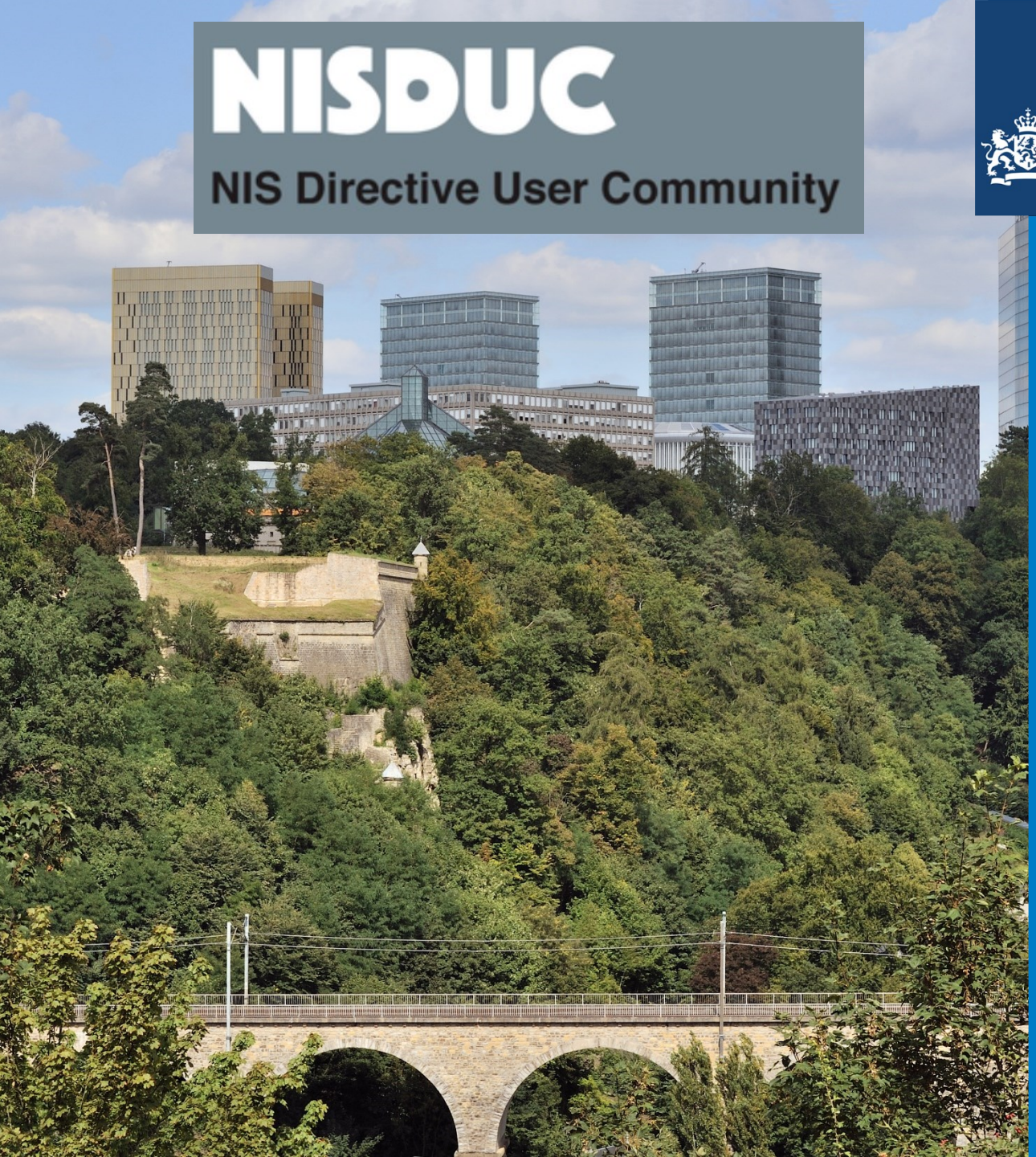


Case study workshop DSP Supervision

Best practices and lessons learnt

Rob Augustinus

Radiocommunications Agency Netherlands

10 May 2022

Agenda

1. Introduction
2. DSP Supervision
3. DSP Incident cases
4. Learnings & Conclusions

Rob Augustinus
Inspector Specialist
Radiocommunications Agency
(Agentschap Telecom)

Responsible for assessing cybersecurity preparedness and capabilities of:

Operators of Essential Digital Infrastructure Services (OES)

Digital Service Providers (DSPs)

Radiocommunications Agency Netherlands

The Radiocommunications Agency Netherlands implements the laws and regulations for the following areas:

- Digital Infrastructure (NIS)
- Digital Trust Services (eIDAS)
- Telecommunications (EECC)
- Frequency space
- Excavation works
- Space activity registration & licenses

Making sure that everyone complies with the rules, requirements and conditions

+400 employees:
Offices in Groningen and Amersfoort

NIS/Wbni Supervision

Energy sector

- Transport and distribution electricity
- Production, transport and distribution gas
- Oil reserve
- Electricity Production

Digital Infrastructure

- Internet Exchanges
- Top Level Domain - DNS

Digital Service providers (DSPs)

- Cloud services
- Online Market places
- Online Search Engines

EU/NL DSP legislation

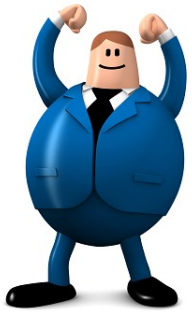
EU NIS Directive:
The Directive on security of network and information systems (NIS)

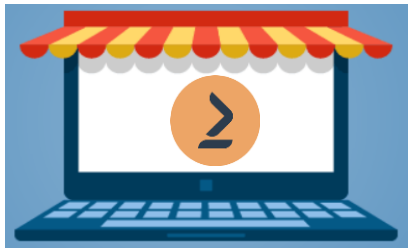
Wbni: Dutch transposition of the NIS directive

IMPLEMENTING REGULATION (EU) 2018/151:
Security measures and incident thresholds for DSPs
(overrules national DSP legislation)

DSP Supervision in NL

+/- 1000 DSPs in The Netherlands



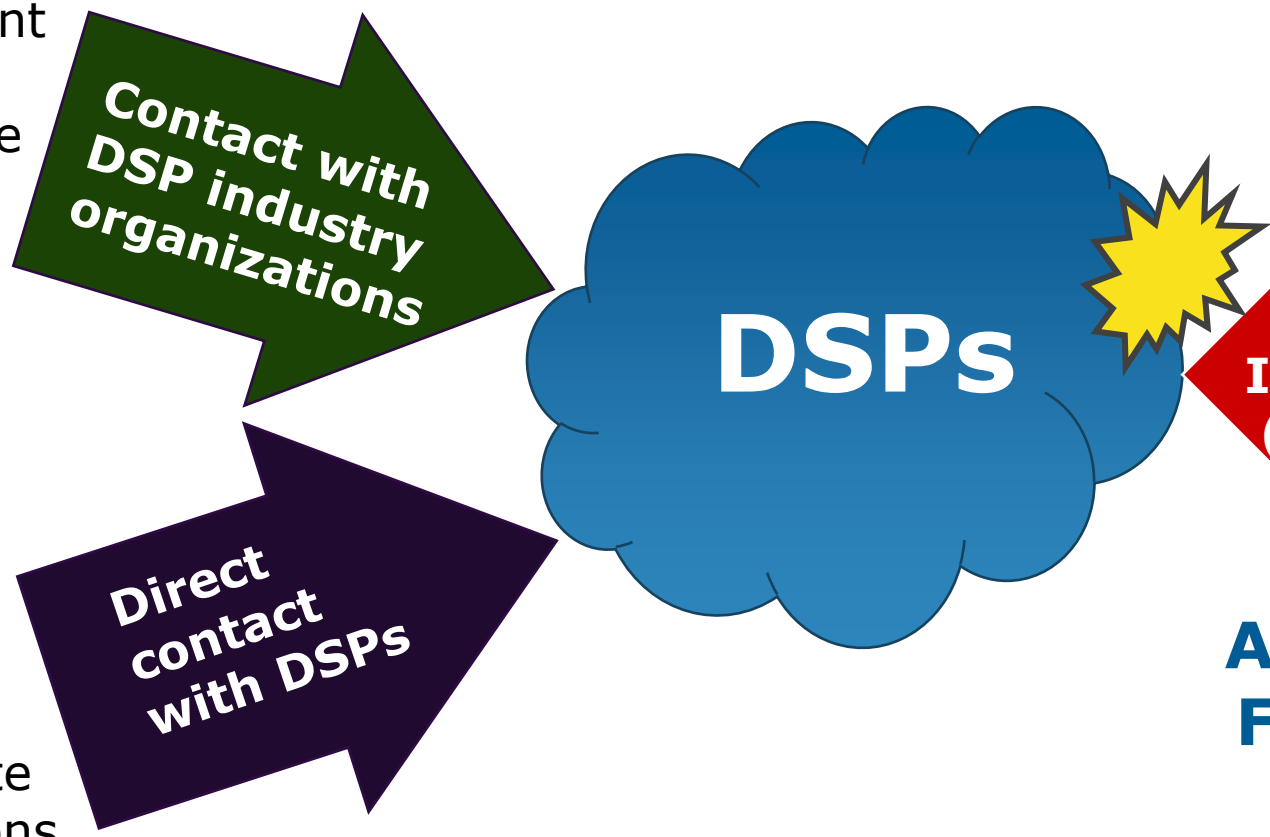


Dutch Cloud Community

Startpagina

Ex-Post DSP Supervision

- Online DSP Self Assessment
- Feedback
- Knowledge sharing



- Incidents notified by DSPs
- Incidents reported in the Media
- Requests from other authorities (EU/NL)

Assessment Framework

- Events
- AT website
- Publications
- Wbni@agentschaptelecom.nl

DSP Incident Investigations – Methodology & Process

Incident Investigation Assessment Framework: ISO 27001

Assessed Control Objectives:

6.1 Risk Management

A.16 Infosec Incident Management

A.17 Business Continuity Management

(Other control objectives may be assessed if applicable)

Data Collection
- Interviews, Evidence gathering

Data Analysis
- Evaluate Controls, Identify findings

Corrective Actions
- Present and discuss findings with DSP, identify corrective actions

Reporting
- Draft report, Review (by lead auditor and DSP), Final report

Follow up
- Check follow up of corrective actions with DSP

Nieuws

Patiëntendossiers door ddos-aanval op clouddienst urenlang onbereikbaar

donderdag 21 april 2022, 12:06 door **Redactie**, 3 **reacties**

Zorgmedewerkers van een niet nader genoemde zorginstelling konden elektronische dossiers van patiënten urenlang niet raadplegen door een ddos-aanval op de clouddienst waar de dossiers waren opgeslagen, wat mogelijk risico voor het verlies van mensenlevens had kunnen hebben. Dat meldt het Agentschap Telecom in het vandaag verschenen **jaarbericht 2021**.

Het Agentschap Telecom houdt in het kader van de Wet Beveiliging Netwerk en Informatiesystemen (Wbni) toezicht op digitale dienstverleners (DSP's). In Nederland is de grootste groep binnen deze sector die van de clouddienstverleners. De overige groep bestaat voornamelijk uit online marktplaatsen. Het afgelopen jaar voerde de toezichthouder bij een aantal DSP's inspecties uit, onder andere naar aanleiding van incidenten waarbij diensten werden verleend aan de zorgsector.

"Een elektronisch patiëntendossier, ondergebracht bij de clouddienst, kon een aantal uren niet worden geraadpleegd door zorgmedewerkers. De verstoring van de clouddienst door een DDoS-aanval had, zoals dat heet, aanzienlijke gevolgen vanwege een mogelijk risico voor het verlies van mensenlevens. Dit was een constatering op basis van een criterium in de Europese regelgeving. Dit was een directe aanleiding voor ons om een incidentinspectie te starten", zo laat het Agentschap Telecom weten.

Bij de verschillende inspecties zijn meerdere problemen geconstateerd die inmiddels door de betreffende clouddienstverleners zijn opgelost. Het Agentschap Telecom zal meer algemene oorzaken en geconstateerde punten met de sector clouddienstverleners delen, zodat die waar nodig verbeteringen kunnen doorvoeren. Met de inspecties wil de toezichthouder naar eigen zeggen de digitale weerbaarheid van digitale dienstverleners verhogen.

Workshop: Cloud incident cases Discussions & Questions

- 2 cases of multiple hours cloud service outages caused by DDoS attacks
- Cloud Services for Health service organizations and Police & Emergency services
- Incidents happened in March and July 2021
- Both incidents investigated by Agentschap Telecom

Which clause of article 4 of DSP implementing regulation 2018 /151 is applicable?

Article 4

Substantial impact of an incident

1. An incident shall be considered as having a substantial impact where at least one of the following situations has taken place:

a) the service provided by a digital service provider was unavailable for more than 5 000 000 user-hours whereby the term user-hour refers to the number of affected users in the Union for a duration of 60 minutes;

b) the incident has resulted in a loss of integrity, authenticity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting more than 100 000 users in the Union;

c) the incident has created a risk to public safety, public security or of loss of life;

d) the incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds EUR 1 000 000.

Incident 1 - Impact

- SaaS service for healthcare organizations (Electronic Patient Record System)
- Customers: Nursing, Home Care, Disability care, and Mental healthcare organizations
- Impact: Nurses and health care workers couldn’t access patient’s medication chart, doctors’ notes and comments regarding patient’s status

Incident 1 – Post Mortem

- The ISP of the cloud service provider was targeted by multiple DDoS attacks during a 3-hour time frame
- The DNS servers of the cloud service provider were hosted by this ISP and sometimes, or not at all, available during the attacks
- DNS traffic to the ISP of the cloud service provider was also blackholed by the ISP of some cloud service customers

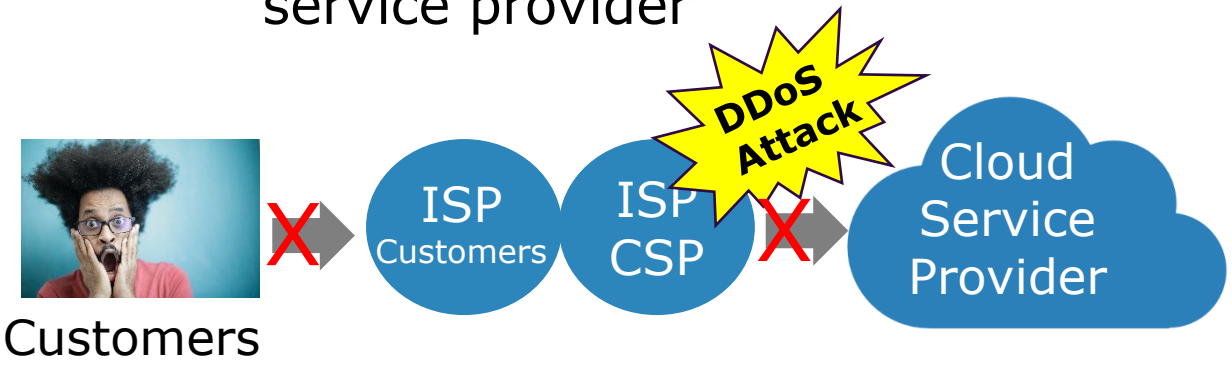
› Who should take corrective actions?

a) The ISP of the cloud service provider

b) The cloud service provider

c) Both the ISP and cloud service provider

d) The customers of the cloud service provider



Which clause of article 4 of DSP implementing regulation 2018 /151 is applicable?

Article 4

Substantial impact of an incident

1. An incident shall be considered as having a substantial impact where at least one of the following situations has taken place:

a) the service provided by a digital service provider was unavailable for more than 5 000 000 user-hours whereby the term user-hour refers to the number of affected users in the Union for a duration of 60 minutes;

b) the incident has resulted in a loss of integrity, authenticity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting more than 100 000 users in the Union;

c) the incident has created a risk to public safety, public security or of loss of life;

d) the incident has caused material damage to at least one user in the Union where the damage caused to that user exceeds EUR 1 000 000.

Incident 2 - Impact

- Cloud workspace and cloud connect services
- Customers: Doctors, Healthcare organizations, Police, Fire Brigades and Ambulance organizations
- Impact: Doctors and health care workers couldn’t access patient’s medication chart, Communication services for Police, Fire Brigades, and Ambulance organizations unavailable

Incident 2 – Post Mortem

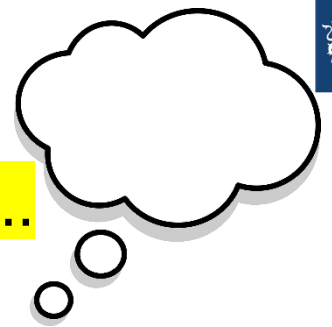
- Who is ultimate responsible that corrective actions are carried out?

a) The ISP of the cloud service provider

b) The cloud service provider

c) Both the ISP and cloud service provider

- 20 minutes DDoS attack on the IP range of the cloud service provider resulted in 2 hours outage
- Traffic to the DNS servers of the cloud service provider was accidentally blocked by the ISP of the cloud service provider
- The ISP of the cloud service provider didn't communicate the blocking of traffic to the cloud service provider



- Some food for thought…
  - Did the cloud service providers take insufficient measures to manage the risk posed to the security of their network and information systems?
  - Do security certifications say anything about compliance to the NIS/Wbni?
  - Do audit reports provide reasonable assurance that cloud service providers are in control of their information security?

Incident 1/2 – Facts

- Both cloud service providers do have a CISO who is responsible for risk management and implementing security controls
- Both cloud service providers have a NEN 7510 Certification for the Dutch Healthcare Sector and an ISO27001 certification
- Both cloud service providers undergo regular third-party audits (ISAE 3402 type II / SOC 2, type II audit reports)


Questions?