European Union Agency
for Cybersecurity
Vasilissis Sofias Str 1
151 24 Maroussi | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

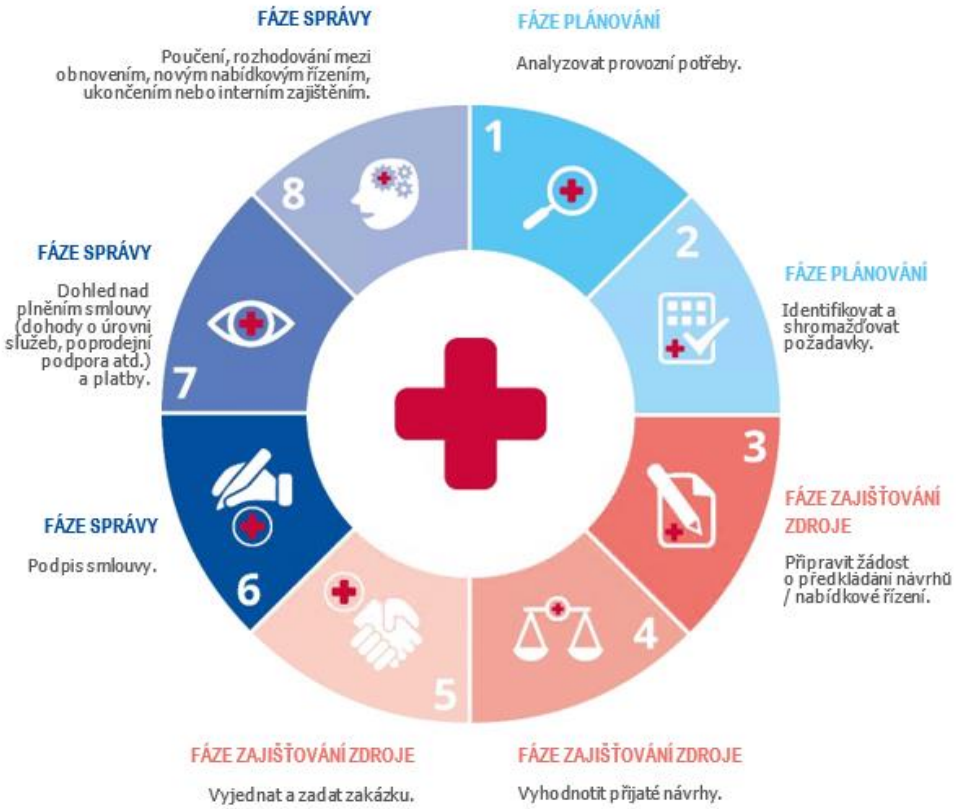
POKYNY PRO ZADÁVÁNÍ ZAKÁZEK V OBLASTI KYBERNETICKÉ BEZPEČNOSTI V NEMOCNICÍCH

Cílem této zprávy je poskytnout „příručku“ zdravotnickým pracovníkům. Řadu postupů a doporučení mohou využít i jiné zdravotnické organizace, protože procesy zadávání zakázek mohou být do značné míry podobné. Tuto zprávu mohou využít zdravotničtí pracovníci na technických pozicích v nemocnicích, tj. vedoucí pracovníci na nejvyšší úrovni: investiční ředitelé, ředitelé informační bezpečnosti, techničtí ředitelé, týmy IT a pracovníci odpovědní za zadávání zakázek ve zdravotnických organizacích. Tento krátký dokument pojednává o klíčových bodech zprávy – více podrobností lze nalézt v publikaci agentury ENISA s názvem: Good practices for the security of Healthcare services (Osvědčené postupy pro zabezpečení služeb zdravotní péče), která byla vydána v únoru 2020.

PROCES ZADÁVÁNÍ ZAKÁZEK

Nemocniční ekosystém se skládá z několika prvků IT, a proto je třeba kybernetickou bezpečnost zkoumat jednotlivě se zaměřením na tyto různé prvky. Kybernetická bezpečnost by měla být součástí všech fází procesu zadávání zakázek. V této části uvádíme společné fáze procesu zadávání zakázek na produkty a služby, včetně zdravotnických prostředků, informačních systémů a infrastruktur.

Obrázek 1: Životní cyklus procesu zadávání zakázek pro nemocnice



- Fáze plánování: Zpočátku nemocnice analyzuje své potřeby a interně shromažďuje požadavky z několika oddělení. Například v případě pořízení nové cloudové služby by měl technický ředitel identifikovat potřeby a porozumět tomu, jaký druh použitelnosti tato služba nabídne.

- Fáze zajišťování zdroje: Poté jsou požadavky převedeny do technických specifikací a ve spolupráci s oddělením pro zadávání zakázek začíná proces zajišťování zdroje (např. jsou zveřejněny informace o nabídkovém řízení). Nemocnice obdrží příslušné nabídky, výbor (včetně technického ředitele / ředitele informační bezpečnosti a/nebo člena týmu IT) nabídky vyhodnotí a vybere nejvhodnější produkty. Jsou vedena jednání s dodavatelem a zakázka je zadána.

- Fáze správy: Nakonec je smlouva (správa a monitorování) v nemocnici přidělena pracovníkovi odpovědnému za příslušnou oblast činnosti Příslušný pracovník je odpovědný za dokončení nabídkového řízení a přijetí případné zpětné vazby od uživatelů o skutečných vlastnostech zařízení / systému / služby.

TYPY ZAKÁZEK V NEMOCNICÍCH

Tabulka 1: Typy zakázek (taxonomie majetku)

Typ zakázky	Popis typu
Klinické informační systémy	Pod tento pojem spadá pořízení jakéhokoli druhu softwaru zaměřeného na lékařskou péči
Zdravotnické prostředky	Jakýkoli přístroj určený k léčbě, zvládání nebo diagnóze onemocnění
Síťová zařízení	Síťové vedení (koaxiální, optické), brány, směrovače, přepínače, brány firewall, VPN, IPS, IDS atd.
Systémy vzdálené péče	Zařízení nebo prostředky určené k poskytování péče mimo nemocniční prostředí, zejména v rámci toho, co se označuje jako „nemocniční služby domácí péče“.
Mobilní klientská zařízení	Veškerý software poskytující zdravotní pomoc nebo shromažďování lékařských údajů, který není přímo připojen k nemocniční síti; například aplikace telemedicíny
Identifikační systémy	Systémy k jedinečné identifikaci pacientů nebo zdravotnického personálu (biometrické skenery, čtečky karet atd.) a zajištění identifikace a/nebo oprávnění k přístupu k systémům IT.
Systémy správy budov	Jakýkoli typ stavby, který je schopen podporovat zdravotnická zařízení.
Průmyslové řídicí systémy	Systémy, které řídí veškeré hmotné aspekty středisek, jako jsou systémy regulace napájení, systémy zámku dveří, bezpečnostní systémy s uzavřeným okruhem.
Odborné služby	Všechny druhy služeb, ať už zajišťované externě či nikoli, poskytované odborníky nebo společnostmi: zdravotnické služby, doprava, účetnictví, inženýrské práce, IT, právní služby, údržba, úklid, stravování atd.
Cloudové služby	Jakýkoli počítačový nebo jiný informační systém, který se nenachází ve zdravotnické budově nebo v zařízení datového centra pod úplnou kontrolou oddělení IT zdravotnického centra.

TAXONOMIE HROZEB

Z různých typů zakázek vyplývají pro prostředí IKT nemocnice různé hrozby. Projděte si taxonomii hrozeb uvedenou v této části společně s oddělením IT, bezpečnostním oddělením nebo oddělením pro řízení rizik a určete, které hrozby jsou pro vaši organizaci nejdůležitější. Tato činnost by měla být součástí úkolů IT v nemocnici bez ohledu na potenciál zadávání zakázek.

Tabulka 2: Typy hrozeb (taxonomie hrozeb)

Hrozba	Příklady
Přírodní jevy	Požár, povodně nebo zemětřesení
Selhání dodavatelského řetězce	Selhání poskytovatele cloudových služeb, selhání poskytovatele sítě, selhání zdroje napájení, selhání / vyloučení odpovědnosti výrobce zdravotnického prostředku
Lidské chyby	Chyba konfigurace zdravotnického systému, neexistence auditních protokolů, neoprávněná kontrola přístupu / její nedostatek nebo neoprávněné procesy, nesoulad (přístup „přineste si vlastní zařízení“ (BYOD)), chyba zdravotnického personálu / pacienta
Zlovolné jednání	Malware (virus, ransomware, přístup „přineste si vlastní zařízení“ (BYOD)), napadení (nelegální těžba kryptoměn, napadení zdravotnických prostředků), sociální inženýrství (techniky phishing a baiting, klonování zařízení), krádež (údaje, zařízení), manipulace se zdravotnickými prostředky, technika skimming, útok na dostupnost služby (DOS), webové útoky, útoky na webové aplikace, vnitřní hrozba, fyzická manipulace / poškození, zneužití totožnosti, kybernetická špionáž, mechanické narušení komponentů
Selhání systému	Selhání softwaru, zastaralý firmware, selhání zařízení, selhání síťových komponentů, nedostatečná údržba

OSVĚDČENÉ POSTUPY PRO KYBERNETICKOU BEZPEČNOST PŘI ZADÁVÁNÍ ZAKÁZEK

Níže uvedený seznam osvědčených postupů není v žádném případě vyčerpávající, poskytuje však spolehlivou výhodu odborníkům IT ve zdravotnictví odpovědným za nákup vybavení v nemocnici. Tento soubor osvědčených postupů je souhrnným výsledkem veškerých příspěvků od dotazovaných zdravotnických pracovníků. Seznam je možné měnit na základě priorit příslušné organizace.

Osvědčený postup č. 1 Zapojit do jednotlivých fází zadávání zakázek oddělení IT s cílem zajistit zohlednění odborných znalostí týkajících se kybernetické bezpečnosti.

Fáze zadávání zakázky: Všechny

Související typy zakázek: Všechny

Související hrozby: Všechny

Osvědčený postup č. 2 Zavést proces identifikace a řízení zranitelnosti s cílem zajistit zohlednění zranitelností před pořízením nových produktů nebo služeb a sledování zranitelnosti stávajících produktů/služeb během jejich celého životního cyklu.

Fáze zadávání zakázky: Všechny

Související typy zakázek: Klinické informační systémy, zdravotnické prostředky, síťová zařízení, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, průmyslové řídicí systémy, cloudové služby

Související hrozby: Všechny

Osvědčený postup č. 3 Vypracovat zásady pro aktualizace hardwaru a softwaru s cílem zajistit, že se u operačního systému a softwaru použijí nejnovější opravy a že se aktualizuje antivirový software.

Fáze zadávání zakázky: Všechny

Související typy zakázek: Zdravotnické prostředky, klinické informační systémy, síťová zařízení, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, průmyslové řídicí systémy, cloudové služby

Související hrozby: Zlovolné jednání, selhání dodavatelského řetězce, selhání systému

Osvědčený postup č. 4 Posílit bezpečnostní kontroly bezdrátové komunikace s cílem zajistit, že přístup k bezdrátovým místním sítím nemocnice je omezený a přísně kontrolovaný.

Fáze zadávání zakázky: Všechny

Související typy zakázek: Zdravotnické prostředky, vzdálená klientská zařízení, identifikační systémy, cloudové služby

Související hrozby: Zlovolné jednání, lidské chyby

Osvědčený postup č. 5 Stanovit zásady testování s cílem zajistit, že nově získané nebo nově nakonfigurované produkty podstoupí penetrační testování a přijatá nápravná opatření jsou v souladu s provozními parametry skutečného prostředí.

Fáze zadávání zakázky: Všechny

Související typy zakázek: Klinické informační systémy, zdravotnické prostředky, síťová zařízení, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, systémy správy budov, průmyslové řídicí systémy, cloudové služby

Související hrozby: Zlovolné jednání, selhání systému, lidské chyby

Osvědčený postup č. 6 Vytvořit plány kontinuity provozu s cílem zajistit, že selhání systému nenaruší hlavní služby nemocnice a že je dobře vymezena úloha dodavatele.

Fáze zadávání zakázky: Všechny

Související typy zakázek: Zdravotnické prostředky, klinické informační systémy, síťová zařízení, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, průmyslové řídicí systémy, cloudové služby

Související hrozby: Zlovolné jednání, selhání dodavatelského řetězce, selhání systému

Osvědčený postup č. 7 Zohlednit problémy interoperability s cílem zajistit, že u komponentů, které jsou již v provozu (starší IT), neexistují žádné bezpečnostní mezery.

Fáze zadávání zakázky: Všechny

Související typy zakázek: Klinické informační systémy, zdravotnické prostředky, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, průmyslové řídicí systémy, cloudové služby

Související hrozby: Selhání systému, lidské chyby, zlovolné jednání

Osvědčený postup č. 8 Zavést testování všech komponentů s cílem zajistit, že poskytnou slibované vlastnosti: ověřit snadnost použití, zkontrolovat správnost výsledků při zatížení a zjistit případné nedostatky zabezpečení (slabé zásady hesel, prolomení SQL).

Fáze zadávání zakázky: Všechny

Související typy zakázek: Klinické informační systémy, zdravotnické prostředky, vzdálená klientská zařízení, identifikační systémy, cloudové služby, průmyslové řídicí systémy, systémy vzdálené péče, systém správy budov, mobilní klientská zařízení

Související hrozby: Zlovolné jednání, lidské chyby, selhání systému, selhání dodavatelského řetězce

Osvědčený postup č. 9 Povolit auditování a protokolování s cílem sledovat útočníky a získat údaje o množství ztracených/odcizených informací, pokud dojde k ohrožení systému.

Fáze zadávání zakázky: Všechny

Související typy zakázek: Zdravotnické prostředky, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, průmyslové řídicí systémy

Související hrozby: Zlovolné jednání, selhání dodavatelského řetězce, selhání systému

Osvědčený postup č. 10 Šifrovat neaktivní a přenášené citlivé osobní údaje vymezením zásad pro systémy, služby nebo zařízení, které zpracovávají zvláštní kategorie osobních údajů podle článku 9 nařízení GDPR.

Fáze zadávání zakázky: Všechny

Související typy zakázek: Zdravotnické prostředky, klinické informační systémy, síťová zařízení, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, průmyslové řídicí systémy, cloudové služby

Související hrozby: Zlovolné jednání, selhání dodavatelského řetězce, selhání systému

Osvědčený postup č. 11 V rámci procesu zadávání zakázek provádět posouzení rizika.

Fáze zadávání zakázky: Fáze plánování

Související typy zakázek: Všechny

Související hrozby: Všechny

Osvědčený postup č. 12 Plánovat síťové, hardwarové a licenční požadavky v předstihu s cílem zjistit, zda je za účelem přizpůsobení se novému systému před instalací nutné provést další upgrady nebo nákupy.

Fáze zadávání zakázky: Fáze plánování

Související typy zakázek: Klinické informační systémy, síťová zařízení, identifikační systémy, průmyslové řídicí systémy.

Související hrozby: Selhání dodavatelského řetězce, selhání systému, přírodní jevy, lidské chyby

Osvědčený postup č. 13 Identifikovat hrozby související s pořizovanými produkty nebo službami a zajistit, aby identifikace hrozeb probíhala nepřetržitě během celého životního cyklu zakázky.

Fáze zadávání zakázky: Fáze plánování a správy

Související typy zakázek: Všechny

Související hrozby: Všechny

Osvědčený postup č. 14 Oddělit síť s cílem zajistit, že lze síťový provoz izolovat a/nebo filtrovat za účelem omezení nebo zabránění přístupu mezi zónami sítě.

Fáze zadávání zakázky: Fáze plánování a zajišťování zdroje

Související typy zakázek: Zdravotnické prostředky, klinické informační systémy, síťová zařízení, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, průmyslové řídicí systémy, cloudové služby

Související hrozby: Zlovolné jednání, selhání dodavatelského řetězce, selhání systému

Osvědčený postup č. 15 Určit požadavky na síť s cílem zajistit interoperabilitu a předcházet mezerám po vytvoření topologie sítě a komponentů.

Fáze zadávání zakázky: Fáze plánování

Související typy zakázek: Klinické informační systémy, síťová zařízení, identifikační systémy, průmyslové řídicí systémy, cloudové služby, systémy vzdálené péče, mobilní klientská zařízení.

Související hrozby: Selhání dodavatelského řetězce, selhání systému, přírodní jevy

Osvědčený postup č. 16 Stanovit základní bezpečnostní požadavky a při výběru dodavatelů je převést do kritérií způsobilosti.

Fáze zadávání zakázky: Fáze plánování a zajišťování zdroje

Související typy zakázek: Zdravotnické prostředky, klinické informační systémy, síťová zařízení, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, průmyslové řídicí systémy, cloudové služby

Související hrozby: Zlovolné jednání, selhání dodavatelského řetězce, selhání systému

Osvědčený postup č. 17 Vytvořit zvláštní žádost o předkládání návrhů při pořizování cloudových služeb s přihlédnutím k regulačním požadavkům a požadavkům zásad.

Fáze zadávání zakázky: Fáze plánování a zajišťování zdroje

Související typy zakázek: Cloudové služby

Související hrozby: Zlovolné jednání, selhání dodavatelského řetězce

Osvědčený postup č. 18 Upřednostnit pořizování majetku, který je certifikován podle systémů/norem kybernetické bezpečnosti.

Fáze zadávání zakázky: Fáze zajišťování zdroje

Související typy zakázek: Zdravotnické prostředky, klinické informační systémy, síťová zařízení, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, průmyslové řídicí systémy, cloudové služby

Související hrozby: Zlovolné jednání, selhání dodavatelského řetězce, selhání systému

Osvědčený postup č. 19 Při plánování pořízení nového systému nebo služby provést posouzení vlivu na ochranu osobních údajů.

Fáze zadávání zakázky: Fáze zajišťování zdroje

Související typy zakázek: Klinické informační systémy, zdravotnické prostředky, síťová zařízení, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, odborné služby, cloudové služby

Související hrozby: Zlovolné jednání, lidské chyby

Osvědčený postup č. 20 Nastavit brány, které zajišťují připojení starších systémů/strojů a poskytují hraniční kontrolu v případě problémů uvnitř těchto skupin.

Fáze zadávání zakázky: Fáze zajišťování zdroje a správy

Související typy zakázek: Zdravotnické prostředky, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, průmyslové řídicí systémy

Související hrozby: Zlovolné jednání, selhání dodavatelského řetězce, selhání systému

Osvědčený postup č. 21 Poskytovat odbornou přípravu v oblasti kybernetické bezpečnosti o bezpečnostních postupech organizace s cílem zajistit, že interní zaměstnanci nebo externí smluvní partneři / konzultanti pracující v prostorách organizace absolvovali náležitou odbornou přípravu.

Fáze zadávání zakázky: Fáze zajišťování zdroje a správy

Související typy zakázek: Všechny

Související hrozby: Zlovolné jednání, lidské chyby

Osvědčený postup č. 22 Vypracovat plány reakce na incidenty, které pokrývají nově získané produkty nebo systémy.

Fáze zadávání zakázky: Fáze zajišťování zdroje a správy

Související typy zakázek: Zdravotnické prostředky, klinické informační systémy, síťová zařízení, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, průmyslové řídicí systémy, cloudové služby

Související hrozby: Zlovolné jednání, selhání dodavatelského řetězce, selhání systému

Osvědčený postup č. 23 Zapojit dodavatele/výrobce do správy incidentů a stanovit jasné podmínky v žádosti o předkládání návrhů.

Fáze zadávání zakázky: Fáze zajišťování zdroje a správy

Související typy zakázek: Zdravotnické prostředky, klinické informační systémy, síťová zařízení, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, průmyslové řídicí systémy, cloudové služby

Související hrozby: Zlovolné jednání, selhání dodavatelského řetězce, selhání systému

Osvědčený postup č. 24 Plánovat a sledovat údržbu všech zařízení s cílem zajistit odpovídající úroveň funkčnosti a rozhodovat o případných aktualizacích/opravách atd.

Fáze zadávání zakázky: Fáze zajišťování zdroje a správy

Související typy zakázek: Klinické informační systémy, síťová zařízení, zdravotnické prostředky, systémy správy budov, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, průmyslové řídicí systémy, cloudové služby

Související hrozby: Lidská chyba, selhání systému, přírodní jevy

Osvědčený postup č. 25 Je třeba minimalizovat vzdálený přístup a spravovat jej tak, aby externí komunikace s dodavatelem byla omezena pouze na zařízení, které musí ovládat.

Fáze zadávání zakázky: Fáze zajišťování zdroje a správy

Související typy zakázek: Zdravotnické prostředky, klinické informační systémy, síťová zařízení, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, průmyslové řídicí systémy, cloudové služby

Související hrozby: Zlovolné jednání, selhání dodavatelského řetězce, selhání systému, lidské chyby

Osvědčený postup č. 26 Vyžadovat opravu všech komponentů a zahrnout informace do žádosti o předkládání návrhů.

Fáze zadávání zakázky: Fáze zajišťování zdroje a správy

Související typy zakázek: Zdravotnické prostředky, klinické informační systémy, síťová zařízení, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, průmyslové řídicí systémy, cloudové služby

Související hrozby: Zlovolné jednání, selhání dodavatelského řetězce, selhání systému

Osvědčený postup č. 27 Zvyšovat povědomí zaměstnanců o kybernetické bezpečnosti s cílem zajistit, aby si byli vědomi rizik spojených s nově získanými produkty nebo službami.

Fáze zadávání zakázky: Fáze správy

Související typy zakázek: Všechny

Související hrozby: Všechny

Osvědčený postup č. 28 Provádět inventarizaci majetku a správu konfigurace s cílem zajistit, že se zařízení vhodně aktualizují, pokud se v prostředí IKT přidá nebo odebere nějaký komponent, a že existují základní bezpečnostní konfigurace pro komponenty IKT a jsou správně spravovány.

Fáze zadávání zakázky: Fáze správy

Související typy zakázek: Klinické informační systémy, zdravotnické prostředky, síťová zařízení, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy

Související hrozby: Zlovolné jednání, lidské chyby, selhání systému

Osvědčený postup č. 29 Zavést zvláštní mechanismy kontroly přístupu pro zařízení zdravotnických prostředků, která by měla být také fyzicky chráněna a přístupná pouze specializovaným pracovníkům.

Fáze zadávání zakázky: Fáze správy

Související typy zakázek: Zdravotnické prostředky, systém správy budov, identifikační systémy

Související hrozby: Zlovolné jednání, lidské chyby

Osvědčený postup č. 30 Naplánovat penetrační testování tak, aby se provádělo často nebo po změně v architektuře/systému, a zahrnout podmínky do žádosti o předkládání návrhů.

Fáze zadávání zakázky: Fáze zajišťování zdroje a správy

Související typy zakázek: Zdravotnické prostředky, klinické informační systémy, síťová zařízení, systém vzdálené péče, mobilní klientská zařízení, identifikační systémy, průmyslové řídicí systémy, cloudové služby

Související hrozby: Zlovolné jednání, selhání dodavatelského řetězce, selhání systému