Koncepcia bezpečnosti, verzia 7.0

Smart Remote Services

Systémová podpora.

Vždy, keď nás potrebujete.

siemens-healthineers.com

Unrestricted

SIEMENS Healthineers

Obsah

Smart Remote Services

Systémová podpora.

Vždy, keď nás potrebujete.

Lepšia služba. Pokoj mysle.
Umožňuje vám sústrediť sa na to najdôležitejšie – starostlivosť o pacienta.

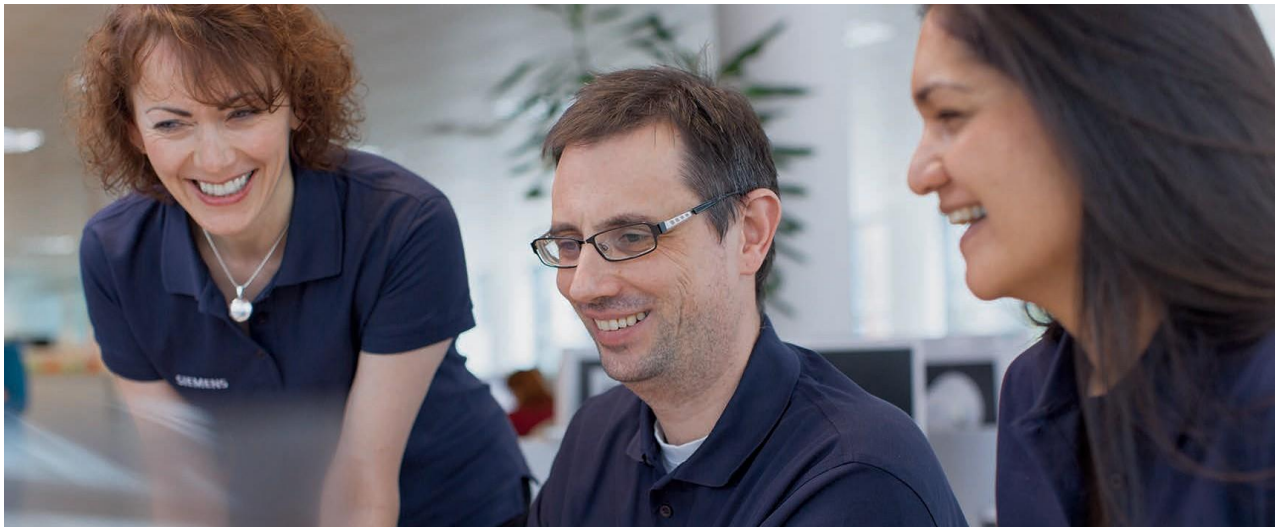
Vysoká dostupnosť systému, dôveryhodná diagnostika, optimalizovaný pracovný postup - na to, aby sme vždy boli schopní naplniť vaše očakávania ohľadom fungovania systému sa, v súlade s individuálnymi zmluvnými podmienkami, systematicky zameriavame na proaktivitu. Na diaľkové monitorovanie v reálnom čase, rýchlu používateľskú podporu v prípade problémov s aplikáciou a preventívnu údržbu zdravotníckych zariadení. Na proaktívnu analýzu a vopred zabezpečenú logistiku v súvislosti s plánovaním a realizáciou servisných úloh. A na inteligentné procesy, ktoré nám pomáhajú neustále sa zlepšovať.

Takýmto spôsobom pomáhame zabrániť vzniku porúch systému a výkyvom kvality ešte pred tým, než k ním dôjde. To všetko, aby ste mohli kráčať k úspechu – za lepšie využitie systému, efektivitu procesov a produktivitu. Proaktívne.

Bezpečnosť údajov a ochrana prístupu bola pre nás od samého začiatku najvyššou prioritou. Naša koncepcia bezpečnosti je rozdelená na dve hlavné časti.

Začneme všeobecnou prevádzkou a vysvetlíme základnú koncepciu inteligentných vzdialených služieb Smart Remote Services (SRS), náš servisný proces, aplikačnú podporu a technické možnosti našich produktov. Táto prvá časť je určená hlavne pre rádiológov, správcov nemocníc a technických manažérov, ktorí majú záujem získať základný prehľad o tom, ako SRS funguje a čo robíme na zabezpečenie ochrany osobných údajov.

Druhá časť – technická a organizačná koncepcia, je určená odborníkom na IT a dátovú bezpečnosť, ktorí potrebujú do detailov poznať, aké technické a organizačné bezpečnostné opatrenia realizujeme za účelom dosiahnutia vysokej miery bezpečnosti a ochrany osobných údajov pacientov. V tejto časti je vysvetlené, akým spôsobom sa nadväzuje spojenie s SRS, ako vyzerá naša bezpečnostná infraštruktúra a čo robíme, aby sme zabránili kybernetickým útokom



Úvod

Účel, rozsah a použitie

Táto bezpečnostná koncepcia opisuje opatrenia, ktoré v spoločnosti Siemens Healthineers realizujeme za účelom ochrany údajov pacientov pri poskytovaní SRS služieb na našich zdravotníckych zariadeniach, a to v oblasti technickej podpory, ako aj v oblasti ich klinického využitia. Používa sa v súvislosti so všetkými produktmi, pri ktorých je v ponuke služba SRS.

Bezpečnosť údajov ako základná podmienka

Pri návšteve lekára pacient očakáva, že budú dodržané predpisy ohľadom ochrany osobných údajov. To sa obzvlášť týka všetkých požiadaviek súvisiacich s bezpečnosťou a súkromím údajov. V kontexte bezpečnosti vzdialených služieb a aplikačnej podpory má povinnosť chrániť tieto údaje aj poskytovateľ zdravotnej starostlivosti, aj spoločnosť Siemens Healthineers. Technické a organizačné opatrenia, ktoré Siemens Healthineers využíva za účelom ochrany údajov súvisiacich s pacientmi, ako aj infraštruktúra slúžiaca na zabezpečenie služieb SRS, sú predmetom tejto koncepcie bezpečnosti.

Servis pre zdravotnícke zariadenia

Vzhľadom na to, že moderné zdravotnícke zariadenia, ich údržba a starostlivosť o ne sú čoraz zložitejšie, SRS zareagovala na túto výzvu poskytnutím dodatočnej podpory servisným technikom Siemens Healthineers priamo na mieste, aby mohli optimálnym spôsobom vykonávať servis systému. V niektorých prípadoch býva jednoducho efektívnejšie a rýchlejšie najprv zistiť príčinu problémov v systéme pomocou diaľkovej diagnostiky a pokiaľ je to možné, opraviť problém na diaľku. Aj v prípadoch, keď oprava na diaľku nie je možná, informácie získané pomocou diaľkovej diagnostiky môžu pomôcť servisnému technikovi Siemens Healthineers priamo na mieste.

To však nie je všetko. Vďaka našim proaktívnym službám nereagujeme až po vzniku problému, ale konáme preventívne. Náš softvér nezávisle monitoruje niektoré dôležité parametre vášho systému. Následne sa doručená správa analyzuje a v prípade potreby sa spustí preventívna diaľková oprava.

Ak hodnoty prekročia alebo klesnú pod vopred stanovené medze, systém automaticky odošle správu do nášho Centra starostlivosti o zákazníkov. Pacienti to nepocítia. Problém uvedený v správe môžeme odstrániť aj priamo na mieste a v rámci uzavretej servisnej zmluvy.

Či už ide o opravu na mieste alebo na diaľku, mnohé problémy možno zistiť a odstrániť na základe technických údajov zo systému. Prístup k údajom pacientov vo väčšine prípadov nie je potrebný. Ak by bolo v nejakých ojedinelých prípadoch potrebné zabezpečiť prístup k súborom údajov alebo k snímkam obsahujúcim údaje pacientov, pokiaľ je to možné, údaje pacientov budú pred odoslaním spoľahlivo automaticky odstránené.
V prípade kategórií produktov, pri ktorých toto nie je technicky možné, alebo ak to neumožňuje samotná úloha (napríklad pri prístupe k databázam), prístup k údajom pacientov v maximálnej možnej miere obmedzujeme a zároveň realizujeme osobitné technické a organizačné bezpečnostné opatrenia.

Použitie štandardného riešenia

Stále viac výrobcov ponúka k svojím produktom vzdialené služby v rôznych konfiguráciách. To vedie k zvýšenému počtu rôznych vzdialených spojení medzi zákazníkmi a výrobcami produktov, ako aj k zvýšeným administratívnym nákladom pre zákazníka. Zvýšená administratívna náročnosť však môže zvýšiť aj pravdepodobnosť bezpečnostných nedostatkov. Tomu sa chceme vyhnúť. Ponúkame riešenie vytvorené a schválené výrobcami v USA, Európe a Japonsku v rámci Spoločného výboru pre bezpečnosť a ochranu súkromia NEMA/COCIR/JIRA (www.nema.org/medical/spc).

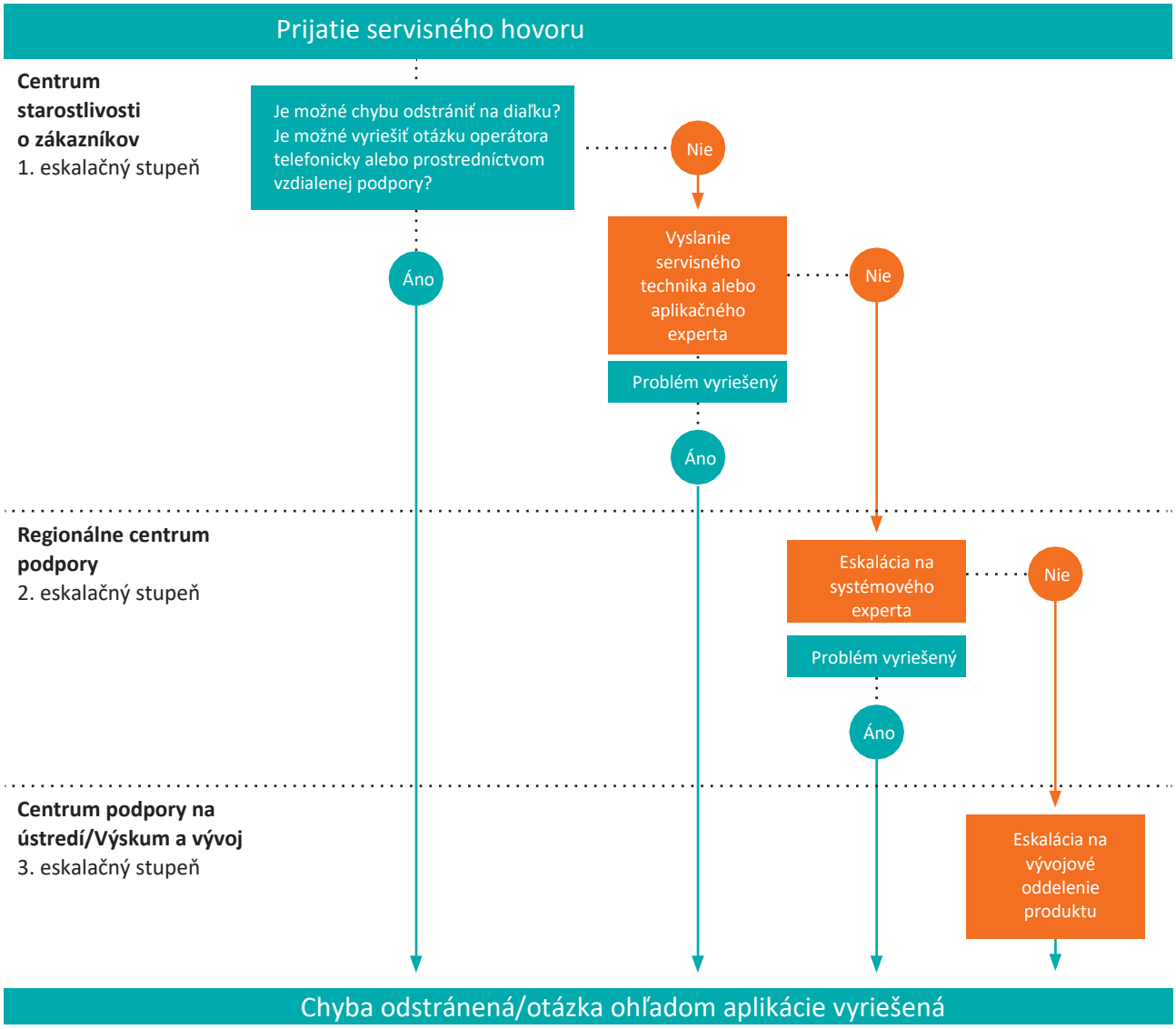
Toto riešenie zohľadňuje technickú realizovateľnosť v zákazníckych organizáciách rôznej zložitosti, ako aj základné právne požiadavky v USA (HIPAA), v Európe a v Japonsku. Vďaka tomu naši zákazníci vedia oveľa ľahšie splniť všetky platné právne požiadavky.

Siemens Healthineers je jedným z prvých výrobcov zdravotníckych zariadení na svete, ktorý zaviedol medzinárodne platný systém riadenia informačnej bezpečnosti (ISMS) na vzdialené služby zdravotníckych zariadení a softvérových systémov. Systém je certifikovaný nemeckou spoločnosťou TÜV Süd podľa medzinárodnej normy ISO 27001.

Vzdialený prístup v servisnom procese Siemens Healthineers

Na obrázku č. 1 je znázornený schematický diagram celého procesu eskalácie servisných volaní, vrátane pracovných činností vykonávaných zvyčajne priamo na mieste. Po prijatí správy o udalosti, Centrum starostlivosti o zákazníkov pomocou diaľkovej diagnostiky SRS zistí viac o charaktere problému a jeho možných príčinách. Ak je to možné, chyba sa opraví na diaľku. V opačnom prípade vyšleme servisného technika alebo experta na príslušnú aplikáciu, ktorý vyrieši problém na mieste na základe informácií získaných pomocou vzdialenej diagnostiky (1. eskalačný stupeň).

Ak sa problém nepodarí vyriešiť, eskalujeme ho na Regionálne centrum podpory (2. eskalačný stupeň), kde odborníci špecializujúci sa príslušný systém alebo skupinu systémov majú hlbšie technické znalosti. Ak sa problém ani teraz nepodarí vyriešiť, informácia sa preposiela (3. eskalačný stupeň) do Centra podpory na ústredí, prípadne na oddelenie vývoja daného produktu, kde budú pracovať na vašom probléme špecialisti.



Obr. č. 1:
Proces eskalácie pri vybavovaní servisných hovorov

Aplikačná podpora

Množstvo rôznych aplikácií a nastavení parametrov v jestvujúcom systéme môže viesť k otázkam používateľov, ktoré si vyžadujú okamžitú odpoveď. Prostredníctvom služby SRS môžeme získať prístup do vášho systému – za predpokladu, že nám k tomu dáte súhlas. Postup je jednoduchý: Ak potrebujete pomoc, stačí sa obrátiť na naše Centrum starostlivosti o zákazníkov. Pomocou našej zabezpečenej infraštruktúry SRS sa servisné centrum spojí s vašim systémom.

Od nášho špecialistu dostanete identifikačné číslo relácie. Toto identifikačné číslo je potrebné zadať do príslušného dialógového okna. Až po potvrdení vyskakovacieho okna, ktoré obsahuje vyhlásenie o ochrane osobných údajov, v ktorom sa uvádza, že zamestnanec spoločnosti Siemens Healthineers môže potenciálne zobraziť údaje pacienta, dôjde k zdieľaniu vašej obrazovky. Následne vás bude náš špecialista môcť krok za krokom previesť aplikáciou.

Technické možnosti produktov Siemens Healthineers

Našim cieľom je bezpečnosť a ochrana osobných údajov

Pri všetkých činnostiach služby SRS je naším cieľom pristupovať k údajom pacientov len v prípadoch, keď je to absolútne nevyhnutné a iba v minimálnej, technicky požadovanej miere. Dôsledným uplatňovaním tohto štandardu sa nám podarilo splniť tento cieľ vo väčšine kategórií našich výrobkov.

Zabezpečená a spoľahlivá infraštruktúra SRS v kombinácii s náležitými organizačnými opatreniami umožňuje zabezpečiť dôvernosť a ochranu súkromia údajov pacientov. Infraštruktúra je založená na prepojení vášho systému a vzdialeného servera Siemens Healthineers prostredníctvom VPN spojenia využitím trend určujúceho moderného softvéru pre údržbu zariadení. Dostupné funkcie závisia od verzie softvéru a samotného produktu. Tu je potrebné rozlišovať medzi produktmi, ktoré používajú náš aplikačný softvér *syngo*®[1] a ostatnými produktami. K tej druhej skupine patria hlavne niektoré pracoviská PACS.

Aplikačný softvér *syngo*

syngo je nami vyvinuté softvérové riešenie, ktoré v prípade proaktívneho technického servisu pred odoslaním informácií do Centra starostlivosti o zákazníkov zamaskuje údaje o pacientoch. Najnovšia verzia[2] softvéru s*yngo* vám navyše umožňuje predvoliť používateľov, ktorí budú mať povolenie prístupu ku konkrétnym údajom na ich zariadení. Rozhodnutie o tom, kedy poskytnúť našim servisným technikom alebo vašim zamestnancom prístup ku konkrétnym údajom je teda výhradne na vás, pričom udelený prístup môžete kedykoľvek zablokovať.

Kategórie produktov, ktoré nepoužívajú *syngo*

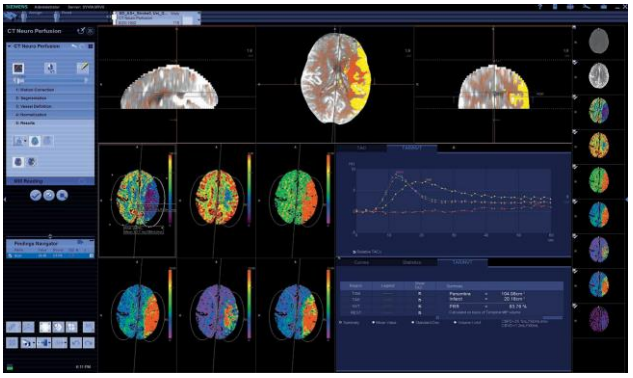
Primárnou funkciou týchto produktov je riadenie databáz, čo technicky obmedzuje našu schopnosť skryť alebo odstrániť údaje týkajúce sa pacientov. V závislosti od druhu problému si činnosti údržby databáz niekedy vyžadujú prístup k údajom v databáze. V tomto prípade sú naše technické a organizačné opatrenia (pozrite kapitolu "Koncepcia technického a organizačného zabezpečenia" od strany 7) spolu so zabezpečenou a spoľahlivou infraštruktúrou SRS (pozrite časť "Bezpečnostná infraštruktúra SRS" na strane 9) navrhnuté tak, aby zabezpečili ochranu osobných údajov pacientov.

Funkcie online podpory (aplikačná podpora)

Vzdialený prístup k vašim systémom za účelom online podpory (napríklad v prípade otázok používateľov ohľadom prevádzky) sa tiež poskytuje prostredníctvom nástrojov na vzdialenú správu počítača. Tieto nástroje presne 1:1 replikujú obrazovku vášho monitora v Centre starostlivosti o zákazníkov a umožňujú aplikačnému expertovi diaľkové ovládanie. Z technického hľadiska je to však možné len vtedy, ak na to výslovne povolíte prístup. Takáto autorizácia sa vyžaduje pre každú jednu reláciu samostatne. Počas celej relácie ste telefonicky spojený s vašou kontaktnou osobou v Siemens Healthineers. Okrem toho môžete v týchto prípadoch sledovať priebeh online podpory a v prípade potreby ukončiť prístup poskytnutý Centru starostlivosti o zákazníkov.

Proaktívne servisné činnosti

Jednou z našich proaktívnych servisných služieb je, že vaše zariadenie aktívne odosiela vopred stanovené systémové údaje do Centra starostlivosti o zákazníkov. Súčasťou sú technické údaje, ako napríklad systémové logy, štatistické údaje (napríklad počet reštartov a skenov) a údaje o spoľahlivosti systému. Tieto proaktívne služby nevyžadujú prístup alebo prenos údajov súvisiacich s pacientmi.



Obr. č. 2:
Používateľské rozhranie *syngo*: Anonymizácia zdravotných informácii

[1] *syngo je registrovaná ochranná známka spoločnosti Siemens Healthcare GmbH*

[2] *Informáciu o verzii softvéru vo vašom systéme môžete získať od zástupcu spoločnosti Siemens Healthineers*

Prehľad

V nasledovnej časti sú opísané technické a organizačné opatrenia, ktoré používame na zabezpečenie vysokej úrovne ochrany osobných údajov a bezpečnosti. Viac informácií o jednotlivých prvkoch bezpečnostnej infraštruktúry SRS nájdete v časti "Bezpečnostná infraštruktúra SRS" na strane 9.

Nadviazanie spojenia

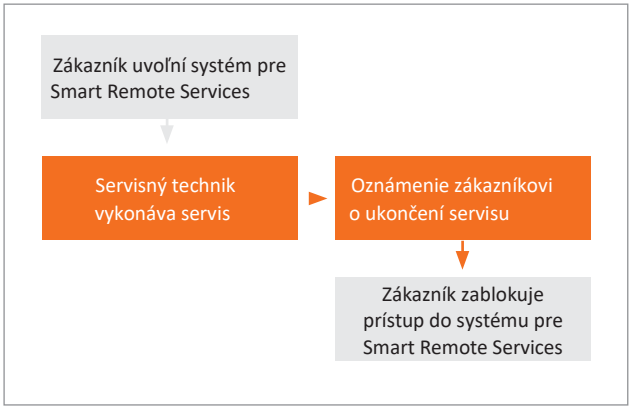
O tom, do akej miery zákazník, pomocou nášho aplikačného softvéru *syngo,* udelí prístup do systému, záleží výhradne na ňom. Na vytvorenie relácie aplikačnej podpory je potrebné vygenerovať heslo relácie. Inými slovami, prístup k vášmu monitoru zdieľate s našim odborníkom vždy od prípadu k prípadu a po vyriešení problému sa spojenie ukončí. Prístup do vašich systémov bez vášho súhlasu nie je možný. Pri nadväzovaní spojenia za účelom vzdialeného servisu si môžete zvoliť štyri úrovne prístupu:

- **Bez prístupu**
  Prístup poskytujete vždy pre každý prípad samostatne za účelom realizácie schválenej úlohy. Vyšetrovania pacientov pomocou systému môžu naďalej prebiehať.

- **Obmedzený prístup**
  Autorizovaný servisný technik Siemens Healthineers má obmedzený prístup do vášho systému. Je možné zadefinovať časový limit a vyšetrenia pacientov môžu naďalej prebiehať.

- **Trvalý obmedzený prístup**
  Autorizovaný servisný technik má trvalý obmedzený prístup do vášho systému. Inými slovami, prístup nie je časovo obmedzený. Vyšetrenia pacientov môžu prebiehať.

- **Úplný prístup**
  Autorizovaný servisný technik má úplný prístup do vášho systému. Kým sa vykonáva vzdialený servis, vyšetrenia pacientov nemôžu prebiehať. Jednotlivé úrovne prístupu určujú, do akej miery a v akom časovom rámci chcete poskytnúť prístup do vášho systému. Bez ohľadu na to, akú úroveň prístupu zvolíte, pred prenosom sú údaje pacientov automaticky blokované a vy máte vždy vo svojej moci udeliť alebo zmeniť prístupové práva podľa potreby.



Obr. č. 3
Priebeh SRS činností na úrovni "bez prístupu"

Najčastejšie zvolenou úrovňou prístupu býva „trvalý obmedzený prístup“, ale vždy si môžete vybrať aj úroveň „bez prístupu“. Obrázok č. 3 znázorňuje postup pri realizácii vzdialenej servisnej úlohy na tejto úrovni. Za účelom vytvorenia čo najbezpečnejšieho spojenia sme pevne stanovili spôsob, ako servisní technici Siemens Healthineers Service môžu vstupovať do zákazníckych systémov. V závislosti od technických možností sa konkrétne zariadenie alebo konkrétne zákaznícke implementácie môžu odlišovať od informácií uvedených v tomto dokumente.

Riadenie prístupu

Nevyhnutnou podmienkou akejkoľvek servisnej činnosti je, aby ste výslovne povolili prístup k SRS a aby ste určili, kto má povolený prístup do systému. Prístup sa povoľuje výlučne za účelom identifikácie alebo opravy chýb. Nastavovanie parametrov merania, ako napr. prístupom k protokolom skenovania, je technicky možné iba počas aplikačnej podpory a iba s vaším súhlasom. Po uplynutí určitého času nečinnosti sa relácia SRS vo vašom systéme automaticky ukončí.

Princíp štyroch očí

Zákazníkovi sa na jeho systémovej obrazovke zobrazí vizuálny indikátor, že momentálne prebiehajú vzdialené servisné činnosti. Naši servisní technici/aplikační experti sa okrem toho s vami budú telefonicky zhovárať a vysvetľovať vám, aké činnosti momentálne vykonávajú. Počas každej relácie SRS môžu zamestnanci zákazníka servisnému expertovi kedykoľvek prerušiť prístup do systému. V takom prípade sa všetky spustené servisné programy riadeným spôsobom okamžite vypnú tak, aby to nemalo vplyv na dlhodobú bezpečnú prevádzku systému, na ktorom sa vykonávala údržba.

Protokolovanie vzdialených prístupov

V platforme SRS sa zaznamenáva každý priamy prístup do vášho systému spolu s časovou značkou. Okrem toho má každý servisný technik/aplikačný expert pridelený jedinečný identifikátor používateľa, ktorý sa tiež zaznamenáva do daného logu. Vďaka tomu vám za primeraný čas (tri pracovné dni od prijatia žiadosti) vieme dať informáciu o tom, ktorý odborník a kedy mal prístup k údajom. Tieto logy archivujeme minimálne jeden rok.

Oznámenie e-mailom pred pripojením

Ďalšou možnosťou je prostredníctvom vzdialeného servera Siemens Healthineers na požiadanie aktivovať e-mailovú službu, ktorá vašim technickým, klinickým a/alebo riadiacim pracovníkom poskytne podrobné údaje o spojení pri každom diaľkovom spojení. K tomuto e-mailu možno doplniť ešte druhú správu pri odpojení, v ktorej je uvedený dôvod zásahu a voľný text, ktorý môže obsahovať, napríklad, podrobnosti o vykonaných činnostiach alebo o úspešnom ukončení úlohy.

Ochrana súkromia pozdĺž prenosovej cesty

Na ochranu údajov zákazníkov pred neoprávneným prístupom počas prenosu využívame moderné metódy šifrovania. Všetky spojenia cez internet sú zvyčajne šifrované. Viac informácií nájdete v časti "Bezpečnostná infraštruktúra SRS" na strane 9.

Organizačné opatrenia

Naši servisní technici/aplikační experti si uvedomujú potrebu zachovania dôvernosti údajov pacientov a chápu závažnosť dôsledkov, ak by sa neriadili príslušnými požiadavkami. Oprávnenie vykonávať vzdialené služby na zdravotníckych systémoch majú iba vyškolení servisní technici/aplikační experti, ktorí si ctia ochranu a bezpečnosť osobných údajov. Na vzdialenom serveri spoločnosti Siemens Healthineers je uložený elektronický zoznam týchto vybraných servisných zamestnancov, ako aj ich príslušné prístupové práva.

Bezpečnostná infraštruktúra SRS

V tejto kapitole sú uvedené dodatočné technické informácie o nasledujúcich prvkoch bezpečnostnej infraštruktúry SRS: autentifikácia a autorizácia servisných technikov/aplikačných expertov na platforme SRS, "demilitarizovaná zóna" (DMZ) medzi intranetom Siemens Healthineers a internetom, protokoly a služby používané pri prenose, ako aj prípadné bezpečnostné opatrenia v zákazníckej sieti.

Autentifikácia a autorizácia našich servisných technikov a voliteľných obchodných partnerov

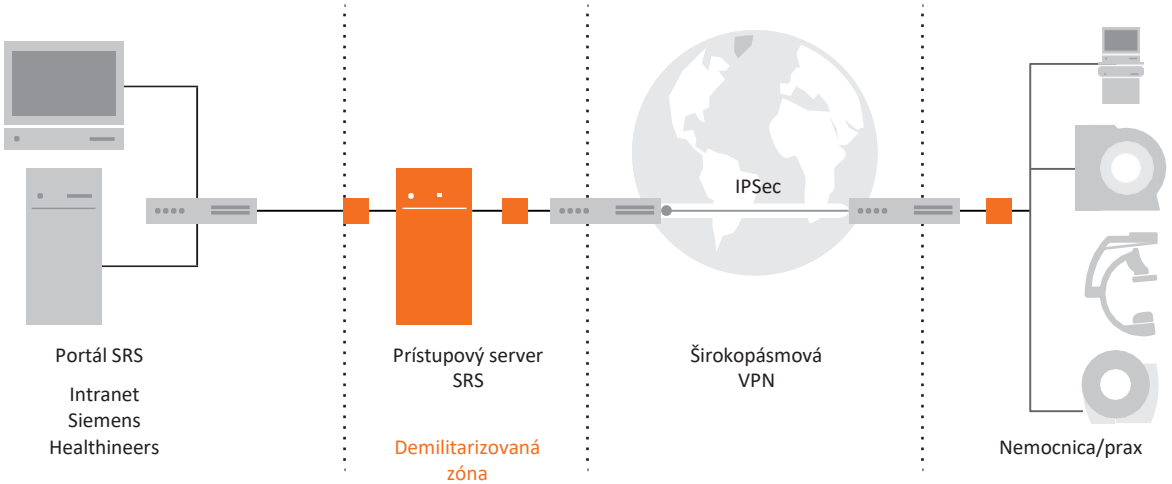
Centrálna platforma pre údržbu (portál SRS), ktorú používa Centrum starostlivosti o zákazníkov, sa nachádza na intranete našej spoločnosti. Prístup na portál SRS je silne zabezpečený a vyžaduje platnú dvojfaktorovú autentifikáciu pomocou čipovej karty. Ako záložné riešenie je možná autentifikácia pomocou identifikačného čísla používateľa SRS, hesla a jednorazového PIN kódu zaslaného prostredníctvom SMS/e-mailu. Koncepcia viacúrovňových servisných domén definuje, ktorí používatelia majú povolený prístup ku ktorým systémom. To znamená, že servisní technici/aplikační experti môžu priamo pristupovať iba k tým systémom zákazníkov, na ktoré majú výslovne oprávnenie. Okrem toho sú technikovi sprístupnené iba tie funkcie SRS, na ktoré má výslovne oprávnenie. Cez túto platformu nie sú prístupné žiadne ďalšie systémy v zákazníckej sieti, ktoré nespravuje spoločnosť Siemens Healthineers. Komplexnosť služieb pre našich zákazníkov niekedy vyžadujú využitie servisných partnerov. Na zaistenie rovnakej úrovne bezpečnosti služieb poskytovaných týmito obchodnými partnermi je k dispozícii voliteľné rozšírenie našej bezpečnostnej infraštruktúry. Obchodní partneri sa musia autentifikovať pomocou dvojfaktorovej autentifikácie, aby získali prístup ku konkrétnym systémom schváleným spoločnosťou Siemens Healthineers. Okrem našich vysokých bezpečnostných štandardov je zabezpečené aj súvislé protokolovanie všetkých vzdialených servisných činností.

Demilitarizovaná zóna

Kvôli ochrane vášho intranetu a intranetu Siemens Healthineers proti recipročným problémom a útokom sme zabezpečili prístupový server SRS (ide o Linux server) v demilitarizovanej zóne (DMZ). Spojenie medzi servisným technikom/aplikačným expertom a vašim systémom sa nevykonáva na priamo. Končí sa v prístupovom serveri SRS pomocou funkcie reverzného proxy. To znamená, že spojenie nadviazané z intranetu Siemens Healthineers končí na prístupovom serveri SRS.

Tento server následne nadviaže spojenie s vašim systémom a zrkadlí komunikáciu prichádzajúcu od vás späť na intranet. Tým sa zabráni možnosti komunikácie medzi intranetom Siemens Healthineers a vašou sieťou prostredníctvom nepovolených protokolov. Zrkadlia sa iba vopred definované protokoly. Táto architektúra je navrhnutá tak, aby poskytovala lepšiu ochranu proti:

- Neoprávnenému prístupu z jednej siete do druhej (napríklad hackerov)
- Prístup zo siete tretej strany (napríklad z Internetu)
- Prenos vírusov alebo iných škodlivých programov medzi sieťami



Obr. č. 4: Bezpečnostná infraštruktúra SRS

Zabezpečenie prenosovej cesty

Virtuálna privátna sieť (VPN) cez Internet
Odporúčame vytvoriť bezpečné širokopásmové spojenie cez internet, čo vám poskytne nasledujúce výhody: vysoká úroveň zabezpečenia, veľmi vysoká rýchlosť prenosu údajov a trvalá dostupnosť, ako aj prístup ku všetkým službám na báze SRS, ako napr. elektronické poskytovanie aktualizácií softvéru. VPN spojenie medzi DMZ a vstupom do vašej siete zabezpečené protokolom IPSec ponúka najmodernejšie technické riešenie, aké je v súčasnosti k dispozícii. V prípade mobilných systémov ponúkame na spojenie medzi systémom a DMZ aj zabezpečenú VPN na báze SSL (Secure Socket Layer). Možno už máte príslušnú infraštruktúru. V takom prípade sú naši technici pripravení pomôcť vám skoordinovať parametre potrebné na spojenie, ktoré je následne potrebné zabezpečiť proti neoprávneným zmenám. Ak nemáte k dispozícii koncový bod VPN, Siemens Healthineers vám poskytne Cisco koncový bod VPN, potrebný na spojenie s SRS.

Koncový bod VPN na našej strane je tiež smerovač Cisco. Upozorňujeme, že v zriedkavých prípadoch sa môže stať, že nie je možné nadviazať funkčné spojenie s modelmi iných výrobcov kvôli problémom so systémovou kompatibilitou. Ak sa stretnete s takouto situáciou, obráťte sa na miestneho zástupcu spoločnosti Siemens Healthineers.

Technické bezpečnostné opatrenia
Na zaistenie dodatočnej bezpečnosti ponúkame nasledovné technické opatrenia:

- **Prístupové zoznamy**
  Prístupové zoznamy ACL (access control lists) na vašom servisnom smerovači plnia podobnú funkciu ako firewall: povoľujú iba prenos údajov z/na známe IP adresy. Dátový prenos je smerovaný cez reverzný proxy v DMZ do systému: pozrite kapitolu "Demilitarizovaná zóna" na strane 9. Zabraňujú tiež tomu, aby Siemens Healthineers mal prístup do iných častí vašej siete a tiež znemožňuje prístup tretích strán.
- **IPSec a SSL chránia údaje pred neoprávnenou úpravou a prezeraním inými osobami**
  Siemens Healthineers používa na šifrovaný a autentifikovaný prenos údajov zavedený štandard IP Security (IPSec) so zdieľanými (pre-shared) tajnými šifrovacími kľúčmi. Tieto kľúče pozostávajú z ľubovoľného reťazca náhodných znakov.
  Na výmenu informácií o šifrovacích kľúčoch sa používa Internet Security Association and Key Management Protocol (ISAKMP). Použitie autentifikačnej hlavičky (AH) zabezpečuje neporušenosť vašich údajov pomocou transformačnej (hash) metódy MD5, SHA1, SHA-256, SHA-384 alebo SHA-512.
  Encrypted Secure Payload (ESP) zabezpečuje dôvernosť údajov pomocou šifrovania algoritmami 3DES, AES alebo AES-GCM (AES-128, AES-192, AES-256, AES-GCM 128, AES-GCM 256). Na zabezpečenie výmeny kľúčov možno použiť rôzne skupiny Diffie Hellman (1-768 bit, 2-1024 bit, 5-1536 bit, 14-2048 bit, 15-3072 bit, 16-4096 bit, 19-256 bit ec, 20-384 bit ec, 21-521 bit ec, 24-2048/256 bit).
  Pri mobilných zariadenia sa používa protokol SSL. Pred nadviazaním spojenia musí byť zariadenie zaregistrované jednorazovým heslom (OTP). Toto heslo sa vygeneruje na základe jedinečných údajov systému a bude platné len na tento proces registrácie. SSL spojenie so serverom VPN možno nadviazať len vtedy, ak bol certifikát servera podpísaný interným certifikačným orgánom (CA) spoločnosti Siemens. Tým sa zabezpečí, že iba toto konkrétne zariadenie môže komunikovať so servermi SRS. Ďalšia transformácia na základe hardvéru zabezpečuje, aby žiadna neoprávnená kópia softvéru nemohla nadviazať spojenie s SRS.
- **Vylepšené možnosti ovládania pomocou ladenia (voliteľné)**
  Ak chcete na vašom servisnom routerii prijímať službu SNMP (Single Network Management Protocol) alebo správy Syslog, alebo ak chcete vidieť aktuálnu konfiguráciu servisného routera, kontaktujte miestneho zástupcu spoločnosti Siemens Healthineers.

Bezpečnostné opatrenia pre internetovú konektivitu

Internetová konektivita (IBC) vychádza z koncepcie bezpečnosti SRS a využíva technológiu SSL VPN. Táto technológia poskytuje bezpečný a súkromný komunikačný mechanizmus pre prenos dát a iných informácií medzi IBC a SRS tým, že vytvorí priamy sieťový tunel so šifrovanými údajmi. Tým prispieva k ochrane vašich údajov pred zverejnením a pred nakazením vírusovou infekciou od neautorizovaných tretích strán počas spojenia s SRS. Siete SSL VPN rýchlo získavajú uznanie v rámci celého odvetvia ako veľmi funkčné a ekonomické riešenie na vzdialený prístup.

IBC umožňuje spojenie zákazníckych systémov s portálom SRS použitím internetového pripojenia bez ďalších hardvérových požiadaviek a závislosti od IP adresy. Takéto riešenie ponúka väčšiu mobilitu systému pri zachovaní konektivity a zabezpečenia SRS.

Bezpečnostné opatrenia v zákazníckej sieti

Firewall
Okrem vyššie uvedených bezpečnostných opatrení môžete smerovať všetku komunikáciu, ktorá si vyžaduje prístup k sieti cez vami spravovaný firewall. To vám poskytuje úplnú kontrolu nad vašou komunikáciou.

Prístup do systému
Keď uvoľníte prístup do vášho systému, servisný technik/aplikačný expert sa musí pred tým, ako bude môcť prepnúť systém do servisného režimu autentifikovať vo vašom systéme časovo-obmedzeným heslom. Heslá sa musia riadiť príslušnými požiadavky spoločnosti Siemens Healthineers, ktoré zodpovedajú medzinárodným normám a sú priebežne aktualizované.

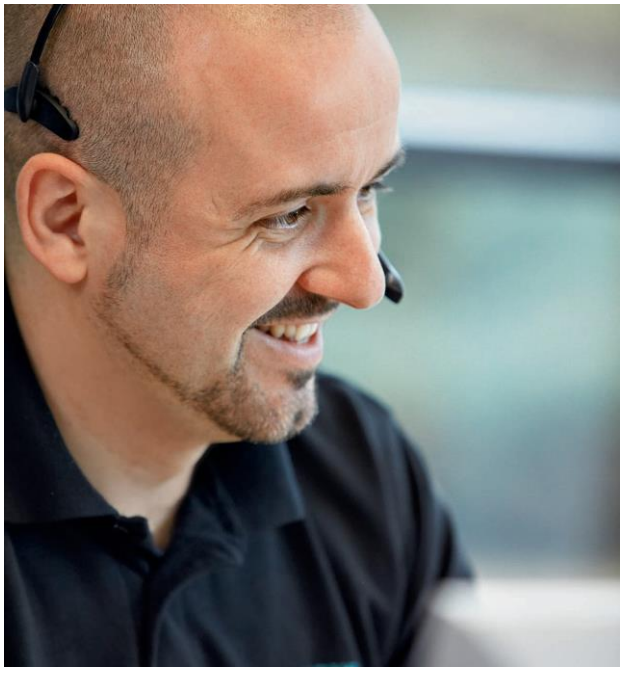
Prenos údajov z vašich systémov na vzdialený server
Pri niektorých našich proaktívnych službách sa z vášho systému odosielajú diagnostické údaje na server SRS, a to automaticky (podľa konfigurácie vášho systému), alebo na výslovnú žiadosť servisného technika. V takýchto prípadoch sa prenášajú iba technické údaje, nie údaje pacientov.

Prenos údajov zo vzdialeného serveru do vašich systémov
V prípade našich služieb aktualizácie softvéru, vzdialenej distribúcie softvéru a ochrany pred vírusmi (Remote Software Distribution and Virus Protection) sa údaje automaticky odosielajú zo serverov SRS do vašich systémov. Sem patria, napríklad, antivírusové vzorce správania. Tento typ prenosu sa vykonáva len s vašim predchádzajúcim súhlasom.

Ochrana proti kybernetickým útokom

Chránené servery SRS

Prístupový server SRS je Linux server a jeho spôsob prevádzky sa riadi smernicami informačnej bezpečnosti Siemens. Účinnosť ochranných opatrení sa pravidelne kontroluje s cieľom zabezpečiť, aby sa servery SRS vždy prevádzkovali s najnovšími technológiami.



Ochrana zákazníckych systémov

Pripojením vašich systémov k našej DMZ budete môcť jednak ťažiť z bezpečnostných opatrení, ktoré sú dané architektúrou platformy – pozrite si časť Demilitarizovaná zóna na strane 9, a navyše spojenia s vašim systémom budú zabezpečené najmodernejšou technológiou. Pokiaľ budete využívať váš prístup na internet výhradne na účely SRS, vírusové infekcie sú vďaka našej bezpečnostnej infraštruktúre nepravdepodobné. Ak však využívate internetové pripojenie aj na iné účely, odporúčame vám prijať vhodné opatrenia na ochranu vášho systému.

Žiadna hrozba z e-mailovej komunikácie
Niektoré typy systémov posielajú e-maily (bez príloh) na prístupový server SRS, pričom ide o prenos iba uvedeným smerom. E-maily odoslané z vášho systému na prístupový server SRS sa postupujú na príslušný poštový server Siemens Healthineers a následne príjemcovi. Poštový server Siemens Healthineers kontroluje všetky e-maily na prítomnosť vírusov a reaguje v súlade so smernicami spoločnosti Siemens tak, aby intranet Siemens Healthineers nebol ohrozený. Keďže v opačnom smere (do vášho systému) sa žiadne e-maily neposielajú, infikovanie systému týmto spôsobom je nepravdepodobné.

Žiadna hrozba spôsobená kontaktom s infikovanými zákazníckymi systémami
Infikovanie prístupového servera SRS prostredníctvom kontaktu s infikovaným systémom zákazníka je

nepravdepodobné, pretože medzi týmito systémami neexistuje priame IP smerovanie (pozrite si vysvetlenie funkcie reverzného proxy v časti „Demilitarizovaná zóna“ na strane 9).

Produkty, funkcie a/alebo ponúkané služby (uvedené v tomto dokumente) nie sú komerčne dostupné vo všetkých krajinách a/alebo vo všetkých alternatívach. Ak z regulačných alebo iných dôvodov v niektorých krajinách nie sú služby uvedené na trh, ponuku služieb nemožno zaručiť. Ďalšie podrobnosti si prosím vyžiadajte od miestnej organizácie Siemens Healthineers.

Siemens Healthineers Headquarters
Siemens Healthcare GmbH Henkestr. 127
91052 Erlangen, Germany
Telefón: +49 9131 84-0
siemens-healthineers.com

Vydala spoločnosť Siemens Healthcare GmbH · iPDF · 6219 0718 · © Siemens Healthcare GmbH, 20198