KYBERNETICKÁ BEZPEČNOSŤ DIGITÁLNYCH ZDRAVOTNÍCKYCH RIEŠENÍ[1]

CYBER SECURITY OF DIGITAL HEALTHCARE SOLUTIONS

Michal Rampášek[2]

Abstrakt: Cieľom príspevku je analyzovať rastúce právne nároky na kybernetickú bezpečnosť digitálnych zdravotníckych riešení v kontexte platnej a budúcej legislatívy EÚ. Pozornosť sa sústreďuje na systémy elektronických zdravotných záznamov (EHR), wellness aplikácie, zdravotnícke pomôcky a produkty určené na nosenie na tele na účely zdravotného monitorovania – vrátane tých, ktoré nespadajú pod rámec Nariadenia EÚ 2017/745 o zdravotníckych pomôckach (MDR) a Nariadenia EÚ 2017/746 o diagnostických zdravotníckych pomôckach in vitro (IVDR). Príspevok porovnáva požiadavky vyplývajúce z Nariadenia EÚ 2024/2847 o kybernetickej odolnosti (CRA), Nariadenia EÚ 2025/327 o európskom priestore pre zdravotné údaje (EHDS), ako aj z existujúcich predpisov týkajúcich sa zdravotníckych pomôcok. Osobitný dôraz sa kladie na problematiku zabezpečenia dát, riadenia zraniteľností, aktualizácií softvéru a interoperabilitu systémov v kontexte ochrany súkromia a verejného zdravia. Príspevok zároveň poukazuje na právne výzvy pri regulácii hybridných produktov, ktoré kombinujú prvky spotrebiteľskej elektroniky s funkciami zdravotného monitorovania. Cieľom je prispieť k odbornej diskusii o primeranom právnom rámci pre kybernetickú bezpečnosť v oblasti telemedicíny a digitálneho zdravotníctva.

Kľúčové slová: kybernetická bezpečnosť, digitálne produkty, zdravotníctvo, regulácia

Abstract: The aim of this paper is to analyze the growing legal requirements for cybersecurity in digital healthcare solutions in the context of current and future EU legislation. The focus is on electronic health record (EHR) systems, wellness apps, medical devices, and wearable products for health monitoring purposes—including those that do not fall under the scope of EU Regulation 2017/745 on medical devices (MDR) and EU Regulation 2017/746 on in vitro

[1] Financované Európskou úniou Next GenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-V01-00002

[2] Ústav práva informačných technológií a práva duševného vlastníctva, Právnická fakulta Univerzity Komenského v Bratislave

doi: 10.46282/bpf.2025.08

diagnostic medical devices (IVDR). The paper compares the requirements arising from Regulation EU 2024/2847 on cyber resilience (CRA), Regulation EU 2025/327 on the European Health Data Space (EHDS), as well as existing regulations on medical devices. Particular emphasis is placed on data security, vulnerability management, software updates, and system interoperability in the context of privacy and public health protection. The paper also highlights the legal challenges in regulating hybrid products that combine consumer electronics with health monitoring functions. The aim is to contribute to the expert discussion on an appropriate legal framework for cybersecurity in the field of telemedicine and digital health.

Key words: cyber security, digital products, healthcare, regulation

Úvod

Digitalizácia zdravotníctva zvyšuje závislosť pacientov a poskytovateľov zdravotnej starostlivosti od softvérových a cloudových riešení[3] – od systémov elektronických zdravotných záznamov (EHR) cez wellness aplikácie a nositeľné zariadenia až po zdravotnícke pomôcky. Táto technologická transformácia prináša nielen nové príležitosti v oblasti telemedicíny a personalizovanej starostlivosti, ale aj nové kybernetické hrozby, nárast kybernetických útokov na kritickú infraštruktúru zdravotníctva[4] sa kybernetická bezpečnosť stala dôležitou témou pre výrobcov, používateľov a regulačné orgány. Na jednej strane sa to odzrkadľuje v rastúcom počte predpisov týkajúcich sa kybernetickej bezpečnosti zdravotníckych pomôcok[5] a na strane druhej v náraste počtu výrobcov, ktorí vo svojej dokumentácii popisujú

[3] CEROSS Aaron, BERGMANN Jeoren, Tracking the presence of software as a medical device in US food and drug administration databases: retrospective data analysis JMIR Biomed Eng, 6 (4) (2021 Nov 3), Article e20652, [26.9.2025]. Dostupné na: doi: 10.2196/20652, CEROSS Aaron, BERGMANN Jeoren, Evaluating the presence of software-as-a-medical-device in the Australian therapeutic goods register
Prosthes Multidiscip Digit Publ Inst, 3(3) (2021 Sep), pp. 221-228, [26.9.2025]. Dostupné na: doi:10.3390/prosthesis3030022

[4] ABBOU Benyamine , et al., When all computers shut down: the clinical impact of a major cyber-attack on a general hospital, Frontiers in Digital Health, Volume 6 – 2024 [26.9.2025]. Dostupné na: https://doi.org/10.3389/fdgth.2024.1321485

[5] FREYER Oscar , et al. Consideration of cybersecurity risks in the benefit-risk analysis of medical devices: scoping review J Med Internet Res, 26 (1) (2024 Dec 24), Article e65528, [26.9.2025]. Dostupné na: doi: 10.2196/65528

doi: 10.46282/bpf.2025.08

opatrenia kybernetickej bezpečnosti, vrátane obranných mechanizmov, systémov reakcie alebo prísnych testov.[6]
Výskumy ukazujú, že prepojené zariadenia, najmä v prostredí vzdialeného monitorovania pacientov alebo domácej nemocnice, poskytujú veľký priestor pre útoky zo strany rôznych subjektov.[7] Rovnako tak, napríklad prepojená inzulínová pumpa by mohla byť terčom útočníkov, ktorí by mohli zmeniť dávkovanie inzulínu. Takéto útoky by potom mohli, ak by neboli zavedené primerané opatrenia na zmiernenie rizika, viesť k poškodeniu pacienta, kde nesprávne dávkovanie inzulínu mohlo spôsobiť hyperglykemickú alebo hypoglykemickú kómu. Okrem toho by prepojená pumpa mohla byť vstupným bodom do systému poskytovateľa zdravotnej starostlivosti, čo by útočníkom umožnilo spôsobiť poskytovateľovi ďalšie škody, napr. prostredníctvom ransomvérového útoku.

Súčasný regulačný rámec

Nariadenie EÚ 2017/745 o zdravotníckych pomôckach (MDR)[8] a Nariadenie EÚ 2017/746 o diagnostických zdravotníckych pomôckach in vitro (IVDR)[9] stanovujú povinnosti výrobcov zdravotníckych pomôcok týkajúce sa bezpečnosti (*safety*), riadenia rizík a informačnej bezpečnosti.
Podľa článku 2 ods. 1 MDR sa za „zdravotnícku pomôcku" považuje akýkoľvek nástroj, prístroj, zariadenie, ale aj softvér, ktorý je výrobcom určený na použitie u ľudí na jeden alebo viac špecifických medicínskych účelov (diagnostických, terapeutických, preventívnych a pod.), pričom hlavný účinok sa nedosahuje farmakologickými, imunologickými ani metabolickými prostriedkami. Analogicky IVDR v článku 2 ods. 2 zahŕňa aj softvér určený na diagnostické účely in vitro. V ďalšom texte preto používame pojem zdravotnícke pomôcky ako zastrešujúci termín pre obidve kategórie.
Je potrebné zdôrazniť, že softvér sa kvalifikuje ako zdravotnícka pomôcka iba vtedy, ak je výrobcom špecificky určený na medicínske účely podľa definície MDR/IVDR.

[6] STERN Ariel Dora , et. al, Cybersecurity features of digital medical devices: an analysis of FDA product summaries BMJ Open Br Med J Publ Group, 9 (6)(2019 Jun 1), Article e025374 [26.9.2025]. Dostupné na: https://bmjopen.bmj.com/content/9/6/e025374

[7] YAQOOB Tahreem, et al. Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—a review IEEE Commun Surv Tutor, 21 (4)(2019), pp. 3723-3768, [26.9.2025]. Dostupné na: 10.1109/COMST.2019.2914094, a
OSTERMANN Max , et al Cybersecurity in the HaH: Assessment of Patient Risks when using IoMT devices Zenodo (2024), [26.9.2025]. Dostupné na: 10.5281/zenodo.14545326

[8] Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745 z 5. apríla 2017 o zdravotníckych pomôckach, zmene smernice 2001/83/ES, nariadenia (ES) č. 178/2002 a nariadenia (ES) č. 1223/2009 a o zrušení smerníc Rady 90/385/EHS a 93/42/EHS

[9] Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/746 z 5. apríla 2017 o diagnostických zdravotníckych pomôckach in vitro a o zrušení smernice 98/79/ES a rozhodnutia Komisie 2010/227/EÚ

doi: 10.46282/bpf.2025.08

Naopak, softvér na všeobecné účely, aj keď je využívaný v zdravotníctve, alebo softvér zameraný na podporu zdravého životného štýlu či pohody (tzv. wellness aplikácie) sa za zdravotnícku pomôcku nepovažuje. Rozhodujúce je teda **určenie výrobcu,** nie fyzické umiestnenie alebo technické prepojenie softvéru.

Kybernetická bezpečnosť v MDR a IVDR

Požiadavky na kybernetickú bezpečnosť sú zakotvené v **prílohách I oboch** nariadení, ktoré obsahujú tzv. všeobecné požiadavky na bezpečnosť a výkon.
Všeobecné požiadavky na bezpečnosť a výkon ukladajú výrobcom zdravotníckych pomôcok povinnosť navrhovať a vyrábať pomôcky tak, aby za bežných podmienok používania boli bezpečné, účinné a dosahovali určený výkon bez ohrozenia zdravia pacientov či používateľov. Základom je systematické riadenie rizík počas celého životného cyklu pomôcky, ktoré zahŕňa identifikáciu a analýzu známych aj predvídateľných nebezpečenstiev, vyhodnotenie súvisiacich rizík, zavádzanie a revíziu kontrolných opatrení a reagovanie na nové informácie zo systému dohľadu po uvedení na trh. Riziká musia byť eliminované alebo minimalizované prostredníctvom bezpečného návrhu, primeraných ochranných opatrení a poskytovania jasných bezpečnostných informácií používateľom. Výrobca je ďalej povinný zohľadniť faktory ľudskej chyby, ergonomické aspekty a predpokladané schopnosti používateľov, pričom musí zabezpečiť, že vlastnosti a výkon pomôcky zostanú stabilné počas celej jej životnosti aj pri záťažových situáciách. Pomôcky musia byť odolné voči rizikám vyplývajúcim z prepravy a skladovania a všetky známe či predvídateľné riziká a vedľajšie účinky musia byť redukované na úroveň prijateľnú vo vzťahu k prínosu pre pacienta. V kontexte kybernetickej bezpečnosti sa tieto požiadavky transponujú do povinnosti výrobcov zahrnúť do návrhu a výroby také opatrenia, ktoré chránia pomôcku pred nežiaducim pôsobením IT prostredia, neoprávneným prístupom a narušením integrity dát.
Konkrétne bod 14.2 prílohy I MDR vyžaduje, aby pomôcky boli navrhnuté tak, aby minimalizovali riziká vyplývajúce z negatívneho pôsobenia softvéru a IT prostredia, v ktorom fungujú. Článok 17 ďalej stanovuje povinnosť výrobcu definovať minimálne požiadavky na hardvér, vlastnosti IT sietí a bezpečnostné opatrenia potrebné na správne fungovanie softvéru vrátane ochrany pred neoprávneným prístupom.

Usmernenia MDCG

Na podporu jednotného uplatňovania MDR/IVDR bola zriadená Koordinačná skupina pre zdravotnícke pomôcky (***Medical Device Coordination Group* - MDCG)**[10], poradný

[10] MDR, článok 103 a 104

doi: 10.46282/bpf.2025.08

orgán Európskej komisie. MDCG vydáva nezáväzné, ale prakticky významné usmernenia.
Usmernenie MDCG 2019-16 Rev. 1 – *Guidance on Cybersecurity for Medical Devices* poskytuje výrobcom usmernenia o tom, ako splniť všetky príslušné základné požiadavky prílohy I k MDR a IVDR v súvislosti s kybernetickou bezpečnosťou. Vzhľadom na zložitosť dodávateľských reťazcov zdravotníckych pomôcok a úlohu, ktorú zohrávajú rôzni prevádzkovatelia pri zabezpečovaní ochrany pomôcok pred neoprávneným prístupom a možnými kybernetickými hrozbami, sa však uvádzajú ďalšie úvahy týkajúce sa očakávaní od iných subjektov ako výrobcov. Požiadavky na kybernetickú bezpečnosť sa týkajú aspektov pred uvádzaním na trh aj po uvedení na trh. Je však potrebné dodať, že ide iba o odporúčania, ktoré naviac ani bližšie neuvádzajú povinnosť viesť zoznam softvéru (*Software Bill of Materials* - SBOM), zaviesť politiku koordinovaného zverejňovania zraniteľností či pravidelne hlásiť incidenty.
Ďalšie usmernenie MDCG 2019-11 – *Guidance on Qualification and* ***Classification of Software*** upresňuje, za akých podmienok sa softvér považuje za zdravotnícku pomôcku a ako sa klasifikuje. To má zásadný význam najmä pri **AI aplikáciách a digitálnych zdravotných riešeniach,** kde hranice medzi wellness aplikáciou a regulovanou pomôckou nie sú vždy zreteľné.
Viacerí autori už identifikovali potrebu posilnenia MDCG 2019-16 a navrhujú zaviesť **systematické požiadavky na transparentnosť (napr. SBOM)** a oznamovanie kybernetických bezpečnostných incidentov. [11][12]

Vzťah k iným predpisom

MDR/IVDR majú **postavenie *lex specialis***, a teda ich požiadavky na kybernetickú bezpečnosť majú prednosť pred všeobecnými právnymi predpismi, ako sú napr. **Smernica** 2014/53/EU **o rádiových zariadeniach (***Radio Equipment Directive* –

[11] ANDROUTSOS Christos. , et al. MDCG 2019-16 Guidelines: Case Study-Based Assessment and Path Forward, I. Praça, S. Bernardi, P.R.M. Inácio(Eds.), Cybersecurity Cham, Springer Nature, Switzerland (2025), pp. 338-355, [26.9.2025]. Dostupné na: doi: 10.1007/978-3-031-94855-8_22;
[12] TAYLOR Steve, et al. A Way Forward for the MDCG 2019-16 Medical Device Security Guidance, Proc 17th Int Conf PErvasive Technol Relat Assist Environ, Association for Computing Machinery, New York, NY, USA (2024), pp. 593-599, [26.9.2025]. Dostupné na: doi: 10.1145/3652037.3663894

doi: 10.46282/bpf.2025.08

RED)[13] alebo **nariadenie EÚ** 2024/2847 **o** kybernetickej odolnosti (*Cyber Resilience Act* - CRA). [14] [15]
Výrobcovia zdravotníckych pomôcok sa môžu zároveň stať „dôležitými subjektmi" podľa **smernice EÚ 2022/2555 (NIS2),** ak spĺňajú veľkostné kritériá, avšak táto úprava sleduje **odolnosť subjektov.** V rámci tohto príspevku sa sústredíme výlučne na **produktovo orientované požiadavky kybernetickej bezpečnosti.**

Smernica o rádiových zariadeniach (RED) a Delegované nariadenie Komisie 2022/30

RED predstavuje základný právny rámec EÚ pre uvádzanie rádiových zariadení na trh. Okrem tradičných požiadaviek na elektrickú bezpečnosť, elektromagnetickú kompatibilitu a efektívne využívanie rádiového spektra, bola jej pôsobnosť v oblasti kybernetickej bezpečnosti významne posilnená prijatím Delegovaného nariadenia Komisie 2022/30.[16] Od 1. augusta 2025 sa pre výrobcov stali záväznými nové povinnosti podľa článku 3 ods. 3 písm. d), e) a f) RED, ktorých cieľom je: (i) zabezpečiť integritu a funkčnosť sietí, (ii) chrániť osobné údaje a súkromie používateľov a (iii) predchádzať podvodom a zneužívaniu zariadení.
Tieto povinnosti sa vzťahujú na širokú paletu zariadení, od domácich poplachových systémov (alarmov) až po nositeľnú elektroniku monitorujúcu zdravotný stav alebo pohodu (napr. športové hodinky, fitness náramky, merače tepu). Z hľadiska klasifikácie ide teda aj o produkty súvisiace so zdravím, ktoré však nespadajú pod definíciu zdravotníckych pomôcok podľa MDR alebo IVDR. Pre všetky produkty v pôsobnosti RED platí povinnosť označenia CE, ktoré podmieňuje ich voľný pohyb na vnútornom trhu EÚ.
Delegované nariadenie 2022/30 výslovne vylučuje z pôsobnosti tie rádiové zariadenia, ktoré už spadajú pod MDR alebo IVDR. Dôvodom je, že obidve nariadenia obsahujú špecifické požiadavky kybernetickej bezpečnosti na zdravotnícke pomôcky a diagnostické pomôcky in vitro, ktoré pokrývajú rovnaké oblasti rizík, aké sú riešené

[13] Smernica Európskeho parlamentu a Rady 2014/53/EÚ zo 16. apríla 2014 o harmonizácii právnych predpisov členských štátov týkajúcich sa sprístupňovania rádiových zariadení na trhu, ktorou sa zrušuje smernica 1999/5/ES
[14] Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti)
[15] LUDVIGSEN Kaspar Rosager, The role of cybersecurity in medical devices regulation: future considerations and solutions Law Technol Hum, 5 (2) (2023), pp. 59-77, [26.9.2025]. Dostupné na: 10.5204/lthj.3080
[16] Delegované nariadenie Komisie (EÚ) 2022/30 z 29. októbra 2021, ktorým sa dopĺňa smernica Európskeho parlamentu a Rady 2014/53/EÚ, pokiaľ ide o uplatňovanie základných požiadaviek uvedených v článku 3 ods. 3 písm. d), e) a f) uvedenej smernice

doi: 10.46282/bpf.2025.08

v článku 3 ods. 3 písm. d), e) a f) RED.[17] Zariadenia patriace pod MDR alebo IVDR teda nie sú zaradené do tried rádiových zariadení, ktoré musia spĺňať nové základné kybernetické požiadavky RED.
Na rozdiel od nariadení MDR/IVDR, kde implementácia požiadaviek kybernetickej bezpečnosti stojí primárne na povinnostiach výrobcov a odporúčaniach MDCG, je pri RED podpora súladu s právom EÚ posilnená aj prostredníctvom európskych harmonizovaných noriem.[18] Európska komisia prijala 30. januára 2025 vykonávacie rozhodnutie (EU) 2025/138, ktorým sa publikovali prvé tri harmonizované normy – EN 18031-1:2024 a nadväzujúce ďalšie dve časti. Tieto normy poskytujú výrobcovi „harmonizovanú" cestu, ako preukázať súlad s požiadavkami RED.
RED a súvisiace nariadenia Komisie tak zapĺňajú regulačnú medzeru v oblasti nositeľnej elektroniky a ďalších zariadení pre zdravie a pohodu, ktoré síce neslúžia na medicínske účely, no spracúvajú citlivé osobné údaje a sú potenciálnym cieľom kybernetických útokov. V porovnaní s MDR/IVDR sa tu kybernetická bezpečnosť premieta priamo do harmonizovaných noriem, čo posilňuje právnu predvídateľnosť a praktickú aplikáciu požiadaviek zo strany výrobcov. Zároveň je však potrebné dodať, že požiadavky RED na kybernetickú bezpečnosť majú **prechodný charakter**. Európska komisia už avizovala, že budú zrušené a nahradené požiadavkami vyplývajúcimi **CRA**, ktorý má omnoho širší rozsah pôsobnosti a dotkne sa všetkých produktov s digitálnymi prvkami vrátane softvéru. CRA tak zabezpečí jednotný horizontálny rámec pre kybernetickú bezpečnosť produktov v EÚ, zatiaľ čo RED zostane primárne technickou reguláciou pre rádiové zariadenia.

Nový legislatívny vývoj: CRA a EHDS

Významným posunom v európskom regulačnom prostredí je prijatie **nariadenia CRA** a **nariadenia (EÚ) 2025/327 o európskom priestore pre zdravotné údaje (*European Health Data Space* – EHDS)**.[19] Obe nariadenia zásadne menia rámec kybernetickej bezpečnosti a spracúvania elektronických zdravotných údajov v EÚ.

[17] Delegované nariadenie Komisie 2022/30, recitál č. 15
[18] SCHAPEL, Harm: 'The New Approach to the New Approach: The Juridification of Harmonised Standards in EU Law.' (2013) Maastricht Journal of European and Comparative Law, 20 (4): 521–33 [13.9.2024]. Dostupné na: https://doi.org/10.1177/1023263X1302000404.; VAN GESTEL, Rob a MICKLITZ Hans-W.: "European Integration through Standardisation: How Judicial Review Is Breaking Down the Club House of Private Standardisation Bodies" [2013] *Common Market Law Review* 145-182 [26.9.2025]. Dostupné na: https://doi.org/10.54648/cola2013007; ELIANTONIO Mariolina a COLOMBO Carlo, "Harmonized Technical Standards as Part of EU Law: Juridification with a Number of Unresolved Legitimacy Concerns?" [2017] *Maastricht Journal of European and Comparative Law*, 323-340 [26.9.2025]. Dostupné na: https://doi.org/10.1177/1023263X17709753.
[19] Nariadenie Európskeho parlamentu a Rady (EÚ) 2025/327
z 11. februára 2025 o európskom priestore pre zdravotné údaje a o zmene smernice 2011/24/EÚ a nariadenia (EÚ) 2024/2847

doi: 10.46282/bpf.2025.08

Akt o kybernetickej odolnosti (CRA)

CRA reaguje na dlhodobo nedostatočnú úroveň kybernetickej bezpečnosti mnohých produktov s digitálnymi prvkami, ako aj na oneskorené či absentujúce bezpečnostné aktualizácie. Jeho ambíciou je poskytnúť jednotný rámec povinností výrobcom, dovozcom a distribútorom softvérových a hardvérových produktov, ktoré obsahujú digitálne komponenty, vrátane **wellness aplikácií a zariadení**, ktoré nie sú zdravotníckymi pomôckami. Z pôsobnosti CRA sú totiž výslovne vylúčené zdravotnícke pomôcky a diagnostické zdravotnícke pomôcky in vitro, keďže ich oblasť je už pokrytá MDR a IVDR.

CRA vychádza z toho, že nariadenia MDR aj IVDR sa vzťahujú aj na určitý nezabudovaný softvér a zohľadňovanie celoživotného cyklu. Tieto požiadavky ukladajú výrobcom povinnosť vyvíjať a konštruovať svoje produkty pri uplatnení zásad riadenia rizika a so stanovením požiadaviek, ktoré sa týkajú bezpečnostných opatrení IT a zodpovedajú postupom posudzovania zhody. Okrem toho je od decembra 2019 zavedené osobitné usmernenie ku kybernetickej bezpečnosti zdravotníckych pomôcok, ktorým sa výrobcom zdravotníckych pomôcok vrátane diagnostických pomôcok in vitro poskytuje usmernenie k tomu, ako splniť všetky príslušné základné požiadavky kybernetickej bezpečnosti stanovené v prílohe I k uvedeným nariadeniam.[20] S týmto tvrdením si dovolím polemizovať. CRA zjavne odkazuje na usmernenie MDCG 2019-16 Rev. 1, ktoré ako poukazujem v tomto príspevku zďaleka neobsahuje niektoré podstatné požiadavky na zdravotnícke pomôcky, ktoré sú obsiahnuté v prílohe č. 1 CRA.

CRA zavádza v prílohe č. 1 základné požiadavky na kybernetickú bezpečnosť, a to ako pre oblasť vlastností produktu s digitálnym prvkom ako pre požiadavky na riešenie zraniteľností , ktoré musia byť dodržiavané počas celého životného cyklu produktu. Patria sem napríklad:

- uvádzanie produktov na trh bez známych zneužiteľných zraniteľností,
- zabezpečenie produktov v štandardnej konfigurácii,
- povinnosť poskytovať bezpečnostné aktualizácie vrátane možnosti ich automatickej inštalácie,
- ochrana pred neoprávneným prístupom a zabezpečenie dôvernosti, integrity a dostupnosti údajov,
- obmedzenie plochy útoku a zavedenie mechanizmov logovania a monitorovania činností.

CRA ďalej zavádza povinnosť **systematického riadenia zraniteľností** vrátane tvorby **zoznamu softvérových komponentov (SBOM)**, ktorý má uľahčiť identifikáciu závislostí a sledovanie nových hrozieb v dodávateľskom reťazci. Vybrané dôležité a kritické produkty budú podliehať povinnému posúdeniu zhody

[20] CRA, recitál č. 25

doi: 10.46282/bpf.2025.08

treťou stranou. Všetky produkty musia niesť označenie CE, pričom hlavné povinnosti nadobudnú účinnosť od 11. decembra 2027.
Pre prax to znamená, že hybridné produkty, napríklad prístroj regulovaný podľa MDR, ktorý je prepojený s mobilnou aplikáciou podliehajúcou CRA, budú musieť spĺňať súbežne obe právne regulácie, s odlišnými požiadavkami na kybernetickú bezpečnosť.

Nariadenie o európskom priestore pre zdravotné údaje (EHDS)

Nariadenie EHDS predstavuje prvý komplexný právny rámec pre **primárne a sekundárne využitie elektronických zdravotných údajov** v EÚ. Jeho cieľom je vytvoriť harmonizovanú infraštruktúru pre bezpečný prístup, zdieľanie a opätovné použitie zdravotných údajov v celej Únii, s dôrazom na interoperabilitu a kybernetickú bezpečnosť.
Kľúčovým prvkom EHDS sú povinnosti pre systémy elektronických zdravotných záznamov (EHR) a wellness aplikácie.
Systém EHR je definovaný ako softvér alebo kombinácia hardvéru a softvéru, ktorý umožňuje spracúvanie prioritných kategórií zdravotných údajov (anamnéza, diagnózy, výsledky vyšetrení, liečba). Systém SHR musí obsahovať dva povinné harmonizované softvérové komponenty:

- *európsky komponent interoperability* – umožňujúci výmenu údajov v jednotnom európskom formáte,
- *európsky komponent logovania* – zabezpečujúci zaznamenávanie prístupov k údajom (identita, kategória údajov, čas, pôvod).

Wellness aplikácia je definovaná ako softvér určený na spracovanie zdravotných údajov mimo poskytovania zdravotnej starostlivosti (napr. fitness aplikácie, aplikácie na sledovanie spánku či stravovania). Tieto aplikácie nemusia spĺňať povinnosti EHR, pokiaľ však deklarujú interoperabilitu so systémami EHR, musia implementovať harmonizované komponenty interoperability a logovania.
EHDS zavádza aj povinnosti pre **držiteľov zdravotných údajov** (*health data holders*), vrátane výrobcov zdravotníckych pomôcok, a pre **používateľov údajov** (*health data users*), ktorí získavajú údaje na sekundárne účely, napríklad výskum v zdravotníctve.
Ustanovenia nariadenia EHDS sa začnú uplatňovať od 26. marca 2027, pričom väčšina povinností týkajúcich sa primárneho použitia údajov sa bude zavádzať postupne až do roku 2031.
CRA a EHDS tak spolu s existujúcimi predpismi MDR, IVDR a RED vytvárajú komplex právnych povinností, ktoré majú priamy dosah na kybernetickú bezpečnosť a interoperabilitu digitálnych zdravotníckych riešení. CRA sa orientuje na **produktovú kybernetickú bezpečnosť** v širšom zmysle (vrátane wellness aplikácií a IoT

doi: 10.46282/bpf.2025.08

zariadení), zatiaľ čo EHDS prináša **nový rámec pre zdieľanie a ochranu zdravotných údajov v týchto zariadeniam či aplikáciách**.

Porovnanie EÚ – USA

Prístup Európskej únie a Spojených štátov amerických (USA) ku kybernetickej bezpečnosti zdravotníckych pomôcok sa v zásade zhoduje v cieľoch – zabezpečiť **bezpečný dizajn, systematické riadenie rizík počas celého životného cyklu zariadenia a schopnosť reagovať na zraniteľnosti**. Rozdiely sa však prejavujú v **miere preskriptívnosti, rozsahu a vynútiteľnosti jednotlivých požiadaviek**.

USA – legislatívny rámec a FDA požiadavky

Kongres v roku 2022 novelizoval federálny zákon o potravinách, liekoch a kozmetike (***Food, Drug, and Cosmetic Act* - FD&C Act)** a zaviedol nové ustanovenie § 524B, ktorý explicitne ustanovil povinnosti pre tzv. kybernetické zariadenia (***cyber devices***).[21][22] Podľa § 524B(c) ide o zdravotnícke pomôcky, ktoré:

1. obsahujú softvér validovaný, inštalovaný alebo autorizovaný výrobcom,
2. majú schopnosť pripojenia na internet, a
3. obsahujú technologické prvky, ktoré môžu byť zraniteľné kybernetickými hrozbami.

Výrobca pred uvedením takéhoto zariadenia na trh je povinný (§ 524B(a), (b)):

- predložiť plán monitorovania **po uvedení na trh a riešenia zraniteľností**, vrátane zavedeného procesu koordinovaného oznamovania zraniteľností,
- navrhnúť, vyvíjať a udržiavať procesy, ktoré zabezpečia primeranú úroveň kybernetickej bezpečnosti a umožnia pravidelné aktualizácie a záplaty,
- predložiť softvérový zoznam komponentov (SBOM) zahŕňajúci komerčný, open-source aj tzv. krabicový softvér.

[21] Text právneho predpisu je dostupný online na: https://www.congress.gov/bill/117th-congress/house-bill/2617/text

[22] Úrad pre kontrolu potravín a liečiv (Food and Drug Administration - FDA) v roku 2023 vydal usmernenie k praktickej aplikácii pri posudzovaní žiadostí pred uvedením na trh podľa § 524B: Cybersecurity in medical devices: refuse to accept policy for cyber devices and related systems under section 524b of the fd&c act; guidance for industry and food and drug administration staff; availability, [26.9.2025] dostupné na: https://www.federalregister.gov/documents/2023/03/30/2023-06646/cybersecurity-in-medical-devices-refuse-to-accept-policy-for-cyber-devices-and-related-systems-under

doi: 10.46282/bpf.2025.08

FDA následne vydala usmernenie, ktoré spresňuje očakávanú dokumentáciu (napr. modely hrozieb, bezpečnostnú architektúru, stratégie aktualizácií, formát SBOM).[23] Pri porovnaní s EÚ, na rozdiel od právnej úpravy v USA, MDR/IVDR (ani MDCG 2019-16 Rev.1) neobsahujú **explicitnú povinnosť predkladať SBOM**, ani podrobné procesné požiadavky na oznamovanie zraniteľností. Táto asymetria zároveň vedie k paradoxu. **Produkty mimo oblasti zdravotníckych pomôcok (napr. wellness aplikácie či niektoré nositeľné zariadenia) budú v EÚ, po 11. decembri 2027 (dátum uplatňovania CRA), čeliť prísnejším požiadavkám kybernetickej bezpečnosti než samotné zdravotnícke pomôcky**. V dôsledku toho sa môže vytvoriť regulačná disproporcia, kedy digitálne produkty podliehajú silnejšiemu režimu ako zariadenia s priamym dopadom na zdravie pacientov.

Záver

Rastúce kybernetické hrozby jasne ukazujú, že existujúci právny rámec EÚ v oblasti zdravotníckych pomôcok je fragmentovaný a v mnohých aspektoch má iba odporúčací charakter. Nariadenia MDR a IVDR predstavujú zásadný posun v chápaní kybernetickej bezpečnosti ako integrálnej súčasti bezpečnosti pacienta a zdravotníckej pomôcky. Zároveň však pretrvávajú významné výzvy spojené so zabezpečením jednotnej implementácie s novými horizontálnymi právnymi predpismi, akými sú CRA či EHDS.

Nariadenia MDR a IVDR predstavujú príklad toho, ako možno do sektorovej regulácie integrovať kybernetickú bezpečnosť. CRA a EHDS pritom predstavujú krok vpred v oblasti regulácie kybernetickej bezpečnosti, no zároveň vytvárajú určitú regulačnú medzeru, keďže zdravotnícke pomôcky ostávajú mimo záväzných požiadaviek kybernetickej bezpečnosti.

V rámci návrhu *pro futuro* je preto podľa môjho názoru nevyhnutné:

a) zaviesť povinnosť výrobcov zdravotníckych pomôcok vytvárať a udržiavať SBOM, systematické riadenie zraniteľností, vrátane povinného koordinovaného zverejňovania zraniteľností a oznamovania incidentov pre zdravotnícke pomôcky,
b) harmonizovať pravidlá pre hybridné produkty (napr. MDR zariadenia s mobilnými aplikáciami alebo cloudovými komponentmi podliehajúcimi CRA).

[23]Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Guidance for Industry and Food and Drug Administration Staff Document issued on June 27, 2025. [26.9.2025]. Dostupné na: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions

doi: 10.46282/bpf.2025.08

Tak bude možné vytvoriť ucelený a predvídateľný právny rámec pre kybernetickú bezpečnosť digitálnych zdravotníckych riešení, ktorý zabezpečí ochranu pacientov, poskytovateľov zdravotnej starostlivosti aj verejného zdravia.

Zoznam použitej literatúry

1. CEROSS Aaron, BERGMANN Jeoren, Tracking the presence of software as a medical device in US food and drug administration databases: retrospective data analysis JMIR Biomed Eng, 6 (4) (2021 Nov 3), Article e20652, [on-line]. Dostupné na: doi: 10.2196/20652,
2. CEROSS Aaron, BERGMANN Jeoren, Evaluating the presence of software-as-a-medical-device in the Australian therapeutic goods register Prosthes Multidiscip Digit Publ Inst, 3(3) (2021 Sep), pp. 221-228, [on-line]. Dostupné na: doi:10.3390/prosthesis3030022
3. ABBOU Benyamine , et al., When all computers shut down: the clinical impact of a major cyber-attack on a general hospital, Frontiers in Digital Health, Volume 6 – 2024 [on-line]. Dostupné na: https://doi.org/10.3389/fdgth.2024.1321485
4. FREYER Oscar , et al. Consideration of cybersecurity risks in the benefit-risk analysis of medical devices: scoping review J Med Internet Res, 26 (1) (2024 Dec 24), Article e65528, [on-line]. Dostupné na: doi: 10.2196/65528
5. STERN Ariel Dora , et. al, Cybersecurity features of digital medical devices: an analysis of FDA product summaries BMJ Open Br Med J Publ Group, 9 (6)(2019 Jun 1), Article e025374 [on-line]. Dostupné na: https://bmjopen.bmj.com/content/9/6/e025374
6. YAQOOB Tahreem, et al. Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—a review IEEE Commun Surv Tutor, 21 (4)(2019), pp. 3723-3768, [on-line]. Dostupné na: 10.1109/COMST.2019.2914094
7. OSTERMANN Max , et al Cybersecurity in the HaH: Assessment of Patient Risks when using IoMT devices Zenodo (2024), [on-line]. Dostupné na: 10.5281/zenodo.14545326
8. SCHAPEL, Harm: 'The New Approach to the New Approach: The Juridification of Harmonised Standards in EU Law.' (2013) Maastricht Journal of European and Comparative Law, 20 (4): 521–33 [on-line]. Dostupné na: https://doi.org/10.1177/1023263X1302000404
9. VAN GESTEL, Rob a MICKLITZ Hans-W.: "European Integration through Standardisation: How Judicial Review Is Breaking Down the Club House of

Private Standardisation Bodies" [2013] *Common Market Law Review* 145-182 [on-line]. Dostupné na: https://doi.org/10.54648/cola2013007;
10. ELIANTONIO Mariolina a COLOMBO Carlo, "Harmonized Technical Standards as Part of EU Law: Juridification with a Number of Unresolved Legitimacy Concerns?" [2017] *Maastricht Journal of European and Comparative Law*, 323-340 [on-line]. Dostupné na: https://doi.org/10.1177/1023263X17709753.
11. ANDROUTSOS Christos. , et al. MDCG 2019-16 Guidelines: Case Study-Based Assessment and Path Forward, I. Praça, S. Bernardi, P.R.M. Inácio(Eds.), Cybersecurity Cham, Springer Nature, Switzerland (2025), pp. 338-355, [on-line]. Dostupné na: doi: 10.1007/978-3-031-94855-8_22;
12. TAYLOR Steve, et al. A Way Forward for the MDCG 2019-16 Medical Device Security Guidance, Proc 17th Int Conf PErvasive Technol Relat Assist Environ, Association for Computing Machinery, New York, NY, USA (2024), pp. 593-599, [on-line]. Dostupné na: doi: 10.1145/3652037.3663894
13. LUDVIGSEN Kaspar Rosager, The role of cybersecurity in medical devices regulation: future considerations and solutions Law Technol Hum, 5 (2) (2023), pp. 59-77, [on-line]. Dostupné na: 10.5204/lthj.3080
14. FOOD AND DRUG ADMINISTRATION, *Cybersecurity in medical devices: refuse to accept policy for cyber devices and related systems under section 524b of the fd&c act; guidance for industry and food and drug administration staff; availability*, [on-line]. dostupné na: https://www.federalregister.gov/documents/2023/03/30/2023-06646/cybersecurity-in-medical-devices-refuse-to-accept-policy-for-cyber-devices-and-related-systems-under
15. FOOD AND DRUG ADMINISTRATION, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions Guidance for Industry and Food and Drug Administration Staff Document issued on June 27, 2025. [on-line]. Dostupné na: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions

Kontaktné údaje

JUDr. Michal Rampášek
rampasek1@uniba.sk
Ústav práva informačných technológií a práva duševného vlastníctva Právnickej fakulty Univerzity Komenského v Bratislave

doi: 10.46282/bpf.2025.08