cesnet

KAM KRÁČÍ KYBERBEZPEČNOST?

Jan Kolouch
CESNET

září 2021
Plzeň

cesnet

- Zájmové sdružení právnických osob

VVŠ, SVŠ, AV ČR aj.

https://www.cesnet.cz/sluzby/

- **CESNET-CERTS**

Bezpečnostní tým
Řešení bezpečnostních incidentů + prevence

cesnet

Kyberbezpečnost?

Ajay Grewal • 3. a více
CCIE Security#55637 | CEH
1 týden • Upraveno

InfoSec 1990: You need AntiVirus
InfoSec 1998: You need honeypots
InfoSec 2004: You need DLP
InfoSec 2007: You need IPS/IDS
InfoSec 2010: You need behavior blocking
InfoSec 2013: You need Sandboxing , Threat extraction, emulation
InfoSec 2015: You need ATP/APT
InfoSec 2017: You need machine learning
The entire time: Maybe patch your stuff first? InfoSec: Nah, that's boring.

cesnet

LEGISLATIVA EU

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679

ze dne 27. dubna 2016

o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)

https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679&from=CS

EU SCOPE

https://cclab.com/news-details/european-union-to-regulate-it-security-of-critical-infrastructures/106

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/1148

ze dne 6. července 2016

o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii

https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN

Cyber security act

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2019/881

ze dne 17. dubna 2019

o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“)

https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32019R0881&from=EN

cesnet

NIS2

Proposal for a
DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166

Za tímto účelem návrh Komise rozšiřuje oblast působnosti stávající směrnice o bezpečnosti sítí a informací **přidáním nových odvětví na základě jejich kritičnosti pro hospodářství a společnost a zavedením jasného omezení velikosti** - což znamená, že **budou zahrnuty všechny střední a velké společnosti ve vybraných odvětvích v rozsahu.**

Členským státům zároveň ponechává určitou flexibilitu při identifikaci menších subjektů s vysokým profilem bezpečnostního rizika.

https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

cesnet

DOPAD

Návrh rovněž odstraňuje rozdíl mezi provozovateli základních služeb a poskytovateli digitálních služeb.

Subjekty by byly klasifikovány na základě jejich důležitosti a rozděleny do příslušných a důležitých kategorií, v důsledku čehož by byly podrobeny různým režimům dohledu.

Návrh posiluje požadavky na zabezpečení pro společnosti zavedením přístupu k řízení rizik, který poskytuje minimální seznam základních bezpečnostních prvků, které je třeba použít.

Návrh zavádí přesnější ustanovení o procesu hlášení incidentů, obsahu hlášení a harmonogramu.

Sectors covered by NIS 1	Sectors covered by NIS 2 proposal
"Operators of essential services" category	"Essential entities" category
	All sectors from NIS 1
Healthcare providers	Additional health-related services - including pharma, some medical device manufacturers, researchers
Digital infrastructure - IXPs, DNS services, TLD registries)	Additional digital infrastructure services - cloud computing services, data centers, CDNs, network providers
Drinking water	Waste water
Transport	Space
Financial market infrastructure	Public Administration
Energy	
Banking	
"Digital service providers" category	"Important entities" category
Online marketplaces	Online marketplaces
Online search services	Online search services
Cloud services	Social networking services
	Food production & distribution
	Postal services
	Waste management
	Chemical manufacturers
	Manufacturing - medical devices, electronic products and equipment, machinery, vehicles and transport equipment

https://www.rapid7.com/blog/post/2021/04/20/overview-of-the-eus-draft-nis-2-directive/

cesnet

NIS covered sectors

- Finance
- Health
- Energy
- Banking
- Transport
- Water
- Digital Infrastructure
- Digital Service Providers

NIS2 expanded scope

- Providers of public electronic communications networks or services
- Digital services such as social networking service platforms and data centre services
- Waste water and waste management
- Space
- Manufacturing of certain critical products (such as pharmaceuticals, medical devices, chemicals)
- Postal and Courier Services
- Foods
- Public administration

Komise dále navrhuje řešit bezpečnost dodavatelských řetězců a dodavatelských vztahů tím, že bude požadovat, aby jednotlivé společnosti řešily rizika kybernetické bezpečnosti v dodavatelských řetězcích a dodavatelských vztazích.

Na evropské úrovni návrh posiluje kybernetickou bezpečnost dodavatelského řetězce pro klíčové informační a komunikační technologie.

Členské státy ve spolupráci s Komisí a agenturou ENISA provedou koordinovaná hodnocení rizik kritických dodavatelských řetězců, přičemž budou vycházet z úspěšného přístupu přijatého v kontextu doporučení Komise o kybernetické bezpečnosti sítí 5G.

https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

cesnet

CER
– CRITICAL ENTITIES RESILIENCE

Návrh

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY

o posílení odolnosti kritických subjektů

https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52020PC0829&from=EN

„odolností“:
schopnost předcházet incidentům, které narušují nebo mohou narušit provoz kritického subjektu, **odolávat jim, zmírňovat** je, **absorbovat je**, přizpůsobit se jim a **zotavit se z nich**

Čl. 5 odst. 3

Každý členský stát vytvoří seznam určených kritických subjektů a zajistí, aby tyto kritické subjekty byly informovány o svém určení jako kritických subjektů do jednoho měsíce od tohoto určení, přičemž budou rovněž informovány o svých povinnostech podle kapitol II a III a o datu, od kterého se na ně ustanovení těchto kapitol vztahují.

cesnet

NIS2 – kybernetické hrozby

z. č. 480/2004 Sb., ZSIS

z. č. 181/2014 Sb., ZKB

z. č. 127/2005 Sb., ZoEK

GDPR

eIDAS

Hybridní hrozby

CER – fyzické hrozby

DOPRAVA

ENERGETIKA

TELEKOMUNIKACE

BANKOVNICTVÍ

INFRASTRUKTURA FINANČNÍCH TRHŮ

DIGITÁLNÍ INFRASTRUKTURA

VEŘEJNÁ SPRÁVA

ZDRAVÍ

PITNÁ A ODPADNÍ VODA

VESMÍR

DIGITÁLNÍ INFRASTRUKTURA

- Poskytovatelé výměnného uzlu internetu [ve smyslu čl. 4 bodu (X) směrnice o bezpečnosti sítí a informací 2]
- Poskytovatelé služeb DNS [ve smyslu čl. 4 bodu (X) směrnice o bezpečnosti sítí a informací 2]
- Registry internetových domén nejvyšší úrovně (registry TLD) [ve smyslu čl. 4 bodu (X) směrnice o bezpečnosti sítí a informací 2]
- Poskytovatelé cloudových služeb [ve smyslu čl. 4 bodu (X) směrnice o bezpečnosti sítí a informací 2]
- Poskytovatelé služeb datového střediska [ve smyslu čl. 4 bodu (X) směrnice o bezpečnosti sítí a informací 2]
- Poskytovatelé sítí pro doručování obsahu [ve smyslu čl. 4 bodu (X) směrnice o bezpečnosti sítí a informací 2]
- Poskytovatelé služeb vytvářejících důvěru ve smyslu čl. 3 bodu 19 nařízení (EU) č. 910/2014
- Poskytovatelé veřejné sítě elektronických komunikací ve smyslu čl. 2 bodu 8 směrnice (EU) 2018/1972 nebo poskytovatelé služeb elektronických komunikací ve smyslu čl. 2 bodu 4 směrnice (EU) 2018/1972, pokud jsou jejich služby veřejně dostupné

cesnet

APLIKOVATELNOST NIS2 A CER?

cesnet

2025

cesnet

KYBERLEGISLATIVA ČR

Zákon č. **181/2014 Sb., o kybernetické bezpečnosti** a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

- Vyhláška č. **82/2018 Sb**., o kybernetické bezpečnosti;
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích;
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury;
- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby;

Cloudové vyhlášky

- Vyhláška č. **315/2021** Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci
- Vyhláška č. **316/2021** Sb., o některých požadavcích pro zápis do katalogu cloud computingu

https://nukib.cz/cs/infoservis/aktuality/1742-nukib-vydava-prvni-dve-cloudove-vyhlasky/

- Vyhláška č. 3: do konce roku 2021

- Věcný záměr vyhlášek

https://nukib.cz/cs/infoservis/aktuality/1610-vyzva-odborne-verejnosti-k-podani-pripominek/

cesnet

JUDIKATURA

Rozsudek SDEU C-311/18 (Schrems II)

https://curia.europa.eu/juris/liste.jsf?num=C-311/18

Rozsudek: 23 Cdo 2793/2020-409

https://www.nsoud.cz/Judikatura/ns_web.nsf/0/CE7E4199754CE1D2C125874200435976/$file/Vyhla%C5%A1.%20zn%C4%9Bn%C3%AD%20rozsudek%2023%20Cdo%202793_2020.pdf

DAILYMAIL.CO.UK | OD DAILY MAIL

Japan's minister of cybersecurity has NEVER used a computer

cesnet

DĚKUJI ZA POZORNOST

MÁTE NĚJAKÉ DOTAZY?

doc. JUDr. Jan Kolouch, Ph.D.
jan.kolouch@cesnet.cz