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

# SMJERNICE ZA NABAVU U PODRUČJU KIBERSIGURNOSTI U BOLNICAMA

Svrha je ovog izvješća da posluži kao „vodič" zdravstvenim radnicima. Brojne navedene prakse i preporuke bit će korisne i drugim zdravstvenim organizacijama jer postupci nabave mogu biti vrlo slični. Bit će od koristi zdravstvenim radnicima koji obavljaju funkcije iz područja informacijskih tehnologija u bolnicama, tj. članovima izvršnog osoblja na rukovodećim položajima kao što su glavni službenik za informacijske tehnologije (CIO), glavni službenik za informacijsku sigurnost (CISO) i glavni službenik za tehnologiju (CTO), te timovima za IT i službenicima za nabavu u zdravstvenim organizacijama. U ovom kratkom dokumentu navode se samo ključne točke izvješća, a za dodatne pojedinosti pogledajte publikaciju ENISA-e: „Dobre sigurnosne prakse ENISA-e u području usluga zdravstvene zaštite", koja je objavljena u veljači 2020.

## POSTUPAK NABAVE

Budući da bolnički ekosustav obuhvaća nekoliko sastavnih elemenata koji se temelje na informacijskoj tehnologiji, aspekte kibersigurnosti potrebno je razmotriti zasebno s obzirom na sve te različite sastavne elemente. Kibersigurnost bi trebala biti dio svih različitih faza postupka nabave. U ovom odjeljku iznosimo zajedničke faze postupaka nabave za pribavljanje proizvoda i usluga, uključujući medicinske proizvode, informacijske sustave i infrastrukturu.

**Slika 1.** Životni ciklus postupka nabave u bolnicama


- Faza planiranja: Bolnica najprije analizira svoje potrebe i interno prikuplja zahtjeve različitih odjela. Na primjer, u slučaju nabave nove usluge računalstva u oblaku glavni službenik za tehnologiju trebao bi utvrditi potrebe i ustanoviti na koji će se način ta usluga moći upotrebljavati.

- Faza provedbe: Nakon toga se na temelju zahtjeva oblikuju tehničke specifikacije, a u suradnji s uredom za nabavu započinje provedba postupka nabave (npr. objavljuje se natječaj). Bolnica prima predmetne ponude, koje odbor (u čijem je sastavu glavni službenik za tehnologiju / glavni službenik za informacijsku sigurnost i/ili član tima za IT) zatim ocjenjuje i odabire najprikladnije proizvode. Zatim se vode pregovori s izvođačem i dodjeljuje se ugovor.

- Faza upravljanja: Naposljetku se ugovor (odnosno upravljanje ugovorom i njegovo praćenje) dodjeljuje rukovoditelju odgovornom za to područje u okviru bolnice. Nadležni službenik odgovoran je za zatvaranje natječajnog postupka i primanje povratnih informacija od korisnika o stvarnim radnim karakteristikama opreme/sustava/usluge.

## VRSTE NABAVE U BOLNICAMA

**Tablica 1.** Vrste nabave (klasifikacija imovine)

| Vrsta nabave | Opis vrste |
|---|---|
| **Klinički informacijski sustavi** | Uključuje nabavu bilo koje vrste softvera usmjerenog na pružanje zdravstvene skrbi |
| **Medicinski proizvodi** | Bilo koja vrsta hardvera namijenjenog liječenju, kontroli ili dijagnosticiranju bolesti |
| **Mrežna oprema** | Mrežni vodovi (koaksijalni, optički), pristupnici, usmjerivači, prekidači, vatrozidovi, virtualne privatne mreže, sustav za sprečavanje neovlaštenih aktivnosti, sustav za otkrivanje neovlaštenog upada itd. |
| **Sustavi za pružanje skrbi na daljinu** | Oprema ili uređaji za pružanje skrbi izvan bolničkog okruženja, posebno onoga što se danas naziva „pružanjem bolničke njege u domu pacijenta” |
| **Mobilni klijentski uređaji** | Svi softverski programi koji se upotrebljavaju za pružanje zdravstvene pomoći ili prikupljanje medicinskih podataka koji nisu izravno povezani s bolničkom mrežom; na primjer telemedicinske aplikacije |
| **Identifikacijski sustavi** | Sustavi za jedinstvenu identifikaciju pacijenata ili medicinskog osoblja (skeneri biometrijskih identifikatora, čitači kartica itd.), koji se upotrebljavaju kako bi se zajamčila identifikacija i/ili odobrio pristup informacijskim sustavima |
| **Sustavi za upravljanje zgradama** | Sve vrste građevina u kojima mogu poslovati medicinske ustanove |
| **Industrijski kontrolni sustavi** | Sustavi koji se upotrebljavaju za nadzor svih fizičkih aspekata medicinskog centra, kao što su sustavi za regulaciju potrošnje energije, sustavi za zaključavanje vrata, sigurnosni sustavi zatvorenog kruga |
| **Profesionalne usluge** | Usluge iz bilo kojeg područja, neovisno o tome eksternalizira li se njihovo pružanje, koje pružaju stručnjaci ili poduzeća: usluge iz područja medicine, prijevoza, računovodstva, inženjerstva, informacijske tehnologije, prava, održavanja, čišćenja, ugostiteljstva itd. |
| **Usluge računalstva u oblaku** | Bilo kakav komunikacijski i informacijski sustav ili drugi informacijski sustav koji se ne nalazi u zgradi bolnice ili u objektu podatkovnog centra pod potpunim nadzorom odjela za informacijsku tehnologiju medicinskog centra |

## KLASIFIKACIJA PRIJETNJI

Različite vrste nabave povezane su s različitim prijetnjama okružju IKT-a u bolnicama. Pregledajte klasifikaciju prijetnji opisanu u ovom odjeljku zajedno sa svojim odjelom za IT, sigurnost ili rizike kako biste utvrdili prijetnje koje su najrelevantnije za vašu organizaciju. Ta bi aktivnost trebala biti dio zadaća u području IT-a u bolnicama bez obzira na mogućnost nabave.

**Tablica 2.** Vrste prijetnji (klasifikacija prijetnji)

| Prijetnja | Primjeri |
|---|---|
| **Prirodne pojave** | Požari, poplave ili potresi |
| **Propusti i neispravnosti u lancu opskrbe** | Propusti za koje je odgovoran pružatelj usluga računalstva u oblaku ili pružatelj mrežnih usluga, prekid napajanja energijom, neispravnost medicinskih proizvoda za koju je odgovoran proizvođač / neodgovornost proizvođača |
| **Ljudske pogreške** | Pogreška u konfiguraciji medicinskog sustava, nepostojanje revizijskih dnevnika aktivnosti, nepostojanje kontrole neovlaštenog pristupa / neadekvatni postupci, nesukladnost (korištenje vlastitom računalnom opremom na radnom mjestu), pogreške medicinskog osoblja ili pacijenata |
| **Zlonamjerne radnje** | Zlonamjerni softver (virusi, ucjenjivački softver, korištenje vlastitom računalnom opremom na radnom mjestu), softver za preuzimanje nadzora (zlonamjerno rudarenje kriptovaluta, hakiranje medicinskih uređaja), socijalni inženjering („phishing”, „baiting”, tj. krađa podataka mamljenjem, kloniranje uređaja), krađa (podataka, uređaja), neovlašteno mijenjanje medicinskih proizvoda, krađa kartičnih podataka, uskraćivanje usluge, internetski napadi, napadi putem internetskih aplikacija, unutarnja prijetnja, fizička manipulacija/šteta, krađa identiteta, kiberšpijunaža, mehaničko ometanje rada sastavnih elemenata |
| **Kvarovi u sustavu** | Softverske greške, zastarjeli integrirani softver, kvarovi na uređajima, zakazivanje mrežnih komponenti, nedostatno održavanje |

## DOBRE PRAKSE ZA POTREBE NABAVE U PODRUČJU KIBERSIGURNOSTI

Popis primjera dobre prakse u nastavku ni u kojem slučaju nije iscrpan. Međutim, primjena navedenih praksi daje znatnu prednost zdravstvenom radniku stručnom u području IT-a koji je odgovoran za nabavu opreme u bolnici. Skup dobrih praksi zajednički je rezultat doprinosa svih zdravstvenih radnika s kojima su provedeni razgovori. Čitatelj može prilagoditi popis na temelju prioriteta svoje organizacije.

### Dobra praksa br. 1: Uključivanje odjela za IT u različite faze postupka nabave kako bi se osiguralo da se uzima u obzir stručno znanje u području kibersigurnosti

**Faze nabave:** sve

**Povezane vrste nabave:** sve

**Povezane prijetnje:** sve

### Dobra praksa br. 2: Provedba postupka za utvrđivanje ranjivosti i upravljanje njima kako bi se osiguralo da se ranjivosti uzmu u obzir prije nabave novih proizvoda ili usluga te kako bi se osiguralo da se ranjivosti postojećih proizvoda/usluga prate tijekom njihova životnog ciklusa

**Faze nabave:** sve

**Povezane vrste nabave:** klinički informacijski sustavi, medicinski proizvodi, mrežna oprema, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, industrijski kontrolni sustavi, usluge računalstva u oblaku

**Povezane prijetnje:** sve

### Dobra praksa br. 3: Razvoj politike u području ažuriranja hardvera i softvera kako bi se osigurala primjena najnovijih zakrpa namijenjenih vašem operativnom sustavu i softveru te kako bi se osiguralo ažuriranje antivirusnog softvera

**Faze nabave:** sve

**Povezane vrste nabave:** medicinski proizvodi, klinički informacijski sustavi, mrežna oprema, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, industrijski kontrolni sustavi, usluge računalstva u oblaku

**Povezane prijetnje:** zlonamjerne radnje, propusti i neispravnosti u lancu opskrbe, kvarovi u sustavu

### Dobra praksa br. 4: Poboljšavanje sigurnosnih kontrola bežične komunikacije kako bi se osiguralo da je pristup bežičnim mrežama bolnice ograničen i pod strogim nadzorom

**Faze nabave:** sve

**Povezane vrste nabave:** medicinski proizvodi, klijentski uređaji za rad na daljinu, identifikacijski sustavi, usluge računalstva u oblaku

**Povezane prijetnje:** zlonamjerne radnje, ljudske pogreške

### Dobra praksa br. 5: Uspostavljanje politika testiranja kako bi se osiguralo da se novostečeni ili tek konfigurirani proizvodi podvrgnu penetracijskom testiranju te da se poduzmu korektivne mjere u skladu s operativnim parametrima stvarnog okružja

**Faze nabave:** sve

**Povezane vrste nabave:** klinički informacijski sustavi, medicinski proizvodi, mrežna oprema, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, sustavi za upravljanje zgradama, industrijski kontrolni sustavi, usluge računalstva u oblaku

**Povezane prijetnje:** zlonamjerne radnje, kvarovi u sustavu, ljudske pogreške

### Dobra praksa br. 6: Utvrđivanje planova kontinuiteta poslovanja kako bi se osiguralo da kvarovi u sustavu ne ometaju pružanje osnovnih bolničkih usluga te da je uloga pružatelja usluga jasno definirana

**Faze nabave:** sve

**Povezane vrste nabave:** medicinski proizvodi, klinički informacijski sustavi, mrežna oprema, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, industrijski kontrolni sustavi, usluge računalstva u oblaku

**Povezane prijetnje:** zlonamjerne radnje, propusti i neispravnosti u lancu opskrbe, kvarovi u sustavu

### Dobra praksa br. 7: Uzimanje u obzir pitanja interoperabilnosti kako bi se osiguralo da ne postoje sigurnosni propusti u odnosu na postojeće komponente (postojeću IT opremu)

**Faze nabave:** sve

**Povezane vrste nabave:** klinički informacijski sustavi, medicinski proizvodi, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, industrijski kontrolni sustavi, usluge računalstva u oblaku

**Povezane prijetnje:** kvarovi u sustavu, ljudske pogreške, zlonamjerne radnje

### Dobra praksa br. 8: Omogućavanje ispitivanja svih komponenti kako bi se zajamčilo da će ostvariti predviđene rezultate: provjeriti jednostavnost upotrebe, provjeriti točnost rezultata pod opterećenjem i provjeriti sigurnosne nedostatke (politika u pogledu slabih lozinki, SQL injekcija)

**Faze nabave:** sve

**Povezane vrste nabave:** klinički informacijski sustavi, medicinski proizvodi, klijentski uređaji za rad na daljinu, identifikacijski sustavi, usluge računalstva u oblaku, industrijski kontrolni sustavi, sustavi za pružanje skrbi na daljinu, sustavi za upravljanje zgradama, mobilni klijentski uređaji

**Povezane prijetnje:** zlonamjerne radnje, ljudske pogreške, kvarovi u sustavu, propusti i neispravnosti u lancu opskrbe

### Dobra praksa br. 9: Omogućavanje provedbe revizija i vođenja evidencije kako bi se pronašli napadači i utvrdilo koliko je informacija izgubljeno/ukradeno u situacijama u kojima je sustav bio ugrožen

**Faze nabave:** sve

**Povezane vrste nabave:** medicinski proizvodi, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, industrijski kontrolni sustavi

**Povezane prijetnje:** zlonamjerne radnje, propusti i neispravnosti u lancu opskrbe, kvarovi u sustavu

### Dobra praksa br. 10: Šifriranje osjetljivih osobnih podataka u mirovanju i onih u tranzitu oblikovanjem politike za sustave, usluge ili uređaje u okviru kojih se obrađuju posebne kategorije osobnih podataka iz članka 9. Opće uredbe o zaštiti podataka

**Faze nabave:** sve

**Povezane vrste nabave:** medicinski proizvodi, klinički informacijski sustavi, mrežna oprema, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, industrijski kontrolni sustavi, usluge računalstva u oblaku

**Povezane prijetnje:** zlonamjerne radnje, propusti i neispravnosti u lancu opskrbe, kvarovi u sustavu

### Dobra praksa br. 11: Provedba procjene rizika kao dijela postupka nabave

**Faze nabave:** planiranje

**Povezane vrste nabave:** sve

**Povezane prijetnje:** sve

### Dobra praksa br. 12: Planiranje unaprijed zahtjeva povezanih s mrežom, hardverom i licencijama kako bi se utvrdilo moraju li se provesti dodatne nadogradnje i/ili kupnje prije ugradnje novog sustava kako bi se on mogao upotrebljavati

**Faze nabave:** planiranje

**Povezane vrste nabave:** klinički informacijski sustavi, mrežna oprema, identifikacijski sustavi, industrijski kontrolni sustavi

**Povezane prijetnje:** propusti i neispravnosti u lancu opskrbe, kvarovi u sustavu, prirodne pojave, ljudske pogreške

### Dobra praksa br. 13: Utvrđivanje prijetnji povezanih s proizvodima ili uslugama za koje se provodi nabava i osiguravanje da se prijetnje kontinuirano utvrđuju u svim fazama životnog ciklusa postupka nabave

**Faze nabave:** planiranje, upravljanje

**Povezane vrste nabave:** sve

**Povezane prijetnje:** sve

### Dobra praksa br. 14: Razdvajanje mreže kako bi se osiguralo da se mrežni promet može izolirati i/ili filtrirati u svrhu ograničavanja i/ili sprječavanja pristupa među različitim zonama mreže

**Faze nabave:** planiranje, provedba

**Povezane vrste nabave:** medicinski proizvodi, klinički informacijski sustavi, mrežna oprema, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, industrijski kontrolni sustavi, usluge računalstva u oblaku

**Povezane prijetnje:** zlonamjerne radnje, propusti i neispravnosti u lancu opskrbe, kvarovi u sustavu

### Dobra praksa br. 15: Utvrđivanje zahtjeva mreže kako bi se osigurala interoperabilnost i izbjegli propusti nakon uspostave topologije mreže i njezinih komponenti

**Faze nabave:** planiranje

**Povezane vrste nabave:** klinički informacijski sustavi, mrežna oprema, identifikacijski sustavi, industrijski kontrolni sustavi, usluge računalstva u oblaku, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji

**Povezane prijetnje:** propusti i neispravnosti u lancu opskrbe, kvarovi u sustavu, prirodne pojave

### Dobra praksa br. 16: Utvrđivanje osnovnih zahtjeva u pogledu sigurnosti i njihovo prenošenje u kriterije prihvatljivosti pri odabiru dobavljača

**Faze nabave:** planiranje, provedba

**Povezane vrste nabave:** medicinski proizvodi, klinički informacijski sustavi, mrežna oprema, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, industrijski kontrolni sustavi, usluge računalstva u oblaku

**Povezane prijetnje:** zlonamjerne radnje, propusti i neispravnosti u lancu opskrbe, kvarovi u sustavu

### Dobra praksa br. 17: Izrada posebnog zahtjeva za dostavu prijedloga namijenjenog za nabavu usluga računalstva u oblaku u kojem se uzimaju u obzir regulatorni zahtjevi i zahtjevi politike

**Faze nabave:** planiranje, provedba

**Povezane vrste nabave:** usluge računalstva u oblaku

**Povezane prijetnje:** zlonamjerne radnje, propusti i neispravnosti u lancu opskrbe

### Dobra praksa br. 18: Davanje prednosti nabavi imovine koja je certificirana u skladu s programima/normama u području kibersigurnosti

**Faze nabave:** provedba

**Povezane vrste nabave:** medicinski proizvodi, klinički informacijski sustavi, mrežna oprema, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, industrijski kontrolni sustavi, usluge računalstva u oblaku

**Povezane prijetnje:** zlonamjerne radnje, propusti i neispravnosti u lancu opskrbe, kvarovi u sustavu

### Dobra praksa br. 19: Provedba procjena učinka na zaštitu podataka pri planiranju nabave novog sustava ili usluge

**Faze nabave:** provedba

**Povezane vrste nabave:** klinički informacijski sustavi, medicinski proizvodi, mrežna oprema, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, profesionalne usluge, usluge računalstva u oblaku

**Povezane prijetnje:** zlonamjerne radnje, ljudske pogreške

### Dobra praksa br. 20: Uspostava pristupnika kojima se osigurava povezanost postojećih sustava/uređaja te nadzor granica između njih u slučaju problema unutar tih skupina

**Faze nabave:** provedba, upravljanje

**Povezane vrste nabave:** medicinski proizvodi, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, industrijski kontrolni sustavi

**Povezane prijetnje:** zlonamjerne radnje, propusti i neispravnosti u lancu opskrbe, kvarovi u sustavu

### Dobra praksa br. 21: Osiguravanje osposobljavanja u području kibersigurnosti o sigurnosnim praksama organizacije kako bi se osiguralo da interno osoblje ili vanjski izvođači/savjetnici koji rade u prostorima organizacije budu primjereno osposobljeni

**Faze nabave:** provedba, upravljanje

**Povezane vrste nabave:** sve

**Povezane prijetnje:** zlonamjerne radnje, ljudske pogreške

### Dobra praksa br. 22: Izrada planova za odgovor na incidente koji obuhvaćaju novostečene proizvode ili sustave

**Faze nabave:** provedba, upravljanje

**Povezane vrste nabave:** medicinski proizvodi, klinički informacijski sustavi, mrežna oprema, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, industrijski kontrolni sustavi, usluge računalstva u oblaku

**Povezane prijetnje:** zlonamjerne radnje, propusti i neispravnosti u lancu opskrbe, kvarovi u sustavu

### Dobra praksa br. 23: Uključivanje dobavljača/proizvođača u upravljanje incidentima i postavljanje jasnih uvjeta u zahtjevu za dostavu prijedloga

**Faze nabave:** provedba, upravljanje

**Povezane vrste nabave:** medicinski proizvodi, klinički informacijski sustavi, mrežna oprema, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, industrijski kontrolni sustavi, usluge računalstva u oblaku

**Povezane prijetnje:** zlonamjerne radnje, propusti i neispravnosti u lancu opskrbe, kvarovi u sustavu

### Dobra praksa br. 24: Izrada rasporeda održavanja i praćenje aktivnosti održavanja za svu opremu kako bi se osigurala odgovarajuća razina funkcionalnosti i odlučilo o eventualnim ažuriranjima/zakrpama itd.

**Faze nabave:** provedba, upravljanje

**Povezane vrste nabave:** klinički informacijski sustavi, mrežna oprema, medicinski proizvodi, sustavi za upravljanje zgradama, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, industrijski kontrolni sustavi, usluge računalstva u oblaku

**Povezane prijetnje:** ljudske pogreške, kvarovi u sustavu, prirodne pojave

### Dobra praksa br. 25: Daljinski pristup trebalo bi svesti na najmanju moguću mjeru i primjenjivati tako da vanjska komunikacija s dobavljačem bude ograničena samo na uređaj koji mora kontrolirati

**Faze nabave:** provedba, upravljanje

**Povezane vrste nabave:** medicinski proizvodi, klinički informacijski sustavi, mrežna oprema, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, industrijski kontrolni sustavi, usluge računalstva u oblaku

**Povezane prijetnje:** zlonamjerne radnje, propusti i neispravnosti u lancu opskrbe, kvarovi u sustavu, ljudske pogreške

### Dobra praksa br. 26: Zahtijevanje zakrpa za sve komponente i uključivanje informacija u zahtjev za dostavu prijedloga

**Faze nabave:** provedba, upravljanje

**Povezane vrste nabave:** medicinski proizvodi, klinički informacijski sustavi, mrežna oprema, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, industrijski kontrolni sustavi, usluge računalstva u oblaku

**Povezane prijetnje:** zlonamjerne radnje, propusti i neispravnosti u lancu opskrbe, kvarovi u sustavu

### Dobra praksa br. 27: Informiranje članova osoblja o kibersigurnosti kako bi se osiguralo da budu svjesni rizika povezanih s novostečenim proizvodima ili uslugama

**Faze nabave:** upravljanje

**Povezane vrste nabave:** sve

**Povezane prijetnje:** sve

### Dobra praksa br. 28: Upravljanje inventarom imovine i konfiguracijama kako bi se osiguralo da se inventar na odgovarajući način ažurira kada se bilo koja komponenta doda ili ukloni iz okružja IKT-a; postoje osnovne sigurnosne konfiguracije za komponente IKT-a i njima se upravlja na odgovarajući način

**Faze nabave:** upravljanje

**Povezane vrste nabave:** klinički informacijski sustavi, medicinski proizvodi, mrežna oprema, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi

**Povezane prijetnje:** zlonamjerne radnje, ljudske pogreške, kvarovi u sustavu

### Dobra praksa br. 29: Uspostavljanje namjenskih mehanizama kontrole pristupa prostorijama u kojima se nalaze medicinski proizvodi, koje bi trebale biti i fizički zaštićene i dostupne samo specijaliziranom osoblju

**Faze nabave:** upravljanje

**Povezane vrste nabave:** medicinski proizvodi, sustavi za upravljanje zgradama, identifikacijski sustavi

**Povezane prijetnje:** zlonamjerne radnje, ljudske pogreške

### Dobra praksa br. 30: Zakazivanje penetracijskih testiranja redovito ili nakon promjene u arhitekturi/sustavu i uključivanje uvjeta u zahtjev za dostavu prijedloga

**Faze nabave:** provedba, upravljanje

**Povezane vrste nabave:** medicinski proizvodi, klinički informacijski sustavi, mrežna oprema, sustavi za pružanje skrbi na daljinu, mobilni klijentski uređaji, identifikacijski sustavi, industrijski kontrolni sustavi, usluge računalstva u oblaku

**Povezane prijetnje:** zlonamjerne radnje, propusti i neispravnosti u lancu opskrbe, kvarovi u sustavu