Cybersecurity en digitale weerbaarheid

Het wettelijke kader

Adriaan Hagdorn / NS
19 januari 2022

Europese kader

- Richtlijn beveiliging netwerk- en informatiesystemen (*NIB-richtlijn*)
  - Hoog en geharmoniseerd niveau beveiliging netwerk- en informatiesystemen in EU
  - Bevordering weerbaarheid en continuïteit
  - Goede werking Europese markt
- Europese cyberbeveiligingsverordening (*Cybersecurity Act*)
  - Grondslag Agentschap EU voor cyberbeveiliging (ENISA)
  - Waarborgen werking (continuïteit) Europese markt door hoog cyberbeveiligingsniveau
  - Bewustwording, advies, expertise, coördinatie, cyberbeveiligingscertificering

    zie www.enisa.europa.eu
- Algemene verordening gegevensbescherming (*AVG-verordening*) -

  Bescherming persoonsgegevens
  - Meldplicht (o.a. bij datalek)
  - Toezicht (in NL de Autoriteit persoonsgegevens (AP))

Beleidsmatige aspecten NL

- Beheer van hoofdspoorweginfrastructuur en personen- en goederenvervoer daarover zijn in maart 2021 aangemerkt als een voor de continuïteit *vitaal proces* (“Vitaal-B”) en daarmee als “*vitale infrastructuur*” in NL

- Op 21 juli 2021 publiceerde IenW de *Roadmap Vitaal Spoor* om de weerbaarheid te vergroten, met aanbevelingen voor IenW en spoorsector

  NB: betreft niet alleen cyber maar ook terrorisme, klimaat en pandemieën e.d.

- IenW maakte een “*Vitaliteitsbeoordeling”* wie Aanbieder van een Essentiële Dienst (AED) in de zin van de Wet beveiliging netwerk- en informatie-systemen (Wbni) zouden moeten worden

Nederlands kader: gelaagde opbouw

- Wet beveiliging netwerk- en informatiesystemen (Wbni)
  - Implementatie NIB-richtlijn (zorgplichten, meldplicht en toezicht)

- Besluit beveiliging netwerk- en informatiesystemen (Bbni)
  - Benoemen van de sectoren waarop Wbni van toepassing is (waaronder vervoer)

- Regeling beveiliging netwerk- en informatiesystemen (Rbni)
  - Generieke normen, meer op detailnivo
  - Risicobeheer op basis van een informatie security systeem

- Sectorale technische standaarden
  - Privaat karakter

Wbni enBbni

- Wbni is van toepassing op

(i) *digitale dienstverleners* (online marktplaatsen en zoekmachines, cloudcomputerdiensten)

(ii) *aanbieders van essentiële diensten (AED's)*

- energie (netbeheerders, gastransport, NAM)
- vervoer (lucht, water, weg en hoofdspoor)
- bankwezen
- drinkwaterbedrijven
- digitale infrastructuur (o.a. aanbieders van internetknooppunten)

(iii) *andere vitale aanbieders*

- nucleaire sector
- waterbeheer en -keringen Rijkswaterstaat
- financiële en elektronische communicatienetwerken en –diensten (> 1 miljoen eindgebruikers)

Wbni

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

- De minister van JenV (NCSC)

  - Wijst Aanbieders van Essentiële Diensten (AED's) aan (ook minister van IenW doet dat)
  - Is contactpunt voor nationale *Cyber Security Incident Response Teams* (SCIRT's)
  - Is SCIRT voor AED's
  - Verstrekt informatie over dreigingen en incidenten aan o.a. AED's
  - Is instantie voor (vrijwillige) melding van ernstige incidenten
  - Verleent bijstand bij treffen van maatregelen om continuïteit te borgen of te herstellen
  - Monitort toepassing NIB-richtlijn
  - Verricht analyses en doet technisch onderzoek naar dreigingen
  - Stelt Nationale Cybersecurity Strategie vast
  - Is nationaal contactpunt voor grensoverschrijdende samenwerking

Wbni

- Een AED
  - *Ontvangt dreigings- en incidentinformatie* van het NCSC
  - Heeft *recht op bijstand* van het NCSC
  - Neemt *passende en evenredige, organisatorische en technische maatregelen* om
    a) zijn IT-systemen (hard- en software en de data) te beschermen o.b.v. dreigings- en risicoanalyse en
    b) gevolgen incidenten te beperken (*dubbele zorgplicht*)
  - Heeft een Informatie Security Managementsysteem (ISMS)
  - Moet ernstige IT-incidenten melden aan NCSC/SCIRT en eventueel aan AP (*meldplicht)*
  - Is onderworpen aan *toezicht* (audit, aanwijzing, boete)

    NB: bij transport en drinkwater houdt ILenT toezicht
- Ook transport (weg, water, lucht en hoofdspoor) valt onder Wbni
- Aanwijzing ProRail, NS en regionale personenvervoerders als AED
  - Goederenvervoerders van gevaarlijke stoffen uitsluitend “vitaal”
  - Stadsvervoerders?

Nederlands kader (Rbni)

- AED heeft Informatie Security Management Systeem (ISMS) met - Verbetercyclus
  - Beschrijving interne organisatie
  - Beschrijving netwerk- en informatiesystemen
  - Maatregelen ter voorkoming van cyberincidenten (patchmanagement, back-ups, fysiek beveiligingsbeleid)
  - Wijze van detectie, melden, loggen en response
  - Herstelbeleid (continuïteitsplannen en back-ups)

Sectorale technische standaarden

- Onder meer ISO-2700x- en ISA/IEC 62443x-standaarden
- Zie ENISA-rapport *Railway Security*, *Good practices in cyber risk management (*november 2021)
- Eigen bedrijfsstandaarden

Advies Cyber Security Raad

CSR adviseert € 833 miljoen extra voor integrale aanpak cyberweerbaarheid

Verbeter regie overheid op samenwerking en informatiedeling. Kom tot één nationale strategie

Extra aandacht en steun voor vitale processen

Versterken handhavingsketen cybercrime

Verhoog kennispositie

Nieuwsbericht | 06-04-2021 | 15:21

Onderzoeksraad voor Veiligheid

- OvV-rapport *Kwetsbaar door software. Lessen n.a.v. beveiligings-lekken door software van Citrix*, 16 december 2021

Nederlandse overheidsorganisaties en bedrijven zijn zeer kwetsbaar voor cyberaanvallen en er is geen nationale structuur waarbinnen alle potentiële slachtoffers van cyberaanvallen tijdig worden gewaarschuwd

- Belangrijkste aanbevelingen aan:

Kabinet:
- Waarschuw tijdig alle potentiële slachtoffers van cyberaanvallen
- Verplicht alle organisaties verantwoording af te leggen hoe zij risico's beheersen

EC:
- Leg verantwoordelijkheid fabrikanten vast in een Europese verordening (wet)

Fabrikanten van software:
- Ontwikkel *good practices* om software veiliger te maken
- Waarschuw en help afnemers als kwetsbaarheden gesignaleerd worden

Ministers van BZK en EZK:
- Initieer en bevorder dat organisaties en consumenten veiligheidseisen formuleren en afdwingen bij softwarefabrikanten

Nieuwe regelgeving (nationaal)

- Voorstel Wet bevordering digitale weerbaarheid bedrijven
  - grotere rol van minister van EZK
  - alle bedrijven (dus ook niet-vitale) krijgen dreigings- en incidentinformatie van NCSC

- Voorstel aanpassing Wbni
  - ook andere partijen (aanbieders) krijgen dreigings- en incidentinformatie

NB: Zijn ambtelijke concepten die zomer 2021 werden geconsulteerd Zie www.overheid.nl/gesloten internetconsultaties

Nieuwe Europese regelgeving

- December 2020: EC lanceert *EU Cybersecurity Strategy for the Digital Decade*
- Nieuwe NIB 2-richtlijn om cyberweerbaarheid in EU verder te verhogen
- Wijzigingen:
  - onderscheid *essentiële* (o.a. transport) en *belangrijke sectoren*
  - ook ziekenhuizen, post- en koeriersdiensten, food, chemie, data centres, openbaar bestuur maakindustrie (o.a. computer, elektronisch, machines etc.), space en grotere bedrijven vallen er onder. Voor spoor: ook *exploitanten van dienstvoorzieningen*
  - aanmoediging gebruik gestandaardiseerde beveiligingsnormen
  - certificeringsverplichting voor “essentiële entiteiten”
  - kwetsbaarhedenregister
  - ketenbenadering (*supply chain*)
  - verscherping en harmonisering meldplichten
  - verscherping toezicht (o.a. boetes, persoonlijke aansprakelijkheid topbestuurders en mogelijkheid van toezicht vooraf)
- Aanvaard door de Raad. Nu trilogues EC, Raad en EP

Conclusies (1)

- Cybersecurity is een “*chefsache*”. Iedere organisatie - of die nou AED is of niet - moet er mee aan de slag

- Dat betekent voortdurend – van dag tot dag - vaststellen
  (i) welke IT-systemen en data (extra) bescherming behoeven en
  (ii) wat een adequate beveiligingsstandaard is om incidenten, gelet op
  - te verwachten risico’s, zoveel als mogelijk te voorkomen en
  - als het gebeurt, de gevolgen daarvan zoveel mogelijk te beperken

- Het ISMS geeft voor AED’s wettelijk verplichte handvatten maar kan uiteraard door iedere partij vrijwillig worden toegepast

Conclusies (2)

- In de logistieke en vervoerketen wordt voortdurend data uitgewisseld. Omdat de ketting zo sterk is als de zwakste schakel en cyber(dreigings)ontwikkelingen snel gaan, is voortdurende samenwerking en afstemming noodzakelijk
- Bepaal sectorbreed, met de spoorindustrie en softwareleveranciers, *good practices* en beveiligingsstandaarden. Actualiseer deze voortdurend
- Voor nationaal en internationaal spoorvervoer gebeurt dat in CSIRT's, ENISA en andere organisaties, zoals de CER, ERA, UIC en EIM

  NB: al dit overleg vergt op zichzelf óók afstemming
- Afstemming en uitwerking met IenW o.b.v. aanbevelingen *Roadmap Vitaal Spoor*
- Gelet op de ontwikkelingen op het gebied van wetgeving en het OvV-rapport, mag worden verwacht dat op termijn meer partijen dan AED's door NCSC worden voorzien van dreigings- en incidentinformatie

Dank voor uw aandacht!

Vragen?

Adriaan Hagdorn / NS Legal
adriaan.hagdorn@ns.nl
06 55743900