Memorandum

Initiatives to coordinate the cyber security of the Ministry of Health sector – hSOC

September 2020

Current status, reasons for the initiative

• Healthcare in the Czech Republic faces a growing risk of cyber attacks.
• There are big differences in the level of IT support and needs of individual hospitals.
• There are large differences in the perception of cyber security as a priority by hospital management or founders.
• There is a lack of systematic and conceptual insight how to ensure cyber security both of individual hospitals and of the department as a whole.
• There is a lack of a shared vision how to take advantage of digital technologies to transform healthcare.
• There is no discussion on how to use the shared infrastructure (Cesnet e-infrastructure, hospital data centers, state and regional networks, regional technological centers…).
• The cyber security in the healthcare sector is fundamentally underestimated in terms of personnel and finances.
• There is a possibility of getting significant financial resources (typically investments, EU funds) and there is a risk of their inefficient use.
• Usage of the results of the MoH questionnaire survey on cyber security in hospitals (no feedback) for the possible implementation of corrective measures and justification of money from the funds.
• The real threat of cyber attacks on individual hospitals and a larger number of medical facilities is growing daily.

Vision - Target state

Healthcare providers operate secure information technology with sufficient technical and personnel background being supported by centralized protection of the SOC type.

Estimated furt of steps to achieve the target state

• Create an interest platform to support the coordination of cyber security in the Ministry of Health.
• Establish the position of cyber security coordinator of the Ministry of Health, directly subordinate to the Minister.
• The undersigned signatories of the initiative propose to this position Mr. Petr Pavlinec.
• Establish a community team of healthcare cyber security led by the coordinator of cyber security of the Ministry of Health.
• Among the expected outputs of this team are:
  o Creation of basic uniform rules of information security (methodology for risk analysis, asset evaluation, information evaluation, etc.) with maximum use of existing good practice

methodologies of NUKIB, NAKIT, ZoKB, VoKB, ČSN 2700X).
- o Define basic preconditions of personnel & financial resources to implement proposed measures.
- o Propose the purpose, objectives and legal form of the entity that would be able to implement joint activities of important actors in the field of of healthcare cyber security (state and regional hospitals, state, regions, academic sector/education, Cesnet) - SOC (Security Operation Center).

• Share good and best practice in cyber security.
• Share good practices in the acquisition and new technologies implementation.
• Establish communication channels for effective transmission of information and alerts on cyber threats in health care.
• Inite the creation of a secure closed data network and shared services of state hospitals based on the services of the CESNET association.
• Establish a joint research institute of the Ministry of Health and the CIIRC CTU for cyber security.

Possible activities of the proposed entity (SOC) should include, for example:

• Security aspects of operation and monitoring of secure network infrastructure.
• Coordinate an Early Warning System for threats.
• Security aspects of the operation of selected shared information systems of the Ministry of Health (e.g. the National Contact Point of Electronic Health).
• Prepare training programs for employees (incl.managers) of health service providers in the field of cyber security.
Possibility of central education (e-learning) + local differences (training).
Minimum mandatory item of the education plan.
• Provide laboratory services for safety testing and certification.
• Establish a shared accredited CSIRT/response team.

Signatories of the initiative:

Name	Organization	e-mail (an org representative)
Petr Pavlinec	Kraj Vysočina	pavlinec.p@kr-vysocina.cz
Dušan Chvojka	Nemocnice Na Homolce	dusan.chvojka@homolka.cz
Antonín Hlavinka	FN Olomouc	antonin.hlavinka@fnol.cz
Jan Kvaček	Nemocnice Na Bulovce	martin.konir@bulovka.cz
Vladimír Mařík	ČVUT	Vladimir.Marik@cvut.cz
Martin Mareček	FNUSA	martin.marecek@fnusa.cz
Ctirad Procházka	ÚVN	prochcti@uvn.cz
Miroslav Sučík	ÚVN	miroslav.sucik@uvn.cz
Lenka Lhotská	ČVUT CIIRC & FBMI	lenka.lhotska@cvut.cz
Oto Sládek	ČVUT FEL Kybertec s.r.o.	sladek@kybertec.com
Michal Trefil	Odborný léčebný ústav Paseka, p.o.	trefil@olupaseka.cz
Radek Řechka	Oblastní nemocnice Příbram, a.s.	radek.rechka@onp.cz
Jiří Smetana	ZZS Karlovarského kraje	vaclav.kucera@zzskvk.cz
Jan Gruntorád	CESNET	kosnar@cesnet.cz
Andrea Rakovičová	ZZS Olomouckého kraje	jan.strasky@zzsol.cz
Vladimír Dzurilla	NAKIT	Vladimir.Dzurilla@nakit.cz
Libor Seneta	Zdravotnická záchranná služba Královéhradeckého kraje	senetali@zzskhk.cz
Ivan Veselý	Všeobecná fakultní nemocnice	Ivan.Vesely@vfn.cz