NIS Directive and its implications

Zuzana Duračinská • zuzana.duracinska@nic.cz •
06.03.2018, Berlin

CZ DOMAIN
REGISTRY

CZ.NIC

- operation of the domain name registry for the .CZ domain
- Operation of Czech National CSIRT
- Role and duties of National CSIRT are part of national legislation on cyber security
- Operator of National CSIRT have to have **formal agreement** with National Cyber and Information Security Agency

Why NIS (network and information systems) **Directive?**

(1) Network and information systems and services play a vital role in society. Their **reliability and security** are essential to economic and societal activities, and in particular to the functioning of the internal market

(2) The magnitude, frequency and impact of **security incidents** are increasing

What does it bring?

- Definition of new terms in legislation…

  incident, CSIRT, security strategy, digital service providers, essential services

- Obligation for states to transpose the directive…

  until may 2018

- Incident reporting and security measures in place for some operators…

  operators of essential services and digital service providers

What states have to do?

- Define national competent authority and single point of contact
- Designate CSIRT(s)
- Adopt national strategy for network and information systems
- **Identify operators of essential services**

Operators of essential services

- (a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
- (b) the provision of that service depends on network and information systems; and
- (c) an incident would have significant disruptive effects on the provision of that service

Who would that be???

- Energy
- Transport
- Banking
- Financial market infrastructure
- Health sector
- Drinking water supply and distribution
- Digital infrastructure (**IXPs**, DNS service providers, TLD name registries)

IXP

- States will have to identify IXPs while taking into account
- (a) **the number of users** relying on the service provided by the entity concerned;
- (b) the **dependency of other sectors** referred to in Annex II on the service provided by that entity;
- (c) the **impact that incidents could have**, in terms of degree and duration, on economic and societal activities or public safety;
- (d) the **market share** of that entity;
- (e) the **geographic spread** with regard to the area that could be affected by an incident;
- (f) the **importance of the entity** for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

Type of service	Type of subject	Special criteria	Impact criteria
Connecting technically independent networks	An Internet Exchange (IXP) service provider, existing for the purpose of interconnecting networks that are separate from a technical and organizational point of view	(a) Interconnection of more than 50 autonomous networks and an average data stream measured over a five-minute in 24-hour interval is over 50 Gbps.	The impact of a cyber-security incident on an information system or an electronic communications network on which the provision of a service is dependent may cause (i) serious limitation or disruption of the type of service affecting more than **50 000 persons,** ii. severe constraint or disruption of another basic service, or restriction or disruption of the critical infrastructure element, iii. an economic loss of more than **0.25% of GDP**, iv. unavailability of a service type for more than **1 600 people,** which is not substitutable in any other way without incurring unreasonable costs, or v. Disturbance of **public safety** in a significant part of the administrative district of a municipality with extended powers which may require the implementation of the rescue and disposal works of the integrated rescue system.

DIGITAL SERVICES

- Online market place
- Online search engine
- Cloud computing service

- Those will have to identify themselves
- Implementing regulation in place since January 30th 2018 → shall apply from 10 May 2018

Implementing regulation for DSP

- security of network and information systems and of their physical environment (security of supplies, availability of systems…)
- incident handling (detection processes, reporting incidents…)
- business continuity management
- monitoring, auditing and testing

→ all of that have to be documented

Which incidents have to be reported by DSP?

- 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.**

Legislation in Czech republic

- Act on Cyber security
- Initiative to cover critical infrastructure and important system
- Critical infrastructure was identified on mutual agreement between bureau and operator in selected area – energy sector, health-care..
- In effect since 01.01.2015

Implementation of NIS Directive

- NIS is implemented in legislation – effective since 01.08.2017
- Only slight changes to Act of Cybersecurity
- Implementation is lead by National Cyber and Information Security Agency
- New subjects were added to legislation (among others IXs)

Recommendations

- Find out who is responsible for implementing NIS Directive
- See how they define IXPs
- Talk to them about criteria for identifying IXPs
- See what kind of requirements you will have to meet if you'd be identified as operator of essential services

Questions?

- zuzana.duracinska@nic.cz

Co-financed by the European Union
Connecting Europe Facility

cz.nic | CZ DOMAIN REGISTRY