

AIRGAP 02

AIRGAP 02 JE HARDWAROVÉ ZAŘÍZENÍ PRO VYTVÁŘENÍ BEZPEČNÉHO ROZHRAŇÍ PRO OBOUSMĚRNÝ PŘENOS INFORMACÍ MEZI DVĚMA INFORMAČNÍMI SYSTÉMY SE ZACHOVÁNÍM JEJICH GALVANICKÉHO ODDĚLENÍ.

Zcela nový a ojedinělý bezpečnostní produkt AirGap 02 přináší reálnou možnost zajištění výměny informací mezi certifikovaným informačním systémem určeným pro zpracování utajovaných informací a necertifikovaným systémem nebo sítí. Využitelnost tohoto bezpečnostního produktu je však širší a najde uplatnění všude tam, kde je nutné provádět pravidelnou i nepravidelnou výměnu informací mezi informačními systémy s rozdílnou bezpečnostní úrovní a to jedním nebo oběma směry.

[BEZ VÝMĚNY INFORMACÍ TO NEJDE]

Dnešní provozní požadavky a potřeby uživatelů nespočívají jen v oblasti komfortního zpracování informací, ale i v dostatku správných informací na správném místě a ve správném čase. Toto platí jak pro většinu standardních informačních systémů, tak pro velmi citlivé informační systémy, nebo dokonce certifikované informační systémy, které zpracovávají utajované informace. Bezpečnostní architekt je pak postaven do situace, kdy musí vybudovat informační systém s požadovanou úrovní zabezpečení často i za cenu částečného nebo úplného oddělení od tzv. veřejných, resp. nedůvěryhodných počítačových sítí, a současně musí řešit požadavek včasné a pravidelné výměny informací, které ale jsou často dostupné jenom a právě v nedůvěryhodných počítačových sítích. Bezpečnostní rizika, která by přinesla propojení zabezpečeného informačního systému s jinými systémy, nutí bezpečnostního architekta hledat jiná alternativní – vysoce bezpečná řešení.

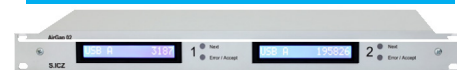
Omezené možnosti řešení oboustranné výměny dat

Pro realizaci bezpečného rozhraní k zajištění jednosměrného toku informací směrem pouze do zabezpečeného informačního systému existují, vedle AirGap 02 také jiná, již známá řešení, například v podobě implementace tzv. „datové diody“. Pokud je však požadován také export dat ze zabezpečeného informačního systému nebo oboustranná výměna dat mezi zabezpečeným informačním systémem a jeho okolím, je už situace výrazně horší. Ne že by neexistovala nějaká ojedinělá řešení, ale často znamenají značné finanční investice (v řádech jednotek až desítek milionů korun) a to je právě ten hlavní problém – stávají se tak nedostupnými pro většinu provozovatelů.

Řešení jsou pak postavena například na ruční výměně informací pomocí výměnného média (například pomocí USB Flash Drive). Bezpečnost je pak postavena na faktu, že zabezpečený informační systém není síťově propojený se žádným jiným informačním systémem (je oddělen vzduchovou mezerou – řešení známé jako „princip oddělení pomocí air gap“) a výměnu informací pak provádí důvěryhodná a zaškolená osoba (tzv. operátor přenosu). Na první pohled velice levné a bezpečné řešení, ale využitelné jen pokud nám stačí výměna každou hodinu nebo dvě. Pokud ale má být přenos zahájen např. do jedné minuty od vzniku požadavku, při dostupnosti 24x7x365, tak je toto řešení prakticky nerealizovatelné.

VLASTNOSTI A VÝHODY

- ▶ Hardwarové zařízení pro galvanické oddělení informačních systémů
- ▶ Bezpečné rozhraní pro oboustranný tok utajovaných informací
- ▶ Maximální odolnost rozhraní proti útokům mezi sítěmi
- ▶ Vhodné pro začlenění do informačních systémů zpracovávajících utajované informace podle zákona č. 412/2005 Sb
- ▶ Informace dostupné 24x7x365
- ▶ Finančně dosažitelné řešení
- ▶ Široké pole použitelnosti
- ▶ Možnost optimalizace životnosti
- ▶ Provedení 19" 1U RACK

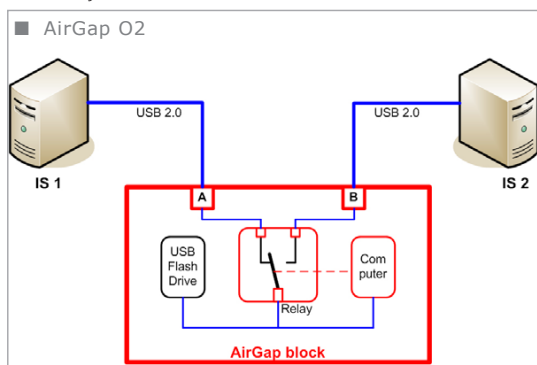


V x Š x H	40 x 485 x 260 mm
Konfigurace:	2 x AirGap blok
Rozhraní:	2 x USB 2.0 pro každý blok
Napájení:	100-240V, 50-60Hz
Příkon:	15W
Hmotnost:	3,140 kg
Teplota prostředí:	-40 až +85 °C (bez kondenzace, relativní vlhkost: 35 - 85 %)
AC/DC zdroj:	-25 až +60°C, max. relativní vlhkost 95%, teplotní pojistka 90°C
Odolnost proti vibracím:	10 až 55 Hz, s dvojitou amplitudou 1,5 mm
Odolnost proti rázům:	selhání funkce 100 m/s ² , zničení 1 000 m/s ²
Životnost doporučená:	500.000 přepnutí
Životnost maximální:	1.000.000 přepnutí
Záruka:	2 roky (při nepřekročení doporučeného počtu přepnutí)
Vyvíjí a vyrábí:	S.ICZ a.s. (dceřiná společnost ICZ a.s.)

[AIRGAP 02]

[AIRGAP 02 ZAJIŠŤUJE GALVANICKÉ ODDĚLENÍ]

Princip použitý v AirGap 02 je chráněn patentovou přihláškou. Zařízení obsahuje dva identické, avšak nezávislé bloky (můžeme hovořit o dvou AirGap v jednom AirGap 02). Každý blok umožňuje přenos informací mezi dvěma počítačovými systémy, u kterých je nutné dodržet jejich galvanické oddělení, a to tak, že se datové informace přenášejí přepojováním vnitřní paměťové jednotky (USB Flash Drive) na úrovni elektrických signálů při současném zajištění galvanického oddělení obou systémů vzduchovou mezerou.



Přepojování je realizováno elektromechanicky pomocí speciálního bezpečnostního relé.

Elektromechanické přepínání splňuje požadavek galvanického a komunikačního oddělení. Vhodným zapojením bezpečnostního relé je zabezpečeno, aby při přepojování v žádném případě nedošlo k přímému propojení obou počítačových systémů. Přepínání relé je řízeno jednoúčelovým počítačem. Bezpečnostní relé přepíná vždy společně vnitřní paměťovou jednotku (USB Flash Drive) a USB rozhraní ovládacího jednoúčelového počítače. Aktuálně připojený počítačový systém po dokončení všech operací s vnitřní paměťovou jednotkou předá přes USB rozhraní pokyn k přepnutí, který vyhodnotí jednoúčelový počítač a přepne bezpečnostní relé na druhý informační systém.

Celkový počet přepnutí každého bloku AirGap 02 je omezen a proto jím poskytovaná možnost ovládání doby přepnutí ze strany vnějších počítačových systémů umožňuje optimalizovat životnost produktu a tím jej předurčuje pro široké pole použitelnosti.

[HODNOCENÍ BEZPEČNOSTI PROSTŘEDKU AIRGAP 02]

Common Criteria

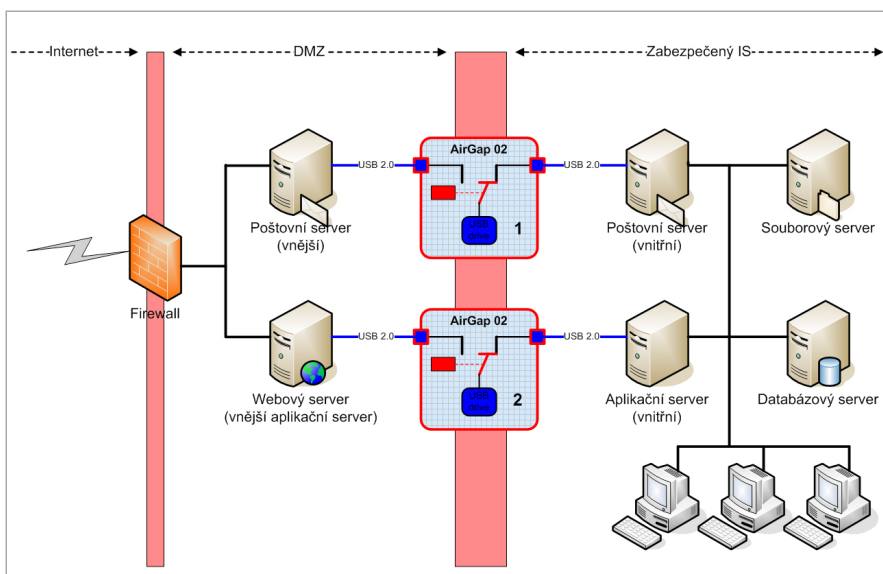
Bezpečnostní prostředek je vyvinut a zdokumentován dle požadavků dokumentů Common Criteria for Information Technology Security Evaluation, September 2006, Version 3.1, Revision 1, CCMB-2006-09-001 (dále jen [CC]),

- ▶ Part 1: Introduction and general model;
- ▶ Part 2: Security functional components;
- ▶ Part 3: Security assurance components.

Požadavky na záruku jsou stanoveny jako míra záruky hodnocení EAL4 rozšířená o ALC_FLR.2 tak, jak jsou definovány v CC verze 3.1, část 3. Nicméně použití fyzikálního oddělení obou propojovaných systémů poskytuje maximální odolnost bezpečnostního rozhraní proti útokům mezi oběma sítěmi.

NBÚ

Hodnocení AirGap 02 provedl NBÚ České Republiky s výrokem, že produkt neporušuje princip galvanického oddělení sítí a je vhodný pro začlenění do informačních systémů zpracovávající utajované informace podle zákona č. 412/2005 Sb., s požadavkem individuálního posouzení takové implementace v rámci certifikace informačního systému nebo v rámci standardního postupu schvalování změn, které ovlivňují bezpečnost v již certifikovaných informačních systémech.



- Organizace, které vyžadují zabezpečený IS (bezpečně oddělený od veřejných sítí jako je například internet) a současně potřebují zajistit základní komunikaci s vnějším světem pomocí standardních poštovních služeb a vlastní webové aplikace. Pomocí vhodné implementace bezpečnostního prostředku AirGap 02 bylo dosaženo úplného galvanického oddělení vnitřního zabezpečeného IS, kdy i při úplném ovládnutí serverů umístěných v DMZ dané organizace vnějším útočníkem, nemůže být proveden žádný síťový útok na vnitřní servery dané organizace.

OBCHODNÍ KONTAKT

ICZ a.s. Na hřebenech II 1718/10
140 00 Praha 4

TEL.: +420 222 271 111

FAX: +420 222 271 112

E-MAIL: marketing@i.cz