bijvoorbeeld: DDoS, spam en phishing zijn verschillende problemen maar voor alle drie worden vaak botnets ingezet, dat zijn netwerken van computers en andere apparaten die geïnfecteerd zijn met malware. Eén ding is zeker: in het cyberdomein kunnen veel vormen van abuse worden bestreden door in te zetten op verminderen van kwetsbaarheden en door versnellen van detectie, melden en acteren op de aangetroffen oorzaken. Dat past bij het gegeven dat de beste resultaten bij bestrijding van (cyber)crime kunnen worden bereikt met het vergroten van de pakkans en het belemmeren van activiteiten: het zogenaamde “barrièremodel”.

ABUSE EN DIGITALE INFRASTRUCTUUR

De volgende vraag is dan hoe onrechtmatigheid het beste kan worden gedetecteerd, waar de kwetsbaarheden zitten en wiens voorzieningen worden misbruikt, en wie de partijen zijn die daar iets aan kunnen doen. De gemeenschappelijke factor is de digitale infrastructuur. Die wordt gerund door ISP’s, (web)hosters, cloud providers, platforms en domein registrars maar ook door andere partijen met eigen in-house internetnetwerken (een AS[3]). Hier vallen ook overheidsdiensten, banken en andere bedrijven met een eigen digitale infrastructuur onder. Het zijn deze netwerken en de systemen waar de abuse zich bevindt. Belangrijk is het gegeven dat voor die partijen eigenlijk geen wezenlijk onderscheid bestaat tussen de verschillende vormen van abuse. De aanbieders van die generieke voorzieningen zien uiteraard de maatschappelijke effecten, maar beschouwen abuse in technische zin als iets wat in hun netwerk niet thuishoort, en dus moet worden verwijderd.

Detectie van abuse (informatie) vindt vrijwel altijd plaats op basis van een URL, domein of IP adres. Dat uit zich in voorzieningen als een onrechtmatig bestand, een site met onrechtmatigheid, een kwetsbaarheid in een server, een email server die misbruikt kan worden, een lek, een daarvoor geregistreerd domein, et cetera. Als de partij die de infrastructuur achter het IP adres of domein beheert daarover geïnformeerd wordt, zit je dicht bij de bron. Kortom, als het mogelijk is om real time informatie uit te wisselen met zulke partijen dan kan sneller ingegrepen worden in die voor abuse gebruikte infrastructuur. Met snel uitwisselen van algemene dreigingsinformatie, informatie over gedetecteerde kwetsbaarheden, ongewenste of onrechtmatige activiteit op systemen en netwerken en met de medewerking van die partijen om snel te handelen op basis van die informatie, wordt het lastiger en dus onaantrekkelijker om daar abuse activiteiten te ontplooien.

NEUTRALE ROL PROVIDERS

De systemen van de providers van digitale infrastructuur, we refereren in dit document aan zulke partijen als DIPs[4], worden vaak misbruikt voor abuse. Het ligt dan voor de hand om te stellen dat zij dat dan zelf moeten voorkomen. Maar de meeste DIPs kunnen niet op eigen initiatief ingrijpen. Ze hebben namelijk een neutrale rol, die stevig is verankerd in het Europese e-commerce directive. De neutrale rol houdt in dat DIPs niet aansprakelijk of verantwoordelijk zijn voor de activiteiten van hun klanten en gebruikers. Dat is een pijler onder het open en vrije internet. Het voorkomt dat DIPs moeten censureren of verplicht worden om de gangen van hun klanten en gebruikers na te gaan.

3 Een AS is een Autonomous System, waarmee een deelnetwerk van het internet wordt aangeduid: een reeks IP adressen met zelfstandige routering.

4 We introduceren de term DIP, “Digital Infrastructure Provider”: Een bewuste keus om verwarring met de juridische term intermediary te vermijden. Immers, een DIP is niet altijd per definitie een intermediary.

Dat neemt niet weg dat DIPs ook een verantwoordelijkheid hebben om te acteren zodra ze kennis hebben van abuse in hun voorzieningen en andere methoden om dat te verwijderen hebben gefaald. Bijvoorbeeld als een externe partij er niet in geslaagd is om abuse te verwijderen na een melding aan de directe veroorzaker en vervolgens de DIP daarover informeert.

Vanuit dit gegeven is de Nederlandse gedragscode NTD[5] (Notice en Takedown) ontwikkeld die inmiddels in veel landen wordt gehanteerd en door Nederlandse providers goed wordt nageleefd.

NTD

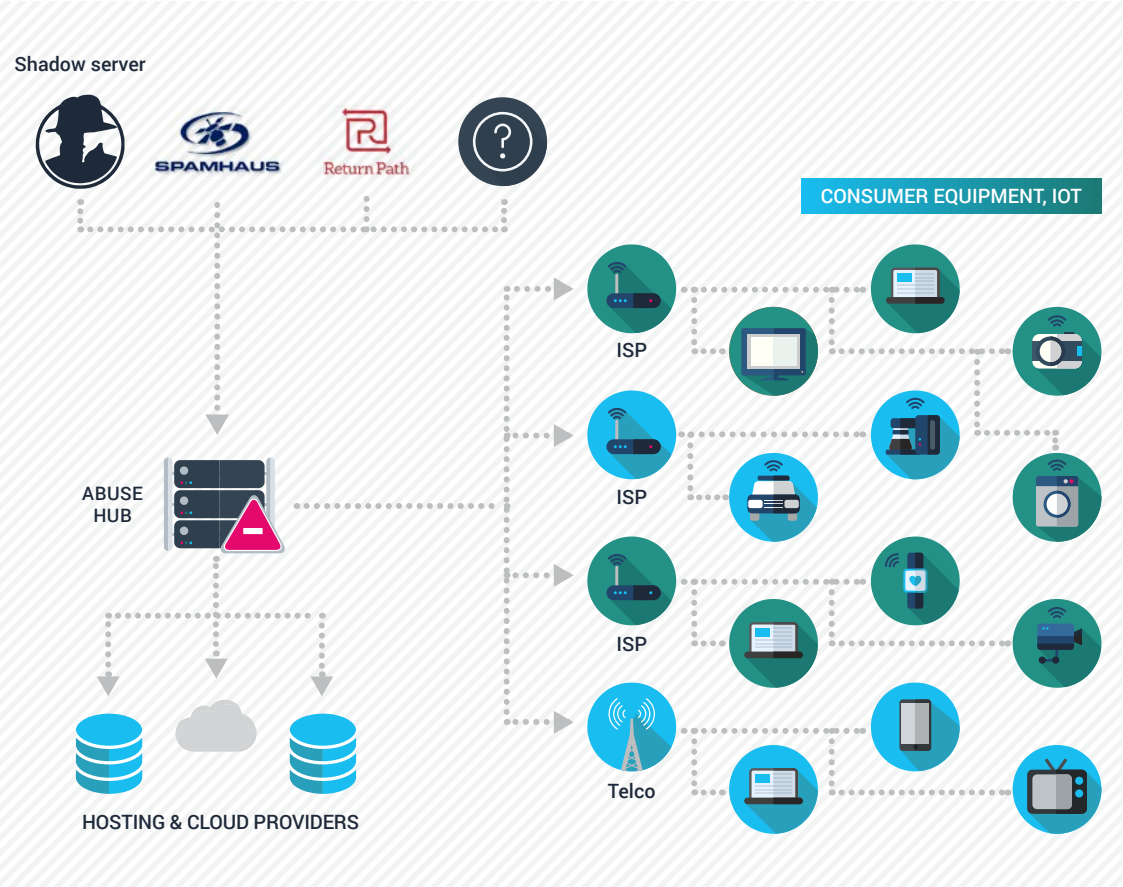
De gedragscode NTD is door de gelijknamige werkgroep van het ECP in 2008 ontwikkeld om intermediaries ondanks hun neutrale rol toch de mogelijkheid te geven om onmiskenbare onrechtmatigheid uit hun netwerken te verwijderen. Bedrijven en burgers die na het indienen van hun klacht bij de direct betrokkenen geen reactie krijgen of geen resultaten zien, kunnen abuse melden aan de betreffende providers. Die hebben daarvoor vaak een speciaal email adres of een abuse helpdesk. Ook worden meldingen gedaan door en via meldpunten: organisaties die gespecialiseerd zijn in bepaalde soorten van abuse. Voorbeelden zijn Het EOKM (Expertisebureau Online Kindermisbruik, ook wel bekend als het “meldpunt kinderporno”), het LMIO (Landelijk Meldpunt Internet Oplichting), de stichting “Opgelet op Internet” en de Fraudehelpdesk. Ze detecteren onrechtmatigheid zelf of ontvangen meldingen van derden. Zij melden dit op hun beurt aan de betrokken partijen, vaak DIPs. Als die de gedragscode NTD hanteren zullen ze na zulke meldingen uitzoeken wat er aan de hand is. Onder meer door afhankelijk van de melding hoor- en wederhoor toepassen bij de betreffende klant of gebruiker. Ze kunnen op basis van hun bevindingen dan besluiten de onrechtmatigheid zelf te beëindigen of te verwijderen.

Naast de systematiek met externe “notifiers” zoals de meldpunten maken providers soms ook gebruik van andere bronnen die abusemeldingen online aanleveren. Providers die zich abonneren op zo’n abuse informatiebron (“abuse feed”), krijgen meldingen over kwetsbaarheden of andere ongewenste activiteit in hun netwerken automatisch toegestuurd, waarop ze kunnen acteren. Voorbeelden van initiatieven rond dit principe zijn de AbuseHUB[6] en het project abuse204.nl[7] van SIDN. Partijen die zulke (betrouwbare) notices aanleveren worden trusted notifiers genoemd. De ontvangers bepalen zelf welke “trust” een notifier heeft, maar in het algemeen is de betrouwbaarheid van bronnen zoals het EOKM of de databases van Shadowserver of Spamhaus, onbetwist.

ABUSEHUB

De AbuseHUB is een dienst van de vereniging Abuse Information Exchange die in 2012 is opgericht door enkele ISP’s om botnets in Nederland aan te pakken. De AbuseHUB combineert informatie over botnet activiteiten of besmette of lekke computers uit allerlei openbare bronnen, zogenaamde “feeds”. Deze informatie wordt in een gestandaardiseerd formaat verstuurd naar de aangesloten deelnemers[8]. Die kunnen daarop snel acteren naar hun gebruikers. Zo worden veel botnets in één klap bestreden. Door de activiteiten van de AbuseHUB is in slechts enkele jaren tijd de botnet activiteit in Nederland bij de access netwerken (ISP’s) flink verminderd.

5 https://ecp.nl/activiteiten/werkgroep-notice-and-takedown/
6 https://www.abuseinformationexchange.nl/
7 Abuse204.nl, “Abuse to zero for NL” is designed to combat phishing and malware in the .nl zone.
8 Een gangbare standaard voor abusemeldingen is iodef.



KNELPUNTEN

Door de afname in absolute aantallen besmette computers bij ISP's (de access netwerken) is het relatieve aandeel van besmette servers bij hosters en andere aanbieders van infrastructuur gestegen. 39% van de botnet infecties is thans afkomstig uit de netwerken van hosters, zo blijkt uit de informatie van TU Delft[9]. Bovendien staat Nederland nog steeds te hoog in de internationale ranglijsten van Abuse[10]. Dat is niet goed voor het imago van Nederland als land waar je veilig en verantwoord online zaken kan doen. De AbuseHUB wordt door hosters echter voornamelijk gezien als een informatiebron voor accessproviders. Of ze zijn van mening dat zo'n aansluiting op AbuseHUB niet nodig is want zulke abuse, denken ze, komt bij hen niet voor – of is alleen een zaak van hun klanten. Maar de data van TuDelft laat zien dat dat niemand immuun is.

Bij het aanspreken van hostingpartijen op aangetroffen abuse is er ook de complexe problematiek van "resellers". Dat zijn partijen, soms buitenlandse, die hosting infrastructuur van een Nederlandse hosting provider doorverkopen onder een eigen label. Het is voor de oorspronkelijke hosting aanbieder dan niet altijd even eenvoudig om te kunnen bepalen waar de abuse zich precies binnen hun infrastructuur bevindt. Soms ontbreken de mogelijkheden om iets weg te halen zonder schade toe te brengen aan andere diensten.

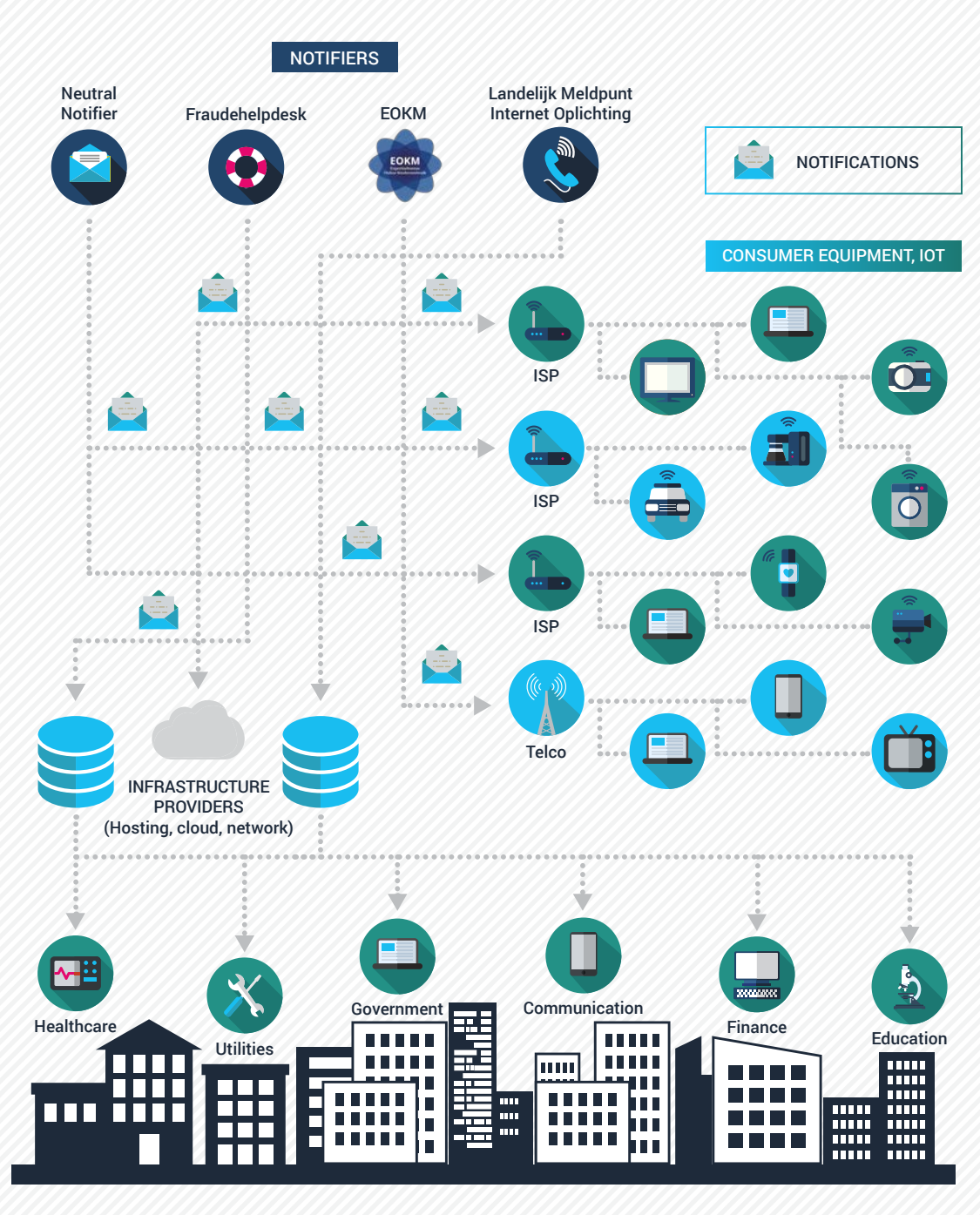
Ook de aanlevering van notices en de toepassing van de gedragscode NTD kent verschillende knelpunten. De meldpunten sturen hun meldingen elk op een eigen manier, meestal via email. Die gangbare praktijk van opstellen en verzenden van notices is niet erg efficiënt. Er is bij hen sprake van tijdrovend handmatig uitzoekwerk om een melding op te stellen en de juiste target voor een melding te achterhalen. Dat komt onder andere doordat de contactinformatie in de public registries van domeinnamen en internetnetwerken niet betrouwbaar is. Het gevolg is dat de email naar zulke

9 http://resolver.tudelft.nl/uuid:3a41c856-6b3a-4bcc-b9e1-1707a6e1aa86

10 https://www.linkit.nl/knowledge-base/118/The_Netherlands_remains_first_in_cybercrime_in_Europe

contacten in veel gevallen niet aankomt of niet wordt gelezen. In dat geval moet via een andere manier contact worden gezocht. Ook komt het voor dat partijen die zelden meldingen ontvangen, meest kleinere DIPs, niet weten wat te doen op het moment dat zij wel een melding krijgen. Daardoor komen ze soms niet in actie. Het gevolg is dat abuse door zulke partijen in het weekend vaak niet wordt behandeld- iets wat cybercriminelen uiteraard ook weten. Soms wordt getwijfeld aan de authenticiteit van de melder. En last but not least negeren enkele hosters de NTD willens en wetens. Zij vallen internationaal op als vrijplaatsen voor CAM en dat bezorgt Nederland een slechte naam[11].

Uit dat beeld dringt zich één evidente conclusie op. Als iedere DIP, groot of klein, notices en andere informatie over abuse op een gestandaardiseerde wijze zou ontvangen, en daar snel en gericht actie op zou ondernemen, dan zal abuse flink kunnen verminderen. Dat geldt ook voor de uitwisseling van informatie met partijen in andere landen. Standaardisatie, informatiedeling, snelheid, en betrokkenheid en bereikbaarheid van zoveel mogelijk partijen zijn hier de sleutelwoorden.



11 Zie het recente rapport van het IWF (Internet Watch Foundation)

DEEL II: HET FABRIC FOR CYBER RESILIENCE

Het “Fabric for Cyber resilience” is een concept voor het versterken van preventie en detectie van abuse en cybercrime. Het idee voor het Fabric is ontstaan naar aanleiding van de opgedane ervaring en inzichten in het project “Abuse 2.0”; een project dat ECP uitvoert in opdracht van het Ministerie van Economische Zaken, in het kader van het PIV (Platform Informatie Veiligheid) bij het ECP[12]. Bij Abuse 2.0 zijn onder andere de ACM, OM, Team HTC, ECP, TU Delft, Ministerie van EZ, ISP’s, NBIP, en ISPConnect en DHPA betrokken. Het doel van Abuse 2.0 is het stimuleren van abuse bestrijding bij en door hosters. Onderdeel van het project is het ontwikkelen van een code of conduct, en het informeren van de door TU Delft geïdentificeerde Nederlandse aanbieders van infrastructuur over hun performance op het gebied van abuse bestrijding. Het idee is dat daardoor de motivatie van DIPs, met name hosters, toeneemt om op de AbuseHUB aan te willen sluiten.

Bij de uitvoering van Abuse 2.0 ontstonden een aantal nieuwe inzichten:

- Er is geen goede en betrouwbare methode te vinden voor het structureel informeren van alle ca 800 partijen die geïdentificeerd zijn in het onderzoek van TU Delft, die abuse notices en informatie over hun performance op het gebied van abuse bestrijding zouden moeten ontvangen. Dat komt doordat de abuse informatie in de RIPE en Whois databases onvoldoende betrouwbaar is, of meldingen naar die adressen niet worden verwerkt.
- Het is (daarom) het meest efficiënt om te streven naar het in één keer aansluiten van de vele partijen op één breed informatienetwerk.
- Aansluiten van vele, vaak kleine partijen kan niet zonder de spreekwoordelijke “stok en wortel”. Omdat er geen wettelijke verplichting is, is een stevig incentive nodig voor zulke partijen om mee te gaan doen. De performance informatie van de TU Delft alleen blijkt onvoldoende te motiveren. Er moet meer worden geboden.

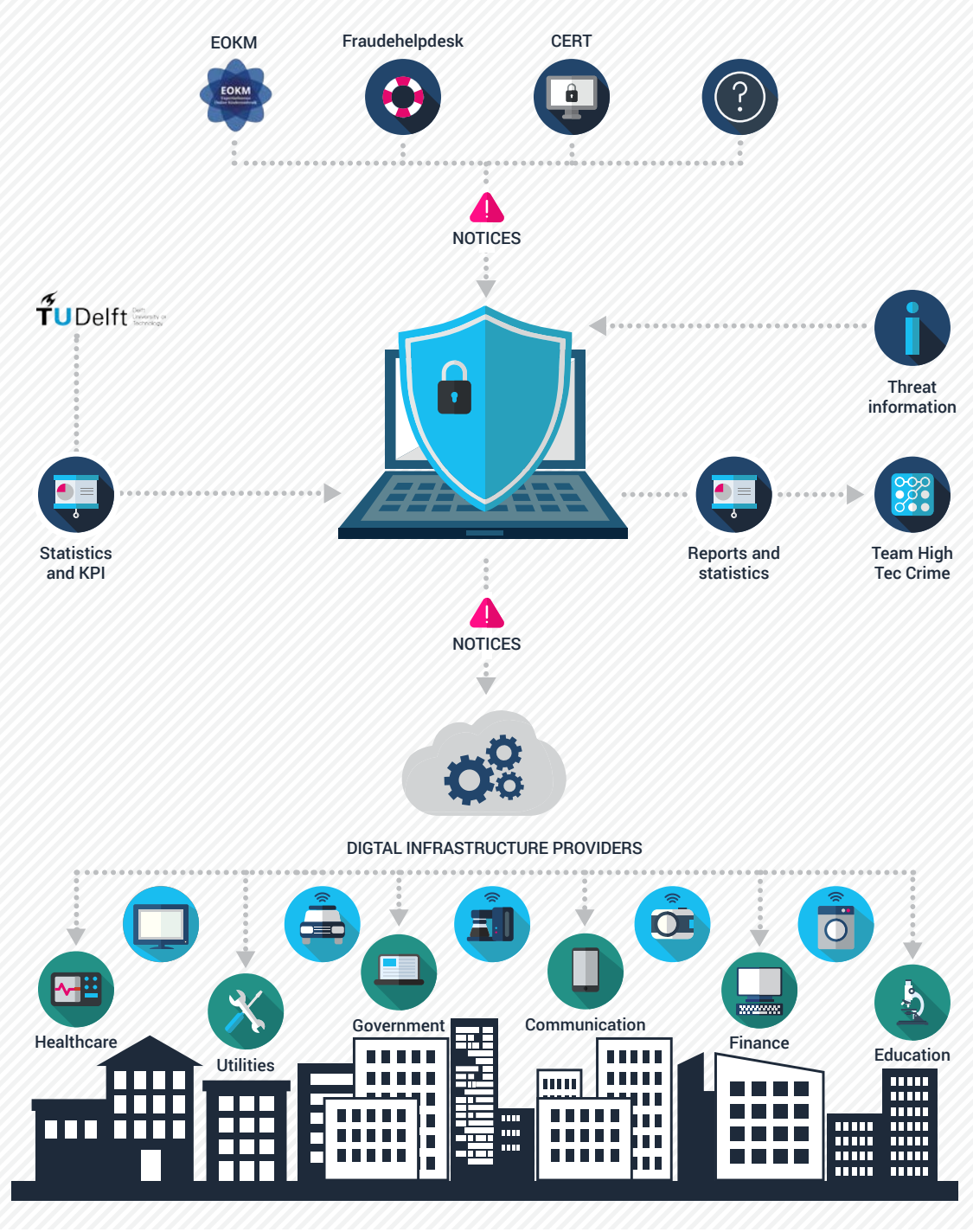
De conclusie is dat er sterke behoefte is aan een landelijk informatieuitwisselingsnetwerk: een landelijke CERT[13], waar alle DIPs op aangesloten zouden moeten worden. Langs die weg kan abuse informatie snel, gericht op een gestandaardiseerde manier worden verspreid en kan elke plek waar abuse voorkomt beter en sneller worden bereikt. Zo wordt bovendien versnippering voorkomen.

De tweede conclusie is dat steviger moet worden ingezet op het uitwerken van de juiste incentives. Alleen zo kunnen alle DIPs worden bewogen om zich aan te sluiten op zo’n landelijke CERT.

Veel organisaties uit de Nederlandse sector digitale infrastructuur zien het belang van zo’n brede, holistische aanpak. Het is essentieel dat zoveel mogelijk organisaties gaan samenwerken met elkaar, en met de overheid. Met als doel het probleem integraal aan te pakken. Want alleen met zo’n brede aanpak, gedragen door de sector zelf, heeft abuse bestrijding werkelijk kans van slagen.

12 www.ecp.nl

13 Een CERT is een Computer Emergency en Response team, CSIRT een Computer Security Incident Response Team.



LANDELIJKE CERT

Een essentieel element van het Fabric for Cyber Resilience concept is het inrichten van een real-time informatienetwerk, dat alle DIPs in Nederland kan verbinden. Naar schatting van TuDelft zijn dat er ca. 800. De nationale CERT functie wordt in Nederland ingevuld door het NCSC. Het mandaat van het NCSC is echter beperkt tot de overheid en kritieke infrastructuur. Daardoor kan informatie die het NCSC ter beschikking heeft of wordt gesteld, niet zonder meer naar alle DIPs worden verstuurd. Ook de AbuseHUB heeft een CERT functie, momenteel voor haar aangesloten leden. Daarnaast heeft de stichting NBIP een functie voor het ontzorgen van kleinere providers op het gebied van wettelijke verplichtingen, en met haar NaWas[14] functie eveneens enkele kenmerken van een CERT.

14 http://www.nbip.nl/diensten/nawas-demand-beveiliging-tegen-ddos/

Door deze en andere partijen zou kunnen worden nagedacht over het ontwikkelen van de gewenste nationale CERT, en over de verschillende functies die van zo'n nationale CERT mogen worden verwacht.

ABUSE-IO

Het Nederlandse open source project Abuse-IO[15] is een initiatief vanuit de Nederlandse hosting sector voor het automatiseren van opstellen, versturen en afhandelen van notices. Abuse-IO hanteert de Iodef standaard voor notices en er is open-source software beschikbaar voor het versturen en afhandelen van zulke berichten. Abuse-IO wordt ingezet voor afhandeling van de kwetsbaarheidsmeldingen van de AbuseHUB. Het systeem is in voortdurende ontwikkeling. Het lijkt daarmee een goede en voor de hand liggende kandidaat voor de inzet als technische oplossing bij zo'n nationale CERT. Door gebruik te maken van de standaard krijgen de notices structuur en kan er meer worden gedaan met de data dan bij gebruik van email. Gedacht kan worden aan statistieken en aan uitwisseling van relevante informatie met justitie.

INCENTIVES

Voor een aansluiting van **alle** DIPS op een landelijke CERT zijn sterke incentives nodig, en een goede methodiek. TU Delft onderzoekt in het kader van Abuse 2.0 het effect van de verschillende methoden om de partijen hiervoor te benaderen. Belangrijk is daarbij de rol van de genoemde incentives.

Er zijn drie voordelen voor DIPS om aan te sluiten. Ten eerste is er het gemak: door aan te sluiten op de nationale CERT kunnen notices van allerlei soorten abuse meldingen desgewenst via één kanaal worden aangeleverd. Ten tweede is er het voordeel van standaardisatie. Door gebruik te maken van de iodef standaard kan de technische diversiteit worden beperkt en krijgt de data waarde. Ten derde: door de aansluiting verkrijgen alle DIPS de TuDelft informatie over hun performance op het gebied van abuse bestrijding, en daarmee direct inzicht in de omvang van abuse op hun platform.

NOTIFIERS

Ook voor meldpunten zijn er voordelen om aan te sluiten op het landelijk netwerk. Abuse-IO is in gesprek met enkele meldpunten over de inzet van het systeem voor opstellen, versturen en volgen van notices. Grote partijen ontvangen hun notices meestal rechtstreeks. Maar de notices zouden, net zoals bij de meldingen van AbuseHUB, en vooral ten behoeve van de kleinere DIPS ook real-time kunnen worden verzonden via de landelijke CERT. Die distribueert zulke meldingen dan via de vaste koppelingen naar de betreffende DIP.

Uiteraard moet zorgvuldig worden bekeken welke notifiers mogen worden aangesloten. Net zoals de AbuseHUB dat nu doet voor meldingen over kwetsbaarheden, mogen ook alleen notices van bekende, trusted notifiers worden verwerkt. Aangesloten partijen moeten altijd kunnen vertrouwen op de authenticiteit en juistheid van meldingen.

ABUSE PERFORMANCE RATINGS

Door TU Delft is in opdracht van het ministerie van Economische Zaken een unieke methodiek ontwikkeld om DIPs uit allerlei informatiebronnen te herkennen, en ze gewogen scores toe te kennen[16]. Deze ranking houdt onder andere rekening met de frequentie, het type en de uptime van bepaalde soorten van abuse en van kwetsbaarheden, en het type van activiteiten van de DIP. Daarbij ontstaan ook overzichten (statistieken) over de aangetroffen abuse per DIP. De bedoeling is om alle DIPs via het landelijk netwerk van deze statistieken te voorzien. Deze informatie is één van de incentives om daarop aan te sluiten. Want daarmee krijgen de DIPs inzicht in hun performance ten opzichte van anderen in het besef dat buitenstaanders zoals hun klanten kunnen zien of en in hoeverre ze hun deel bijdragen aan bestrijding van abuse.

CODE OF CONDUCT

In het kader van het project Abuse 2.0 wordt een code of conduct voor abusebestrijding ontwikkeld. Die verklaring zal omschrijven wat van DIPs wordt verwacht. Gedacht wordt aan het aantoonbaar hanteren van een (industry) best practice[17], het aansluiten op de landelijke CERT en het strikt hanteren van de gedragscode NTD.

Daarnaast kan worden gedacht aan een logo waarmee een DIP aan haar afnemers en de samenleving kan laten zien dat deze abuse bestrijding serieus aanpakt: door de code of conduct te hanteren en het logo te voeren laat je als DIP zien een “Clean network” na te streven. Dat schept duidelijkheid voor iedereen.

FABRIC FOR CYBER RESILIENCE: IEDEREEN MOET MEEDOEN

Met de oprichting van- en aansluiting op AbuseHUB hebben veel grote partijen een uitstekende eerste stap gezet. Dat heeft goede resultaten opgeleverd in de access netwerken. Nu zijn het andere DIPs die steviger zullen moeten gaan inzetten op de bestrijding van abuse. Veel bedrijven claimen dat abuse in hun netwerk niet voorkomt. Maar de informatie van TU Delft laat zien dat niemand immuun is. Die ontwijkende houding zet hun neutrale positie onder druk. En als er geen voortuitgang wordt geboekt, blijft Nederland in negatieve zin opvallen als vrijplaats voor abuse. Dat is niet goed voor het online vestigingsklimaat, en daarmee niet goed voor diezelfde bedrijven. Daarom is het essentieel dat iedereen actief gaat werken aan het bestrijden van abuse binnen hun netwerken en op hun infrastructuur. De tijd dat je online diensten kon leveren zonder je te bekommeren om veiligheid en abuse bestrijding ligt achter ons. Bedrijven die hun kop in het zand steken, of hier niets aan doen, bewijzen de sector en Nederland een slechte dienst. Overheid en sector zijn daarom nu aan zet om de ideeën over zo’n landelijke netwerk verder uit te werken.

Voor een stevig “Fabric for Cyber Resilience” zijn alle draadjes hard nodig.

Met het Fabric for Cyber Resilience wordt de robuustheid van de Nederlandse digitale infrastructuur en de bestendigheid ervan tegen online abuse en cybercrime verbeterd. Daarmee blijft de neutrale rol van providers intact. Door online abuse uit ons land te weren wordt Nederland nog meer een “safe place to do business”, een aantrekkelijke plek voor alle organisaties en bedrijven die Nederland kiezen voor hun online activiteiten.

Mei 2017

16 http://resolver.tudelft.nl/uuid:3a41c856-6b3a-4bcc-b9e1-1707a6e1aa86

17 De m3aawg heeft enkele industry best practices voor abuse bestrijding ontwikkeld