

Modernizace IS se zaměřením na dostupnost a bezpečnost

Komplexní modernizace IS se zaměřením na dostupnost a bezpečnost IS v užívaných objektech SÚKL. Hlavní prioritou projektu bylo vytvořit škálovatelnou a cenově dostupnou komunikační infrastrukturu, přičemž zvláštní důraz byl kladem zejména na bezpečnost této infrastruktury.

Charakteristika zákazníka

Státní ústav pro kontrolu léčiv, je správním úřadem ustaveným zákonem č. 79/1997 Sb. Je organizační složkou státu, jeho nadřízeným orgánem je Ministerstvo zdravotnictví České republiky. Předmět činnosti ústavu je dán zákonnými předpisy. Ústav k zajištění svých úkolů zřizuje regionální pracoviště umístěná mimo sídlo ústavu.

Posláním Státního ústavu pro kontrolu léčiv je v zájmu ochrany zdraví občanů zajistit, aby se v praxi a při klinickém hodnocení používala pouze farmaceuticky jakostní, účinná a bezpečná léčiva, jakostní a bezpečné suroviny pro výrobu a přípravu léčiv a bezpečné a funkční zdravotnické prostředky s informacemi popisujícími jejich objektivně zjištěné vlastnosti a aby údaje z výzkumu léčiv, surovin a prostředků byly věrohodné a byly získávány eticky.

Cíl projektu

Cílem projektu bylo zabezpečení úkolů zadavatele v oblasti evidence léčiv a nakládání s nimi z hlediska nové právní úpravy. Součástí projektu bylo zabezpečené elektronické vedení správních řízení, úprava komunikace při pandemických opatřeních s dalšími navazujícími subjekty. Všechny uvedené cíle umožní zadavateli pouze kvalitní zabezpečená infrastruktura.

Celkový projekt „Modernizace IS se zaměřením na dostupnost a bezpečnost“ se skládal z následujících dílčích oblastí, které spojením v jeden celek splňují požadavek na vybudování kvalitní zabezpečené infrastruktury.

Dílčí oblasti projektu:

- Realizace strukturované-univerzální metalické a optické kabeláže.
- Dodávka a montáž aktivních prvků.
- Implementace serverů, diskového pole a zálohovacího zařízení.
- Dodávka HW a SW pro management a zabezpečení sítě.
- Zabezpečení uživatelských dat, implementace kryptačního software.
- Zajištění vzdáleného přístupu pro regionální pracoviště a pro pracovníky na služebních cestách.
- Dodávka virtualizačního software včetně virtualizace stávajících serverů.
- Dodávka a montáž klimatizace a rozvodů 230V, včetně příslušných dodávek a prací, které zajistí kompletnost a bezvadnou funkčnost celého díla.

Základní údaje o projektu

Zákazník: Státní ústav pro kontrolu léčiv, se sídlem Šrobárova 48, Praha

Řešení: Modernizace IS se zaměřením na dostupnost a bezpečnost

Hlavní přínosy řešení:

- Vytvoření stabilní infrastruktury pro zajištění provozu IS.
- Zabezpečení ochrany citlivých dat prostřednictvím kryptačního software.
- Vybudování nového datového centra s vysokou dostupností a flexibilitou.
- Snížení nákladů na zajištění provozu IS.
- Bezpečné zálohování DAT.
- Zvýšení dostupnosti dat, rozšíření poskytovaných funkcí a zjednodušení správy systémů.
- Zvýšení bezpečnosti vzhledem k datovým tokům a přístupu uživatelů k prostředkům IS.
- Certifikace informačního systému podle ČSN ISO/IEC 27001:2006

- Certifikace dodávaného řešení podle ČSN ISO/IEC 27001:2006.
- zajištění servisních služeb včetně vzdáleného dohledu

Popis řešení

- **Realizace strukturované-univerzální metalické a optické kabeláže**

V rámci projektu byla řešena modernizace pasivní komunikační infrastruktury. Jednalo se o komplexní dodávku nových strukturovaných kabeláží optických i metalických. Byla vytvořena nová komunikační infrastruktura jejímž základem jsou optické páteřní trasy a lokální metalické rozvody.

- **Dodávka a implementace aktivní technologie**

Vzhledem k vysokým technickým nárokům s ohledem na spolehlivost, bezpečnost, maximální zjednodušení správy komunikační infrastruktury a sjednocení použitých technologií byla zvolena aktivní technologie společnosti Cisco Systems. Společnost Cisco Systems je předním světovým výrobcem v oblasti informačních a komunikačních technologií a jako jediná byla schopna poskytnout dostatečně široké portfolio produktů pro zajištění všech požadavků kladených na komunikační infrastrukturu SÚKL.

Vzhledem k tomu, že kvůli finanční výhodnosti jsou datové toky z regionálních pracovišť do centrály SÚKL transportovány přes internet, bylo nutné vyřešit zabezpečení této komunikace. Jako technologie pro zabezpečení těchto komunikací byla zvolena technologie IPSec VPN. Pomocí této technologie byla vytvořena WAN síť topologie HUB and spoke.

Technologie IPSec VPN je v součinnosti s technologií OTP (technologie jednorázových hesel) nasazena také pro zabezpečení vzdáleného přístupu mobilních uživatelů do sítě centrály SÚKL.

Při modernizaci síťové infrastruktury v centrále SÚKL došlo ke kompletní výměně strukturované kabeláže, přístupových aktivních prvků, centrálního aktivního prvku a centrálního firewallu. Díky těmto krokům došlo k přechodu na plně gigabitovou síťovou infrastrukturu s vysokým stupněm bezpečnosti. Aktivní prvky byly vybírány a dimenzovány s ohledem na budoucí implementaci VoIP řešení a maximální spolehlivost, dostupnost, výkon a bezpečnost.

Při modernizaci komunikační infrastruktury v centrále SÚKL byla maximální pozornost věnována bezpečnosti. Centrální firewally jsou osazeny moduly s funkcí IPS a jsou zapojeny v režimu vysoké dostupnosti. Komunikační infrastruktura disponuje dvoustupňovou úrovní zabezpečení, kdy první linii tvoří externí firewally s funkcí IPS a druhou úroveň tvoří firewallový modul instalovaný v centrálním prvku. Pomocí těchto bezpečnostních zařízení bylo vytvořeno několik externích a interních DMZ (sítí s omezeným přístupem) pro zvýšení úrovně ochrany citlivých dat v datovém úložišti SÚKL.

Informace o bezpečnostních incidentech detekovaných na síťových a bezpečnostních zařízeních jsou automaticky vyhodnocovány a korelovány pomocí specializovaného zařízení Cisco MARS.

Sjednocením aktivních prvků tvořících komunikační infrastrukturu na aktivní prvky pouze jednoho výrobce došlo k prokazatelnému snížení provozních nákladů, při jednoznačném zvýšení technologické úrovně komunikační infrastruktury.

Nasazení bezpečnostních prvků do komunikační infrastruktury přispělo ke zvýšení zabezpečení citlivých dat SÚKL.

- **Virtualizace a konsolidace Microsoft serverů**

Základem řešení bylo provedení analýzy stávajícího stavu a návrh na upgrade a konsolidaci stávajících technologií. Na základě této analýzy byla navržena nová struktura sítě. Byla provedena vizualizace serverů, případně převod dat a funkcí na nové servery, včetně návrhu nové struktury AD a systémových politik. Změnila se pravidla přístupu a v souvislost s dalšími technologiemi pro zabezpečení dat byl navrhnout nový systém zálohování a ukládání dat. Na klientských počítačích byla provedena analýza a následné úpravy pomocí politik a pravidel pro používání programů umožnily zavést jednotné prostředí

definovanými aplikacemi. Pomocí nasazení systému pro správu aktualizací WSUS je prosazováno zabezpečení serverů i stanic. Na firewallu ISA 2006 bylo nasazena autentizace uživatelů, která ve spojení s produktem třetí strany umožňuje sledování internetových přístupů a jejich vyhodnocování.

Microsoft Exchange 2003 umožňuje uživatelům přístup k OWA s dvoufaktorovou autentizací pomocí předmětů s jednorázovým heslem. Pro mobilní uživatele je k dispozici funkce Activesync pro mobilní telefony na platformě Windows Mobile a bezpečné připojení k emailové schránce na cestách pomocí programu Outlook.

- **Implementace serverů, diskového pole a zálohovacího zařízení**

Státní ústav pro kontrolu léčiv řešil zvyšující se požadavky na IT infrastrukturu. Jednalo se zejména o požadavky na zvyšování počtu serverů, diskových kapacit a z toho vyplývající požadavky na zálohovací zařízení. Stávající řešení s jednotlivými servery s tradičním řešením ukládání dat na lokální disky již nevyhovovalo a také výkon stávajících serverů nedostačoval používaným aplikacím. Z tohoto důvodu došlo k rozhodnutí najít celkové koncepční řešení IT infrastruktury, které by zabezpečilo bezproblémový chod IT infrastruktury nyní i v budoucnosti.

Jako optimální řešení daného zadání se ukázalo vytvoření virtuální infrastruktury na bázi VMware Infrastructure 3 a vytvoření nové fibre channel SAN infrastruktury. SAN infrastruktura byla navržena dle výchozích požadavků, skládá se z jednoho diskového pole DELL CX3-20, dvou FC switchů Brocade 200E, páskového autoloaderu DELL ML6010 a tří nových serverů DELL 2950. SAN infrastruktura byla dále doplněna dvěma stávajícími servery DELL 1950, jeden pro účely zálohování a druhý pro vytvoření Virtual Centra pro správu virtuální infrastruktury.

Na tři nové servery byl nainstalován VMware ESX Server ve verzi Enterprise. VMware ESX Server je základem dynamické IT infrastruktury zajišťující vlastní optimalizaci. Tyto fyzické servery byly následně zařazeny jako „Hosts“ do High Availability clusteru, který byl vytvořen na VMware Virtual Centru. VMware VirtualCenter zajišťuje centralizované řízení, automatický provoz, optimalizaci zdrojů a vysokou dostupnost tohoto prostředí a tím splňuje jeden ze základních požadavků projektu.

- **Zabezpečení uživatelských dat, implementace kryptačního software**

Státní ústav pro kontrolu léčiv musel zabezpečit citlivá data, která shromažďuje v rámci agent, které musí zpracovávat. Zabezpečení citlivých dat musí být jednak z pohledu přístupu k datům, ale i z pohledu jejich uložení. Dále bylo nutné řešit problematiku zabezpečení dat na mobilních zařízeních. Z tohoto důvodu došlo k rozhodnutí najít celkové koncepční řešení zabezpečení dat. Pro řešení problematiky zabezpečení dat bylo vybráno řešení společnosti UTIMACO®Safeware. Vzhledem k rozsahu požadavků na zabezpečení dat byly implementovány následující produkty:

SafeGuard®Easy, který poskytuje kompletní šifrování harddisků na sektorové úrovni u laptopů a pracovních stanicích. Ochrana před bootováním, autentizace uživatele před bootováním a šifrování harddisku za použití výkonných algoritmů garantují ochranu před neautorizovaným přístupem i útokem hackerů. Jeho propracovaný management umožňuje velice jednoduchou centrální správu.

SafeGuard®Advance Security, který poskytuje bezpečnou autorizaci, zvýšenou ochranu integrity a komplexní kontrolu přístupu uživatele do heterogenních sítí, zařízení a aplikací. Umožňuje chránit cenná data společností i před odcizením vlastním zaměstnancem. Řešení umožňuje speciální ochranu a kontrolu všech dostupných připojovaných zařízení a médií (USB Flash disk, CD, DVD, tiskárny, fotoaparáty...).

SafeGuard®LAN Crypt, který nabízí ochranu dat a přístupů přes více úrovně šifrování pro uchovávané soubory, složky, adresáře, typy souborů na lokálních i síťových discích, databázových nebo terminálových serverech, ale i paměťových médiích a zařízeních. Umožňuje jednoduché rozdělení funkce systémový administrátor a správce bezpečnosti včetně centrální správy.

Hodnocení zákazníka

Celá realizace proběhla velmi rychle a bez závažnějších problémů. Po dobu implementace nebyl provoz SÚKL přerušen a zaměstnanci Ústavu prováděné změny nijak neomezovaly v jejich činnostech. Kompletní přechod na novou síťovou infrastrukturu trval zhruba měsíc, kdy nasazování nových technologií probíhalo výhradně mimo pracovní dobu. Konsolidace serverů a infrastruktury nám umožnila rozšíření funkcí a zabezpečení dat. Při virtualizaci a převodu dat jsme dosáhli zvýšení dostupnosti dat. Oddělení serverových rolí nám umožnilo zajistit dostupnost hlavních funkcí IS a zrychlit odezvu pro uživatele. Mobilní uživatelé mohou pracovat pomocí VPN na zabezpečených počítačích bez obavy úniku dat.

*Ing. Tomáš Melen,
náměstek ředitele pro informatiku a ekonomiku, Státní ústav pro kontrolu léčiv*

Produkty a technologie

- CISCO SYSTEMS – aktivní prvky, firewally, IPS a monitorovací systémy, management, řízení přístupu uživatelů
- DELL – servery, disková pole, zálohovací zařízení, aktivní prvky SAN
- VMware – virtualizační software
- MICROSOFT – Windows server 2003, IAS, Exchange
- UTIMACO – SGE, Lancrypt, PnP

PRAHA 102 05, Weilova 2/1144, tel.: +420 267 215 620

OSTRAVA 706 02, Výstavní 2965/97B, tel.: +420 595 953 100

www.netprosyst.cz