Cybercriminaliteit tegen bedrijven in de EU:

Uitdagingen voor rapportage

Beleidsnota

De afgelopen decennia zijn digitale technologieën doorgedrongen in het dagelijks leven van de EU-burgers en het bedrijfsleven. Digitale innovatie heeft de sociaaleconomische ontwikkeling in alle EU-lidstaten bevorderd, maar heeft er ook toe geleid dat onze samenlevingen in toenemende mate zijn blootgesteld aan cyberdreigingen en cyberaanvallen. Cyberbeveiliging is van fundamenteel belang gebleken voor een digitaal en onderling verbonden Europa, waarvan de welvaart en technologische vooruitgang in toenemende mate afhankelijk zijn geworden van cyberveerkracht.

Sinds de uitbraak van de COVID-19-pandemie, die de digitalisering niet alleen in Europa maar over de hele wereld heeft versneld, zijn er nieuwe uitdagingen ontstaan. Bovendien heeft het aanhoudende conflict in Oekraïne de potentiële blootstelling van personen, bedrijven en overheidsinstellingen aan cybercriminaliteit verder versterkt. Lockdowns en telewerken zijn en blijven een kans voor cybercriminelen.[1] Tussen 2021 en 2022 zijn de meest voorkomende cyberdreigingen ransomware, malware, social engineering-dreigingen, bedreigingen tegen gegevens en beschikbaarheid van gegevens (zoals DDoS-aanvallen),[2] en de compromittering van gegevens - waaronder opvallende aanvallen tegen non-profit organisaties en humanitaire instellingen.[3] Het conflict tussen Rusland en Oekraïne heeft de bezorgdheid over cyberveiligheid in de EU verder doen toenemen. Cyberoorlog is een integraal onderdeel van de Russische invasie

Belangijkste Punten

- De twee meest voorkomende soorten cybercriminaliteit tegen het mkb in de EU27 zijn **virussen, spyware of malware** (met uitzondering van ransomware), gevolgd door **phishing, account takeover of impersonatieaanvallen**.
- In 2021 werd **44% van de cyberdelicten** waarmee het mkb in de EU27 te maken kreeg, **aan niemand gemeld**.
- De **belangrijkste factoren voor onderrapportage** zijn het feit dat **het incident intern werd afgehandeld**, het incident niet de moeite van het melden waard was (te triviaal) en het **gebrek aan vertrouwen in de politie en haar digitale competentie**. Andere relevante factoren zijn **het ontbreken van één meldingsmechanisme, belangenverstrengeling met de bedrijfscontinuïteit** en lacunes in het bewustzijn inzake cyberbeveiliging.
- **Publiek-private samenwerking** is essentieel. Deze samenwerking kan worden bevorderd door **harmonisatie** en centralisatie van meldingsmechanismen en **vertrouwenwekkende publiek-private partnerschappen**.

[1] Europol (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021.

[2] ENISA. (2022). ENISA Threat Landscape 2022.

[3] ICRC. (2022, January 19). Sophisticated cyber-attack targets Red Cross Red Crescent data on 500,000 people.

Deze publicatie wordt gefinancierd door het Fonds voor interne veiligheid - Politie van de Europese Unie.
De inhoud van de publicatie geeft uitsluitend de mening van de auteurs weer en valt onder hun uitsluitende verantwoordelijkheid.
De Europese Commissie aanvaardt geen enkele verantwoordelijkheid voor het gebruik van de informatie in de publicatie.

geweest, met vermeende aanvallen op computernetwerken en informatiesystemen van openbare en particuliere instellingen.[4] De frequente koppeling tussen cyber- en traditionele (offline) misdrijven heeft de criminele dreiging verhoogd, aangezien criminelen het internet steeds vaker gebruiken om hun activiteiten uit te breiden en nieuwe methoden en instrumenten voor crimineel gedrag te vinden.

Ondanks de toenemende dreiging die uitgaat van cyberaanvallen en actoren op het gebied van cyberbeveiliging, is er tot op heden nog steeds weinig informatie beschikbaar over de werkelijke omvang en impact van cybercriminaliteit in de EU - met name wat betreft bedrijven en particuliere entiteiten. Het gebrek aan kennis is vooral te wijten aan onderrapportage, dat wil zeggen dat een zeer klein deel van de cyberdelicten onder de aandacht van het strafrechtstelsel komt. Onderrapportage is een van de belangrijkste obstakels voor een accuraat beeld van cybercriminaliteit tegen bedrijven, het draagt bij tot het gebrek aan effectieve publiek-private samenwerking en leidt uiteindelijk tot beperkte strafrechtelijke resultaten.

Factoren voor onderrapportage van cybercriminaliteit

Onderrapportage blijft een van de grootste problemen om inzicht te krijgen in de werkelijke omvang van cybercriminaliteit. Beperkte aangifte heeft gevolgen voor de registratie van cyberdelicten en dus voor de beschikbaarheid van nauwkeurige gegevens over cybercriminaliteit. Een recent onderzoek naar cybercriminaliteit tegen kleine en middelgrote ondernemingen (MKB) in de EU-lidstaten bevestigt dat de aangifte bij de politie laag blijft: 44% van de cyberdelicten dat het mkb heeft getroffen wordt aan niemand gemeld.[5]

Diverse factoren zouden een rol spelen bij de onderrapportage door bedrijven. Een van de meest terugkerende factoren houdt verband met de perceptie dat het incident te triviaal en/of niet de moeite van het melden waard was, of dat het incident intern werd afgehandeld. Andere factoren zijn angst voor reputatieschade en gebrek aan vertrouwen in de politie. Wat het eerste betreft, zijn bedrijven bezorgd dat cyberincidenten openbaar worden wanneer de autoriteiten het onderzoek beginnen, met mogelijke negatieve gevolgen voor het vertrouwen van klanten en investeerders. Wat de tweede factor betreft, hebben bedrijven vaak geen vertrouwen in de digitale competentie van de politieautoriteiten en melden zij het cyberincident daarom niet.

Een andere belangrijke factor, vooral voor kleine bedrijven of bedrijven die niet vaak contact hebben met de politie, is het ontbreken van één meldingsmechanisme. Volgens een cybercriminaliteitsexpert van Interpol zou het goed zijn om een gecentraliseerd cyberbureau te hebben dat zich bezighoudt met gespecialiseerde cybermeldingen. Dit zou het grote aantal meldkanalen en verplichtingen die in veel landen bestaan, verminderen.

Melding van cybercriminaliteit kan ook worden belemmerd door een belangenverstrengeling met de bedrijfscontinuïteit, in verband met verschillen tussen de prioriteiten van bedrijven en rechtshandhavingsinstanties na een cyberaanval. Vanuit het perspectief van bedrijven is de prioriteit na een cyberincident om het bedrijf draaiende te houden. Dit houdt in dat zij moeten herstellen van de aanval, wat inhoudt dat zij weer toegang krijgen tot (versleutelde) gegevens en dat zij uitgebreid tijdverlies en financiële schade vermijden. Zo was in 2021 verloren business het grootste deel van de kosten na een datalek voor bedrijven wereldwijd.[6] Het in kennis stellen van particuliere beveiligingsbedrijven, het oplossen van technische problemen en het terughalen van activa krijgen daarom vaak een hogere prioriteit dan het bewaren van crimineel bewijsmateriaal.

Ten slotte kunnen lacunes in het bewustzijn inzake cyberbeveiliging en in de meldingsplicht aan het hoger management en de bevoegde autoriteiten leiden tot onderrapportage bij de politie. Sommige bedrijven, met name MKB, zijn zich er vaak niet van bewust dat zij slachtoffer zijn geworden omdat zij niet over opgeleid personeel of middelen beschikken om incidenten op te sporen, en zelfs als een incident wordt ontdekt, is het mogelijk dat bedrijven de aanval niet melden omdat zij de ernst ervan onderschatten.[7]

[4] CSIS. (2022, June 16). Cyber War and Ukraine.

[5] European Commission. (2022). Flash Eurobarometer 496 SMEs and cybercrime.

[6] IBM Seurity. (2021). Cost of a Data Breach Report.

[7] Williamson, J. (2016, February 10). Cyber-attack impact severely underestimated by SMEs. The Manufacturer.

Factoren voor onderrapportage als uitdaging op EU-niveau

Cybercriminaliteit en het algemene ondernemingsklimaat in verschillende lidstaten lijken weinig invloed te hebben op de redenen voor onderrapportage. Een nadere beschouwing van drie verschillende EU-landen, namelijk Bulgarije, Nederland en Spanje, biedt een goed voorbeeld. De drie landen hebben een zeer verschillend ondernemingsklimaat wat betreft het aandeel grote en kleine ondernemingen en digitale geletterdheid. Terwijl Nederland een relatief groot aantal grote ondernemingen heeft, bestaat de bedrijvenpopulatie in Spanje en Bulgarije uit een groot aantal mkb-bedrijven.[8] Bovendien hebben de drie doellanden verschillende niveaus van bedrijfsdigitalisering en -transformatie, waaronder beleidsinstrumenten voor digitale privacy en veiligheid. De drie landen staan echter voor vergelijkbare uitdagingen wat betreft factoren voor onderrapportage door bedrijven. Zo meldde ongeveer een op de tien bedrijven in elk land dat zij niet wisten dat de politie cybercriminaliteit behandelt als een veel voorkomende reden om dit soort criminaliteit niet te melden.[9]

Bulgarije

De informatie over cyberbeveiligingsincidenten en cybercriminaliteit in het land wordt verzameld door het nationale Computer Emergency Response Team (CERT) en het Bulgaarse directoraat-generaal voor de bestrijding van georganiseerde misdaad (GDBOP). CERT Bulgaria meldde dat in 2020 ongeveer 2.100 cyberincidenten werden geregistreerd, waarvan de meeste bestonden uit phishing- en malware-aanvallen. Bovendien was er volgens de Bulgaarse vereniging voor cyberbeveiliging in 2021 een toename van 70% van het aantal cyberaanvallen tegen het mkb in Bulgarije in vergelijking met het jaar daarvoor. Uit interviews met deskundigen blijkt dat de GDBOP dagelijks ongeveer tien signalen over cybermisdrijven of pogingen daartoe ontvangt op haar telefoonnummer. De meest voorkomende soorten cyberdelicten tegen bedrijven die aan GDBOP zijn gemeld, zijn Business Email Compromise (BEC), phishingaanvallen, ransomware, DDoS-aanvallen (meestal voor overheidssites) en cyberaanvallen door voormalige werknemers. Met name bedrijven die actief zijn in de buitenlandse handel worden vaak getroffen door BEC's.

Tot de meest voorkomende factoren voor onderrapportage behoren een gebrek aan kennis van de cyberbeveiligingsvoorschriften die de melding van cyberaanvallen voorschrijven (Cyber Security Act), weinig vertrouwen in de rechtshandhavingsinstanties en een gebrek aan bewustzijn op het gebied van cyberbeveiliging - ook met betrekking tot de rol die bedrijven kunnen spelen bij het voorkomen en melden van cybercriminaliteit. Bulgaarse bedrijven zijn vaak niet voorbereid op cyberaanvallen door een gebrek aan expertise op het gebied van cyberbeveiliging, investeringen in IT, opleiding van werknemers en cyberbeschermingsmaatregelen. Angst voor reputatieschade, vooral bij grote bedrijven, is een andere belangrijke factor.[10]

Nederland

Het Centraal Bureau voor de Statistiek (CBS) geeft aan dat het aantal cybercrime-incidenten in het land in de periode 2016-2020 is afgenomen. In 2016 kreeg bijna 40% van de Nederlandse bedrijven te maken met een of ander cyberbeveiligingsincident; in 2019 was dat minder dan 20% voor grote bedrijven.[11] Daarnaast waren er 1.610 incidenten in verband met DDoS-aanvallen in 2020, een stijging van 75% ten opzichte van 2019.

Volgens de recente studie van de Europese Commissie gaven de ondervraagde Nederlandse mkb-bedrijven aan dat zij - in de afgelopen 12 maanden – het meeste te maken hebben gehad met phishing, account overname of impersonatie-aanvallen (21% van de mkb-bedrijven), gevolgd door virussen, spyware of malware (exclusief ransomware) (17%), en ongeautoriseerde toegang tot bestanden of netwerken (6%).

[8] Eurostat. (n.d.). Structural business statistics overview.

[9] European Commission. (2022). *Op. cit.*

[10] Interviews met deskundigen van rechtshandhaving, CERT-centrum, cyberbeveiligingsverenigingen en de academische wereld.

[11] CBS. (2021). Cybersecuritymonitor 2020. Central Bureau of Statistics.

Het ernstigste incident vond plaats via oplichting en fraude (34%) en kwaadaardige software (21%).[12] Deze bevindingen komen overeen met eerdere studies, waarin malware, e-fraude, phishing en hacking de meest voorkomende vormen van cybercriminaliteit tegen het mkb in Nederland zijn.[13]

Wat de aangifte van cybercriminaliteit betreft, doet ruwweg 5-10% van de Nederlandse bedrijven die het slachtoffer worden van een externe cyberaanval, daadwerkelijk aangifte.[14] Er zijn verschillende redenen om cybercriminaliteit niet te melden. De meest voorkomende redenen voor onderrapportage houden verband met het feit dat het bedrijf het incident intern afhandelde, het gevoel dat de politie er niets aan kon doen - vandaar het beperkte vertrouwen in de politie en haar cybercompetentie - en het feit dat het cyberincident of de cyberaanval niet zo belangrijk en/of niet de moeite van het melden waard was.[15]

Spanje

In Spanje is informatie over cybercriminaliteit en cyberbeveiligingsaanvallen voornamelijk beschikbaar via statistieken die door het Spaanse nationale instituut voor cyberbeveiliging (INCIBE) aan het ministerie van Binnenlandse Zaken worden gerapporteerd. Uit de meest recente cijfers over particuliere ondernemingen blijkt dat INCIBE-CERT in 2021 in totaal 109.126 cyberbeveiligingsincidenten in Spanje heeft gehad. De twee meest voorkomende vormen van cybercriminaliteit waren malware (29,88%) en fraude (28,60%), gevolgd door aanvallen op kwetsbare systemen (18,9%) en inbraak (6,5%).[16] Wat de onderrapportage van cybercriminaliteit in Spanje betreft, zijn onlangs twee belangrijke redenen genoemd: het feit dat het mkb het incident intern afhandelden (57% van de respondenten), en door het feit dat het incident als te triviaal werd beschouwd en/of niet de moeite van het melden waard was (33%).[17]

Wat is de volgende stap?

Cyberbeveiligingsbewustzijn is een van de belangrijkste aspecten die **particuliere entiteiten** (en individuen) moeten verwerven, met de actieve steun van overheidsinstanties, waaronder rechtshandhavingsinstanties. Dergelijke ontwikkelingen zijn niet alleen nodig om de **digitale geletterdheid** te vergroten, maar ook om de kennis van bedrijven over de relevante en bevoegde autoriteiten in geval van cyberincidenten te vergroten. Effectieve melding van cybercriminaliteit en operationele samenwerking strategieen dienen:

- **Gemeenschappelijke factoren voor het niet doen van aangifte aan te pakken**, zoals het gebrek aan vertrouwen in de politie, de complexiteit van de aangiftemechanismen en de bedrijfscontinuïteit, die vaak een hogere prioriteit krijgt dan het bewaren van crimineel bewijs.
- **Zich te wenden tot bestaande initiatieven om synergieën tot stand te brengen en best-practices verder toe te passen**. Tot de huidige initiatieven en samenwerkingsvormen behoort het No More Ransom Portal, dat in 2016 door Europol en andere partners is gelanceerd om slachtoffers te ondersteunen bij het ontsleutelen van hun apparaten of elektronische bestanden. Een dergelijk platform en beschikbare ontsleutelingsinstrumenten zijn bedoeld om **potentiële zakelijke relaties tussen getroffen bedrijven en de aanvallers te verstoren**, d.w.z. cybercriminelen die slachtoffers kortingen aanbieden voor het gebruik van specifieke ontsleutelingsdiensten.
- Het doen van **melding van cybercriminaliteit als fundamenteel onderdeel van de bestrijding van strafbare feiten in cyberspace te bevorden**, om licht te werpen op de werkelijke omvang van cybercriminaliteit en uiteindelijk de (economische) gevolgen ervan voor particuliere entiteiten te beperken.

[12] European Commission. (2022). *Op. cit.*

[13] Veenstra et al. (2015). Cybercrime among companies. Lectoraat Cybersafety: Leeuwarden

[14] CBS. (2021). Op. cit.; see also Veenstra et al. (2015). *Op. cit.*

[15] European Commission. (2022). *Op. cit.*; van de Weijer, S. et al (2021). Cybercrime Reporting Behaviors Among Small- and Medium-Sized Enterprises in the Netherlands. In M. Weulen Kranenbarg & R. Leukfeldt (Eds.), *Cybercrime in Context: The human factor in victimization, offending, and policing (pp. 303–325). Springer.*

[16] López Gutiérrez et al. (2022). Informe sobre la cibercriminalidad en España 2021. Ministry of Interior: Government of Spain.

[17] European Commission. (2022). *Op. cit.*

De invoering van één gecentraliseerd meldproces zou ook de rapportage over cybercriminaliteit ten goede komen. De eerste stap naar de invoering van één meldmechanisme zou de harmonisatie kunnen zijn van bestaande meldmechanismen en gevestigde publiek-private partnerschappen (PPP's) om het delen van informatie te vergemakkelijken. Bovendien zou een dergelijk mechanisme baat hebben bij via PPP's ontwikkelde vertrouwenwekkende processen, veilige en gecentraliseerde communicatiekanalen en gestandaardiseerde protocollen en gegevensformaten. Vertrouwen tussen bedrijven en rechtshandhavingsinstanties is van cruciaal belang voor het bevorderen van bestaande en nieuwe partnerschappen en betrouwbare mechanismen voor informatie-uitwisseling (met inbegrip van beveiligde platforms) die uiteindelijk de wederzijdse samenwerking tussen verschillende actoren in de strijd tegen cybercriminaliteit kunnen verbeteren.