Příloha č.1

Projekt redesign WAN/LAN

1 CÍL PROJEKTU

Cílem projektu je snížení rizik bezpečnostních incidentů v podnikové síti prostřednictvím její segmentace na menší části (různé typy technologických sítí, administrativní sít) s řízenou vzájemnou komunikací. Projekt by měl obsahovat návrh architektury LAN v koncových lokalitách (61) a v centrální lokalitě, včetně návrhu IP adresace, dle dále uvedených požadavků. Propojení lokalit je realizováno pronajatými datovými trasami připojujícími koncové lokality k centrální lokalitě.

2 TECHNICKÉ POŽADAVKY

Dále jsou uvedeny požadavky na architekturu LAN, které mají být v projektu řešeny.

2.1 Koncové lokality

- možnost konfigurace VLANs (např. administrativa, ASŘ, kamery, atd.), vzájemně oddělených FW, který bude řídit veškerý provoz z i do těchto VLANs
- návrh universálního rozdělení VLANs na základě analýzy stávajícího stavu a provozovaných zařízení v jednotlivých lokalitách
- otázka rychlosti LAN (1 Gbps, 100 Mbps), jejího využití, v případě volby 1 Gbps kontrola využitelnosti stávající strukturované kabeláže a optického vedení v místě, případně návrh výměny či nahrazení
- návrh nasazení typů aktívních prvků v LAN, zvláště pak nahrazení modemových a mikrovlnných spojů dle dále specifikovaných požadavků současně s návrhem kapacity těchto spojů dle provedené analýzy síťového provozu v lokalitách
- aktívní prvky v LAN budou zabezpečeny minimálně proti uvedeným aktivitám: ARP Poison Routing, ARP spoofing, DHCP spoofing, MAC flooding
- správa veškerých aktívních prvků musí být zajištěna zabezpečeným kanálem pomocí SSH
- aktívní prvky musí umožňovat poskytování dat a spolupráci se softwarem FlowMon tak, aby byl veškerý provoz v síti monitorován a analyzován (primárně firewally, routery, případně switche)
- monitoring veškerých aktívních prvků pomocí SNMP dotazů (nikoli trapy) až na úroveň jednotlivých portů
- návrh parametrů aktívních prvků do jednotlivých lokalit a detailní popis jejich vlastností použitelný jako podklad pro výběrové řízení dodání těchto prvků

2.2 Centrální lokalita

Pro centrální lokalitu platí požadavky uvedené u koncových lokalit plus dále uvedené:

- návrh rozdělení VLANs na základě analýzy stávajícího stavu lokality GŘ – různé druhy serverů (využití – správa, aplikační, DMZ apod.), pracovní stanice (zohlednit specifika některých odborů), specifická pracoviště (zasedačky apod.), technologická zařízení a další.
- návrh 10 Gbps páteřní sítě včetně prvků a vedení (stávající vedení otestovat, případně naprojektovat nové) s vazbou i na virtualizační platformu integrovanou v PLa
- návrh síťové konfigurace VMWare serverů a jejich zapojení v případě využití 10 Gbps rozhraní
- návrh využití stávajícího softwaru FlowMon včetně jeho upgrade a rozšíření funkcionalit pro zajištění bezpečnosti a analýzu provozu ve vnitřní síti
- wifi síť pro hosty s přístupem na internet s naprojektováním možnosti zavedení obdobných sítí v koncových lokalitách
- obdobně navrhnout wi-fi síť pro připojení důvěryhodných zařízení (certifikát stroje) do vnitřní sítě, zajištění patřičným hardwarem i softwarem

2.3 IP adresace, přístupy zařízení do sítě

- návrh IP adresace ve všech VLANs na všech lokalitách
- návrh vlastností přidělování IP adres ve vnitřních sítí PLa pouze registrovaným zařízením (MAC) s odmítnutím přístupu všech ostatních zařízení s výjimkou přístupu do wifi sítí pro hosty, zvážit centrální či lokální řešení včetně návrhu odpovídajícího softwaru (příp. hardwaru)
- návrh řešení pro provoz zaměstnaneckých mobilních zařízení (především notebooků), umožňující přístup pouze do určených VLANs a určených lokalit v případě připojení uvnitř PLa i v případě připojení z internetu přes VPN nebo přes interní wi-fi.
- návrh řešení přístupu servisních organizací (lokální i vzdálený) na servisovaná zařízení s ohledem na bezpečnost a zajištění pro registrované MAC adresy

3 OBECNÉ POŽADAVKY

Projekt musí mimo návrhu cílového stavu nastínit i cestu (návrh postupu, doporučení), jak se k tomuto cílovému stavu dobrat:

- návrh postupu upgradu redesignu všech lokalit včetně centra v HK, stanovení časové náročnosti, s ohledem na minimalizaci doby výpadků při výměně, konfiguraci a zprovoznění
- návrh eventuálního rozdělení celé akce do postupných etap, zhodnocení důsledků rozdělení této akce do jednotlivých etap
- odhad celkové ceny nového řešení i jednotlivých etap při postupné realizaci
- preferovat řešení od jednoho výrobce (jednotná správa aktívních prvků, udržitelné nároky na rozsah a spektrum znalostí administrátorů)
- stanovení všech parametrů pro výběr HW i SW tak, aby bylo příslušnou část projektu možné použít jako podklad pro výběrové řízení na HW a kompletní službu montáže, konfigurace a zprovoznění
- zhodnocení náročnosti správy navrženého řešení, návrh školení zainteresovaných správců a doporučení jejich počtu s ohledem na počet lokalit a jejich rozptýlenost

Projektová dokumentace se považuje za dokončenou okamžikem jejího odsouhlasení a schválení objednatelem.