

Doplnění specifikace vlastností nabízených zařízení z hlediska bezpečnosti a podpory aplikací

1. Bezpečnostní nástroje na ochranu komunikačních sítí

- a) Popište Vámi navrženou implementaci šifrování mezi aktivními prvky sítě a mezi aktivními prvky sítě a koncovými zařízeními.
- b) Uveďte Vámi navržené použití standardizovaných šifrovacích metod.
- c) Popište jak je řešena odolnost přenosové technologie proti odposlechu a případné kompromitaci přenášeného obsahu.
- d) Popište vliv šifrování na zatížení provozu aktivních prvků.
- e) Uveďte způsob, jak implementovat šifrování mezi aktivními prvky sítě, transparentní pro přenášené rámce.
- f) Popište systém centralizované správy bezpečnostních politik v síťové infrastruktuře s využitím Vámi nabízených zařízení.
- g) Popište Vámi nabízený způsob napojení na PKI pro systémy centralizované správy bezpečnostních politik, za předpokladu, že implementace PKI infrastruktury je nedílnou součástí služeb komunikační infrastruktury zajišťující ochranu důvěrnosti a integrity přenášených dat a která bude sloužit pro vydávání certifikátů jednotlivým zařízením a systémům připojeným do komunikační sítě v rámci sítě GDS s využitím vlastní resortní veřejné certifikační autority. Uveďte proto Vámi nabízený návrh distribuce certifikátů pro nová klientská zařízení připojovaná do sítě.
- h) Popište Vámi nabízený způsob šifrování aplikačního provozu nad MPLS VPN infrastrukturou při zajištění dynamického provozu, tj. bez předem definovaných bod-bod tunelů.
- i) Popište způsob a možnosti aplikace bezpečnostních pravidel přímo na přístupových prvcích sítě (ve vazbě na požadovaný centralizovaný systém správy přístupu sítě – LAN, WiMAX, VPN). Mobilita uživatelů a podpora různých typů přístupu do sítě s sebou nese nové nároky na řízení tohoto přístupu. Cílem je eliminovat nesourodé a izolované možnosti správy přístupu v prostředí LAN, WLAN a VPN a vybudovat jednotný systém unifikovaného přístupu do sítě, plně redundantní, splňující nároky na vysokou dostupnost.
- j) Popište způsob detekce typu a stavu zařízení. Pod stavem zařízení rozumíme, jestli zařízení splňuje nebo nesplňuje určitá bezpečnostní kritéria, nejen z hlediska identifikace mapováním skupinové bezpečnostní politiky podle active directory nebo LDAP, ale i např., jestli je instalována konkrétní verze antiviru, jestli je zapnutý personální FW, jaká je hodnota určitých registrů, jestli běží konkrétní procesy, jaký je typ zařízení a operačního systému, jaké je místo a technologie připojení, jaký je použitý autentizační protokol, jaké je jméno SSID při WiFi přístupu, apod.
- k) Popište rozhraní API pro komunikaci s MDM managementem pro získání informací o koncové stanici nebo pro instruování MDM z rozhraní bezpečnostního managementu.

- l) Specifikujte u Vašich zařízení konkrétní možnosti kryptografických algoritmů Suite-B na VPN koncentrátorech a VPN klientovi. (např. metoda IPsec s podporou Suite-B s kryptografickými algoritmy AES-GCM/GMAC šifrování, IKEv2, SHA-2 autentizace ESP paketu, šifry na bázi eliptických křivek ECDH a ECDSA).
- m) Popište způsob správy klientských zařízení (mobilních i stacionárních), aplikaci bezpečnostních politik na VPN koncentrátoru podle bezpečnostní role uživatele, typu zařízení, stavu zařízení (např. jestli je instalována konkrétní verze antiviru, zapnutý personální FW, jaká je hodnota určitých registrů, jestli běží konkrétní procesy, apod.). Uveďte podporované platformy pro SW VPN klient.
- n) Uveďte možnosti přístupu k aplikacím nebo serverům uvnitř sítě přes webový prohlížeč včetně metod šifrování pro VPN koncentrátor. Funkci www portálu zpravidla poskytuje právě VPN koncentrátor.
- o) Specifikujte relevantní funkce bezpečnostního managementu a uveďte možnosti napojení na další systémy jako SIEM, threat management, apod.
- p) Popište bezpečnostní pravidla firewallu určujícího jaký provoz může být přenášén dovnitř sítě. Popište funkci firewallu, který musí zajišťovat rozlišení provozu podle typu aplikace (např. musí zamezovat tunelování na portech pro určité síťové služby), klasifikovat webové stránky do kategorií a servery podle reputace.
- q) Popište, pro analýzu provozu procházejícího bezpečnostním perimetrem, použití IPS systému na odhalení útoků na zranitelnosti v síti při konkrétních operačních systémech a aplikacích použitých v síti s nastavením Vámi nabízeného systému k porovnání vzorků (signatur) tak, aby byl relevantní ke konkrétnímu obrazu sítě. Předpokládá se použití samostatných bran pro email a web provoz.
- r) Uveďte, jakým způsobem navrhujete využít prostředky síťové infrastruktury pro poskytnutí informací o datových komunikacích ve vztahu k detekcím bezpečnostních událostí. Tyto informace by měly být korelovány se sledováním chování síťové infrastruktury, tak aby bylo možné detekovat, že se v síti vyskytuje kompromitovaná stanice se zasíláním dat na centrální systém s automatickou aktivací předdefinované akce nebo metodologie.
- s) Popište, jaké jsou možnosti poskytnutí relevantních informací pro forenzní analýzu bezpečnostního incidentu na konkrétní platformě „threat management“?
- t) Specifikujte, jaké nástroje nabízíte k detekci bezpečnostních incidentů (např. mapování interní infrastruktury a aplikací, odhalení systémů s bezpečnostními slabými místy, distribuce škodlivého SW, snaha o komunikaci s řídicími systémy botnet sítě, export dat, apod.).
- u) Uveďte, jaké nástroje včetně jejich charakteristiky nabízíte k detekci tzv. „Zero Day“ útoků mimo výše uvedené. Tj. útoků, které nelze odhalit čistě kontrolou na datové vzorky (signatury).
- v) Popište návrh centralizované infrastruktury pro pevný a bezdrátový přístup se společným operačním systémem, společným konfiguračním rozhraním, jednotným řízením přenosového pásma (QoS politiky) s jednotným monitorováním uživatelů a se společnou správou celé infrastruktury pro pevný a bezdrátový přístup (jedním nástrojem).

2. Monitorování aplikací a požadavky na jejich transport v síťové infrastruktuře

- a) Popište, jakým způsobem bude navrhovaná komunikační infrastruktura monitorovat aplikační toky na end-to-end úrovni, a to jak z pohledu samotné infrastruktury (využití přenosového pásma, síťové zpoždění apod.), tak především z pohledu koncového

uživatelé (odezva konkrétních aplikací, počty aplikačních transakcí, poruchové stavy aplikací v korelaci na stav sítě apod.).

- b) Popište navrhovanou podporu multimediálních aplikací (interaktivní komunikace pomocí hlasu a videa – point-to-point nebo vícebodová spojení), online nástrojů pro týmovou spolupráci uživatelů (sdílení dokumentů, pracovní plochy) a jejich transport z pohledu nastavení QoS a přidělování přenosového pásma. U multibodových multimediálních spojení popište návrh multicast technologie (architektury a řešení signalizace požadavků na zdroje a služby).
- c) Uveďte, jaké nástroje pro prevenci detekce, troubleshooting a izolaci problémů, ztrátu malých fragmentů komunikace, vyššího rozptylu zpoždění, asymetrického směřování a simulace reálných multimediálních aplikací nabízíte v navrhovaném řešení.
- d) Popište nabízená zařízení z hlediska sběru informací o aktuální a dlouhodobé spotřebě elektrické energie, jak vlastních infrastrukturních prvků, tak i koncových zařízení a také způsoby řízení jejich spotřeby.