Implementeringen av NIS-direktivet

En sammanställning av direktivets implementering i Estland, Nederländerna, Storbritannien och Tyskland

SOFIA OLSSON, MARGARITA JAITNER

FOI-R--4741--SE
ISSN 1650-1942 Januari 2019

Sofia Olsson, Margarita Jaitner

Implementeringen av NIS-direktivet

En sammanställning av direktivets implementering i Estland, Nederländerna, Storbritannien och Tyskland

Titel	Implementering av NIS direktivet
Title	Implementation of the NIS directive
Rapportnrr	FOI-R--4741--SE
Månad	Januari
Utgivningsår	2019
Sidor	56 p
Kund	MSB
Forskningsområde	5. Krisberedskap och samhällssäkerhet
FoT-område	Ej FoT
Projektnr	E13659
Godkänd av	Lars Höstbeck
Ansvarig avdelning	Försvarsanalys
Exportkontroll	Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen.

Sammanfattning

I juli 2016 antog Europaparlamentet det så kallade NIS-direktivet för att uppnå en gemensam hög nivå av säkerhet i nätverks- och informationssystem inom unionen. Direktivet, som omfattar leverantörer av samhällsviktiga tjänster inom sju sektorer och digitala tjänster, trädde i kraft maj 2018. Bland annat föreskriver rättsakten att EU-medlemsstaterna identifierar relevanta samhällsviktiga tjänster, inrättar processer för att hantera direktivets krav samt förankrar direktivet i den nationella lagstiftningen.

Följande studie kartlägger implementeringen av NIS-direktivet i fyra av medlemsländerna; Estland, Nederländerna, Storbritannien och Tyskland. Både integrationen av direktivets krav i medlemsländernas nationella lagstiftning samt processer för exempelvis incidentrapportering belyses.

Till grund för studien ligger de utvalda EU-medlemsländernas offentligt tillgängliga överväganden gällande implementering, lagtexter och mötesanteckningar från NIS-samarbetsgruppens sammankomster vilka behandlar diverse aspekter av implementeringen av direktivet.

Nyckelord: NIS-direktivet, cybersäkerhet, EU, samhällsviktiga tjänster, kritisk infrastruktur, incidentrapportering

Summary

In July 2016, the European Parliament adopted the so-called NIS Directive in order to achieve a common high level of security in networks and information systems within the Union. The Directive covers providers of essential services in seven predefined sectors as well as digital services. The Directive, which came into force in May 2018, required inter alia that the Member States identify relevant essential services, establish processes to address the requirements of the Directive as well as adjust legislation where necessary.

This study considers various aspects of the implementation of the Directive in four Member States: Estonia, the Netherlands, Great Britain and Germany. Both the integration of the Directive's requirements in the member states' national legislation and establishment of processes for e.g. incident reporting lie within the focus of this study.

The study is based upon publicly available considerations regarding implementation held within the selected member states, legislative documents as well as documentation gathered at the NIS-Cooperation meetings, where a variety of aspects of the implementation of the Directive has been discussed.

Keywords: NIS-directive, cybersecurity, the EU, critical infrastructure protection, incident reporting

Innehållsförteckning

Förkortningar

CCD COE	Cooperative Cyber Defence Center of Excellence
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CDN	Content Delivery Networks
DNS	Domännamnsystem
DSP	Digital Service Provider – leverantör av digitala tjänster
ENISA	Europeiska unionens byrå för nät- och informationssäkerhet
EU	Europeiska unionen
IKT	Informations- och kommunikationsteknologi
ISP	Internet Service Provider
IXP	Internet Exchange Point
OES	Operator of Essential Service – leverantör av samhällsviktiga tjänster
SPOC	Single Point of Contact

Estland

CSA	Cyber Security Act
EEA	Estonian Emergency Act
RIA	Riigi Infosüsteemi Amet (Information Systems Authority)

Nederländerna

Bbni	Beslult beveiliging netwerk – en informatiesystemen (Dekretet för skydd av nätverk och informationssystem)
COVA	Centraal Orgaan Voorraadvorming Aardolieproducten (centrala bränslelagringen)
CSBN	Cybersecuritybeeld Nederland (lägesbild om Nederländernas cybersäkerhetsarbete)
Csw	Cybersecurity Wet (Cybersäkerhetslagen)
EZK	Ministerie van Economische Zaken en Klimaat (Ekonomi och klimatministeriet)
FKI	Finansiella kärninfrastruktur
ILT	Inspectie Leefomgeving en Transport (Inspektionen för miljö och transport)
NCSC	National Cyber Security Centrum
NCSOC	Cybersecurity Operations Center
NCTV	Nationaal Coördinator Terrorismebestrijding en Veiligheid (Nationell koordinator för kontraterrorism och säkerhet)

Wbni	Wet beveiliging netwerk- en informatiesystemen (Lagen för skydd av nätverk och informationssystem)
Wgmc	Wet Gegevensverwerking en Meldplicht Cybersecurity (Lagen för databehandling och Cybersäkerhetsrapportering)

Storbritannien

BEIS	Department for Business, Energy & Industrial Strategy
CAA	Civilian Aviation Authority
CCA	Centre for Cyber Assessment
CESG	Communications-Electronics Security Group
CPNI	Centre for the Protection of National Infrastructure
DEFRA	Department for Environment, Food and Rural Affairs
DfT	Department for Transportation
DHSC	Department of Health and Social Care
GCHQ	Government Communications Headquarter
ICO	Information Commissioner´s Office
NCSC	National Cyber Security Centre
Ofcom	Office of communications
Ofgem	Office of Gas and Electricity Markets

Tyskland

AIC	Agentur für Innovationen in der Cybersicherheit (Agentur för innovation inom cybersäkerhet)
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Myndigheten för befolkningsskydd och katastrofhjälp)
BKA	Bundeskriminalamt (Federala förbundspolisen)
BMI	Bundesministerium des Innern, für Bau und Heimat (Ministeriet för inrikes affärer)
BND	Bundesnachrichtendienst (Federala underrättelsetjänsten)
BSI	Bundesamt für Sicherheit in der Informationstechnik (Myndigheten för säkerhet inom informationsteknik)
MIRT	Mobile Incident Response Teams
NCS	Nationaler Cyber-Sicherheitsrat (Nationella cybersäkerhetsrådet)
ZITiS	Zentrale Stelle für Informationstechnik im Sicherheitsbereich (Centrala kontoret för informationsteknik inom säkerhetsområdet)

1 Inledning

I juli 2016 antog Europaparlamentet det så kallade NIS-direktivet[1] med åtgärder för att uppnå en hög gemensam nivå på säkerhet i nätverks- och informationssystem inom den Europeiska unionen (EU). NIS-direktivet trädde i kraft i maj 2018.

Direktivet ställer nya krav på säkerhet i nätverks- och informationssystem som används av leverantörer av samhällsviktiga tjänster och leverantörer av digitala tjänster: bland annat säkerhetsåtgärder, incidentrapportering och tillsyn kopplat till detta. Detta avser dock enbart de system som har betydelse för tillhandahållandet av respektive tjänst. Samhällsviktiga tjänster omfattar tjänster inom energisektorn, transportsektorn, bankverksamhet, finansmarknadens infrastruktur, hälso- och sjukvårdssektorn samt leverans och distribution av dricksvatten.

NIS-direktivet harmoniserar nivån av informations- och nätverkssäkerhet bland medlemsländerna som var och en har sina individuella förutsättningar vad gäller informationssamhällets mognadsgrad, men även andra aspekter som rättsliga förutsättningar. De specifika tjänster som ingår i ett medlemslands samhällsviktiga tjänster skiljer sig beroende på landets individuella förutsättningar så som exempelvis geografi eller ekonomi. Detta kan förklaras av att det är medlemsländernas ansvar att identifiera tjänsterna. I sin tur leder detta till att det krävs olika tillvägagångssätt för att integrera de genom NIS-direktivet tillkomna kraven juridiskt, men även processer för incidentrapportering och andra förvaltningsstrukturer.

1.1 Syfte och mål

Syftet med denna studie är att skapa en generell överblick över konkreta tillvägagångsätt för att implementera NIS-direktivet i fyra av EU:s medlemsländer: Estland, Nederländerna, Storbritannien och Tyskland. Studien presenterar en översiktlig jämförelse av implementeringen av NIS-direktivet i de fyra ovan nämnda EU-medlemsstaterna.

Själva implementeringen av direktivet belyses utifrån flera aspekter. Direktivet har krävt förändringar i nationell lagstiftning. Implementeringen har också fodrat etablering (eller bekräftelse) av tillsynsmyndigheter samt etablering av kontrollprocesser för att garantera direktivets efterlevnad, såväl som konkreta processer för en effektiv incidentrapportering av störningar i nätverks- och informationssystem hos samhällsviktiga och/eller digitala tjänster.

1.2 Avgränsningar och metod

Studien avgränsas till de fyra namngivna EU-medlemsländerna: Estland, Nederländerna, Storbritannien och Tyskland. Urvalet av de specifika länderna har skett i samråd med uppdragsgivaren för denna rapport. Det kan noteras att samtliga länder har kommit långt i sin implementering.

Det empiriska underlaget som ligger till grund för studien består i huvudsak av:

- Mötesrapporteringen från den svenska representationen vid NIS-samarbetsgruppen på EU-nivå. Bland annat har dessa gett underlag för statusrapportering och för hur medlemsländerna har resonerat kring svårigheter och utmaningar i förhållande till implementeringen av direktivet.
- Ländernas egen rapportering om implementeringsåtgärder via officiella webbresurser på engelska, nederländska och tyska. Materialet sammanställer

[1] Europaparlamentets och rådets direktiv (EU) 2016/1148 av den 6 juli 2016 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem i hela unionen.

överväganden om rättslig implementering, offentliga konsultationer, information till berörda operatörer av samhällsviktig infrastruktur och dylikt. En språklig avgränsning har gjorts vid material på andra språk än engelska, nederländska eller tyska, vilket särskilt gäller studien av Estland.

- I fallet Estland har den tillgängliga dokumentationen på engelska alternativt tyska bedömts som otillräcklig i sin omfattning och har därför kompletterats med en intervju med biträdande generaldirektören för RIA, Estlands myndighet för informationssystem som även ansvarar för implementeringen av NIS-direktivet i Estland. Samtidigt som intervjupersonen bedöms vara mycket sakkunnig bör informationen som förmedlas i ett samtal bedömas som expertkunskap snarare än medlemsstatens officiella ståndpunkt.

Eftersom syftet med studien är att följa implementeringen av NIS-direktivet, faller andra aktiviteter som syftar till förbättring av nivån av informations-säkerheten i de olika medlemsländerna utanför studien och nämns därför enbart i de sammanhang det är oundvikligt. Även deskriptiva beskrivningar av medlemsländernas utgångsläge innan NIS-direktivet ligger utanför studiens gränser och ges därför enbart då det krävs för att kunna förstå de implementeringsrelaterade åtgärderna.

1.3 Disposition

Inledningsvis ges en kortfattad bakgrund till NIS-direktivet och dess syfte samt vilka uppgifter NIS-direktivet ålägger centrala aktörer inom medlemsstaterna. Därefter beskrivs respektive lands implementering av direktivet utifrån följande struktur; inledningsvis ges en överblick av förändringar i nationell lagstiftning som implementeringen förorsakat. Därefter sammanfattas och belyses centrala aktörer. Avslutningsvis ges en sammanställning av processer som har, eller har planerats att, etableras i respektive land för att kunna efterleva direktivets krav. Studien avslutas med en diskussion av resultatet samt en jämförelse länderna emellan.

2 NIS-direktivet

Direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverks- och informationssystem, vanligen kallat NIS-direktivet[2], är en bindande rättsakt[3] antagen av EU 2016 och som implementeras sedan 2018. Direktivet syftar till att åstadkomma en harmoniserad och hög lägsta nivå av nätverks- och informationssäkerhet över olika sektorer inom samhällsviktig verksamhet i hela EU. Direktivet tillgodoser ett behov av att stärka tillförligheten och säkerheten i nätverks- och informationssystem i en tid när dessa spelar en allt viktigare roll för ekonomisk- och samhällelig verksamhet, likväl som för den europeiska inre marknadens funktion. Då nätverks- och informationssystem är av en sådan karaktär att en incident i ett medlemsland kan ha en kaskad- och/eller dominoeffekt, tjänar det EU att ha ett harmoniserat system för incidenthantering och främja en gemensam riskhanteringskultur.[4]

För Sveriges del innebär direktivet exempelvis att en lag om informationssäkerhet för samhällsviktiga och digitala tjänster antagits.[5] Direktivet är dessutom en del av ett bredare europeiskt policyinitiativ för att stärka nätverks-, informations-, och cybersäkerheten samt integritet och konsumenters tillit till digitala tjänster. Ett exempel är Den allmänna dataskyddsförordningen 2016/679 (GDPR), vilket ska tillämpas av samhällsviktiga aktörer vid implementeringen av NIS-direktivet[6], och den i december 2018 antagna COM(2017) 477 (”Cyber Security Act”) om ett gemensam europeisk standardiserings, ackrediterings, och certifieringssystem för cybersäkerhet i informations- och kommunikationsteknologi (IKT). Förslaget kompletterar NIS-direktivet med att utveckla just den branschpraxis som direktivet främjar, det vill säga standardisering av IKT och även teknologi som kommer tillämpas inom samhällsviktiga sektorer.

Varje medlemsland måste i enlighet med NIS-direktivet utse en *nationell kontaktpunkt (single point of contact, SPOC)*, ett *CSIRT (computer security incident response team)* samt nationella *tillsynsmyndigheter*.

Den nationella kontaktpunkten ska agera som plattform för internationellt samarbete och delta i exempelvis NIS-samarbetsgruppen inom vilken god praxis och verktyg för en smidig implementering diskuteras.

Varje medlemsstat ska utse en eller flera säkerhetsincidenthanteringsorgan, s.k. *CSIRT*. Dessa ska vara ständigt tillgängliga och ta emot incidentrapporter från samhällsviktiga- och digitala tjänster. Vid behov ska CSIRT-enheten skicka vidare incidentrapporter till berörda tillsynsmyndigheter.

Utöver incidentrapporthantering ska CSIRT-enheter tillhandahålla varningar om risker och incidenter (samt analys av desamma), vara en samverkande aktör med privat sektor och delta i det inomeuropeiska CSIRT-nätverket. De är således vitala för det gränsöverskridande cybersäkerhetssamarbete som direktivet föreskriver.

Tillsynsmyndigheternas uppdrag är att utöva tillsyns över att NIS-direktivet efterföljs av berörda aktörer och att implementeringen av lagar och föreskrifter sker korrekt. De beslutar även om sanktionsavgifter vid överträdelser.

Det finns två fastslagna för direktivet viktiga tidsangivelser:

---

[2] EU. *Direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverk- och informationssystem.* 2016.

[3] EU Kommissionen. *Typer av EU-rättsakter*. N.D. https://ec.europa.eu/info/law/law-making-process/types-eu-law_sv (hämtad 2018-09-25). Hur direktivet införlivas i var stats nationella lagstiftning är upp till varje medlemsstat.

[4] EU. *Direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverk- och informationssystem.* 2016.

[5] SFS 2018:1174. *Lag om informationssäkerhet för samhällsviktiga och digitala tjänster.* 2018.

[6] EU. *Direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverk- och informationssystem.* 2016.

- I maj 2019 ska EU-kommissionen presentera en rapport om medlemsstaternas följdriktighet i identifierande av samhällsviktiga tjänster, och
- I maj 2021 ska EU-kommissionen utvärdera direktivets funktion med ett särskilt fokus på strategisk och operationellt samarbete.

Tabell 1. Fastslagna tidsangivelser för NIS-direktivet

DATUM	UPPGIFT
9 maj 2018	Sista dag för införlivning av NIS-direktivet i nationell lag
9 november 2018	Sista dag för överlämnade av förteckning över samhällsviktiga tjänster till EU-kommissionen. Information om antal leverantörer inom varje sektor samt uppgift om deras betydelse för sektorn ska lämnas in till kommissionen.
Maj 2019	Kommissionen presenterar rapport om medlemsstaternas följdriktighet i identifierandet av samhällsviktiga tjänster
Maj 2021	Kommissionen presenterar sin utvärdering av direktivets funktion med särskilt fokus på strategiskt och operationellt samarbete

3 Estland

Estland har länge varit ett föregångsland i cybersäkerhetsfrågor och profilerar sig aktivt som en ”e-nation”. Detta innebär exempelvis en långt framskriden digitalisering inom offentlig förvaltning, att medborgare har eID-kort och kan rösta online samt ett e-medborgarskapsprogram (*e-residency*). E-medborgarskapsprogrammet ger fysiska och juridiska personer utanför Estland tillgång till estniska tjänster så som bankväsendet eller företagsregistreringen och riktar sig främst till företagare verksamma i områden som inte är beroende av fysiskt närvaro.[7]

Profileringen som ”e-nation” har varit framgångsrik i den mån att ett flertal internationella cybersäkerhetscenter och tankesmedjor har etablerat sitt säte i landet, varav Nato:s Cooperative Cyber Defence Center of Excellence (NATO CCD COE) är ett av de mest kända. Även på estniska högskolor och universitet drivs en rad framgångsrika program inom digitaliserings- och cybersäkerhetsområdet.

Som ett av de första länderna i världen antog landet 2008 en nationell cybersäkerhetsstrategi. Den nuvarande cybersäkerhetsstrategin sträckte sig ursprungligen till 2017 men har förlängts med ett år.[8] Den fokuserar exempelvis på identifiering och hantering av risker, säkerställandet av samhällsviktiga tjänster och ökad effektivitet i bekämpandet av cyberbrott. Likaså genomför *Riigi Infosüsteemi Amet* (RIA), den statliga myndigheten för informationssystem, årligen en utvärdering av Estlands cybersäkerhet.[9]

3.1 Lagstiftning

Estland har länge förespråkat att en lagstiftning på EU-nivå skulle harmonisera nivån av cybersäkerhet bland medlemsländerna.[10] Till grund för Estlands strävan efter harmoniseringen av cybersäkerhetsarbetet inom EU ligger också förståelsen för de ömsesidiga beroenden av fungerande kommunikationer länderna emellan som gränsöverskridande verksamheter kan innebära. Även en förståelse för samhällsviktiga tjänsters beroende av strömförsörjning och kommunikationstjänster har bidragit till Estlands engagemang, både nationellt och på EU-nivå. Bland annat konstaterade en utredning genomförd av RIA att en störning av strömförsörjningen eller inom kommunikationstjänstesektorn skulle potentiellt ha stor inverkan på det estniska samhället så väl som på statliga funktioner.[11]

Uku Säreanno, vice generaldirektör för RIA, poängterar att NIS-direktivet inte kom som någon överraskning för Estland utan att direktivet innebär ett naturligt nästa steg för nätverks- och informationssäkerheten.[12] Inte desto mindre ledde implementeringen till en ny lagstiftning. Cybersäkerhetslagen *Küberturvalisuse seadus* (Cyber Security Act, CSA) antogs i det estniska parlamentet *Riigikogu* i maj 2018.[13] Lagen samlar en tidigare fragmenterad lagstiftning om hur cybersäkerheten ska hanteras på statlig nivå och är ett tydligare ramverk.[14] Före CSA var det bara två sektorer som enligt lag var skyldiga att rapportera in incidenter; kommunikationsföretag och s.k. betrodda serviceleverantörer av e-identifikation och e-transaktioner.[15] Gällande den digitala infrastrukturen har Estland

[7] E-Estonia. *How Estonia became a global heavyweight in cyber security*. 2017. (hämtad 2018-11-14)
[8] Ministry of Economic Affairs and Communication. *Cyber Security Strategy 2014-2017.* 2014. https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf (hämtad 2018-11-14).
[9] RIA. *Annual Cyber Security Assessment 2018 Estonian Information System Authority.* 2018.
[10] Särekanno, U. *Telefonintervju. 2018-11-26.*
[11] RIA. *Annual Cyber Security Assessment 2018 Estonian Information System Authority.* 2018.
[12] Särekanno, U. *Telefonintervju. 2018-11-26.*
[13] Riigikogu. *Cyber Security Act.* 2018. https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/K%C3%BCberturvalisuse%20seadus (hämtad 2018-10-30)
[14] RIA. *Annual Cyber Security Assessment 2018 Estonian Information System Authority.* 2018.
[15] Riigikogu. *Electronic Communications Act.* 2016

tidigare saknat lagstiftning kring ISP:s, DNS och toppdomäner, vilken således har behövt kompletteras. CSA tillgodoser dock främst ett nationellt behov av en slimmad och tydligare lagstiftning, då Estland redan till en stor del har implementerat praxis, strukturer och processer som NIS-direktivet föreskriver. [16]

CSA följer delvis Estlands beredskapslagstiftning, *Hädaolukorra seadus* (Estonia Emergency Act, EEA) från 2009, till exempel gällande definitionen av en samhällsviktig tjänst.[17] Definitionen har en holistisk syn på verksamheten bakom en samhällsviktig tjänst, vilket innebär att också byggnader och personal tillhör definitionen. EEA listar även ett antal sektorer som omfattar den samhällsviktiga verksamheten. Enligt inrikesministeriet finns det 45 samhällsviktiga tjänster och 167 leverantörer av dessa: 131 statliga och privata företag, 19 stiftelse, 16 statliga myndigheter och en kommunal institution (2017).[18]

Redan i EEA står skrivet att utsedd aktör, i detta fall inrikesministern, vartannat år ska genomföra översyn av samhällsviktiga tjänster för att garantera deras kontinuitet och säkerhet. EEA föreskriver också att en leverantör av en samhällsviktig tjänst bland annat är skyldig att utföra riskuppskattning av driftkontinuitet och ha en plan för fortsatt drift. Dessutom etablerade EEA krav på inrapportering av incidenter och att tillsynsrättigheter ges till utsedda myndigheter.[19] CSA bygger också på delvis på *Elektroonilise side seadus,* lagen om elektronisk kommunikation.[20]

CSA går längre än NIS-direktivets föreskrifter, dels då Estlands utgångspunkt har varit att många av kraven redan tillgodoses inom tidigare lagstiftning vilket har gett tillfälle att förstärka den nationella lagstiftningen. Exempelvis medräknades möjligheten för RIA att stänga ner vissa tjänster vid incidenter alternativt om de inte uppfyller tillsynsmyndigheternas föreskrifter. Det förhållandevis omfattande mandatet motiveras genom att lagstiftningen handlar om att säkerställa hela det estniska cyberekosystemets kontinuitet[21] men ska enbart komma till användning då detta bedöms vara enda handlingsalternativet.[22] RIA får dessutom begära ut anonymiserad information om nätverkstrafiken för att kunna identifiera ursprunget till en attack.[23]

Estland går även längre i sin definition av samhällsviktiga tjänster samt tröskeln för att anses vara OES[24], utöver det som föreskrivs i NIS-direktivet. Därför definieras public service som en samhällsviktig tjänst. För närvarande pågår överväganden för att säkerställa hur public service ska möta kraven fastlagda i CSA. Enbart det tekniska perspektivet tillgodoses, aspekter som avser kognitiv information faller alltså utanför ramen för arbetet med NIS-direktivet.[25]Även ekosystemet kring valen pekas ut som en sektor där OES verkar. Utöver detta ingår även småskaliga läkarmottagningarna i OES.[26] Den fullständiga listan över Estlands samhällsviktiga tjänster uppdateras vartannat år.[27]

[16] Särekanno, U. *Telefonintervju. 2018-11-26.*
[17] En samhällsviktig tjänst är en service som har en överväldigande effekt på samhällets funktion och att ett avbrott i en sådan är ett direkt hot mot medborgarna eller mot andra operatörer och leverantörer av andra samhällsviktiga tjänster eller tjänster av generellt intresse.
[18] Siseministerium. [Inrikesministeriet Estland]. *Crisis management.* 2017. https://www.siseministeerium.ee/en/activities/crisis-management (hämtad 2018-11-12)
[19] Vabariigi Valitsus [Republiken Estland] *Emergency Act.* 2009.
[20] Ras, K. *Estonia as a leader in increasing cybersecurity.* 2018. https://www.pism.pl/publications/bulletin/no-68-1139 (hämtad 2018-11-21)
[21] Särekanno, U. *Telefonintervju 2018-11-26.*
[22] RIA. *Annual Cyber Security Assessment 2018 Estonian Information System Authority.* 2018.
[23] Ibid.
[24] Samhällsviktiga tjänster förkortas ibland *OES* och digitala tjänster *DSP*. OES står för Operators of Essential Service, DSP för Digital Service Providers.
[25] Säreanno, U. *Telefonintervju 2018-11-26*
[26] Ibid.
[27] Riigikogu. *Cyber Security Act.* 2018. https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/K%C3%BCberturvalisuse%20seadus (hämtad 2018-10-30).

CSA föreskriver att incidentrapportering måste ske till RIA inom 24 timmar, förutsatt att händelsen har en betydande påverkan. För digitala tjänster gäller anmälningsplikten så fort incidenten upptäckts. Även möjlighet till frivillig rapportering föreskrivs i lagen, motiverat med att det ger RIA en möjlighet att tidigt upptäcka nya och potentiella hot och risker.[28] Lagstiftningen konsoliderar kraven på samhällsviktiga tjänsteleverantörer genom att tillgodose behovet av säkerhet i nätverks- och informationssystem. Likt redan existerande regleringar, måste tjänsteleverantörer uppskatta säkerheten i sina system, sårbarheter i kontinuiteten av tjänsten och risker för slutanvändaren. Tjänster och systemen som hanterar eller bearbetar säkerhetsklassificerad information undantas specifikt från lagens krav.[29]

3.2 Aktörer

RIA är den myndighet som ansvarar för och skyddar Estlands digitala sfär. Den har till uppgift att utveckla och administrera Estlands informationssystem och koordinera den nationella cybersäkerheten, vilket innefattar cyberincidentrespons, regleringar och översyn såväl som krisberedskap och krishantering. RIA är ansvarig för Estlands plattform för e-förvaltning, den nationella eID-infrastrukturen samt ett verktyg som agerar gränssnitt mellan Estlands administrativa databaser, X-road. RIA levererar även datakommunikation och internettjänster till statliga myndigheter och lokala styren.[30] RIA innehar dessutom både CERT- och CSIRT-uppgifter[31] vilket ger myndigheten god kännedom om systemen. Estland ser sig som mycket effektiv i sin incidenthantering och lyfter gärna fram sin CSIRT-enhet som ledande i EU.[32] Myndigheten verkar under Ministeriet för ekonomiska angelägenheter och kommunikation och har närmare 150 medarbetare.[33]

Estland har valt att även centralisera koordinationen och tillsynen inom ramen för NIS-direktivets implementering. RIA är den enda tillsynsmyndigheten för OES och DSP samt koordinerar och deltar i internationella utbyten, agerar SPOC och, som ovan nämnt, CSIRT/CERT-EE.[34] Lagen ger RIA ökade befogenheter och slår fast vilket mandat RIA har, något som uppfattas som positivt då RIA tidigare har haft en mer informell auktoritet, [35] och i och med ikraftträdandet av CSA har många av de redan existerande processer och strukturer som funnits inom och i relation till RIA lagstadgats. RIA i egenskap av tillsynsmyndighet ansvarar för utdömande av eventuella sanktionsavgifter. Dessa kan uppgå till 20 000 EUR.

[28] RIA. *Annual Cyber Security Assessment 2018.* 2018.
[29] Riigikogu. *Cyber Security Act.* 2018. https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/K%C3%BCberturvalisuse%20seadus (hämtad 2018-10-30).
[30] Ministry of Economic Affairs and Communication. *Cyber Security Strategy 2014-2017.* 2014. https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf (hämtad 2018-11-14).
[31] RIA. *CERT-EE.* 2018. https://www.ria.ee/en/cyber-security/cert-ee.html (hämtad 2018-11-30)
[32] Särekanno, U. *Telefonintervju 2018-11-26.*
[33] Ibid.
[34] RIA. *Annual Cyber Security Assessment 2018 Estonian Information System Authority.* 2018.
[35] Riigikogu. *Electronic Communications Act.* 2016.

Tabell 2. Sammanställning över sektorer samt tillsynsmyndigheterna

SEKTOR	TILLSYNSMYNDIGHET
Energi	RIA
Transport	
Bankverksamhet och finansmarknadens infrastruktur	
Hälso- och sjukvård	
Leverans och distribution av dricksvatten	
Digital infrastruktur	
Digitala tjänster	

3.3 Processer

För Estland har inte NIS-direktivet och dess föreskrifter kommit som någon större överraskning, många av de processer och åtgärder som andra länder har behövt skapa har i Estland redan existerat och främst behövt justeras för att tillgodose de exakta kraven i direktivet. En aspekt som kan lyftas fram som särskilt viktig för Estland är inkluderandet av samhällsviktiga tjänster relaterade till det jämförbart stora antalet e-tjänster som tillhandahålls både av privata aktörer men även inom förvaltningen, vilket innefattar e-röstningssystemet.

RIA rapporterar årligen om cybersäkerhetsläget i Estland, vilket utgör en pelare i kontinuiteten av satsningarna och som på så vis möjliggör uppföljning av åtgärder och snabb reaktion på uppkomna behov. Den senaste rapporten, daterat 2018, konstaterar att sjukvårds- och hälsosektorn är i behov av särskilt stöd.[36] Rapporten vittnar dessutom om överväganden kring hur NIS-direktivets föreskrifter ska implementeras i energisektorn. Energisektorn tillsammans med hälsosektorn och finanssektorn bedöms av Estland som de mest riskutsatta sektorerna.[37] Dessa konstateranden ger en intressant utgångspunkt för att följa upp Estlands egen utvärdering av NIS-direktivets implementering.

CSA har fastlagt att RIA ska tillhandahålla ett register för cyberincidenter för att kunna kartlägga och analysera dem med syftet att ytterligare stärka preventiva åtgärder. Tillgång till registret ska vara begränsat och data ska enbart vara för internt bruk.[38]

RIA har under en längre tid haft i uppdrag att utöva tillsyn över samhällsviktiga tjänster, hantering av cyberincidenter samt att koordinera den nationella cybersäkerheten. Man har således haft goda förutsättningar att på ett effektivt och förtjänstfullt vis implementera NIS-direktivets krav. Verksamheten som faller inom ramen för NIS-direktivets implementering tillfaller olika enheter inom RIA. Förutom operationscentrumet, som även inrymmer CERT-EE, finns det en enhet för standardisering och översyn som har till uppgift att se till att CSA och i förlängningen NIS-direktivet efterföljs. I skrivande stund jobbar RIA på att ta fram formen för incidentrapportering. Trots att Estland har haft sina nationella standarder för informationssäkerhet och inrapportering av incidenter, gjordes bedömningen att det är nödvändigt att ta tillfället i akt för att vidareutveckla dessa.[39] Krishanteringscentret utarbetar diverse övningar, ger stöd till samhällsviktiga tjänster och har övergripande krishanteringsansvar. Policyenheten jobbar med NIS-samarbetsgruppen,

[36] RIA. *Annual Cyber Security Assessment 2018 Estonian Information System Authority.* 2018.
[37] Ibid.
[38] Riigikogu. *Cyber Security Act.* 2018. https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/K%C3%BCberturvalisuse%20seadus (hämtad 2018-10-30).
[39] Särekanno, U. *Telefonintervju 2018-11-26.*

NIS-arbetsgrupper, inom internationella projekt och med preventiva program såsom kurser för äldre och för företag som syftar till att stärka cyberhygienen i samhället. RIA har dessutom, enligt egen uppgift, ett starkt samarbete med den privata sektorn.[40]

För Estland har de främsta utmaning i relation till NIS-direktivet varit gränsöverskridande beroenden (*cross-border dependencies*) och företrädare för RIA har uttryckt ett behov av en större förståelse för och ett förbättrat samarbete kring hantering av de tjänster som NIS-direktivet reglerar och som bedrivs över nationsgränser. Estland har hittills försökt att främja arbetet med utveckling av normer för gränsöverskridande verksamhet inom ramen för NIS-samarbetsgruppen och avser att fortsätta driva denna fråga.[41] CSA föreskriver också samhällsviktiga tjänster att alla cyberincidenter som stör en tjänst som har gränsöverskridande verksamhet alltid ska räknas som betydande.[42] Detta kan ses som ytterligare stöd och ett uppmuntrande till de andra EU-medlemsländerna.

[40] Ibid.
[41] Ibid.
[42] Riigikogu. *Cyber Security Act.* 2018. https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/K%C3%BCberturvalisuse%20seadus (hämtad 2018-10-30).

4 Nederländerna

Nederländerna ser sig som ett föregångsland inom digitalisering och cybersäkerhet.[43] Cyberattacker inriktade på kritisk infrastruktur anses vara ett reellt hot mot den nationella säkerheten, varför Nederländerna förordar stärkt cybersäkerhet inom privat såväl som offentlig sektor, nationellt och internationellt.[44]

Landet har sedan länge ett väl utvecklat och omfattande lagstiftning- och policyramverk. Nederländernas första nationella cybersäkerhetsstrategi antogs 2011 och uppdaterades 2013.[45]

Landet har väl utvecklade cybersäkerhetsstrukturer. Nederländernas nationella cybersäkerhetscenter NCSC presenterar årligen en publikation om landets cybersäkerhetsarbete, Cybersecuritybeeld Nederland (CSBN). I 2018 års publikation slås fast att det finns ett kontinuerligt digitalt hot mot den nationella säkerheten samtidigt som det nederländska samhället och ekonomin blivit allt mer digitalt beroende. Därför kommer konsekvenser av attacker och utfall vara betydande och i vissa fall innebära omfattande störningar. Det konstateras också att inte alla aktörer vidtar tillräckliga åtgärder, vilket exemplifieras med WannaCry-attacken 2017, då det i efterhand noterades att fler än hälften av landets sjukhus drabbades av utpressningsmasken.[46] CSBN 2018 fastställer att incidenter hade kunnat förhindras och konsekvenserna hade varit lindrigare om aktörer hade antagit nödvändiga och grundläggande cybersäkerhetsåtgärder.[47]

Under NCSC ligger även ett nationellt Cybersecurity Operations Center (NCSOC), en hotline för cyberincidenter som är öppen dygnet runt. NCSOC identifierar också nya cyberhot och informations- och kommunikationstekniska sårbarheter samt agerar CERT för den nationella regeringen.[48] Den nederländska regeringen tar emot stöd och råd från det nederländska cybersäkerhetsrådet, Cybersecurity Raad, som skapades 2011 som ett led i den nationella cybersäkerhetsstrategin. Rådet har 18 medlemmar, sju från den privata sektorn, sju från den offentliga samt fyra från akademin.[49]

I april 2018 presenterade Nederländerna en övergripande cybersäkerhetsagenda med sju ambitionsmål för att göra Nederländerna till ett digitalt säkrare land.[50] I maj samma år skapades de Cybersecurity Alliantie, cybersäkerhetsalliansen. Tanken är att den ska vara en allians mellan staten och den privata sektorn. Under de första månaderna har cybersäkerhetsalliansen fokuserat på tre projekt varav projektet för att stärka kunskaps- och informationsutbytet kring bästa cybersäkerhetspraxis sektorerna emellan kan komma att bli det som är mest relevant i förhållande till NIS-direktivet. [51]

[43] Rijkswaterstaat. *Office for European Programmes (Bureau Brussels).* N.d. https://www.rijkswaterstaat.nl/english/about-us/international-cooperation/bureau-brussels.aspx (hämtad 2018-10-31).
[44] Brooijmans, M. *The fight for cybersecurity in the Netherlands.* Holland Fintech. 2018. https://hollandfintech.com/2018/03/fight-cybersecurity-netherlands/ (hämtad 2018-10-31).
[45] Ibid.
[46] Schellevis, J. *Zeker vijftien ziekenhuizen geïnfecteerd met ransomware.* 2017. https://nos.nl/artikel/2179941-zeker-vijftien-ziekenhuizen-geinfecteerd-met-ransomware.html (hämtad 2018-11-26).
[47] Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) *Cybersecuritybeeld Nederland, CSBN 2018.* 2018.
[48] NCTV. *Incident Response. 24-uurshulp.* N.d. https://www.ncsc.nl/incident-response/24-uurshulp.html (hämtad 2018-11-12).
[49] NCTV. *Cyber Security*. N.d https://www.nctv.nl/organisatie/cs/index.aspx (hämtad 2018-11-05); Cyber Security Raad. *Dutch Cyber Security Council.* N.d. https://www.cybersecurityraad.nl/index-english.aspx (hämtad 2018-11-05).
[50] För de sju målen, se: NCTV. *Nederlandse Cybersecurity Agenda.* N.d. https://www.nctv.nl/ncsa/index.aspx (hämtad 2018-11-05).
[51] NCTV. *Nederlandse Cybersecurity Alliantie.* 2018. https://www.nctv.nl/cybersecurityalliantie/index.aspx (hämtad 2018-11-01).

4.1 Lagstiftning

Nederländerna hade tidigt kommit långt i implementeringen av NIS-direktivet och man anser sig vara ett av de drivande länderna bakom skapandet av direktivet.[52] Insikten om att Nederländerna behövde stärka sin cybersäkerhetslagstiftning går delvis att spåra till upptäckten och följderna av DigiNotarintrånget[53] som skedde 2011. Några år senare, i oktober 2017 trädde Wet Gegevensverwerking en Meldplicht Cybersecurity, lagen för databehandling och cybersäkerhetsrapportering, förkortad Wgmc, i laga kraft.[54] Lagen ligger till grund för implementeringen av NIS-direktivet i Nederländerna, men bedömdes inte vara tillräckligt omfattande. Därför föreslogs istället lagen om cybersäkerhet, Cybersecuritywet, eller Csw som sedan, för att undvika onödig förvirring döptes om till Wet beveiliging netwerk- en informatiesystemen, lagen för skydd av nätverk och informationssystem eller Wbni. Den nya lagen som antogs i oktober 2018 inkorporerar den gamla lagstiftningen i sin helhet. Den gamla lagstiftningen upphörde att gälla när den nya trädde i kraft.[55]

Wbni föreskriver OES såväl som DSP att vidta lämpliga och proportionella tekniska och organisatoriska åtgärder för att hantera säkerhetsrisker samt att de ska hålla en hög teknisk standard, dvs. ”proportionell” nivå anpassad till riskerna. Gällande incidentrapportering slår lagen fast att leverantörer utan dröjsmål ska rapportera in incidenter. För DSP gäller liknande regler med inrapporteringsplikt till behörig myndighet och till CSIRT-enheten vid Ministerie van Economische Zaken en Klimaat, EZK.

Konfidentiella uppgifter regleras i artikel 20 i Wbni. Justitie- och säkerhetsministern kan ta beslut om hantering av sekretessbelagda uppgifter vid behov för att kunna utföra de uppgifter som avses i artikel tre i Wbni. Dessa kan då spåras tillbaka till en leverantör utan dess samtycke, men endast i den utsträckning det är användbart för att främja åtgärder som förhindrar eller begränsar samhällsstörningar. Information kan enbart ges till CSIRT:s eller andra krisgrupper som utsetts av ministern samt de underrättelse- och säkerhetstjänster som avses i lagen om underrättelse- och säkerhetstjänst från 2002. CSIRT-enheten för digitala tjänster följer Wbni NIS-direktivets skrivelser om sekretess.

Beträffande förvaltningen kring NIS-direktivets implementering följer Wbni direktivets krav gällande tillsynsmyndigheternas uppgifter att utöva tillsyn samt utdöma sanktionsavgifter i händelse av överträdelse gentemot lagen. Sanktionsavgifter kan utdömas upp till 5 miljoner EUR.[56]

Wbni fastställer dessutom vilka aktörer som ska ha det övergripande ansvaret för respektive sektor och dess tillsynsmyndigheter.

[52] Rijksoverheid NL. *‘Building Digital Bridges’. International Cyber Strategy – Towards an integrated international cyber policy.* 2017.

[53] Diginotar-intrånget var en attack mot den nederländske certifikatutfärdaren DigiNotar som skedde 2011. Vid upptäckten konstaterades det att angriparen hade skapat falska certifikat för ett flertal domäner, bland annat google.com. Intrånget föreföll syfta till att spionera på iranska medborgare.

[54] National Cyber Security Center. *Wet gegevensverwerking treedt 1 oktober 2017 gedeeltelijk in werking.* 2017. https://www.ncsc.nl/actueel/nieuwsberichten/wet-gegevensverwerking-treedt-1-oktober-2017-gedeeltelijk-in-werking.html (hämtad 2018-11-06).

[55] Rijksoverheid NL. *Cybersecurity act submitted to House of Representatives.* 2018. https://www.government.nl/latest/news/2018/02/15/cybersecurity-act-submitted-to-house-of-representatives (hämtad 2018-10-31).

[56] Staatsblad van het koninkrijk der Nederlanden. *Nr 387:2018. Wet van 17 oktober 2018, houdende regels ter implementatie van richtlijn (EU) 201671148 (Wet beveiliging netwerk- en informatiesystemen)*. 2018.

Tabell 3. Sammanställning över aktörer ansvariga för sektorerna med OES

SEKTOR	ANSVARIG AKTÖR
Energi	EZK
Transport	Minister van infrastructuur en waterstaat
Finansmarknadens infrastruktur	De Nederlandsche Bank NV
Bankinfrastruktur	De Nederlandsche Bank NV
Leverans och distribution av dricksvatten	Minister van infrastructuur en waterstaat
Hälsa	Minister van Volksgezongheid, Welzijn en Sport
Digital infrastruktur	EZK

4.2 Aktörer

Nederländernas nationella cybercenter, Nationaal Cyber Security Centrum (NCSC) är en central aktör för nationens cybersäkerhet[57] samt för implementeringen av NIS-direktivet. NCSC är en undergren av den nationella samordnaren för kontraterrorism och säkerhet, Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en myndighet under justitie- och säkerhetsdepartementet. NCSC är även nationell kontaktpunkt för NIS-samarbetet inom EU, SPOC. Även CSIRT-enheten för samhällsviktiga tjänster ligger under NCSC. NCSC tar också emot frivilliga incidentrapporter från aktörer som inte direkt berörs av Wbni.

Nederländska radiokommunikationsmyndigheten, Agentschap Telecom,[58] som verkar under EZK, agerar CSIRT för leverantörer av digitala tjänster genom en enhet som ska vara i drift från och med 1 januari 2019.[59] Incidentrapporteringen skall ske både till tillsynsmyndigheten och till CSIRT på grund av att respektive inrapportering har olika ändamål. En tydlig skillnad är att tillsynsmyndigheten har till uppdrag att se till att varje leverantör följer lagen samt informera andra eventuellt berörda sektorer. CSIRT i sin tur har till uppgift att erbjuda stöd och råd beroende på situationen men har inte något tillsynsansvar. CSIRT är således en operativ aktör.[60]

De genom Wbni utsedda ansvariga aktörerna för respektive sektor har i sin tur utsett tillsynsmyndigheter som även hanterar utfärdandet av sanktionsavgifter i händelse av överträdelser.

[57] National Cyber Security Center. *Wet gegevensverwerking treedt 1 oktober 2017 gedeeltelijk in werking.* 2017. https://www.ncsc.nl/actueel/nieuwsberichten/wet-gegevensverwerking-treedt-1-oktober-2017-gedeeltelijk-in-werking.html (hämtad 2018-11-06).

[58] Agentschap Telecom kan jämföras med den svenska Post- och Telestyrelsen.

[59] Staatsblad van het Koinkrijk der Nederlanden. *No. 389. Besluit van 30 oktober 2018 tot aanwijzing van het CSIRT voor digitale diensten en tot vaststelling van het tijdstip van inwerkingtreding van de Wet en het Besluit beveiliging netwerk – en informatiesystemen.*. 2018. https://zoek.officielebekendmakingen.nl/stb-2018-389.html (hämtad 2018-11-12).

[60] Ministerie van Economische Zaken en Klimaat. *Wet beveiling Netwerk- en Informatiesystemen (Wbni) voor Digitale Dienstverleners.* 2018.

Tabell 4. Sammanställning över sektorer med respektive ansvarig aktör samt tillsynsmyndigheterna

SEKTOR	ANSVARIG AKTÖR	TILLSYNSMYNDIGHET
Energi	EZK	Agentschap Telecom
Digital infrastruktur	EZK	Agentschap Telecom
Bankinfrastruktur	De Nederlandsche Bank NV	De Nederlandsche Bank NV
Finansmarknadens infrastruktur	De Nederlandsche Bank NV	De Nederlandsche Bank NV
Transport	Minister van infrastructuur en waterstaat	Inspectie Leefomgeving en Transport (ILT)
Dricksvattenförsörjning	Minister van Infrastructuur en Waterstaat	Inspectie Leefomgeving en Transport (ILT)
Hälsa	Minister van Volksgezongheid, Welzijn en Sport	Inspectie Gezondheidzorg en Jeugd
Digitala tjänster	EZK	Agentschap Telecom

4.3 Processer

Samtidigt med Wbni antogs, togs även dekretet för skydd av nätverk och informationssystem, Besluit beveiliging netwerk- en informatiesystemen, Bbni,[61] i bruk. Bbni antogs för att tydliggöra vilka sektorer som omfattas av lagarna och vilka som anses ha anmälningsplikt vid händelse av en incident. Bbni pekar alltså ut de operatörer av samhällsviktiga tjänster för vilka Wbni, och därmed även NIS-direktivet, gäller.[62] Likt Wbni har även Bbni en föregångare som i sin helhet har inkorporerats i det nya dekretet[63] och utvidgats för att motsvara NIS-direktivets krav. Utvidgningen omfattar den centrala bränslelagringen, Stichting Centraal Orgaan Voorraadvorming Aardolieproducten (COVA), Maastricht Upper Area Control Centre, samt administratörer av toppdomäner.

Bbni delar upp den samhällsviktiga infrastrukturen i två kategorier, A och B, beroende på hur stora konsekvenser eventuella incidenter skulle ha på det övriga samhället. Ett kännetecken för kategori A-processer är exempelvis att det finns risk för kaskad- och/eller dominoeffekter. Anledningen till denna uppdelning är att det ska vara lättare att prioritera i händelse av samtidiga incidenter samt vilka tjänsters motståndskraft som främst bör utvecklas.[64]

Som ett resultat av diskussioner mellan relevanta privata och offentliga aktörer från olika sektorer, likväl som myndigheter och justitiedepartementet som föranledde dekretet, gjordes en inventering av varje sektor för att fastställa de leverantörer som bör ha en incidentrapporteringsskyldighet. Utöver de i NIS-direktivet reglerade sektorerna har Nederländerna även listat kärnenergi, telekommunikationsnätverk och vattenreglering i sin

[61] Staatsblad van het Koinkrijk der Nederlanden. *No. 388. Besluit van 30 oktober 2018, houdende regels ter uitvoering van de Wet beveiliging netwerk- en informatiesysteme (Besluit beveiliging netwerk- en informatioesystemen).* 2018. https://zoek.officielebekendmakingen.nl/stb-2018-388.html (hämtad 2018-11-12).
[62] NCTV. *Wat staat er in de Wet beveiliging netwerk- en informatiesystemen?.* N.d. https://www.nctv.nl/Wbni/index.aspx (hämtad 2018-11-12).
[63] Förgångaren till Bbni var Besluit meldeplicht cybersecurity, vilket antogs 2017.
[64] Staatsblad van het Koinkrijk der Nederlanden. *No. 476. Besluit meldeplicht cybersecurity*. 2017. https://zoek.officielebekendmakingen.nl/stb-2017-476.html (hämtad 2018-11-05)

helhet som sektorer med leverantörer av samhällsviktiga tjänster.[65] Dessa benämns som övriga viktiga leverantörer och omfattas av anmälningsskyldighet av allvarliga incidenter, fast de egentligen inte ingår i NIS-direktivets tillämpningsområde.[66] Här frångår man alltså NIS-direktivet och utökar dess omfattning. Kärnkraften pekades ut som en viktig sektor på grund av sin politiska känslighet liksom eventuella ekonomiska och sociala konsekvenser av en händelse, samt dess unika karaktär. Den klassificeras som A-vital. Valet att peka ut vattenreglering, vilket till exempel inbegriper hantering av kanaler och slussar, som en samhällsviktig sektor beror på landets geografi.

Det är dock noterbart att implementeringen inte i samtliga avseenden går utöver NIS-direktivets krav. Några av de sektorerna som direktivet föreskriver utelämnas eller förenklas i Bbni. Detta berör i synnerhet hälso- och sjukvårdssektorn, digital infrastruktur samt transport- och finansmarknadssektorn. Nederländerna har således inte utsett någon OES inom järnvägstransport eller vägtransport. Resonemanget bakom detta är att en störning av dessa system inte kommer att leda till några betydande konsekvenser för samhället eftersom det finns alternativa transportsätt att tillgå. När det gäller hälso- och sjukvårdssektorn motiveras utelämningen genom att vården i Nederländerna inte är centralt organiserad och en incident kommer vanligen att begränsas till en institution. I de fall där en incident påverkar fler än en institution är vården i den berörda institutionen dessutom vanligtvis fortfarande tillgänglig. Det anses vara osannolikt att ett stort antal vårdaktörer i flera regioner påverkas av en incident samtidigt, delvis då institutionerna inte köper programvaran på gemensam upphandling och inte behandlar uppdateringar samtidigt.[67] Valet av de övriga sektorerna motiveras genom att NIS-direktivet ger medlemsstaterna möjlighet att efter två år utvärdera implementeringen och dess konsekvenser.

Gällande finansmarknadssektorn syftar kraven på aktörer inom den s.k. finansiella kärninfrastrukturen (FKI). FKI-institutionerna är institutioner som ansvarar för de viktigaste transaktionsflödena i de utsedda samhällsviktiga finansiella tjänsterna såsom kreditinstitut, handelsplattformar, och andra finansiella institut som spelar en viktig roll i transaktionskedjor för sådana tjänster. Vilka som ingår i FKI bestäms årligen av den nederländska centralbanken, De Nederlandsche Bank.[68]

För att identifiera relevanta leverantörer av digitala tjänster som bör omfattas av incidentrapporteringsplikten tillämpar Bbni ett volymkriterium då antalet autonoma system kopplade till internetnoden knyts till ett tröskelvärde. Detta kriterium är både lätt att verifiera samt används av andra länder, så som Tyskland, vilket förenklar harmoniseringen bortom ländernas gränser.

Uppskattningsvis kommer ca 60 leverantörer att anses vara OES och 150-200 digitala tjänster att vara DSP.[69] Då de flesta sektorerna där OES är verksamma identifierades redan i dekretet som föregick Bbni samt skyldigheten att rapportera allvarliga incidenter till NCSC redan fastställdes i lagstiftningen som föregick implementeringen av NIS-direktivet, är processerna hos många av leverantörerna redan etablerade. De övriga

[65] Staatsblad van het Koinkrijk der Nederlanden. *No. 476. Besluit meldeplicht cybersecurity*. 2017. https://zoek.officielebekendmakingen.nl/stb-2017-476.html (hämtad 2018-11-05)
[66] Staatsblad van het Koinkrijk der Nederlanden. *No.388. Besluit van 30 oktober 2018, houdende regels ter uitvoering van de Wet beveiliging netwerk- en informatiesysteme (Besluit beveiliging netwerk- en informatioesystemen)* 2018. https://zoek.officielebekendmakingen.nl/stb-2018-388.html (hämtad 2018-11-12).
[67] Staatsblad van het Koinkrijk der Nederlanden. *No. 476. Besluit meldeplicht cybersecurity*. 2017. https://zoek.officielebekendmakingen.nl/stb-2017-476.html (hämtad 2018-11-05)
[68] Staatsblad van het Koinkrijk der Nederlanden. *No.388. Besluit van 30 oktober 2018, houdende regels ter uitvoering van de Wet beveiliging netwerk- en informatiesysteme (Besluit beveiliging netwerk- en informatioesystemen)* 2018. https://zoek.officielebekendmakingen.nl/stb-2018-388.html (hämtad 2018-11-12).
[69] Kamerstuk. Tweede Kamer der Staten-Generaal. *Regels ter implementatie van richtlijn (EU) 2016/1148 (Cybersercuritywet).* 2018.

leverantörerna meddelas om att de har blivit utsedda som OES av respektive sektors tillsynsmyndighet.[70]

Slutligen kan konstateras att Bbni är ett relativt omfattande dekret som samtidigt på inget vis är statiskt. I gällande versionen av dekretet finns ett förbehåll om att det redan vid nästa revidering kommer att tilläggas fler leverantörer inom den digitala sektorn, i synnerhet sådana som levererar datasystem till statliga organisationer.

[70] Ministerie van Economische Zaken en Klimaat. *Wet beveiling Netwerk- en Informatiesystemen (Wbni) voor Digitale Dienstverleners.* 2018.

5 Storbritannien

Inledningsvis kan konstateras att brittiska regeringens intention hittills har varit att implementera EU:s strategier och policies inom ramen för arbetet mot stärkt och harmoniserad cybersäkerhet inom unionen. Implementeringen är tänkt att gälla även efter det förmodade brittiska utträdet ur EU.[71] Storbritannien vill behålla en internationell karaktär i sitt cybersäkerhetsarbete, vilket också uttrycks i landets rådande cybersäkerhetsstrategi. Det nuvarande strategiska dokumentet gäller fram till 2021 och syftar till att stärka Storbritanniens resiliens och ställning i det internationella digitala landskapet.[72] Strategin vill uttryckligen stärka det internationella cybersäkerhetssamarbetet inom ramen för EU, Nato och FN då det är Storbritanniens uppfattning att ett sådant samarbete kommer stärka den kollektiva säkerheten.[73]

5.1 Lagstiftning

Implementeringsprocessen i Storbritannien inleddes med ett flertal konsultationer med privata och offentliga aktörer inom de berörda sektorerna som på detta vis har blivit involverade i lagstiftningsprocessen samt direktivets administrativa implementering.

The Network and Information Systems Regulations 2018 (NIS Regulations 2018) lades fram i april 2018[74] och är den lagstiftning som reglerar Storbritanniens implementering av NIS-direktivet. I den fastslås de mandat och uppdrag aktörer har för att säkerställa att direktivet följs. Regleringen föreskriver bland annat att en nationell NIS-strategi ska antas. Den befintliga nationella cyberstrategin som sträcker sig från 2016-2021 anses uppfylla de krav NIS-direktivet ställer.[75] Strategin adresserar åtgärder och tillämpningsramar för att säkerställa att strategins syfte uppfylls samt fastslår roller och ansvar för nyckelaktörer ansvariga för implementeringen av strategin. Strategin adresserar även åtgärder gällande beredskap, resonans och återhämtning, inkluderat samarbete mellan offentlig och privat sektor såväl som utbildningsinitiativ relaterade till strategin. Bedömningen är att den uppfyller de krav på strategiska mål och prioriteringar som NIS-direktivet föreskriver.

Regleringen har tydliga instruktioner kring vad en OES ska inrapportera i händelse av en incident. En sådan inrapportering måste innefatta bland annat form och påverkan, eventuella gränsöverskridande följder och hur länge incidenten pågått/pågick. Inrapportering ska enligt föreskriften ske inom 72 timmar efter att leverantören eller operatören har blivit medveten om incidenten.

Storbritannien förordar dessutom att det är statens uppdrag att identifiera och meddela de aktörer som anses tillhandahålla samhällsviktiga tjänster. Det konstateras även att ett antal aktörer inom vissa sektorer inte möter de formella kraven men anses ändå vara leverantörer av samhällsviktiga tjänster. Dessa omfattas av undantag genom myndighets- eller regeringsbeslut, som i sin tur grundas i en bedömning gällande nationell säkerhet, hot

[71] Department for Digital, Culture, Media and Sport. *The Network and Information Systems Regulation 2018.* 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701054/Network_Information_Systems_Directive_Final_Impact_Assessment.pdf (Hämtad 2018-10-09)

[72] HM Government. *National Cyber Security Strategy 2016-2021*. 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (hämtad 2018-11-07)

[73] Ibid.

[74] Department of Digital, Culture, Media and Sport. *NIS Directive and NIS Regulations 2018.* 2018. https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018 (hämtad 2018-10-08)

[75] ICO. *The role of the National Cyber Security Centre (NCSC)*. 2018. https://ico.org.uk/for-organisations/the-guide-to-nis/the-role-of-the-national-cyber-security-centre-ncsc/

mot den allmänna säkerheten eller möjligheten att en störande incident kan ha signifikant påverkan på samhället och/eller ekonomin. [76]

Även hanteringen av digitala tjänsteleverantörer utreddes via konsultation och beslutet fattades att DSP med fler än 50 anställda och en omsättning av minst £10 miljoner[77] skall omfattas av den nya lagstiftningen. Denna definition ligger i enlighet med kraven fastställda i NIS-direktivet.

5.2 Aktörer

Det brittiska National Cyber Security Centre (NCSC) är den centrala aktören för Storbritanniens arbete med cybersäkerhet och har ett övergripande ansvar för att hålla samman Storbritanniens cybersäkerhetsstrategi på nationell nivå, att hantera och analysera nationella cyberincidenter samt ge stöd till myndigheter, lagstiftare och privata företag.

NCSC grundades i samband med ikraftträdandet av den brittiska cybersäkerhetsstrategin och är en undergren av Government Communications Headquarters (GCHQ).[78] NCSC inbegriper numera de förmågor som redan fanns inom National Technical Authority for Information Assurance (CESG), d.v.s. informationssäkerhetsgrenen av GCHQ, inom CPNI – Centre for the Protection of National Infrastructure, inom CERT-UK samt inom CCA, Centre for Cyber Assessment.

NCSC är den nationella kontaktpunkten i Storbritannien och upprätthåller som sådan förbindelse med andra relevanta myndigheter i EU-medlemsstaterna, NIS-samarbetsgruppen samt CSIRT-nätverket. NCSC agerar dessutom CSIRT för Storbritannien.[79]

Storbritannien har valt att utnämna ett flertal tillsynsmyndigheter för de olika sektorerna. Ett bärande argument för detta val är att varje tillsynsmyndighet antas ha relativt god insyn i hur sektorn fungerar samt har god kunskap om de leverantörer och operatörer som agerar inom respektive sektor. Valet motiverades ytterligare med att NIS-direktivets föreskrifter måste tas på allvar inom varje sektor och bli en central del av de vedertagna sektorsspecifika regleringarna.

Tillsynsmyndigheternas uppdrag är att utöva tillsyn över att föreskriften följs, att publicera guider för att underlätta implementeringen, hålla lista över alla OES samt deras relevans i relation till undersektorer. Vidare ansvarar de för att konsultera och samarbeta med informationskommissionären i händelse av persondataincidenter, samt samarbeta och konsultera med relevanta myndigheter inom rättsväsendet, systermyndigheter i andra EU-medlemsländer, den nationella kontaktpunkten samt den nationella CSIRT-enheten.

I Storbritannien är det upp till varje OES att anmäla sig till utsedd tillsynsmyndighet före det fastslagna anmälningsdatumet. Det är dock upp till tillsynsmyndigheten att besluta om aktören bör omfattas av NIS-föreskriften. Tillsynsmyndigheterna har även mandatet att besluta om sanktionsavgifter i händelse av överträdelser. För digitala tjänster är ICO,

[76] Department for Digital, Culture, Media and Sport. *Security of Network and Information Systems. Public Consultation.* 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/636207/NIS_Directive_-_Public_Consultation__1_.pdf (hämtad 2018-10-09).

[77] Department for Digital, Culture, Media and Sport. *The Network and Information Systems Regulation 2018.* 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701054/Network_Information_Systems_Directive_Final_Impact_Assessment.pdf (Hämtad 2018-10-09).

[78] För mer information kring NCSC och dess uppdrag utöver NIS-direktivet, se HM Governement. *National Cyber Security Strategy 2016-2021*. 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (hämtad 2018-11-07).

[79] National Cyber Security Centre. *Introduction to the NIS Directive.* N.d. https://www.ncsc.gov.uk/guidance/introduction-nis-directive (hämtad 2018-10-25).

Information Commissioner's Office, tillsynsmyndigheten. Denna institution ansvarar i övrigt för dataskyddsfrågor. För exempel på inrapporteringsformulär för ICO, se bilaga 1.

Tabell 5. Sammanställning över sektorer samt tillsynsmyndigheterna

SEKTOR	TILLSYNSMYNDIGHET
Energi	BEIS Ofgem Department of Finance (Nordirland)
Transport (luft)	CAA DfT
Transport (järnväg)	DfT (England, Wales och Skottland) Department of Finance (Nordirland)
Transport (vatten)	DfT
Transport (väg)	DfT (England, Wales) Scottish Ministers (Skottland) Department of Finance (Nordirland)
Bankverksamhet och finansmarknadens infrastruktur (incidentrapportering)	Financial Conduct Authority
Bankverksamhet och finansmarknadens infrastruktur (cross-border dependencies)	Bank of England Sector Resilience Team
Hälso- och sjukvård	DHSC (England) The Welsh Ministers (Welsh) The Scottish Ministers (Skottland) Department of Finance (Nordirland)
Leverans och distribution av dricksvatten	DEFRA (England) The Welsh Ministers (Wales) The drinking water quality regulator for Scotland Department of Finance (Nordirland)
Digital infrastruktur	OFCOM
Digitala tjänster	ICO

5.3 Processer

År 2016 inleddes en process för att få klarhet över vilka effekter NIS-direktivet bedömdes ha i Storbritannien. Processen innebar ett flertal formella konsultationer mellan berörda offentliga och privata aktörer. Inledningsvis genomfördes en påverkansuppskattning (”impact assessment”) som innebar att ett antal berörda privata aktörer tillfrågades om deras uppfattning av direktivet generellt samt hur det skulle kunna påverka deras verksamhet. Påföljande konsultationer avhandlade de flesta aspekterna av implementeringen från frågan om vilka roller och mandat som skulle tillfalla vilka aktörer

till storleken på sanktionsavgifterna. På detta sätt lyckades Storbritannien involvera många intressenter i utvecklingen, samtidigt som regeringen fick möjlighet att argumentera för sina beslut.

I konsultationerna kring identifikation av och krav på OES kritiserades exempelvis trösklarna för att identifieras som en samhällsviktig tjänst. Enligt utomstående experter är de i Storbritannien definierade trösklarna mycket höga, vilket innebär att straffen som kan utdömas är betydande men samtidigt enbart tillämpas vid svåra överträdelser.[80] Detta kan ses som ett symptom på att Storbritannien möjligen har lagt mera vikt på konsultationer och den resulterande lagstiftningen än förvaltningen för att säkerställa en korrekt implementering av NIS-direktivet.

En av de främsta debatterna i förhållande till NIS i Storbritannien har gällt sanktionsavgifterna vilka redan i konsultationsfasen förslogs ha ett tak på 17 miljoner pund, en summa som skiljer sig markant från övriga EU-medlemsländer. Under debatten huruvida denna sanktionsregim skulle antas lyftes argument såsom att för höga avgifter skulle avskräcka aktörers benägenhet till frivillig incidentrapportering. Från den brittiska regeringens sida slogs dock fast att sanktionsregimen ska ligga fast på den förhållandevis höga nivån, delvis för att det ska vara signifikant för att på så vis vara ett incitament för beteendeförändringar, men också för att man vill harmonisera sanktionsregimen med den man applicerar i GDPR-lagstiftningen. Argumentet är att det kommer ge en kontinuitet och följdriktighet i den brittiska cybersäkerhetslagstiftningen.[81] Avgifterna går till The Consolidated Fund[82], med undantag för överträdelser som skett i Wales eller Skottland i vilket fall de ska tillfalla den walesiska respektive skotska Consolidated Fund.[83]

En annan konsekvens av konsultationen blev att regeringen gjorde ett tillägg i den föreslagna incidentrapporteringsstrukturen för NIS. Förändringen syftar till att separera incidentrespons från incidentnotifiering. Incidentrespons är i detta sammanhang primärt en supportfunktion för operatörer genom vilken regeringen kan bistå med assistans. Incidentrapportering är istället en mer regelmässig notifieringsprocess. Incidenter måste rapporteras in inom 72 timmar efter upptäckt. En oro är dock att det kan uppstå situationer då leverantörerna inte identifierar en incident inom tidsramen.

För att operatörer och leverantörer ska ges tid att implementera de nödvändiga säkerhetsåtgärderna kommer tillsynsmyndigheterna under det första året prioritera att få en tydligare bild över hur säkerheten inom nätverks- och informationssystem ser ut i respektive sektor. Operatörer och leverantörer förväntas under tiden ha inlett en analys av sina system och redan existerande säkerhetsåtgärder för att på så vis förstå var svagheterna finns.

Avslutningsvis kan konstateras att Storbritanniens implementeringsplaner ligger i enlighet med NIS-direktivets minimumkrav. Landet har för närvarande ingen ambition att överstiga dessa.[84] Samtidigt bör det hållas i åtanke att regleringen som implementerar NIS-direktivet ska följas upp tre år efter ikraftträdandet och att regeringen har signalerat att det vid

[80] Karsberg C. *Intervju 2018-11-12.* 2018.
[81] Department for Digital, Culture, Media and Sport. *Security of Network and Information Systems. Public Consultation.* 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/636207/NIS_Directive_-_Public_Consultation__1_.pdf (hämtad 2018-11-09).
[82] The Consolidated Fund är ett gemensamt konto för statens inkomster i Storbritannien. För Skottland och Wales existerar egna sådana konton.
[83] UK Government. *No. 506, Electronic communications. The Network and Information Systems Regulations 2018.* 2018. https://www.legislation.gov.uk/uksi/2018/506/made (hämtad 2018-11-07).
[84] Department for Digital, Culture, Media and Sport. *The Network and Information Systems Regulation 2018.* 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701054/Network_Information_Systems_Directive_Final_Impact_Assessment.pdf (Hämtad 2018-10-09).

uppföljningstillfället kan finnas anledning att utöka lagen för att inkludera kemikalieindustrin samt livsmedels- och jordbrukssektorn.[85]

Tabell 6: Uppskattning av antal aktörer berörda av NIS-direktivet inom fem av sju sektorer (exkluderat finansmarknadstjänster)[86]

SEKTOR	ANTAL
Dricksvattenförsörjning och distribution	19
Digital infrastruktur	18
Energi	47
Hälsa	268
Transport	80
Digitala tjänster	172

[85] Department for Digital, Culture, Media and Sport. *Security of Network and Information Systems. Public Consultation.* 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/636207/NIS_Directive_-_Public_Consultation__1_.pdf (hämtad 2018-10-09).

[86] Department for Digital, Culture, Media and Sport. *Impact Assessment (IA).* 2018.

6 Tyskland

Tysklands första nationella cybersäkerhetsstrategi antogs 2011. Sedan dess har den uppdaterats och den nu gällande strategin är från 2016.[87] Strategin identifierar fyra handlingsområden inom vilka Tyskland måste stärka sin cybersäkerhet. Det tredje av dem slår fast att skydd av den kritiska infrastrukturen är av största vikt och ska stå i centrum för gemensamma ansträngningar från stat och företag[88] och har således mest relevans för NIS-direktivet.

Den nationella strategin från 2011 har etablerat två federala cybersäkerhetsenheter. *Cyber-Abwehrzentrum*,[89] ett nationellt cyberresponscenter som samarbetar med andra myndigheter likväl som med den federala polisen, underrättelsetjänsten och tull. Huvudmålet är att analysera cybersäkerhetsincidenter och tillgodose rekommendationer till *Nationaler Cyber-Sicherheitsrat* (NCS). NCS ansvarar för implementeringen av cybersäkerhetstrategin och består av representanter för det federala kansliet, utrikesdepartementet, ett antal berörda departement och representanter för förbundsstaternas regeringar.[90]

2015 stiftade Tyskland en relativt omfattande it-säkerhetslag vilken har legat till grund för hur landet har tagit sig an utmaningen att införliva NIS-direktivet i den nationella lagstiftningen.

6.1 Lagstiftning

Som ovan nämnt antog förbundsdagen i juli 2015 *das IT-Gesetz* (IT-Sicherheitsgesetz), den tyska it-säkerhetslagen. Den anger ett enhetligt ramverk för samarbete mellan stat och leverantörer inom den kritiska infrastrukturen. Lagen föreskriver att s.k. KRITIS-företag och leverantörer, dvs. leverantörer och operatörer av samhällsviktiga tjänster, måste upprätthålla en hög standard på sina system och sin teknik (”stand der Technik”[91]) samt anmäla driftstörningar och incidenter till *Bundesamt für Sicherheit in der Informationstechnik*, BSI. Vartannat år ska alla aktörer påvisa att de på ett tillfredställande sätt uppfyller kraven på en hög nivå av systemsäkerhet.

Förutom att stärka BSI:s ställning stärker it-säkerhetslagen även *Bundeskriminalamt* (BKA), *Bundesnachrichtendienst* (BND) och *Bundesamt für Verfassungsschutz* och respektive myndighets arbete gentemot cyberkriminalitet. Efterhand som it-säkerhetslagen uppdaterades för att omfatta fler verksamhetssektorer, så lades till finans och försäkringsväsendet, hälsosektorn samt transportsektorn till i samband med lagets första uppdatering 2017.[92] För hälsosektorn innebär det att alla sjukhus med fler än 30 000 inlagda patienter årligen stämplats som kritisk infrastruktur och måste därför följa de nya reglerna. Detta gäller 110 sjukhus och kliniker.

[87] Bundesministerium des Innern, für Bau und Heimat. *Cyber-Sicherheitsstrategie für Deutschland.* 2016. https://www.bmi.bund.de/cybersicherheitsstrategie/ (hämtad 2018-11-07).
[88] Ibid.
[89] BSI. *Cyber-Abwehrzentrum. Enge Kooperation, klare Trennung der Befugnisse.* N.d. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/Cyber-Abwehrzentrum/cyberabwehrzentrum_node.html (hämtad 2018-11-09).
[90] Cyberwise. *Germany*. N.d. https://www.cyberwiser.eu/germany-de (hämtad 2018-10-29).
[91] ”Stand der Technik” eller ”state of the art” är en juridisk term som för att reglera teknik när utvecklingen av den är snabbare än lagstiftningen som reglerar den. Istället för att försöka fastslå konkreta tekniska kriterier för vad som ska regleras så används detta begrepp vilket är klart mer flytande. Vad som vid en viss tidpunkt är ”stand der Technik” kan exempelvis bedömas utefter nationella eller internationella standards och normer såsom DIN, ISO eller DKE. Se BSI. *Fragen und Antworten zum Inkrafttreten des IT-Sicherheitsgesetzes.* N.d. https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/FAQ/FAQ_IT_SiG/faq_it_sig_node.html (hämtad 2018-10-18).
[92] Ibid.

It-säkerhetslagen kan ses som en grundstomme för införlivandet av NIS-direktivet i Tyskland. Då it-säkerhetslagen innefattar mycket av det som NIS-direktivet föreskriver har den tyska implementeringsprocessen upplevts relativt friktionsfri i och med att många av kraven som NIS-direktivet fastslår redan har uppfyllts. Således finns redan mekanismer och processer som är etablerade och inkörda.[93]

Med IT-Gesetz som grundläggande lagstiftning har förbundsdagen även antagit *Gesetz zur Umsetzung der NIS-Richtlinie* vilken fastlägger nödvändiga anpassningar och utvidgningar av den nationella lagstiftningen. Exempelvis reglerar den NIS-direktivets utvidgade krav på leverantörer av energiomsorgsnät[94], offentliga kommunikationsnät och offentliga telekommunikationstjänster. Tidigare gällde bara anmälningsplikten av it-störningar för energinätsleverantörer vars anläggningar uppfyllde kraven på kritisk infrastruktur såsom de bestämts av *BSI-Kritisverordnung.* Som en konsekvens av NIS-direktivet utökas anmälningsplikten till att omfatta alla energinätverksoperatörer. Även de digitala tjänsterna omfattas numera av en utökad lagstiftning. Tysklands främsta utmaning i relation till NIS-direktivet har gällt just digitala tjänster. Det har tidigare funnits regler gällande krav på att hålla en mycket hög kvalitet på den applicerade tekniken, men det har inte funnits någon anmälningsplikt.

Vissa tjänster uppgraderas till samhällsviktiga såsom domänregistratorer vilka faller under kategorin digital infrastruktur. Samtidigt slog den tidigare it-säkerhetslagen fast att it-housing och Content Delivery Networks (CDN) skulle ses som kritisk infrastruktur vilket påkallar frågan om vad som ska klassas som digitala tjänster respektive digitala infrastruktur inom direktivet. [95]

BSI beräknar att ungefär 500-1500 företag och aktörer påverkas av de tillägg gällande digitala tjänster som NIS-direktivet påbjuder Tyskland att införa.

NIS-direktivet har inneburit en förändring i den tyska telekommunikationslagen. Anledningen är att den som erbjuder kommunikationstjänster nu får större befogenhet i hantering av sina användares datatrafik. I händelse av en störning får nu datatrafiken ledas om, så länge användaren blir notifierad. Mycket av de tyska telekommunikationstjänsterna är privatägda och det finns en oro över att BSI nu får befogenhet att inskränka tjänster, exempelvis genom att hindra datatrafik, och hänvisa till NIS-direktivet. Denna kritik har främst riktats mot att NIS-direktivet inte fullt ut beskriver när och till vilken grad denna mekanism får användas, vilket i sin tur lämnar det upp till leverantörens tolkning.[96]

6.2 Aktörer

Genom it-säkerhetslagen och NIS-direktivet har *Bundesamt für Sicherheit in der Informationstechnik* BSI fått utökade befogenheter och förtroende. Utöver att vara tillsynsmyndighet till alla sektorer, CSIRT samt nationell kontaktpunkt[97] så har BSI fått nya uppgifter och mandat. Tidigare var BSI främst ansvarig för den kritiska infrastrukturens säkerhet, men i och med anpassningen till NIS-direktivet har mandatet utvidgats till att även inkludera nätverks- och informationssäkerhet. BSI har dessutom fått en förstärkt kontrollfunktion som utökat samarbetet mellan förbundsstaterna och centralstyrningen. BSI får nu erbjuda förbundsstaterna förstärkt understöd och tekniskt

[93] BSI. *Gesetz zur Umsetzung der NIS-Richtlinie. Mehr Aufgaben und Befugnisse für das BSI.* N.d. https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS-Richtlinie.html(hämtad 2018-10-18).

[94] Det tyska begreppet *Energieversorgungsnetz* omfattar försörjning med elektricitet och gas.

[95] Schallbruch M. *NIS-Richtlinie verabschiedet: Schwierige Umsetzung für digitale Dienste.* 2016. https://www.cr-online.de/blog/2016/07/15/nis-richtlinie-verabschiedet-schwierige-umsetzung-fuer-digitale-dienste/ (hämtad 2018-10-25).

[96] Meyer, L., Kummer, W. *Umsetzungsgesetz zur europäischen NIS-Richtlinie tritt in Kraft.* 2017. https://www.datenschutz-notizen.de/umsetzungsgesetz-zur-europaeischen-nis-richtlinie-tritt-in-kraft-2518461/ (hämtad 2018-10-25).

[97] Bundestag. *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz).*2015.

expertis.[98] Alla leverantörer måste anmäla sig till BSI och lämna kontaktuppgifter till ansvariga hos respektive leverantörer.[99]

Trots dessa större befogenheter är det BSI:s uttryckliga önskan att fortsätta med och fördjupa samarbetet med näringslivet, industrin och samhället i stort, då man anser att utmaningarna enbart kan lösas gemensamt.[100] En starkt bidragande orsak till förordandet av offentligt/privat samarbete är att regeringen anser att en stark tysk it-industri behöver en modern och stark ekonomisk politik.[101]

Varför Tyskland har valt att tilldela BSI tillsynsansvaret för samtliga sektorer är relativt okommenterat, men en anledning kan vara att Tyskland är uppdelat i 16 förbundsstater med långtgående egna befogenheter. Att koordinera samtliga delstaters samhällsviktiga och digitala tjänster skulle innebära en betydande administrativ och förvaltningsmässig utmaning. BSI i sin tur är en federal myndighet samt en av de äldsta på området cybersäkerhet.

Tabell 7. Sammanställning över sektorer med respektive tillsynsmyndighet

SEKTOR	TILLSYNSMYNDIGHET
Energi	BSI
Transport	
Bankverksamhet och finansmarknadens infrastruktur	
Hälso- och sjukvård	
Leverans och distribution av dricksvatten	
Digital infrastruktur	
Digitala tjänster	

6.3 Processer

Enligt egen utsago har den tyska NIS-implementeringsprocessen hittills varit relativt friktionsfri. Detta eftersom många av direktivets krav, så som incidentrapporteringen, redan var tillgodosedda och vissa processer redan etablerade sedan en tid tillbaka.

BSI har inom ramen för förordningen för identifiering av kritisk infrastruktur tagit fram en metod för att identifiera kritisk infrastruktur, MIKI.[102] MIKI innebär ett samarbete mellan BSI, inrikesministeriet, *Bundesministerium des Inneren, für Bau und Heimat* (BMI), Myndigheten för befolkningsskydd och katastrofhjälp, *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe* (BBK) och industriaktörer inom en internetbaserad samarbetsplattform för skydd av kritisk infrastruktur, UP KRITIS. Detta är ett sätt för att ytterligare främja samarbetet mellan stat och industri samt för att stävja eventuella

[98] BSI. *Gesetz zur Umsetzung der NIS-Richtlinie. Mehr Aufgaben und Befügnisse für das BSI.* N.d. https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS_Richtlinie_node.html (hämtad 2018-10-18).
[99] BSI. *Neuregelungen für Betreiber von Energieversorgungsnetzen, öffentlichen Telekommunikationsnetzen und öffentlich zugänglichen Telekommunikationsdiensten.* N.d. https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Neuregelungen_EnWG/neur_EnWG.html (hämtad 2018-10-18).
[100] BSI. *Gesetz zur Umsetzung der NIS-Richtlinie. Mehr Aufgaben und Befugnisse für das BSI.*N.d. https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS_Richtlinie_node.html (hämtad 2018-10-19)
[101] Bundesministerium des Innern, für Bau und Heimat. *Cyber-Sicherheitsstrategie für Deutschland*. 2016.
[102] BSI. *Resiliente IT in Kritischen Infrastrukturen – UP KRITIS und IT-Sicherheitsgesetz als Wegereiter. Jahreskonferenz IT-Sicherheit für Kritische Infrastrukturen 21.06.2016.* 2016. https://www.itskritis.de/_uploads/user//K_UpKRITIS.pdf (hämtad 2018-10-29).

incidenter. Detta ramverk kan antas ha använts under identifieringen av operatörer som omfattas av NIS, utöver de redan identifierade.

När det gäller incidentrapporteringen är de krav som åläggs OES i Tyskland mer omfattande än vad NIS-direktivet anger (se bild 1). En incident omfattas av rapporteringskravet även om den hade kunnat leda till betydande störningar men inte har gjort det. Dessutom inkluderas även incidenter eller störningar av sådan typ som inte per se har inverkan på tillgängligheten av tjänsten utan här gäller de vedertagna cybersäkerhetsmålsättningarna. Även kraven för DSP är strängare och inkluderar incidenter som potentiellt kan leda till betydande störningar.[103]

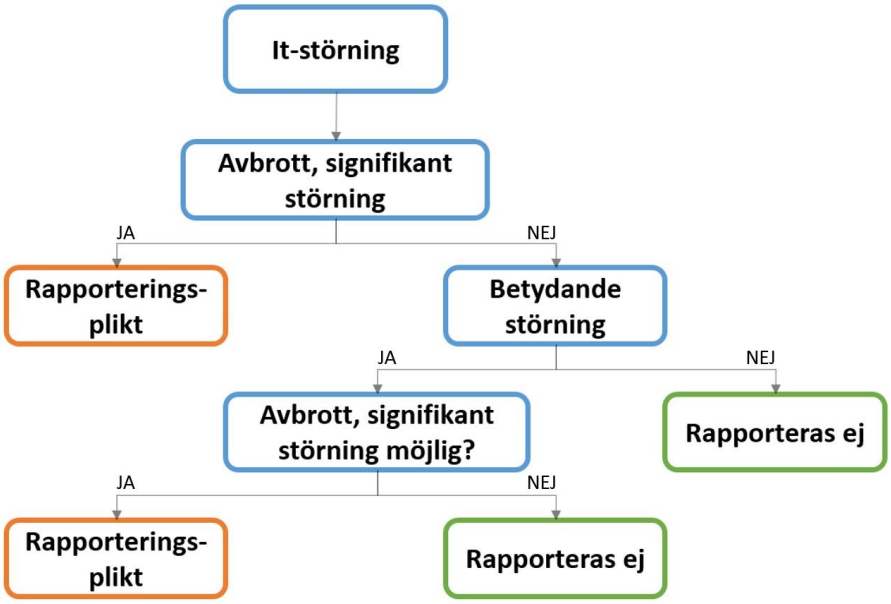

Bild 1. Beslutshjälp för rapporteringsplikten[104]

Incidentrapporteringen används sedan av BSI för analys och upprättande av aktuell lägesbild. Dessutom används information för åtgärdsförslag och varningar till andra aktörer samt för vidare arbete med skydd av kritisk infrastruktur i samarbete med BKK och andra relevanta myndigheterna. BSI erbjuder anonymisering av att de enstaka incidentrapporterna.[105] Det är värt att notera att processen för rapporteringen är oförändrad sedan 2016 då it-säkerhetslagen trädde i kraft, det vill säga före implementeringen av NIS-direktivet. Ett exempel på incidentrapportering återfinns i Bilaga 2 i denna rapport.

Från energisektorn och dess intresseorganisationer har det kommit kritik mot NIS-direktivet, bland annat gällande att Europeiska unionens byrå för nätverks- och informationssäkerhet, ENISA:s, roll är oklar vis-a-vis den nationella lagstiftningen. Vidare efterfrågas en tydlig och transparent process gällande en eventuell framtida certifiering. Detta tyder på att även om tyska myndigheter upplever att implementeringen har skett relativt friktionsfritt finns det vissa sektorer som vill vara delaktiga i den uppföljande utvärderingen och kunna lämna synpunkter.

[103] Leister, H. *Internetsicherheit in Europa: Zur Gewährleistung der Netz- und Informationssicherheit durch Informationsverwaltungsrecht.* 2018.
[104] Bundesamt für Sicherheit in der Informationstechnik. *Meldeplicht.* N.d. https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Neuregelungen_KRITIS/Meldepflicht/meldepflicht_node.html;jsessionid=CFED870946F853156575F7811D3B536D.1_cid351#doc7540234bodyText2 (hämtad 2018-10-18)
[105] BSI. *Fragen und Antworten für Betreiber Kritischer Infrastrukturen zur Meldeplicht nach dem IT-Sicherheitsgesetz.* N.d. https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/FAQ/FAQ_zur_Meldepflicht/faq_meldepflicht_node.html#faq10502730 (hämtad 2018-11-29).

Som ett led i detta och för att ytterligare stärka sin förmåga att vara behjälplig vid attacker och incidenter har BSI under 2016 inrättat *Mobile Incident Response Teams*. Dessa MIRTS är specialstyrkor bestående av cybersäkerhetsexpertis från BSI, vilka har möjligheten att ta sig till incidentplatsen snabbt för att på så vis hjälpa på plats. Exempel på incidenter där dessa MIRTS kan aktiveras är cyberattacker på it-styrning av kraftverk eller kemiska tillverkningsanläggningar, dvs. platser där en attack skulle utgöra en akut fara för civilbefolkningen.[106] I undantagsfall kan MIRT hjälpa även andra aktörer, men då måste aktören själv ha efterfrågat stöd från MIRT.[107]

Överlag kan konstateras att NIS-direktivet förefaller hanteras som ett av många kugghjul i det tyska arbetet med cybersäkerheten. I synnerhet då BSI, inom ramen för NIS-relaterade uppgifter i mångt och mycket använder strukturerna som fanns på plats innan direktivet trädde i kraft, exempelvis inrapporteringsprocessen. Tilläggen och ändringarna i processerna som kom till i och med lagen för implementeringen av NIS-direktivet poängteras inte särskilt utan har integrerats närmast obemärkt.

[106] BSI. *Gesetz zur Umsetzung der NIS-Richtlinie. Mehr Aufgaben und Befugnisse für das BSI.* N.d. https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS_Richtlinie_node.html (hämtad 2018-10-19).
[107] BSI. *Die Lage der IT-Sicherheit in Deutschland 2018*. 2018.

7 Diskussion och slutsatser

Denna studie sammanställer de grundläggande dragen i fyra länders arbete med implementeringen av NIS-direktivet. De fyra länderna skiljer sig mycket åt och i många aspekter – från storlek och förvaltningskultur till mognaden på cyberområdet. Således är det inte oväntat att länderna har angripit uppgiften att införliva NIS-direktivet i sin lagstiftning, att implementera lagen och att efterfölja direktivets krav på olika sätt.

Redan inom ramen för NIS-samarbetsgruppen har exempelvis Tyskland poängterat att det inte är givet att alla länder har samma processer eller samma behov och att det därför inte alltid är produktivt att prata om gemensam bästa praxis. Viss befogenhet kan finnas för detta, särskilt när man tittar närmare på de fyra undersökta länderna. Här framstår Nederländernas som ett tydligt exempel på hur man anpassat direktivet efter nationella förutsättningar och behov i och med att landet inkluderat vattenreglering som en samhällsviktig tjänst. Med tanke på landets geografi och samhällsinfrastruktur framstår detta som ett rimligt tillägg. Samtidigt bör noteras att just dessa fyra länder redan håller en relativt hög nivå och har många processer redan etablerade. Därför kan deras erfarenheter vara till stor nytta för andra europeiska länder som inte har kommit lika långt och därför kan ha stor nytt av utbytet av bästa praxis.

Säkerhetspolitiska faktorer nämns av två av länderna, Nederländerna och Estland, som bidragande till respektive lands antagna lagstiftning. Nederländerna har motiverat sin inkludering av kärnkraft som samhällsviktig sektor med kärnkraftsfrågans politiska känslighet. Estland har valt att se infrastrukturen för e-röstning och public service som samhällsviktiga tjänster med hänvisning till att de är sektorer man anser troligt att en främmande makt skulle vara intresserad av att attackera för att orsaka samhälleliga störningar.

Andra faktorer som påverkar implementeringen av direktivet är ländernas olika mognadsgrad gällande digitalisering, vilka resurser staterna har att tillgå, administrativ uppbyggnad, samhällets beroende av nätverks- och informationssystem samt dess ekonomi. Dessa skillnader viktar delvis också hur mycket fokus varje land lägger på respektive sektor. Nederländerna har exempelvis valt bort vissa undersektorer inom transportområdet då eventuella störningar inom dessa inte anses ha en tillräcklig stor påverkan på samhället i och med att det finns alternativa transportsätt att tillgå.

Avseende nationell lagstiftning kan noteras att Estland framförallt utformat sin NIS-relaterade lagstiftning för att förbättra och samla den redan existerande, i enlighet med tidigare identifierade problemområden. Estland motiverade detta med att landet redan hade en cybersäkerhetslagstiftning och etablerade processer som låg nära det NIS-direktivet kräver. Den nya lagen, CSA, innebär dock en mer sammanhängande och genomgripande lagstiftning med harmoniserad taxonomi. Nederländerna å sin sida har valt att i huvudsak uppdatera den lag man antog 2017 för att fullkomligt inkludera NIS-direktivet i den nationella lagstiftningen. Storbritannien har valt att skapat en ny reglering för just NIS-direktivet, vilket delvis föranletts av offentliga konsultationer, men som också till synes är inspirerad av GDRP-lagstiftningen.

Förvaltningsmässigt finns också skillnader länderna emellan. Det är noterbart att Estland och Tyskland har valt att ha en centraliserad tillsyn med en myndighet som utövar tillsyn över alla sektorer. Detta är särskilt intressant med hänsyn till att dessa länder skiljer sig markant i storlek, organisationskultur och delvis mognad inom cyberområdet. I Tyskland och Estland är även denna enda tillsynsmyndighet också nationell kontaktpunkt och bedriver CSIRT-verksamheten. Beslutet att centralisera förvaltningen motiveras av att länderna därigenom har möjligheten att på ett ställe samla behövlig kunskap och kapacitet för att kunna fullfölja NIS-direktivet. På så vis får landet en bättre översikt och effektivare incidenthantering.

Nederländerna och Storbritannien å andra sida har valt en decentraliserad tillsyn med sektorspecifika tillsynsmyndigheter. Dessa länder anser att sektorerna själva har bäst insyn

i den verksamhet som sker inom respektive sektor. Detta begränsar möjligheterna till en samlad bild för en central aktör, till exempel för den nationella kontaktpunkten. Samtidigt finns det som ovan nämnt hos de utsedda tillsynsmyndigheterna en djupgående förståelse för verksamheten inom sektorn och hur den skulle påverkas i diverse scenarion.

Det finns således fördelar och nackdelar med respektive modell. Det bedöms alltså ytterst vara en prioriteringsfråga och ett beslut som rimligtvis grundas i både landets individuella förvaltningsstrukturer och tillgången på cybersäkerhetskompetenser inom de respektive sektorerna.

Alla länder har, i enlighet med NIS-direktivets förskrifter, gett tillsynsmyndigheterna rätten att utdöma sanktionsavgifter till leverantörer och/eller operatörer av samhällsviktiga eller digitala tjänster som inte följer lagstiftningen och uppfyller kraven. Noterbart är dock att dessa sanktionsavgifter skiljer sig markant länderna emellan. Storbritannien har möjlighet att döma ut sanktionsavgifter upp till 17 miljoner pund[108] medan Estland har lagt gränsen vid 20 000 EUR. Storbritannien anser att det är rimligt att lägga avgiften så pass högt dels då den synkroniserar med GDPR-lagstiftningen, dels för att man anser att ett misslyckande i att efterfölja de av NIS uppställda reglerna är att betrakta som ett så pass allvarligt brott att ett straff av en sådan magnitud är skäligt. I relation till Estlands långtgående cybersäkerhetsarbete kan den låga sanktionsavgiftsnivån förefalla som märklig, men kan eventuellt förklaras av en hög tilltro i den egna förmågan att etablera god cyberhygien på andra sätt. Lägre straff kan ge större incitament för att på djupet skapa en konstruktiv riskhanteringskultur. Samtidigt som Estlands lagstiftning stipulerar den lägsta sanktionsavgiftsnivån, har landet också den kortaste tidsramen för incidentrapportering, 24 timmar för samhällsviktiga tjänster. I Storbritannien går gränsen exempelvis vid 72 timmar.

Utöver dessa ovan belysta olikheter finns likheter länderna emellan. En tydlig likhet är etablerandet av ett dedikerat cybercenter. Alla har inte inrättats i samband med NIS-direktivets implementering, men ofta i samband med en cybersäkerhetslagstiftning, vilken i sin tur har varit grundläggande för landets implementering av direktivet.

Inget av länderna har antagit NIS-direktivet, som är en minimiharmoniserande rättsakt, som en ”blueprint” för sin lagstiftning utan samtliga har anpassat den till nationella förutsättningar och behov. Detta leder till att de respektive ländernas nivå av cybersäkerhetsarbete inte blir lika lätt jämförbar och att åtgärderna inte hamnar på en likställd nivå. I detta sammanhang kan konstateras att respektive lands definition av vad som ska anses vara en OES är starkt beroende av graden och karaktären av digitalisering i de olika sektorerna i respektive medlemsstat. Som tidigare nämnt, har till exempel Nederländerna valt att fokusera minimalt på transportsektorn och hälsosektorn med motiveringen att det inte finns aktörer som uppfyller definitionen av OES inom dessa sektorer.

Tabell 8. Överblick tillagda och nedprioriterade sektorer i respektive land

LAND	TILLAGDA SEKTORER
Estland	Public service, e-voteringssystem, småskaliga läkarmottagningar
Nederländerna	Kärnenergi, vattenreglering, telekommunikationsnätverk
LAND	NEDPRIORITERADE SEKTORER
Nederländerna	Hälsa/sjukvård, digital infrastruktur, transport, finansmarknaden

En viktig slutsats som kan dras av de länder som studerats sammanfaller med ett konstaterade som även Uku Särekanno, vice generaldirektör för estniska RIA, gjorde – NIS-direktivet kom inte som någon överraskning utan var snarare ett naturligt nästa steg

[108] Motsvarar ca. 19 miljoner EUR (December 2018).

för nätverks- och informationssäkerheten och cybersäkerhetslagstiftning. Trots att alla länder har fått anta viss ny lagstiftning så förefaller samtliga redan ha haft etablerade strukturer, vilket har underlättat åtminstone den lagstiftande delen av implementeringen av direktivet. Som en jämförelse kan nämnas att GDRP-lagstiftningen var mycket mer transformativ.

En annan slutsats som kan dras är att det finns många svårigheter i att mäta och jämföra hur olika länder har implementerat detta direktiv eftersom att det saknas tydliga faktorer att mäta. Direktivet ger medlemsländerna ett relativt stort spelrum för att själva tolka hur det ska implementeras, vad som berörs och till vilken grad. Det är dessutom oklart huruvida Europeiska kommissionen uppfattas som beredd att använda sig av sanktionsmekanismer för att få alla länder att följa direktivet i och med att relativt få länder har inkommit med informationen enligt kommissionens rapporteringskrav och tidsplan.[109] Samtidigt finns tendenser till att en harmonisering länderna emellan sker utöver den egentliga implementeringen av direktivet, till exempel som ett resultat av arbetet inom NIS-samarbetsgruppen och utbyte av bästa praxis. Ett sådant exempel återfinns inom digitala tjänsters inrapporteringsplikt där Nederländerna tillämpar ett volymkriterium som även används av Tyskland för att identifiera de DSP som omfattas av rapporteringen. Detta förenklar harmoniseringen länderna emellan. Överlag rekommenderas ett vidare studium av implementeringen med fokus på harmonisering och jämförbarhet.

Ytterligare en slutsats som kan dras är att ländernas arbete med NIS-direktivets implementering verkar riktas främst inåt, det vill säga mot de egna sektorerna och institutionerna. Relativt få dokument vittnar om en fokusering utåt och mot gränsöverskridande beroenden, trots att sådana finns även för verksamheter som är både samhällsviktiga och som omfattas av direktivet. Förvisso tar NIS-direktivet relativt lite höjd för gränsöverskridande beroenden. Samtidigt, med tanken på att direktivet syftar till en harmonisering av cybersäkerhetsnivån inom den inre marknaden, blir frågan om inte åtminstone de länderna som uppfattar sina cybersäkerhetsekosystem som väldigt mogna borde ha tagit synliga steg mot att reda ut gränsöverskridande beroende. Det kan även finnas anledning att fundera över huruvida exempelvis företag kan komma att förlägga sin verksamhet i ett land med lägre sanktionsavgifter. Det kan, trots att det är delvis reglerat i NIS-direktivet, bli ett kryphål i regleringen som kan riskera säkerheten i flera länder på grund av kaskad- och/eller dominoeffekter. Det verkar finnas en oro för detta i flera länder men det är för närvarande svårt att finna aktiviteter som är ämnade att hantera detta potentiella problemområde. Medlemsstaterna och Europeiska kommissionens arbete för att komma överens om och reglera gränsöverskridande beroenden, både inom och utom NIS-direktivet eller utanför, är ett ämne som således bör studeras ytterligare.

[109] EU Kommissionen. *Fact Sheet July infringements package: key decisions*. 2018. http://europa.eu/rapid/press-release_MEMO-18-4486_en.htm (hämtad 2018-12-28)

Referenser

Brooijmans, M. *The fight for cybersecurity in the Netherlands.* Holland Fintech. 2018. https://hollandfintech.com/2018/03/fight-cybersecurity-netherlands/ (hämtad 2018-10-31).

Bundesministerium des Innern, für Bau und Heimat. *Cyber-Sicherheitsstrategie für Deutschland.* 2016. https://www.bmi.bund.de/cybersicherheitsstrategie/ (hämtad 2018-11-07).

Bundestag Deutschland. *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)*. 2015.

Bundesamt für Sicherheit in der Informationstechnik. *Cyber-Abwehrzentrum. Enge Kooperation, klare Trennung der Befugnisse.* N.d. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/Cyber-Abwehrzentrum/cyberabwehrzentrum_node.html (hämtad 2018-11-09).

Bundesamt für Sicherheit in der Informationstechnik. *Das IT-Sicherheitsgesetz.* N.d. https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/it_sig_node.html (hämtad 2018-11-21).

Bundesamt für Sicherheit in der Informationstechnik. *Die Lage der IT-Sicherheit in Deutschland 2018*. 2018.

Bundesamt für Sicherheit in der Informationstechnik. *Fragen und Antworten für Betreiber Kritischer Infrastrukturen zur Meldepflicht nach dem IT-Sicherheitsgesetz*. N.d. https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/FAQ/FAQ_zur_Meldepflicht/faq_meldepflicht_node.html#faq10502730 (hämtad 2018-11-21).

Bundesamt für Sicherheit in der Informationstechnik. *Fragen und Antworten zum Inkrafttreten des IT-Sicherheitsgesetzes.* N.d. https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/FAQ/FAQ_IT_SiG/faq_it_sig_node.html (hämtad 2018-10-18).

Bundesamt für Sicherheit in der Informationstechnik. *Gesetz zur Umsetzung der NIS-Richtlinie. Mehr Aufgaben und Befugnisse für das BSI.* N.d. https://www.bsi.bund.de/DE/DasBSI/NIS-Richtlinie/NIS-Richtlinie.html (hämtad 2018-10-18).

Bundesamt für Sicherheit in der Informationstechnik. *Meldeplicht.* N.d. https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Neuregelungen_KRITIS/Meldepflicht/meldepflicht_node.html;jsessionid=CFED870946F853156575F7811D3B536D.1_cid351#doc7540234bodyText2 (hämtad 2018-10-18)

Bundesamt für Sicherheit in der Informationstechnik. *Neuregelungen für Betreiber von Energieversorgungsnetzen, öffentlichen Telekommunikationsnetzen und öffentlich zugänglichen Telekommunikationsdiensten*. N.d. https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Neuregelungen_EnWG/neur_EnWG.html (hämtad 2018-10-18).

Bundesamt für Sicherheit in der Informationstechnik. *Resiliente IT in Kritischen Infrastrukturen – UP KRITIS und IT-Sicherheitsgesetz als Wegbereiter. Jahreskonferenz IT-Sicherheit für Kritische Infrastrukturen.* 2016. https://www.itskritis.de/_uploads/user//K_UpKRITIS.pdf (hämtad 2018-11-07).

CR online. *NIS-Richtlinie verabschiedet: schwierige Umsetzung für digitale Dienste*. 2016. https://www.cr-online.de/blog/2016/07/15/nis-richtlinie-verabschiedet-schwierige-umsetzung-fuer-digitale-dienste/ (hämtad 2018-09-25).

Cyberwise. *Germany*. N.d. https://www.cyberwiser.eu/germany-de (hämtad 2018-10-29).

Cyber Security Raad. *Dutch Cyber Security Council.* N.d. https://www.cybersecurityraad.nl/index-english.aspx (hämtad 2018-11-05).

Department for Digital, Culture, Media and Sport. *Impact Assessment (IA).* 2018.

Department of Digital, Culture, Media and Sport. *NIS Directive and NIS Regulations 2018.* 2018. https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018 (hämtad 2018-10-08).

Department for Digital, Culture, Media and Sport. *Security of Network and Information Systems. Public Consultation.* 2017. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/636207/NIS_Directive_-_Public_Consultation__1_.pdf (hämtad 2018-10-09).

Department for Digital, Culture, Media and Sport. *The Network and Information Systems Regulation 2018*. 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/701054/Network_Information_Systems_Directive_Final_Impact_Assessment.pdf (Hämtad 2018-10-09).

E-Estonia. *How Estonia became a global heavyweight in cyber security*. 2017. (hämtad 2018-11-14).

EU. *Direktiv (EU) 2016/1148 om åtgärder för en hög gemensam nivå på säkerhet i nätverk- och informationssystem i hela unionen*. 2016.

EU Kommissionen. *Typer av EU-rättsakter.* N.D. https://ec.europa.eu/info/law/law-making-process/types-eu-law_sv (hämtad 2018-09-25).

EU Kommissionen. *Fact Sheet July infringements package: key decisions.* 2018. http://europa.eu/rapid/press-release_MEMO-18-4486_en.htm (hämtad 2018-12-28).

HM Government. *National Cyber Security Strategy 2016-2021*. 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (hämtad 2018-11-07).

Information Commissioner's Office. *The role of the National Cyber Security Centre (NCSC)*. 2018. https://ico.org.uk/for-organisations/the-guide-to-nis/the-role-of-the-national-cyber-security-centre-ncsc/ (hämtad 2018-10-31).

Kamerstuk. Tweede Kamer der Staten-Generaal. *Regels ter implementatie van richtlijn (EU) 2016/1148 (Cybersercuritywet).* 2018.

Karsberg, C. *Intervju 2018-11-12.* [MSB]. 2018.

Leisterer, H. *Internetsicherheit in Europa: Zur Gewährleistung der Netz- und Informationssicherheit durch Informationsverwaltungsrecht*. Mohr Siebeck GmbH and KG. 2018. https://www.jstor.org/stable/j.ctv5qdgq9 (hämtad 2018-10-29).

Meyer, L., Kummer, W. *Umsetzungsgesetz zur europäischen NIS-Richtlinie tritt in Kraft.* 2017. https://www.datenschutz-notizen.de/umsetzungsgesetz-zur-europaeischen-nis-richtlinie-tritt-in-kraft-2518461/ (hämtad 2018-10-25).

Ministry of Economic Affairs and Communication. *Cyber Security Strategy 2014-2017.* 2014. https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf (hämtad 2018-11-14).

Ministerie van Economische Zaken en Klimaat. *Wet beveiling Netwerk- en Informatiesystemen (Wbni) voor Digitale Dienstverleners.* 2018.

Nationaal Coördinator Terrorismebestrijding en Veiligheid. *Cybersecuritybeeld Nederland,CSBN 2018*. 2018.

Nationaal Coördinator Terrorismebestrijding en Veiligheid. *Cyber Security*. N.d https://www.nctv.nl/organisatie/cs/index.aspx (hämtad 2018-11-05).

Nationaal Coördinator Terrorismebestrijding en Veiligheid. *Incident Response. 24-uurshulp.* N.d. https://www.ncsc.nl/incident-response/24-uurshulp.html (hämtad 2018-11-12).

Nationaal Coördinator Terrorismebestrijding en Veiligheid. *Nederlandse Cybersecurity Agenda.* N.d. https://www.nctv.nl/ncsa/index.aspx (hämtad 2018-11-05).

Nationaal Coördinator Terrorismebestrijding en Veiligheid. *Nederlandse Cybersecurity Alliantie.* 2018. https://www.nctv.nl/cybersecurityalliantie/index.aspx (hämtad 2018-11-01).

Nationaal Coördinator Terrorismebestrijding en Veiligheid. *Wat staat er in de Wet beveiliging netwerk- en informatiesystemen?.* N.d. https://www.nctv.nl/Wbni/index.aspx (hämtad 2018-11-12).

Nationaal Cyber Security Centrum. *Wet gegevensverwerking treedt 1 oktober 2017 gedeeltelijk in werking.* 2017. https://www.ncsc.nl/actueel/nieuwsberichten/wet-gegevensverwerking-treedt-1-oktober-2017-gedeeltelijk-in-werking.html (hämtad 2018-11-06).

National Cyber Security Centre. *Introduction to the NIS Directive.* N.d. https://www.ncsc.gov.uk/guidance/introduction-nis-directive (hämtad 2018-10-25).

Ras, K. *Estonia as a leader in increasing cybersecurity.* 2018. https://www.pism.pl/publications/bulletin/no-68-1139 (hämtad 2018-11-21)

Riigi infosüsteemi Amet. *Annual Cyber Security Assessment 2018 Estonian Information System Authority.* 2018.

Riigi infosüsteemi Amet. *CERT-EE.* 2018. https://www.ria.ee/en/cyber-security/cert-ee.html (hämtad 2018-11-30).

Riigikogu. *Cyber Security Act.* 2018. https://www.riigikogu.ee/tegevus/eelnoud/eelnou/61815f7a-1025-4aea-9b0e-d9cf97337e59/K%C3%BCberturvalisuse%20seadus (hämtad 2018-10-30).

Riigikogu. *Electronic Communications Act.* 2016.

Rijksoverheid Nederlandse. *'Building Digital Bridges'. International Cyber Strategy – Towards an integrated international cyber policy.* 2017.

Rijksoverheid NL. *Cybersecurity act submitted to House of Representatives 2018-02-15*. 2018. https://www.government.nl/latest/news/2018/02/15/cybersecurity-act-submitted-to-house-of-representatives (hämtad 2018-10-31).

Rijkswaterstaat. *Office for European Programmes (Bureau Brussels).* N.d. https://www.rijkswaterstaat.nl/english/about-us/international-cooperation/bureau-brussels.aspx (hämtad 2018-10-31).

Schellevis, J. *Zeker vijftien ziekenhuizen geïnfecteerd met ransomware.* 2017. https://nos.nl/artikel/2179941-zeker-vijftien-ziekenhuizen-geinfecteerd-met-ransomware.html (hämtad 2018-11-26).

SFS 2018:1174. *Lag om informationssäkerhet för samhällsviktiga och digitala tjänster.* 2018.

Siseministerium. [Inrikesministeriet Estland]. *Crisis management.* 2017. https://www.siseministeerium.ee/en/activities/crisis-management (hämtad 2018-11-12).

Staatsblad van het Koinkrijk der Nederlanden. *No. 476. Besluit meldeplicht cybersecurity*. 2017. https://zoek.officielebekendmakingen.nl/stb-2017-476.html (hämtad 2018-11-05).

Staatsblad van het koninkrijk der Nederlanden. *Nr 387:2018. Wet van 17 oktober 2018, houdende regels ter implementatie van richtlijn (EU) 201671148 (Wet beveiliging netwerk- en informatiesystemen)*. 2018.

Staatsblad van het Koinkrijk der Nederlanden. *Nr. 388. Besluit van 30 oktober 2018, houdende regels ter uitvoering van de Wet beveiliging netwerk- en informatiesysteme (Besluit beveiliging netwerk- en informatioesystemen).* 2018. https://zoek.officielebekendmakingen.nl/stb-2018-388.html (hämtad 2018-11-12).

Staatsblad van het Koinkrijk der Nederlanden. *Nr. 389.Besluit van 30 oktober 2018 tot aanwijzing van het CSIRT voor digitale diensten en tot vaststelling van het tijdstip van inwerkingtreding van de Wet en het Besluit beveiliging netwerk – en informatiesystemen.* 2018. https://zoek.officielebekendmakingen.nl/stb-2018-389.html (hämtad 2018-11-12).

Särekanno, U. *Telefonintervju. 2018-11-26.* 2018.

UK Government. *2018 No. 506, Electronic communications. The Network and Information Systems Regulations 2018.* 2018. https://www.legislation.gov.uk/uksi/2018/506/made (hämtad 2018-11-07).

Universiteit Leiden, Leiden Law Blog. *NIS Directive – update for the Netherlands 2018-01-31.* 2018. https://leidenlawblog.nl/articles/nis-directive-update-for-the-netherlands (hämtad 2018-09-26).

Vabariigi Valitsus [Republiken Estland] *Emergency Act.* 2009.

BILAGA 1 Incidentrapportering Storbritannien

ico.
Information Commissioner's Office

Network and Information Systems Regulations 2018 (NIS) Incident Notification Form

What is the purpose of this form?

This form is for **Relevant Digital Service Providers** (RDSPs) to notify the ICO of a NIS incident. We will use the information you provide to record the incident and, if necessary, investigate further. You are only required to complete this form if you have access to sufficient information that allows you to assess whether the incident's impact is substantial.

If you are **not** an RDSP (eg, if you are an operator of essential services/OES), you must report the incident to your competent authority.

If you are an OES that wants to report a personal data breach resulting from a NIS incident, please contact our helpline on **0330 123 1113**.

Will the information we provide be shared with anyone else?

Under Regulation 12(8) of NIS, the ICO is required to share incident notifications with the National Cyber Security Centre (NCSC) in support of its role as the UK's computer security incident response team (CSIRT). This also supports the UK's strategy to prevent cybercrime and to protect organisations and individuals from such crime. We may also share information with law enforcement agencies such as the National Crime Agency, the National Fraud Intelligence Bureau and Regional Cyber Crime Units as appropriate.

Where an incident has a cross-border impact on two or more EU Member States, the ICO may share information with relevant authorities within those States.

As stated by Regulation 12(12), if we (or the NCSC) are of the view that public awareness about the incident is necessary to prevent and/or manage it, or such awareness is in the public interest, we (or the NCSC) may inform the public about the incident or direct you to do so. However, we will consult with you before taking such a decision.

How do we complete this form?

You should complete and submit this form as soon as possible once an incident has occurred. NIS requires you to notify us without undue delay and no later than 72 hours of becoming aware of an incident. You should provide as much detail as you can, based on the information available to you at the time you notify.

If you don't know the answer to a question, or you are waiting on the completion of an internal investigation, please tell us. In addition to completing the form below, we welcome other relevant supporting information, eg incident or third party forensic reports.

Before completing this form, you should read the section of our Guide to NIS on incident reporting.

You must complete all fields marked with an asterisk (*) where you have information that allows you to do so.

Section A: Your contact details

* Your name:

* Your role in the RDSP:

* Work phone:

* E-mail Address:

Other useful contact information:

Section B: Your digital service details

* Name of your digital service:

* Address of your head office (or UK nominated representative, if applicable):

* Your digital service type:

- Online search engine ☐
- Online marketplace ☐
- Cloud computing service ☐
- Multiple digital services (please specify):

Internal incident ID number or name (if applicable):

* Companies House Registration number:

Section C: Nature of the incident

* Date and time the NIS incident occurred:
* Duration of the NIS incident:
* Type of incident:
  - ☐ Cyber (if so, please also complete Section H)
  - ☐ Non-cyber (if so, please also complete Section I)
  - ☐ Both (if so, please also complete Sections H and I)
* Brief description of the incident:
* Have you identified the root cause of the incident?
  - ☐ Yes ☐ No
* If yes, please describe the cause:
* How did you discover the incident?
* What is the current status of the incident?
  - ☐ Ongoing
  - ☐ Ended
  - ☐ Ongoing but managed
* Please describe the network and information systems affected by the incident and outline the high level function of such systems:

Section D: Impact of the incident

Please refer to the incident notification section of the Guide to NIS, as well as the DSP Regulation, if you are uncertain how to complete this section.

* Number of users affected:
* Geographical area affected:
* Extent of the disruption to the functioning of your service:
* Extent of the impact on economic and societal activities:
* Number of user hours your service was unavailable:

* Has the incident resulted in a loss of integrity, authenticity or confidentiality of stored, transmitted or processed data?

☐ Yes ☐ No

If yes, please specify:

If yes, how many users were affected by this loss?

* Has the incident created a risk to public safety, public security or loss of life?

☐ Yes ☐ No

If yes, please specify:

* Has the incident caused material damage to at least one user in the EU, where such damage exceeds €1 million?

☐ Yes ☐ No

If yes, please specify:

* Do any operators of essential services rely upon your digital service?

☐ Yes ☐ No

If yes, please specify:

* Did the incident have a significant impact on the continuity of the essential service(s)?

☐ Yes ☐ No

If yes, please provide a description of the impact:

* Please describe the actions already taken to mitigate the impact of the incident:

* Please outline any additional steps you intend to take:

Section E: Cross-border incidents

You only need to complete this section if the incident affected users in two or more EU Member States.

* Do you operate in two or more Member States?

☐ Yes ☐ No

Please specify:

* Has the incident had a significant impact on services in another Member State?

☐ Yes ☐ No ☐ Unknown at time of notification

If yes, please describe the impact:

Section F: Personal data

* Did the incident result in, or lead to, a personal data breach?

☐ Yes ☐ No ☐ Unknown at time of notification

* If yes, please provide a brief description:

* If yes, have you reported this as a personal data breach under the GDPR?

☐ Yes ☐ No

Section G: Other agencies and external support

* Have you notified the NCSC of the incident?

☐ Yes ☐ No

* If yes, have you requested the NCSC's support to manage the incident?

☐ Yes ☐ No

* Please describe any other external support you have in place:

* Have you notified any other agencies (eg, National Crime Agency, etc.)?

☐ Yes ☐ No

* If the incident was attributable to a malicious actor, has a suspected perpetrator been identified?

☐ Yes ☐ No

* If yes, please provide additional details about the type of perpetrator:

Section H: Additional information – cyber incidents

NIS requires you to provide any other information that may be useful to us in our investigation. Please complete as much of this section as possible.

* Classification of the incident (please indicate all that apply):

- ☐ Denial of service attack
- ☐ Malware: malware distribution via email (including phishing)
- ☐ Malware: malware distribution via websites
- ☐ Malware: malware infiltration via mobile devices and/or USB media
- ☐ Malware: malware intrusion via network infiltration
- ☐ Malware: malware distribution over other or unknown infection vector (if other, please specify):
- ☐ Malware: ransomware infection
- ☐ Malware: Trojans
- ☐ Man-in-the-Middle attack
- ☐ Identity theft: phishing
- ☐ Identify theft: spoofing
- ☐ Identify theft: pharming
- ☐ Identify theft: other – please specify:
- ☐ Hacking: injection attack
- ☐ Hacking: security misconfiguration
- ☐ Hacking: broken authentication
- ☐ Hacking: other – please specify:
- ☐ Exploitation of a known vulnerability or vulnerabilities in components, services and/or applications (please provide an appropriate reference, eg CVE number):
- ☐ Cryptographic flaw
- ☐ Software malfunction
- ☐ Interference with hardware
- ☐ Hardware malfunction
- ☐ Physical damage
- ☐ Loss or theft of equipment
- ☐ Other (please specify):

Section I: Additional information – non-cyber incidents

NIS requires you to provide any other information that may be useful to us in our investigation. Please complete as much of this section as possible.

* Classification of the incident (please indicate all that apply):

- ☐ Flood
- ☐ Fire
- ☐ Equipment failure
- ☐ Power failure
- ☐ Human error
- ☐ Criminal Damage
- ☐ Natural disaster – please specify:
- ☐ Other – please specify:

Section J: Any other relevant information

If you have any further information that would be useful to us, please provide it here:

Next steps

Sending this form

Please send your completed form to casework@ico.org.uk, with 'NIS incident notification form' in the subject field. Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

When we receive this form, we will contact you within seven calendar days to provide:

- a case reference number; and
- information about our next steps.

If you need any help in completing this form, please contact our helpline on 0303 123 1113 (operates 9am to 5pm Monday to Friday).

BILAGA 2 Incidentrapportering Tyskland

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

Meldeformular

nach § 8b Absatz 4 BSIG

0. Allgemeine Informationen zum Meldenden

0.1	Name des meldenden Unternehmens bzw. der meldenden GÜAS	Trinkwasser-Mustergewinnungswerk
0.2	Betroffene Anlage (Kritische Infrastruktur gemäß BSI-KritisV) (Name und Ort)	Trinkwasser-Mustergewinnungswerk, Musterstadt
0.3	Name des Ansprechpartners für technischen Rückfragen	Frau Erika Mustermann
0.4	Kontaktdaten des Ansprechpartners (E-Mail, Telefonnummer)	e.mustermann@twgw.muster, Tel.: 0000 – 99 99-9099
	Die nachfolgenden Informationen sind bereits erfasst unter der Registrierungsnr.: (dann kein Ausfüllen der Felder 0.5-0.10 notwendig)	
0.5	Name des Hauptansprechpartners (Kontaktstelle gemäß § 8b (3) BSIG)	Herr Max Mustermann
0.6	E-Mail	it-sig@twgw.muster
0.7	Telefon (Festnetz)	0000 – 99 99 9090
0.8	Telefon (Mobil)	0000 – 99 99 999
0.9	Fax	0000 – 99 99 9091
0.10	Notfallkommunikationssysteme (z.B. Satellitentelefon)	

1. Allgemeine Informationen zum Vorfall

1.1	Meldungsart (Mehrfachnennungen möglich)	☐ Freiwillige Mitteilung ohne gesetzliche Verpflichtung ☒ Erstmeldung gemäß gesetzlicher Verpflichtung BSIG §8b (4) ☐ Folgemeldung zu IT-Störungsnummer: ☐ Abschlussmeldung zu IT-Störungsnummer:
1.2	Wie ist Ihre **aktuelle** Lageeinschätzung?	☐ Rot (Ausfall der kritischen Versorgungsdienstleistung auf lokaler, regionaler, nationaler Ebene erwartet bzw. eingetreten) ☒ Orange (Beeinträchtigung der kritischen Versorgungsdienstleistung bis hin zum Notbetrieb erwartet bzw. eingetreten) ☐ Gelb (Verstärkte Auffälligkeiten in der Kritischen Informationsinfrastruktur, aber keine Beeinträchtigung der Versorgungsdienstleistung eingetreten, oder es werden nur geringe Beeinträchtigungen erwartet) ☐ Grau (Keine Auffälligkeiten in der Kritischen Informationsinfrastruktur)
1.3	Zeitpunkt des letzten in die Meldung eingeflossenen Sachstands (Datum, Uhrzeit)	01.04.2016, 13:37 Uhr
1.4	Betroffener Sektor bzw. betroffene Branche	

Energie
- ☐ Elektrizität
- ☐ Gas
- ☐ Mineralöl

Ernährung
- ☐ Ernährungswirtschaft
- ☐ Lebensmittelhandel

Finanz- und Versicherungswesen
- ☐ Banken
- ☐ Börsen
- ☐ Versicherungen
- ☐ Finanzdienstleister

Wasser
- ☒ Öffentliche Wasserversorgung
- ☐ Öffentliche Abwasserbeseitigung

Informationstechnik und Telekommunikation
- ☐ Informationstechnik
- ☐ Telekommunikation

Gesundheit
- ☐ Medizinische Versorgung
- ☐ Arzneimittel und Impfstoffe
- ☐ Labore

Transport und Verkehr
- ☐ Luftfahrt
- ☐ Seeschifffahrt
- ☐ Binnenschifffahrt
- ☐ Schienenverkehr
- ☐ Straßenverkehr
- ☐ Logistik

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

1.5	Welche kritischen Dienstleistungen gem. BSI-KritisV sind betroffen?	Trinkwasserversorgung
	Welche Anlagentypen gem. BSI-KritisV sind betroffen bzw. könnten betroffen sein? (Nummer und Anlagenbezeichnung)	Gewinnungsanlage

2. Beschreibung der IT-Störung

2.1	Welche Grundwerte der Informationssicherheit wurden verletzt? (Mehrfachnennungen möglich)	☒ Verfügbarkeit ☒ Integrität ☐ Authentizität ☐ Vertraulichkeit
2.2	Auf welchem/r IT-System / IT-Prozess / IT-Komponente ist was aufgetreten? (Kurzbeschreibung)	Fehlfunktion und Abstürze der PC-gestützten Pumpensteuerung
2.3	Wie ist es aufgetreten?	Konfigurationsdateien des Programms zur Pumpsteuerung wurden von Locky verschlüsselt
2.4	Welche (erfolgreichen) Gegenmaßnahmen wurden eingeleitet?	Locky wurde vom PC entfernt, Neuinstallation beauftragt
2.5	Datum und Zeit, an dem die IT-Störung eingetreten ist	31.03.2016 20:00 Uhr
2.6	Datum und Zeit, an dem die IT-Störung entdeckt wurde	01.04.2016 08:00 Uhr
2.7	Die IT-Störung hält noch an	☒ Ja ☐ Nein – Dauer (dd:hh:mm):
2.8	Wie ist die IT-Störung aufgefallen? (Mehrfachnennungen möglich)	
	☒ Systemausfall ☒ Fehlverhalten von Systemen ☐ Auswertung von Logfiles ☐ Systemwartung ☐ Technisches (Netz-)Monitoring ☐ Testbetrieb ☐ Hinweise von Dritten ☐ Veröffentlichung von gestohlenen Informationen durch Dritte ☐ Audit, Prüfung, Zertifizierung ☐ Hinweise des BSI ☐ Sonstiges:	

3. Vermutete oder tatsächliche Ursachen

3.1	Physikalischer Schaden (Mehrfachnennungen möglich)	☐ Zerstörung von Geräten ☐ Diebstahl von Geräten ☐ Manipulation von Geräten ☐ Verlust von Geräten ☐ Sonstiges:
3.2	Technisches Versagen (Mehrfachnennungen möglich)	☐ Versagen der Hardware ☐ Überlastung ☐ Software fehlerhaft ☐ Fehlverhalten von Systemen ☐ Sonstiges:
3.3	Organisatorische Ursache (Mehrfachnennungen möglich)	☐ Fehlbedienung ☐ Unautorisierte Nutzung von Ressourcen ☐ Social Engineering ☐ Sonstiges:
3.4	Versagen der genutzten Infrastruktur (Mehrfachnennungen möglich)	☐ Stromausfall ☐ Netzwerkausfall ☐ Kühlungsausfall ☐ Sonstiges:

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

3.5	Technischer Angriff (Mehrfachnennungen möglich)		
	Ausnutzung von Schwachstellen ☐ Nutzung von Systemressourcen (Spam-Relay, Botnetz-Client, C&C-Server, Dropzone-Server) ☐ Code Execution ☐ Protokollschwachstelle ☐ Privilege Escalation ☐ Injection-Angriff ☐ Cross-Site-Scripting ☐ Cross-Site-Request-Forgery ☐ Schwache Algorithmen/Schlüssel ☐ Sonstiges:	**Hacking und Manipulationen** ☐ Webanwendungsbasierte Angriffe, z.B. Drive-by-Exploits ☐ Angriffe auf Webanwendungen, z.B. SQL-Injection, Buffer Overflow ☐ Angriffe auf Anwendungen bzw. Dienste wie DNS, SMTP, FTP ☐ Systematisches Ausprobieren von Passwörtern ☐ Sonstiges:	**Schadprogramme (Malware)** ☒ Malware-Infektion, z.B. durch Trojaner, Rootkits zum Zwecke der Kontrollübernahme, der Datenmanipulation oder des Datenabflusses ☒ Ransomware z.B. Sperren von IT-Systemen zu Erpressungszwecken ☐ Adware, Scareware z.B. zu Betrugszwecken ☐ Multifunktionale Malware z.B. Viren, Würmer, Riskware ☐ Sonstiges:
	Gezielte, mehrstufige kombinierte Angriffe (APT-Angriffe) ☒ Initialer Angriff per E-Mail ☒ Initialer Angriff über Webseiten (Watering hole attack) ☒ Initialer Angriff über manipulierte Hardware (z.B. USB-Stick) ☐ Sonstiges:	**Missbrauch (Innentäter)** ☐ Weitergabe interner Informationen ☐ Unberechtigtes Erlangen von besonderen Zugriffsrechten, z.B. von Administrationsrechten ☐ Missbräuchliche Nutzung von Berechtigungen (insb. von Zugriffsrechten), z.B. durch Externe über Fernwartungszugänge ☐ Sonstiges:	**Identitätsmissbrauch** ☐ Verschleierung einer Identität ☐ Diebstahl von Zugangsdaten, z.B. Identitätsdiebstahl, Phishing, Spear-Phishing, Pharming, Skimming ☐ Diebstahl oder Fälschung von Zertifikaten ☐ Unrechtmäßige Registrierung von Internetdomänen (Cybersquatting) ☐ Sonstiges:
	Verhinderung von Diensten ☐ Überflutung, z.B. (D)DoS ☐ Gezielter Systemabsturz, z.B. Paketfragmentierung ☐ Sonstiges:		**Sonstiges:**
3.6*	Sonstiges (z. B. CVE, Name der Schadsoftware, weitergehende Informationen, ...)	Locky	

4. Allgemeine Informationen zum informationstechnischen Angriff

☐	Es handelt sich **nicht** um einen informationstechnischen Angriff (dann kein Ausfüllen der Felder 4.1-4.5 notwendig)	
4.1	Angriffsart	☐ Gezielter Angriff ☐ Ungerichteter Angriff ☒ Unbekannt
4.2	Bei mehrfachen Angriffen bitte vermutete Anzahl angeben	
4.3*	Vermutete Motivation (Mehrfachnennungen möglich)	☒ Unbekannt ☒ Finanziell ☐ Persönlich ☐ Politisch ☒ Kriminell ☐ Terroristischer Hintergrund (Pflicht für das BSI zur Weitergabe der Meldung an BKA) ☐ Nachrichtendienstlicher Hintergrund (Pflicht für das BSI zur Weitergabe der Meldung an BfV) ☐ Sonstiges:
4.4	Welche Daten sind im Rahmen der bisherigen Analyse der IT-Störung angefallen und können dem BSI zur Verfügung gestellt werden? (Mehrfachnennungen möglich)	☐ Malware-Samples ☐ Hashsummen ☐ Dateinamen ☐ Signaturen ☐ Logfiles ☐ IP-Adressen ☐ URLs ☒ Sonstiges: Keine / unbekannt / Administratoren untersuchen noch
4.5	Strafverfolgung Wenn eine Strafanzeige gestellt wurde und Sie eine Weiterleitung an das BKA wünschen, ergänzen Sie bitte die entsprechenden Detailangaben.	☒ Unbekannt / keine Angabe ☐ Es wurde keine Strafanzeige gestellt ☐ Strafanzeige wurde gestellt Aktenzeichen: Polizeidienststelle: Bundesland: ☐ Weiterleitung der Meldung an BKA durch BSI ist erwünscht ☐ Täter wurde ermittelt

* Freiwillige Angabe

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

5. Informationen zum Ausfall bzw. zur Beeinträchtigung der kritischen Dienstleistungen

5.1	Hat die IT-Störung zu einem Ausfall oder zu einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen) geführt? **Wenn nein**: Welche Umstände oder Gegenmaßnahmen führen dazu, dass es nicht zu einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur kommt? (Bsp.: Unabhängige Parallelversorgung, Angreifer wurde vorher aufgehalten, etc.)	☐ Ja, zu einem Ausfall ☒ Ja, zu einer Beeinträchtigung ☐ Nein (dann kein Ausfüllen der Felder 5.6 bis 5.8 notwendig)
5.2	Inwiefern ist die Funktionsfähigkeit der Kritischen Infrastruktur (also die Verfügbarkeit der kritischen Dienstleistungen) beeinträchtigt bzw. **könnte** sie beeinträchtigt werden? (u.a. welche Systeme und Komponenten sind betroffen bzw. könnten betroffen sein?)	Die Wasserpumpe „Mustermündung“ arbeitet unregelmäßig und liefert nur noch einen Bruchteil der im Normalbetrieb gewonnenen Wassermenge.
5.3	Wie viele Personen könnten Ihres Wissens von der Beeinträchtigung / dem Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur betroffen sein?	☐ < 250.000 Einwohner (bzw. < 50% der in der BSI-KritisV **für Ihre Anlage angegebenen Schwelle**) ☒ 250.000 bis 500.000 (bzw. 50% bis 100%) ☐ 500.000 bis 1.000.000 (bzw. 100% bis 200%) ☐ 1.000.000 bis 5.000.000 (bzw. 200% bis 1000%) ☐ > 5.000.000 Einwohner (bzw. > 1000%) ☐ Es kann keine Aussage gemacht werden
5.4	Wie ist die (potentielle) geographische Verbreitung der Beeinträchtigung / des Ausfalls der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen)? (Stadt, Region, Landkreis, Bundesland, Bundesgebiet)	Musterstadt und umliegender Kreis
5.5	Ist der Vorfall (potentiell) grenzüberschreitend? **Wenn ja:** Welche Staaten sind / wären ebenfalls betroffen?	☐ Ja ☒ Nein
5.6	Von wann bis wann bestand die Beeinträchtigung / der Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen)?	Von ca. (TT.MM.JJJJ hh:mm): Bis ca. (TT.MM.JJJJ hh:mm): ☒ Auswirkung dauert an
5.7	Wann wurde die Beeinträchtigung / der Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistungen) festgestellt?	Am (ca.) (TT.MM.JJJJ hh:mm): 01.04.2016 08:00
5.8	Welche Maßnahmen wurden ergriffen, um die Beeinträchtigung/den Ausfall der Funktionsfähigkeit der Kritischen Infrastruktur (also der kritischen Dienstleistung) zu mindern oder zu beheben?	Suche nach Original-Konfigurationsdateien

6. Sonstiges

6.1*	Weiterführende Informationen	
6.2*	Weiterführende Bewertungen	
6.3*	Weiteres	

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se