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

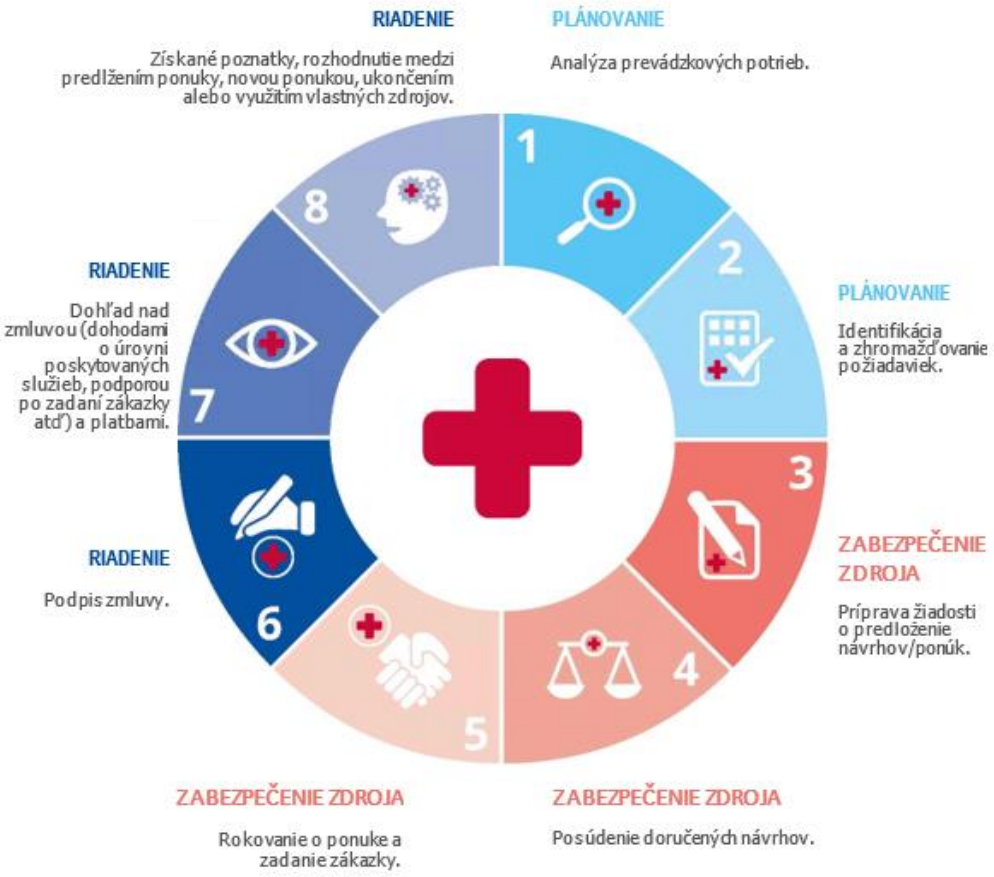
USMERNENIA K OBSTARÁVANIU V OBLASTI KYBERNETICKEJ BEZPEČNOSTI V NEMOCNICIACH

Cieľom tejto správy je plniť funkciu príručky pre zdravotníckych pracovníkov. Mnohé postupy a odporúčania budú užitočné aj pre ďalšie zdravotnícke organizácie, keďže postupy obstarávania sa môžu veľmi podobať. Poslúži zdravotníckym pracovníkom, ktorí pracujú na technických pozíciách v nemocniciach, napr. riadiacim pracovníkom, ako: riadiaci pracovník v oblasti IT, riadiaci pracovník v oblasti bezpečnosti IT, riadiaci pracovník v oblasti technológií, pracovníci IT tímov a pracovníci pre obstarávanie v organizáciách zdravotnej starostlivosti. V tejto krátkej štúdii sa rozoberajú kľúčové prvky správy, preto ak chce čitateľ bližšie informácie, musí si prečítať publikáciu agentúry ENISA: ENISA Good Practices for the Security of Healthcare Services (Osvedčené postupy agentúry ENISA pre bezpečnosť služieb zdravotnej starostlivosti), uverejnenú vo februári 2020.

POSTUP OBSTARÁVANIA

Keďže ekosystém nemocníc pozostáva z niekoľkých IT komponentov, kybernetická bezpečnosť by sa mala v prípade všetkých týchto komponentov skúmať osobitne. Kybernetická bezpečnosť by sa mala zohľadňovať v každej fáze obstarávania. V tejto časti vám predstavíme obvyklé fázy obstarávania na získanie produktov a služieb, ako sú zdravotnícke pomôcky, informačné systémy a infraštruktúry.

Obrázok č. 1: Cyklus obstarávania pre nemocnice



- Fáza plánovania: Najprv nemocnica vykoná analýzu svojich potrieb a zhromaždí interné požiadavky z viacerých oddelení. Ak sa majú napríklad obstarať nové cloudové služby, riadiaci pracovník v oblasti technológií by mal určiť potreby a pochopiť, ako sa tieto služby budú dať využívať.

- Fáza výberu: Následne sa požiadavky premietnu do technických špecifikácií a v spolupráci s oddelením obstarávania sa začne fáza výberu (napr. uverejní sa ponuka). Nemocnici sa doručia dané ponuky a výbor (pozostávajúci z riadiaceho pracovníka v oblasti technológií/riadiaceho pracovníka v oblasti bezpečnosti IT/riadiaceho pracovníka v oblasti IT a člena IT tímu) posúdi ponuky a vyberie najvhodnejšie produkty. Uskutočnia sa rokovania s dodávateľom a zadá sa zákazka.

- Fáza riadenia: Nakoniec sa zákazka (jej riadenie a monitorovanie) postúpi vlastníkovi podniku v rámci nemocnice. Určený pracovník zodpovedá za uzavretie zákazky a zozbieranie spätnej väzby od používateľov o skutočnom výkone zariadenia/systému/služby.

DRUHY OBSTARÁVANIA V NEMOCNICIACH

Tabuľka č. 1: Druhy obstarávania (taxonómia produktov a služieb)

Druh obstarávania	Opis
Systém klinických informácií	Zahŕňa obstarávanie akéhokoľvek softvéru zameraného na lekársku starostlivosť
Zdravotnícke pomôcky	Akýkoľvek hardvér na liečbu, kontrolu alebo diagnózu chorôb
Sieťové zariadenia	Sieťové káble (koaxiálne, optické), brány, smerovače, spínače, firewall, siete VPN, systém prevencie prienikov, systém detekcie prienikov atď.
Systémy starostlivosti na diaľku	Zariadenia alebo pomôcky na poskytovanie starostlivosti mimo nemocničného prostredia, najmä „nemocničné služby v rámci domácej starostlivosti“.
Mobilné zariadenia pre klientov	Všetky softvéry, ktoré poskytujú zdravotnú pomoc alebo získavanie lekárskych údajov, ktoré nie je priamo prepojené s nemocničnou sieťou, napr. aplikácie telemedicíny
Identifikačné systémy	Systémy, ktoré slúžia na jedinečnú identifikáciu pacientov alebo zdravotníckych pracovníkov (biometrické skenery, čítačky kariet atď.) a na zaručenie identifikácie a/alebo oprávnenia prístupu k informačným systémom.
Systémy správy budovy	Akákoľvek stavba, v ktorej sa môže nachádzať zdravotnícke zariadenie.
Priemyselné riadiace systémy	Systémy na riadenie všetkých fyzických aspektov zariadení, ako sú systémy regulácie elektriny, systémy zamykania dverí, bezpečnostné systémy v uzavretom okruhu.
Odborné služby	Všetky druhy služieb zabezpečených externe alebo interne, ktoré poskytujú odborníci alebo spoločnosti: zdravotnícke služby, prevoz, účtovníctvo, strojárske, IT a právne služby, údržba, zásobovanie atď.
Cloudové služby	Akýkoľvek komunikačný alebo informačný systém, ktorý sa nenachádza v budove zdravotníckeho zariadenia alebo v dátovom centre a je pod úplnou kontrolou IT oddelenia zdravotníckeho zariadenia.

TAXONÓMIA HROZIEB

Pri jednotlivých druhoch obstarávania môžu byť nemocničné informačné a komunikačné technológie vystavené rôznym hrozbám. Prejdite si spolu so svojím IT a bezpečnostným oddelením alebo oddelením rizík taxonómiu hrozieb, aby ste identifikovali hrozby, ktoré sú pre vašu organizáciu najrelevantnejšie. Táto činnosť by mala patriť medzi úlohy nemocničného IT tímu bez ohľadu na možnosť obstarávania.

Tabuľka č. 2: Druhy hrozieb (taxonómia hrozieb)

Hrozba	Príklady
Prírodné katastrofy	Požiar, povodeň alebo zemetrasenie
Zlyhanie dodávateľského reťazca	Zlyhanie alebo odmietnutie zodpovednosti na strane poskytovateľa cloudových služieb, poskytovateľa sieťových služieb, dodávateľa elektriny, výrobcu zdravotníckych pomôcok
Ľudské chyby	Chyba pri nastavení zdravotníckeho informačného systému, neexistencia kontrolných záznamov, kontrola neoprávneného prístupu alebo jej nedostatok alebo procesy, nedodržiavanie pravidiel (nosenie si vlastných zariadení), chyba zdravotníckeho pracovníka alebo pacienta
Škodlivé konanie	Malvér, (vírus, ransomware, nosenie si vlastných zariadení), ovládnutie (cryptojacking, medjacking – ovládnutie zdravotníckej pomôcky), sociálne inžinierstvo (phishing, baiting, klonovanie zariadení), krádež (údajov, zariadenia), neoprávnená manipulácia so zdravotníckou pomôckou, skimming, odmietnutie poskytnutia služby, útoky na webe, útoky vo webových aplikáciách, vnútorná hrozba, fyzická manipulácia/poškodenie, krádež totožnosti, kybernetická špionáž, mechanické narušenie komponentov
Zlyhania systému	Zlyhanie softvéru, neaktualizovaný firmvér, zlyhanie zariadenia, zlyhanie komponentov siete, nedostatočná údržba

OSVEDČENÉ POSTUPY NA ZAISTENIE KYBERNETICKEJ BEZPEČNOSTI PRI OBSTARÁVANÍ

Uvedený zoznam osvedčených postupov nie je v žiadnom prípade úplný, poskytuje však značnú výhodu IT pracovníkom v zdravotníctve, ktorí zodpovedajú za nákup zariadení v nemocniciach. Súbor osvedčených postupov je výsledkom kolektívneho zhromaždenia informácií od zdravotníckych pracovníkov, ktorí poskytli rozhovor. Čitateľ si môže zoznam prispôsobiť na základe priorít svojej organizácie.

OP č. 1: Zapojte IT oddelenie do jednotlivých fáz obstarávania, aby sa zabezpečilo zohľadnenie odborných znalostí v oblasti kybernetickej bezpečnosti.

Fázy obstarávania: Všetky

Súvisiace druhy obstarávania: Všetky

Súvisiace hrozby: Všetky

OP č. 2: Zaveďte proces identifikácie a riadenia zraniteľných miest, aby sa zabezpečilo, že zraniteľné miesta sa zohľadnia pred obstaraním nových produktov alebo služieb a že zraniteľné miesta existujúcich produktov alebo služieb sa monitorujú počas ich celého životného cyklu.

Fázy obstarávania: Všetky

Súvisiace druhy obstarávania: Systémy klinických informácií, zdravotnícke pomôcky, sieťové zariadenia, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, priemyselné riadiace systémy, cloudové služby

Súvisiace hrozby: Všetky

OP č. 3: Vypracujte politiku pre hardvérové a softvérové aktualizácie, aby ste zabezpečili, že sa nainštalujú najnovšie opravy v operačnom systéme a softvéri, ako aj aktualizuje antivírusový softvér.

Fázy obstarávania: Všetky

Súvisiace druhy obstarávania: Zdravotnícke pomôcky, systémy klinických informácií, sieťové zariadenia, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, priemyselné riadiace systémy, cloudové služby

Súvisiace hrozby: Škodlivé konanie, zlyhanie dodávateľského reťazca, zlyhania systému

OP č. 4: Zlepšite bezpečnostné kontroly bezdrôtovej komunikácie, aby ste zabezpečili, že prístup k Wi-Fi sieťam v nemocnici je obmedzený a podlieha prísnej kontrole.

Fázy obstarávania: Všetky

Súvisiace druhy obstarávania: Zdravotnícke pomôcky, zariadenia pre klientov na diaľku, identifikačné systémy, cloudové služby

Súvisiace hrozby: Škodlivé konanie, ľudské chyby

OP č. 5: Zaveďte politiky testovania, aby sa zabezpečilo, že novozískané alebo novonastavené produkty prejdú penetračným testom a že nápravné opatrenia sú prijaté v súlade s prevádzkovými parametrami skutočného prostredia.

Fázy obstarávania: Všetky

Súvisiace druhy obstarávania: Systémy klinických informácií, zdravotnícke pomôcky, sieťové zariadenia, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, systém správy budovy, priemyselné riadiace systémy, cloudové služby

Súvisiace hrozby: Škodlivé konanie, zlyhania systému, ľudské chyby

OP č. 6: Vypracujte plány na zabezpečenie kontinuity činností, aby sa zabezpečilo, že zlyhanie systému nenaruší základné služby nemocnice a úloha dodávateľa je jasné stanovená.

Fázy obstarávania: Všetky

Súvisiace druhy obstarávania: Zdravotnícke pomôcky, systémy klinických informácií, sieťové zariadenia, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, priemyselné riadiace systémy, cloudové služby

Súvisiace hrozby: Škodlivé konanie, zlyhanie dodávateľského reťazca, zlyhania systému

OP č. 7: Zohľadnite problémy týkajúce sa interoperability, aby sa zabezpečilo, že neexistujú žiadne nedostatky, pokiaľ ide o bezpečnosť už zavedených komponentov (pôvodných informačných systémov).

Fázy obstarávania: Všetky

Súvisiace druhy obstarávania: Systémy klinických informácií, zdravotnícke pomôcky, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, priemyselné riadiace systémy, cloudové služby

Súvisiace hrozby: zlyhania systému, ľudské chyby, škodlivé konanie

OP č. 8: Umožnite testovanie všetkých komponentov, aby sa zaručilo, že plnia svoj účel: Overte jednoduchosť používania, skontrolujte správnosť výsledkov počas záťaže a skontrolujte nedostatky, pokiaľ ide o bezpečnosť (nedostatočná politika vytvárania hesiel, útok SQL injection).

Fázy obstarávania: Všetky

Súvisiace druhy obstarávania: Systémy klinických informácií, zdravotnícke pomôcky, zariadenia pre klientov na diaľku, identifikačné systémy, cloudové služby, priemyselné riadiace systémy, systém starostlivosti na diaľku, systémy správy budovy, mobilné zariadenia pre klientov

Súvisiace hrozby: Škodlivé konanie, ľudské chyby, zlyhania systému, zlyhanie dodávateľského reťazca

OP č. 9: Umožnite kontrolu a zaznamenávanie údajov na vyhľadanie útočníkov a množstva ukradnutých údajov v prípade, že dôjde k ohrozeniu systému.

Fázy obstarávania: Všetky

Súvisiace druhy obstarávania: Zdravotnícke pomôcky, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, priemyselné riadiace systémy

Súvisiace hrozby: Škodlivé konanie, zlyhanie dodávateľského reťazca, zlyhania systému

OP č. 10: Zašifrujte citlivé osobné údaje v pokoji aj v pohybe vymedzením politiky pre systémy, služby alebo zariadenia spracúvajúce osobitné kategórie osobných údajov podľa článku 9 všeobecného nariadenia o ochrane údajov.

Fázy obstarávania: Všetky

Súvisiace druhy obstarávania: Zdravotnícke pomôcky, systémy klinických informácií, sieťové zariadenia, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, priemyselné riadiace systémy, cloudové služby

Súvisiace hrozby: Škodlivé konanie, zlyhanie dodávateľského reťazca, zlyhania systému

OP č. 11: Uskutočnite posúdenie rizika v rámci postupu obstarávania.

Fázy obstarávania: Plánovanie

Súvisiace druhy obstarávania: Všetky

Súvisiace hrozby: Všetky

OP č. 12: Vopred naplánujte požiadavky na sieť, hardvér a licencie s cieľom určiť, či je pred inštaláciou potrebné uskutočniť dodatočné vylepšenia a/alebo nákupy na účely prispôsobenia novému systému.

Fázy obstarávania: Plánovanie

Súvisiace druhy obstarávania: Systémy klinických informácií, sieťové zariadenia, identifikačné systémy, priemyselné riadiace systémy

Súvisiace hrozby: Zlyhanie dodávateľského reťazca, zlyhania systému, prírodné katastrofy, ľudské chyby

OP č. 13: Identifikujte hrozby súvisiace s obstarávaním produktov alebo služieb a zabezpečte, že identifikácia hrozieb sa uskutočňuje počas celého cyklu obstarávania.

Fázy obstarávania: Plánovanie, riadenie

Súvisiace druhy obstarávania: Všetky

Súvisiace hrozby: Všetky

OP č. 14: Oddeľte svoju sieť, aby sa zabezpečilo, že sieťovú prevádzku možno izolovať a/alebo filtrovať na obmedzenie a/alebo zabránenie prístupu medzi zónami sietí.

Fázy obstarávania: Plánovanie, zabezpečenie zdroja

Súvisiace druhy obstarávania: Zdravotnícke pomôcky, systémy klinických informácií, sieťové zariadenia, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, priemyselné riadiace systémy, cloudové služby

Súvisiace hrozby: Škodlivé konanie, zlyhanie dodávateľského reťazca, zlyhania systému

OP č. 15: Zistite, aké sú požiadavky na sieť, aby sa zabezpečila interoperabilita a zabránilo nedostatkom po vytvorení topológie siete a komponentov.

Fázy obstarávania: Plánovanie

Súvisiace druhy obstarávania: Systémy klinických informácií, sieťové zariadenia, identifikačné systémy, priemyselné riadiace systémy, cloudové služby, systémy starostlivosti na diaľku, mobilné zariadenie pre klientov

Súvisiace hrozby: Zlyhanie dodávateľského reťazca, zlyhania systému, prírodné katastrofy

OP č. 16: Určte základné bezpečnostné požiadavky a pri výbere dodávateľov ich premietnite do kritérií oprávnenosti.

Fázy obstarávania: Plánovanie, zabezpečenie zdroja

Súvisiace druhy obstarávania: Zdravotnícke pomôcky, systémy klinických informácií, sieťové zariadenia, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, priemyselné riadiace systémy, cloudové služby

Súvisiace hrozby: Škodlivé konanie, zlyhanie dodávateľského reťazca, zlyhania systému

OP č. 17: Vytvorte osobitnú žiadosť o predloženie návrhov na obstaranie cloudových služieb s ohľadom na požiadavky týkajúce sa regulácie a politiky.

Fázy obstarávania: Plánovanie, zabezpečenie zdroja

Súvisiace druhy obstarávania: Cloudové služby

Súvisiace hrozby: Škodlivé konanie, zlyhanie dodávateľského reťazca

OP č. 18: Uprednostnite obstarávanie produktov a služieb, ktoré sú certifikované podľa systémov alebo noriem certifikácie kybernetickej bezpečnosti.

Fázy obstarávania: Zabezpečenie zdroja

Súvisiace druhy obstarávania: Zdravotnícke pomôcky, systémy klinických informácií, sieťové zariadenia, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, priemyselné riadiace systémy, cloudové služby

Súvisiace hrozby: Škodlivé konanie, zlyhanie dodávateľského reťazca, zlyhania systému

OP č. 19: Pri plánovaní obstarávania nového systému alebo služby uskutočnite posúdenie vplyvu na ochranu údajov.

Fázy obstarávania: Zabezpečenie zdroja

Súvisiace druhy obstarávania: Systémy klinických informácií, zdravotnícke pomôcky, sieťové zariadenia, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, odborné služby, cloudové služby

Súvisiace hrozby: Škodlivé konanie, ľudské chyby

OP č. 20: Nastavte brány na udržanie pripojenia pôvodných systémov/zariadení a zaveďte kontroly hraníc medzi týmito skupinami pre prípad, že sa v niektorej vyskytne problém.

Fázy obstarávania: Zabezpečenie zdroja, riadenie

Súvisiace druhy obstarávania: Zdravotnícke pomôcky, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, priemyselné riadiace systémy

Súvisiace hrozby: Škodlivé konanie, zlyhanie dodávateľského reťazca, zlyhania systému

OP č. 21: Zaistite odbornú prípravu v oblasti kybernetickej bezpečnosti zameranú na bezpečnostné postupy organizácie, aby sa zabezpečilo, že interní pracovníci alebo externí dodávatelia/konzultanti pracujúci vo vašich priestoroch sú primerane zaškolení.

Fázy obstarávania: Zabezpečenie zdroja, riadenie

Súvisiace druhy obstarávania: Všetky

Súvisiace hrozby: Škodlivé konanie, ľudské chyby

OP č. 22: Vypracujte plány reakcie na incidenty, ktoré sa vzťahujú na novozískané produkty alebo systémy.

Fázy obstarávania: Zabezpečenie zdroja, riadenie

Súvisiace druhy obstarávania: Zdravotnícke pomôcky, systémy klinických informácií, sieťové zariadenia, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, priemyselné riadiace systémy, cloudové služby

Súvisiace hrozby: Škodlivé konanie, zlyhanie dodávateľského reťazca, zlyhania systému

OP č. 23: Do riadenia incidentov zapojte aj predajcu/výrobcu a stanovte jasné podmienky v žiadosti o predloženie návrhov.

Fázy obstarávania: Zabezpečenie zdroja, riadenie

Súvisiace druhy obstarávania: Zdravotnícke pomôcky, systémy klinických informácií, sieťové zariadenia, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, priemyselné riadiace systémy, cloudové služby

Súvisiace hrozby: Škodlivé konanie, zlyhanie dodávateľského reťazca, zlyhania systému

OP č. 24: Naplánujte a monitorujte údržbu všetkých zariadení, aby sa zabezpečila primeraná úroveň funkčnosti a rozhodlo o prípadných aktualizáciách/opravách atď.

Fázy obstarávania: Zabezpečenie zdroja, riadenie

Súvisiace druhy obstarávania: Systémy klinických informácií, sieťové zariadenia, zdravotnícke pomôcky, systémy správy budovy, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, priemyselné riadiace systémy, cloudové služby

Súvisiace hrozby: Ľudské chyby, zlyhania systému, prírodné katastrofy

OP č. 25: Mali by ste minimalizovať prístup na diaľku a spravovať ho spôsobom, aby externá komunikácia s dodávateľom bola obmedzená len na zariadenie, ktoré musí kontrolovať.

Fázy obstarávania: Zabezpečenie zdroja, riadenie

Súvisiace druhy obstarávania: Zdravotnícke pomôcky, systémy klinických informácií, sieťové zariadenia, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, priemyselné riadiace systémy, cloudové služby

Súvisiace hrozby: Škodlivé konanie, zlyhanie dodávateľského reťazca, zlyhania systému, ľudské chyby

OP č. 26: Požadujte opravy všetkých komponentov a uveďte túto informáciu v žiadosti o predloženie návrhov.

Fázy obstarávania: Zabezpečenie zdroja, riadenie

Súvisiace druhy obstarávania: Zdravotnícke pomôcky, systémy klinických informácií, sieťové zariadenia, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, priemyselné riadiace systémy, cloudové služby

Súvisiace hrozby: Škodlivé konanie, zlyhanie dodávateľského reťazca, zlyhania systému

OP č. 27: Zvýšte informovanosť o kybernetickej bezpečnosti medzi pracovníkmi, aby sa zabezpečilo, že si sú vedomí rizík súvisiacich s novozískanými produktmi alebo službami.

Fázy obstarávania: Riadenie

Súvisiace druhy obstarávania: Všetky

Súvisiace hrozby: Všetky

OP č. 28: Vykonávajte inventúru produktov a služieb a riadenie konfigurácie, aby sa zabezpečilo, že inventár je náležite aktualizovaný, ak sa akýkoľvek komponent pridá alebo odstráni z prostredia IKT, a že existujú základné bezpečnostné nastavenia pre komponenty IKT a primerane sa riadia.

Fázy obstarávania: Riadenie

Súvisiace druhy obstarávania: Systémy klinických informácií, zdravotnícke pomôcky, sieťové zariadenia, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy

Súvisiace hrozby: Škodlivé konanie, ľudské chyby, zlyhania systému

OP č. 29: Vytvorte osobitné mechanizmy na kontrolu prístupu k zdravotníckym pomôckam, ktoré by mali byť aj fyzicky chránené a prístupné iba špecializovaným pracovníkom.

Fázy obstarávania: Riadenie

Súvisiace druhy obstarávania: Zdravotnícke pomôcky, systémy správy budovy, identifikačné systémy

Súvisiace hrozby: Škodlivé konanie, ľudské chyby

OP č. 30: Penetračné testy plánujte pravidelne alebo po zmene v architektúre/systéme a podmienky uveďte do žiadosti o predloženie návrhov.

Fázy obstarávania: Zabezpečenie zdroja, riadenie

Súvisiace druhy obstarávania: Zdravotnícke pomôcky, systémy klinických informácií, sieťové zariadenia, systém starostlivosti na diaľku, mobilné zariadenia pre klientov, identifikačné systémy, priemyselné riadiace systémy, cloudové služby

Súvisiace hrozby: Škodlivé konanie, zlyhanie dodávateľského reťazca, zlyhania systému