Základy bezpečného obstarávania v zdravotníctve

Základy bezpečného obstarávania v zdravotníctve

Bezpečné obstarávanie v zdravotníctve nie je len technická téma pre IT oddelenie – je to strategická otázka, ktorá ovplyvňuje fungovanie celého zdravotníckeho zariadenia, kontinuitu poskytovania zdravotnej starostlivosti, a bezpečnosti pacientov, vrátane ich citlivých osobných údajov.

Každý nový prístroj, softvér alebo služba, ktorú zdravotnícke zariadenie nakúpi, sa stáva súčasťou jeho digitálneho ekosystému. Ak tento ekosystém nie je chránený, dôsledky môžu byť vážne.

- **Ohrozenie života pacienta** – výpadok prístroja na JIS v dôsledku kybernetického útoku
- **Strata citlivých údajov** – únik elektronických zdravotných záznamov, ktorý vedie k finančným sankciám a strate reputácie
- **Finančné straty** – výkupné pri ransomvéri, náklady na obnovu
- **Nedostupnosť poskytovania zdravotnej starostlivosti -** neplánované prerušenie prevádzky

Reálne prípady incidentov v praxi potvrdzujú, že pri obstarávaní v zdravotníctve je kybernetická bezpečnosť priamo spojená s ochranou ľudských životov.

Bezpečnosť v zdravotníctve sa týka každého

Zdravotnícke zariadenia v dnešnej dobe fungujú ako komplexná sieť prepojených technológií:

- **Nemocničné informačné systémy (NIS)** – spracúvajú zdravotné záznamy
- **Zdravotnícke pomôcky** – často bývajú pripojené k internetu alebo k internej sieti
- **Cloudové služby** – uchovávajú dáta aj mimo priestorov nemocnice
- **Priemyselné riadiace systémy** – ovládajú dôležité infraštruktúrne prvky (rozvody energie a plynov, výťahy, ventiláciu vzduchu, zabezpečovacie systémy, riadenie technológií operačných sál)

Používanie moderných a bezpečných informačných technológií je nevyhnutnosťou prevádzky každeho poskytovateľa zdravotnej starostlivosti. Každé obstaranie nového systému alebo zariadenia však znamená **pripojenie ďalšieho článku do reťazca.** Tento článok reťazca môže byť len bezpečný, alebo naopak – zraniteľný.

Taxonómia aktív

čo všetko môže byť predmetom bezpečného obstarávania?

Prečo hodnotiť bezpečnosť dodávateľov

Úspešné riadenie kybernetickej bezpečnosti v nemocnici nezávisí len od implementovaných bezpečnostných opatrení, ale aj od bezpečnostných štandardov, ktoré dodržiavajú externí dodávatelia.

Každý partner v dodávateľskom reťazci – od výrobcov zdravotníckych prístrojov, až po poskytovateľov IT služieb – môže predstavovať slabé miesto, ak jeho procesy a technológie nie sú dostatočne zabezpečené. Je dôležité vedieť v akom „zdravotnom" stave je váš partner pre kritické IT služby.

- **Zníženie rizika útokov** – mnohé incidenty sa začínajú práve cez kompromitovanú infraštruktúru dodávateľa
- **Zabezpečenie kontinuity prevádzky** – porucha alebo útok na dodávateľa môže mať okamžitý dopad na zdravotnícke zariadenie a poskytovania zdravotnej starostlivosti.
- **Súlad** – mnohé európske a národné právne predpisy vyžadujú, aby boli riziká dodávateľského reťazca riadené

Životný cyklus bezpečného obstarávania

Kybernetická bezpečnosť nie je jednorazový krok, ale nepretržitý proces, ktorý musí byť súčasťou **každej fázy obstarávania.**

1. Fáza – Plánovanie

- **Analýza potrieb a rizík** – pred obstaraním je potrebné určiť, aké bezpečnostné požiadavky musí riešenie spĺňať
- **Stanovenie kritérií pre dodávateľa** –referencie na realizované riešenia alebo poskytované služby, certifikáty a vykonané posúdenia zhody
- **Požiadavky na integráciu** – zariadenie alebo služba musí byť kompatibilná s existujúcimi systémami a bezpečnostnými politikami
- **Zahrnutie IT a bezpečnostného tímu** – zapojenie odborníkov už v tejto fáze zabráni neskorším problémom

2. Fáza – Akvizícia (obstaranie, výber dodávateľa)

- **Technická špecifikácia** musí obsahovať jasné bezpečnostné požiadavky (šifrovanie, autentifikácia, povinnosť aktualizácií)
- **Overenie dodávateľa** – požiadanie o dokumentáciu typu MDS2, výsledky bezpečnostných testov, preukázanie súladu s príslušnými právnymi predpismi (GDPR, MDR, Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti)
- **Zmluvné podmienky** – definovanie povinností dodávateľa pri aktualizáciách, reakcii na incidenty, podpore.

3. Fáza – Riadenie a prevádzka

- **Priebežné monitorovanie** a reporting – sledovanie incidentov, zraniteľností, výkonu.
- **Pravidelné testovanie** – audity, penetračné testy, kontrola konfigurácie.
- **Pravidelné aktualizácie** - testovanie, plánovanie a nasadenie softwarových aktualizácií a nasledne zdokumentovanie zmien
- **Bezpečné vyradenie zariadenia** – zmazanie alebo zničenie dát pred likvidáciou.

Právne a normatívne rámce

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti

Vyžaduje riadenie rizík a implementáciu bezpečnostných opatrení u prevádzkovateľov základných služieb, vrátane zdravotníctva.

Vyhláška NBÚ č. 227/2025 Z.z.

Upravuje minimálne bezpečnostné opatrenia a úrovne kybernetickej bezpečnosti, ktoré sú povinné aj pre zdravotnícke zariadenia.

Nariadenie EÚ č. 2017/745 o zdravotníckych pomôckach (MDR)

Cieľom Nariadenia (EÚ) č. 2017/745 o zdravotníckych pomôckach (Medical Devices Regulation – MDR) je zabezpečiť, aby zdravotnícke pomôcky uvedené na trh EÚ boli bezpečné, účinné a spoľahlivé počas celého životného cyklu – od návrhu cez výrobu až po používanie. Hlavné požiadavky MDR:

- **Prísnejšie posudzovanie zhody** – výrobky sa zaraďujú do tried rizika (I–III) a podliehajú povinnému posúdeniu zhody; na posúdenie zhody síce neexistuje harmonizovaná certifikačná schéma, avšak postupy posudzovania sú definované v prílohách IX – XI MDR
- **Klinické hodnotenie** – výrobca musí preukázať účinnosť a bezpečnosť výrobku na základe klinických údajov, s cieľom overiť bezpečnosť a výkon výrobku, vrátane klinických prínosov pri jeho používaní
- **Sledovanie po uvedení na trh** – povinnosť výrobcov monitorovať výkon a bezpečnosť výrobkov počas ich používania
- **Vysledovateľnosť** – každá zdravotnícka pomôcka má UDI kód (Unique Device Identification) pre lepšiu identifikáciu a vysledovateľnosť a spätné stiahnutie v prípade rizika

- **Transparentnosť** – údaje o pomôckach sa zhromažďujú v európskej databáze zdravotníckych pomôcok (EUDAMED); zvyšuje sa tým transparentnosť a dôveryhodnosť dodávateľov
- **Zodpovednosť za výrobok** – sú jasne stanovené povinnosti všetkých článkov dodávateľského reťazca, od výrobcov až po distribútorov
- **Kybernetická bezpečnosť** – výrobca musí riešiť aj riziká vyplývajúce z IT a sieťovej prepojenosti zdravotníckych pomôcok

Nariadenie (EÚ) č. 2016/679 všeobecné nariadenie o ochrane údajov (GDPR)

Upravuje ochranu osobných údajov a voľný pohyb týchto údajov v EÚ; pri obstarávaní zdravotníckych technológií je kľúčové overiť, že spracovanie dát pacientov je v súlade s jeho požiadavkami.

Nariadenie Komisie (EÚ) č. 207/2012 o elektronických pokynoch na používanie zdravotníckych pomôcok

Nariadenie umožňuje, aby niektoré zdravotnícke pomôcky mali pokyny na používanie v elektronickej forme (eIFU), ak je zabezpečená ich dostupnosť, čitateľnosť a ochrana pred kybernetickými rizikami.

MDS² – vyhlásenie výrobcu o zabezpečení zdravotníckej pomôcky

MDS² je skratka pre štandardizovaný dokument „Manufacturer Disclosure Statement for Medical Device Security", ktorý výrobcovia poskytujú k svojmu zariadeniu alebo softvéru. Ide o "technický list" zariadenia z pohľadu kybernetickej bezpečnosti. Ide štandardizovaný formulár vypracovaný americkou Národnou asociáciou elektrotechnických výrobcov. Výrobcovia pomocou neho transparentne deklarujú úroveň zabezpečenia svojich výrobkov.

MDS² nie je súčasťou právnych predpisov EÚ, preto v Európe sa používa iba dobrovoľne, v rámci dobrej praxe. Nemocniciam môže pomôcť pri hodnotení rizík, zaraďovaní zariadení do bezpečnostnej architektúry a pri obstarávaní technológií podľa bezpečnostných požiadaviek.

Technické normy

Normy sú odporúčané technické riešenia. Sú tzv. kodifikovanou dobrou praxou a slúžia ako minimálny referenčný rámec. Technické normy sú právne záväzné sú len vtedy, ak na nich odkáže právny predpis (Príklad: MDR (EÚ 2017/745) odkazuje na použitie „harmonizovaných noriem" pre preukázanie zhody). Certifikácia podľa normy je vždy dobrovoľná, ale môže byť požadovaná trhom alebo zákazníkmi ako dôkaz kvality a bezpečnosti.

Existujú určité „znaky" podľa ktorých sa dá rozlíšiť, či je technická norma certifikačná (teda vhodná na certifikačný audit a vydanie certifikátu), alebo len usmerňujúca a informatívna. Certifikačné normy majú v názve spravidla slovo „Požiadavky" („Requirements").

V nasledujúcom zozname sú uvedené rôzne technické normy, ktoré sa využívajú v oblasti zdravotníctva, zdravotníckej informatiky a kybernetickej bezpečnosti.

Norma	Typ	Stručný účel
STN EN ISO 13485	Certifikačná	Systémy manažérstva kvality pre zdravotnícke pomôcky
STN ISO/IEC 20000 – 1	Certifikačná	Požiadavky na systém manažérstva IT služieb
STN EN ISO/IEC 27001	Certifikačná	Systém manažérstva informačnej bezpečnosti (ISMS)
STN EN ISO 27799	Návodová	Špecifické usmernenia pre informačnú bezpečnosť v zdravotníctve
STN EN ISO 12052	Návodová	Digitálne spracovanie obrazov a výmena dát v medicíne
STN EN IEC 80001 – 1	Návodová	Riadenie rizík pri IT sieťach obsahujúcich zdravotnícke pomôcky
STN EN ISO/IEC 27002	Návodová	Katalóg bezpečnostných opatrení (podpora k ISO/IEC 27001)
ISO 22857:2013	Návodová	Usmernenia k ochrane údajov pri cezhraničnom prenose zdravotných dát
STN EN ISO/IEC 27017	Návodová	Opatrenia pre cloudové služby (rozšírenie ISO/IEC 27002)
STN EN ISO/IEC 27018	Požiadavková	Opatrenia na ochranu osobných údajov v cloudoch
STN EN ISO 13972	Požiadavková	Definuje klinické informačné modely a ich štruktúru
STN EN ISO 14971	Požiadavková	Manažment rizík pre zdravotnícke pomôcky
STN EN 62304	Požiadavková	Požiadavky na životný cyklus softvéru zdravotníckych prístrojov
IEC 60364 – 7 – 710	Požiadavková	Elektroinštalácie v zdravotníckych priestoroch, ochrana pacientov a personálu
Séria ISA/IEC 62443	Požiadavkové	Kybernetická bezpečnosť systémov a komponentov, vhodné pre nemocničné IT/OT prostredia

HL7 – štandard pre zdieľanie zdravotníckych údajov

HL7 (Health Level Seven International) je medzinárodná nezisková organizácia a súbor štandardov, ktoré umožňujú bezpečnú a jednotnú výmenu elektronických zdravotných údajov medzi rôznymi informačnými systémami v zdravotníctve.

- Zabezpečuje interoperabilitu medzi nemocnicami, laboratóriami, poisťovňami a mobilnými aplikáciami.
- Znižuje chybovosť a administratívnu záťaž – dáta sa prenášajú automatizovane.
- Podporuje kvalitnejšiu a efektívnejšiu zdravotnú starostlivosť.

HL7 je kľúčovým „jazykom" na výmenu zdravotníckych dát – od klasických nemocničných systémov až po moderné mobilné aplikácie a cloudové služby.

Kybernetické riziká a hrozby v kontexte obstarávania

Zdravotnícke pomôcky

- Používanie zastaraných zariadení bez podpory od výrobcu a bez bezpečnostných aktualizácií.
- Predvolené heslá a slabé zabezpečenie, ktoré zvyšujú riziko neoprávneného prístupu.
- Riziko neautorizovaného vzdialeného prístupu a následného zneužitia zraniteľností.
- Nezabezpečená komunikácia pri prenose dát (chýbajúce šifrovanie).

Nemocničné informačné systémy (NIS)

- Riziko vzájomnej nekompatibility komponentov od rôznych dodávateľov.
- Riziko nezabezpečeného zdieľania dát medzi systémami.
- Interné hrozby – nesprávne používanie alebo zneužitie prístupov zo strany zamestnancov.
- Závislosť od poskytovateľov tretích strán a riziko vendor lock – in.

Cloudové služby

- Výpadky a nedostupnosť služieb, ktoré môžu ohroziť dostupnosť zdravotnej starostlivosti.
- Nedostatočná transparentnosť umiestnenia dát.
- Riziko porušenia GDPR pri prenose alebo spracovaní údajov mimo EÚ.
- Neexistujúci exit plán, t.j. zazmluvnený postup korektného ukončenia služby, napr. v súvislosti so zmenou dodávateľa.

Automatizačné a riadiace systémy (OT)

- IT/OT konvergencia – prepojenie fyzických a digitálnych prvkov ktoré zvyšuje riziko prieniku útokov.
- Možné útoky na kritickú infraštruktúru nemocnice s priamym dopadom na poskytovanie zdravotnej starostlivosti.
- Zastarané technológie bez podpory moderných bezpečnostných mechanizmov.
- Chýbajúca segmentácia sietí medzi IT a OT časťou, ktorá umožňuje šírenie útokov.

Konzultačné služby

- Neoverená odbornosť konzultantov – následné odporúčania bez praktickej hodnoty.
- Závislosť na dodávateľovi – vendor lock-in, ak konzultant neposkytne znalostný transfer.
- Nezohľadnenie špecifík zdravotníckeho prostredia.
- Konflikt záujmov – preferovanie riešení konkrétneho výrobcu namiesto objektívneho prístupu.
- Obmedzený rozsah služieb – napr. chýbajúce pokrytie OT bezpečnosti či riadenia súladu.

Riadené bezpečnostné služby (MSS)

- Nedostatočná zmluva o úrovni služieb (SLA) – nie všetci poskytovatelia MSS zabezpečujú skutočný 24/7 dohľad a rýchlu reakciu.
- Oneskorená reakcia na incidenty – ak v SLA nie je definovaná reakčná doba, incident môže zostať neodhalený alebo dlhodobo nevyriešený.
- Problémy s integráciou – MSS riešenia nemusia spolupracovať s existujúcou infraštruktúrou (IT, OT, IoT).
- Nedostatočné testovanie plánov obnovy (DRP/BCP) – bez pravidelných cvičení môže byť reakcia na veľký incident pomalá alebo neefektívna.
- Riziko porušenia GDPR a úniku zdravotníckych údajov.
- Vendor lock – in – vysoká závislosť od jedného poskytovateľa a komplikovaná migrácia k novému dodávateľovi MSS.

Odporúčané postupy pri obstarávaní

KO kritériá (minimálne, vylučovacie podmienky)

- Zapojenie IT a bezpečnostných tímov do všetkých fáz obstarávania
- NDA s poskytovateľom dodávateľských služieb, implementátora riešenia
- Predloženie Európskeho vyhlásenia o zhode (EU Declaration of Conformity)
- Povinná certifikácia dodávateľa podľa ISO 13485 (kvalita zdravotníckych pomôcok) alebo ISO/IEC 27001(informačná bezpečnosť)
- Preukázanie registrácie výrobku v EUDAMED a overenie jeho UDI kódu
- Predloženie údajov z klinického hodnotenia zdravotníckej pomôcky
- Overenie kvalifikácie a dôveryhodnosti dodávateľa (referencie, história, finančná stabilita)

Kvalitatívne kritériá (hodnotiace a výberové)

- Predloženie MDS² od výrobcu/integrátora – dobrovoľné, ale v SR vhodné ako hodnotiace kritérium
- Pri cloudových službách – doklad o súlade s ISO/IEC 27017 (cloudová bezpečnosť) a ISO/IEC 27018 (ochrana osobných údajov v cloude)
- Pri nemocničných informačných systémoch – podpora štandardov HL7 pre interoperabilitu
- Pri priemyselných riadiacich systémoch – požiadavka na aplikáciu noriem IEC 62443
- Posúdenie kybernetickej bezpečnosti zdravotníckej pomôcky (autentifikácia, patch management, logovanie)
- Požiadavka na šifrovanie dát pri prenose aj pri uložení
- Interoperabilita s existujúcou infraštruktúrou (hardvér, softvér, siete)

Bezpečné obstarávanie je investícia do budúcnosti. Kybernetická odolnosť musí byť rovnocenným kritériom vedľa ceny, kvality a výkonu. Zodpovedný nákup chráni pacientov, personál aj reputáciu zdravotníckeho zariadenia.

ENISA. Procurement guidelines for cybersecurity in hospitals: good practices for the security of Healthcare services. Luxembourg: Publications Office of the European Union, 2020. ISBN 978-92-9204-312-4. DOI 10.2824/943961.