LANPCSe-AES

OCHRANA LAN KOMUNIKACE

S.ICZ, DCEŘINÁ SPOLEČNOST ICZ, PROVĚŘENÁ NÁRODNÍM BEZPEČNOSTNÍM ÚŘADEM ČR (NBÚ) PRO STYK S UTAJOVANÝMI INFORMACEMI AŽ DO STUPNĚ UTAJENÍ „PŘÍSNĚ TAJNÉ“, NABÍZÍ KOMPLEXNÍ SLUŽBY V OBLASTI OCHRANY UTAJOVANÝCH INFORMACÍ.

LANPCSe-AES realizuje vrstvu zaručené ochrany síťové komunikace pro pracovní stanici, na které jsou zpracovávány citlivé nebo utajované informace. Základním rysem certifikovaného kryptografického prostředku LANPCSe-AES je integrace IPSec šifrátoru do podoby interní šifrovací síťové karty, která je umístěna do vnitřku pracovní stanice. Nasazení tohoto kryptografického prostředku tak umožní využít stávající nezabezpečenou komunikační infrastrukturu (kabeláž, aktivní prvky) pro připojení pracovních stanic, nacházejících se v běžných kancelářích, do certifikovaného informačního systému určeného pro zpracování utajovaných informací podle zákona č. 412/2005 Sb.

Při návrhu a výstavbě informačních systémů s využitím LANPCSe-AES dochází k zásadnímu snížení nákladů na fyzické zabezpečení provozních prostorů IS a současně se ztrácí i stávající omezení, která brání efektivnímu využívání a rozšiřování systémů zpracovávajících utajované informace pro běžná pracoviště uživatelů. Implementace LANPCSe-AES vyčlení komunikační infrastrukturu za hranice certifikovaného informačního systému. Tím dojde k eliminaci nákladů potřebných na zvýšení ochrany veškerých komunikačních tras a na zabezpečení prostor datových rozvaděčů. Současně i odpadají náklady na vybudování oddělené duplicitní a souběžně provozované datové sítě a zmizí i jakákoli omezení na geografické rozmístění pracovních stanic uživatelů. Svůj informační systém tak můžete provozovat tam, kde reálně potřebujete, a s minimálními náklady jej můžete přizpůsobovat všem provozním a organizačním změnám.

CERTIFIKACE

Certifikát NBÚ, evidenční číslo K20158, je platný do 22.01.2019 a potvrzuje způsobilost kryptografického prostředku pro ochranu utajovaných informací do a včetně stupně utajení:

- VYHRAZENÉ
- RESTRIENT UE/EU RESTRICTED
- NATO RESTRICTED

Provedení

- Je to samostatný hardwarový kryptografický prostředek (IPSec šifrátor) v podobě rozšiřující síťové karty pro sběrnici PCI Express
- Pro zpřístupnění hardware slouží ovladače síťového rozhraní a pro operační systém nepřináší žádné omezení

Základní funkcionalita

- Kryptografický prostředek se stává nedílnou součástí pracovní stanice, ale kryptografické funkce jsou kompletně odděleny od operačního systému počítače
- Principiální bezpečnost - pracovní stanici mohou po síti opustit pouze zašifrovaná data, operační systém nemůže ovlivnit funkci prostředku
- Eliminuje potřebu oddělené duplicitní a souběžně provozované datové sítě
- Není vyžadována provozní obsluha kryptografického prostředku
- Umožňuje jedno pečetění (jednu ochranu) – ochrana vnitřku pracovní stanice se vztahuje i na ochranu zabudovaného IPSec šifrátoru

Efektivita implementace

- LANPCSe-AES je určen pro standardní počítače kompatibilní s IBM PC s OS MS Windows nebo Linux
- Instalace do OS počítače je realizována pomocí softwarových ovladačů, které samy osobě nevyžadují klasifikaci HDD jako nosiče utajovaných informací
- LANPCSe-AES se v počítači jeví jako standardní síťová karta a z pohledu své obsluhy neklade na uživatele žádné další požadavky (není vyžadována provozní obsluha kryptografického prostředku)
- Výběr prostoru pro umístění počítače s LANPCSe-AES neovlivňuje rozmístění dalších komponent informačního systému

Typické příklady nasazení

- Ochrana komunikace v prostředí LAN i WAN (využití standardní existující nezabezpečené i veřejné komunikační infrastruktury)
- Propojení současných geograficky a síťově izolovaných PC (samostatné stanice určené pro zpracování utajovaných informací). Získání možnosti on-line správy PC a on-line výměny UI, omezení nutnosti exportu UI na nosiče utajovaných informací
- Přesun stávajících pracovních stanic určených pro zpracování UI z oddělených zabezpečených prostor přímo na pracoviště uživatele (prodloužení existujícího certifikovaného IS pro zpracování UI)
- Tvorba nových IS určených pro zpracování UI s plným využitím standardních produktů (např. pro tvorbu komunikační infrastruktury, zajištění síťových služeb, zajištění služeb AD domény včetně správy)
- Bezpečný terminálový provoz určený pro zpracování UI (PC v podobě terminálu bez možnosti ukládání UI na lokální disk)

Klíčové výhody HW šifrovaného spojení s LANPCSe-AES

- Jednotná metoda - standardizace přenosu dat on-line šifrováním mezi počítači, které je pro ostatní komponenty informačního systému zcela transparentní
- HW šifrování veškerých přenášených dat poskytuje jak fyzickou tak logickou bariéru nezávislé ochrany, která je postavena mezi pracovní stanici a komunikační síť
- Umožňuje využití stávající komunikační infrastruktury (kabeláž, aktivní prvky) bez nutnosti provádění změn či omezení její funkce
- Nevyžaduje žádné speciální školení pro koncového uživatele - uživatel není v roli provozní obsluhy kryptografického prostředku
- Prostředek je pro chod operačního systému a aplikací pracovní stanice zcela transparentní (nevyžaduje instalaci žádného aplikačního software mimo ovladačů síťové karty)
- Kryptografické klíče nikdy neopouští LANPCSe-AES (nejsou dostupné pro pracovní stanici)
- Kryptografické algoritmy jsou plně realizované uvnitř LANPCSe-AES a nejsou ovlivnitelné z pracovní stanice
- Poskytuje funkce bezpečného uložení, správy a destrukce šifrovacích klíčů, které jsou nezávislé na chodu operačního systému pracovní stanice
- Umožňuje víceúrovňovou správu kryptografického prostředku a vzdálený dohled
- Umožňuje i provoz v režimu jednoduché lokální správy (nevyžaduje centrum pro řízení a správu)
- Poskytuje nezávislý audit bezpečnostně významných událostí vytvářený na paměťovém modulu v kryptografickém prostředku LANPCSe-AES zajišťující trvalou ochranu proti neoprávněné manipulaci

Výkonný prostředek pro centra

Pro budování rozsáhlých systémů, kdy jednotlivé pracovní stanice vybavené kryptografickým prostředkem LANPCSe-AES přistupují do jednoho nebo více center, jsou pro zajištění dostatečného výkonu / průchodnosti těchto center určeny výkonné hraniční kryptografické prostředky LANPCS-Rack. Tyto prostředky jsou plně kompatibilní s ostatními kryptografickými prostředky rodiny LANPCS (LANPCSe-AES, LANPCS-AES). Podrobné informace o výkonném hraničním kryptografickém prostředku LANPCS-Rack jsou uvedeny v samostatném produktovém listu.

Reference

Implementací kryptografických prostředků LANPCSe-AES s dalšími bezpečnostními produkty S.ICZ (např. PCS1, AirGap 02) je možné vybudovat reálné certifikované informační systémy určené pro zpracování citlivých a utajovaných informací s vysokým uživatelským komfortem a vysokou přidanou bezpečnostní hodnotou. Uživatelé tak mohou z prostředí své kanceláře využívat aplikace pro online zpracování utajovaných informací v rámci své organizace a současně je možné z těchto systémů zajistit i trvalou výměnu informací i mezi organizacemi. Příkladem takového informačního systému je aktualizace IS EU Extranet ČR, který je určen pro národní distribuci oficiálních utajovaných dokumentů rady EU.

Základní parametry LANPCSe-AES

Požadavky na počítač:
- PCI Express rozhraní (volný PCI Express slot pro kartu s délkou 168mm)

Technické parametry:
- rozměry (D x V x Š): 168 x 111 x 14,7 (mm)
- fyzické PCI rozhraní: PCI Express 1.1 x1
- fyzická síťová vrstva: Ethernet 10/100 Mbps (konektor RJ 45)
- základní síťová vrstva: IPv4
- bezpečnostní rozšíření IP: IPsec (RFC 2406 – ESP)
- čtečka ČK: ISO 7816 &EMV 2000 level 1 připojena na interní nebo externí USB konektor LANPCSe-AES
- provozní teplota: 0-45 st. C (vnitřní teplota PC)
- relativní vlhkost: 5-95% (nekondenzující)

Podporované OS:
- MS Windows
- Linux jádro 2.6 a vyšší (preference Linux distribuce Debian)
- podpora 32 i 64 bitové OS

Datová propustnost:
- 40 Mbps (fyzické maximum)
- 34 Mbps (reálný provoz)

Provozní módy:
- manuální režim (provozní konfigurace uložena v čipové kartě)
- autonomní režim (nemá provozní obsluhu kryptografického prostředku, provozní konfigurace uložena v LANPCSe-AES)

Vzdálený dohled:
- ICMP
- SNMP
- přenos logů na FTP

Kryptografie:
- algoritmy: AES 256, HMAC SHA-256, Diffie-Hellman

Interní bezpečnostní funkce:
- fyzikální generátor náhody
- nezávislý čas
- nezávislý audit
- dohledový procesor

Třída kryptografického prostředku:
- CCI

Míry záruk podle Common Criteria:
- vývoj a návrh řešení byl proveden v souladu s požadavky na záruky EAL4+

OBCHODNÍ KONTAKT

S.ICZ a.s. Na hřebenech II 1718/10
140 00 Praha 4
TEL.: +420 222 271 111
FAX: +420 222 271 112
E-MAIL: obchod-SICZ@iczgroup.com