IT Security Solutions

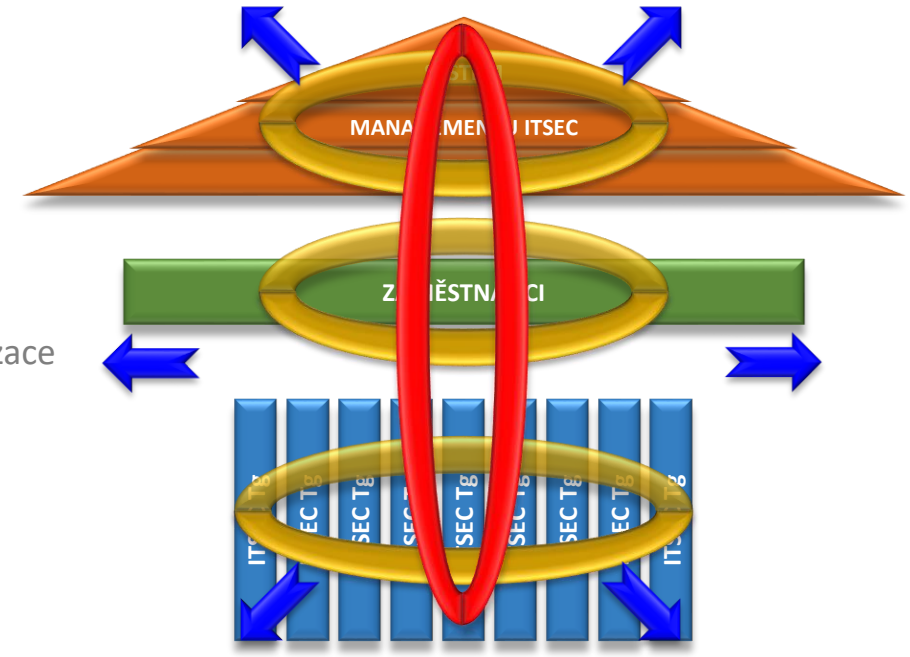
Tech Data

Ing. Miroslav Tůma, Ph.D.
IT Security Specialist
miroslav.tuma@techdata.com
+420 603 457 377

IT Security (ITSEC) – Jediný správný přístup je komplexita!

IT Security - ucelený, smysluplný, účelný a efektivní celek tvořený:

- Systém managementu ITSEC – pravidla
- Lidé (admin, users) – zavedení a dodržování pravidel a jejich realizace
- ITSEC Technologie – realizace ITSEC



Jednotlivé části ITSEC samostatně nedávají smysl a „nic neřeší“ mají význam jen za předpokladu následujících integrací:

- **Vnitřní integrace -** HORIZONTÁLNÍ INTEGRACE

  Jednotlivé části jsou vnitřně integrovány a každá část tvoří homogenní ucelený, smysluplný, účelný a efektivní subcelek ITSEC

- **Vzájemné integrace -** VERTIKÁLNÍ INTEGRACE

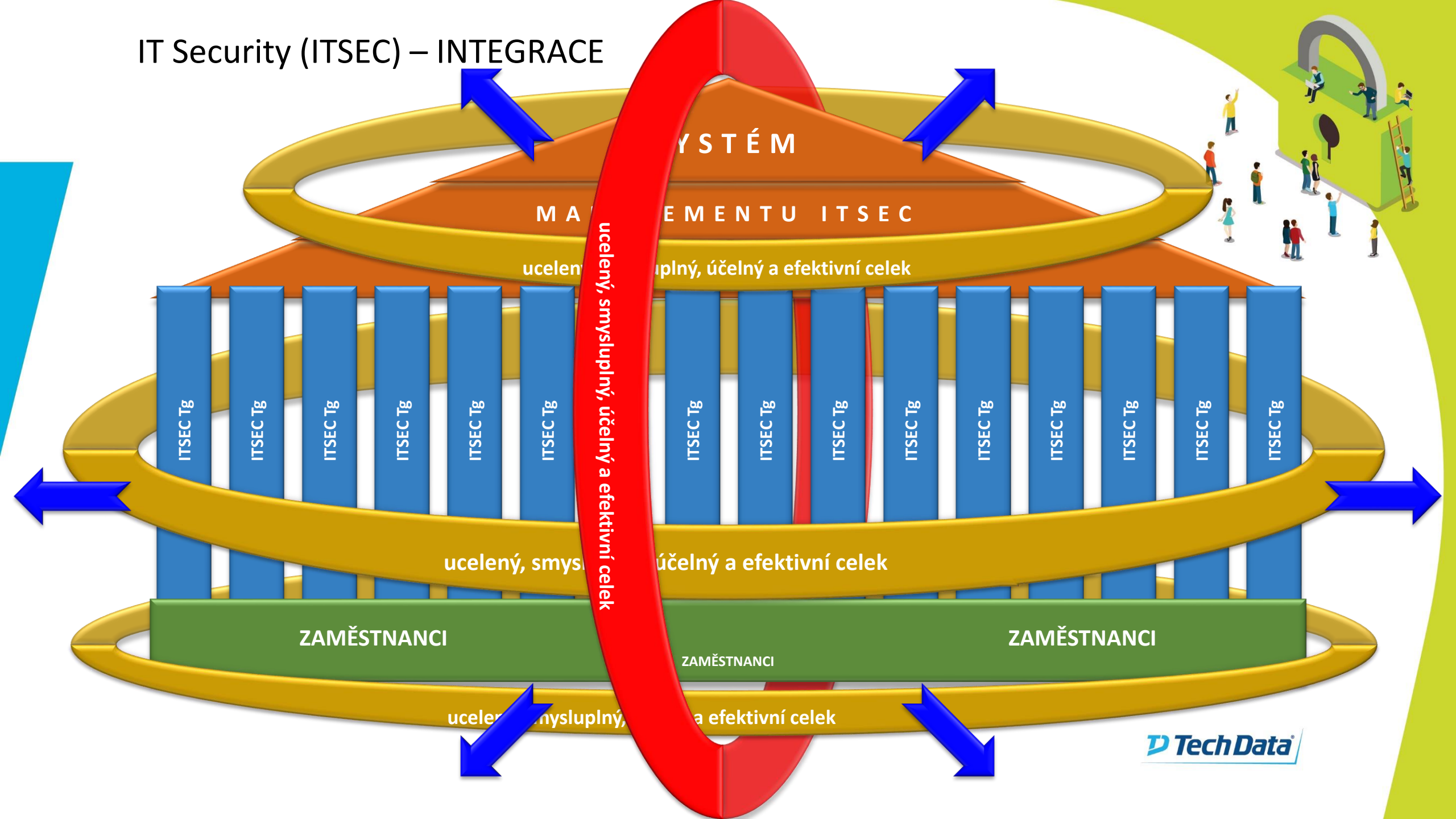
  Všechny tři části - subcelky jsou vzájemně integrovány do homogenního uceleného, smysluplného, účelného a efektivní celku – ITSEC

- **Ucelené integrace -** FIREMNÍ INTEGRACE

  Subcelky ITSEC a vlastní ITSEC jsou smysluplně, účelně a efektivně integrovány do systému řízení firmy a dle konkrétních firemních specifik

TechData

IT Security (ITSEC) – INTEGRACE



IT Security – technologie

IT SECURITY
NA ÚROVNI OPERÁTORA
SCRUBBING „pračka“

IT SECURITY
NA ÚROVNI
A V PERIMETRU

IT SECURITY
NA ÚROVNI
END POINTS

01

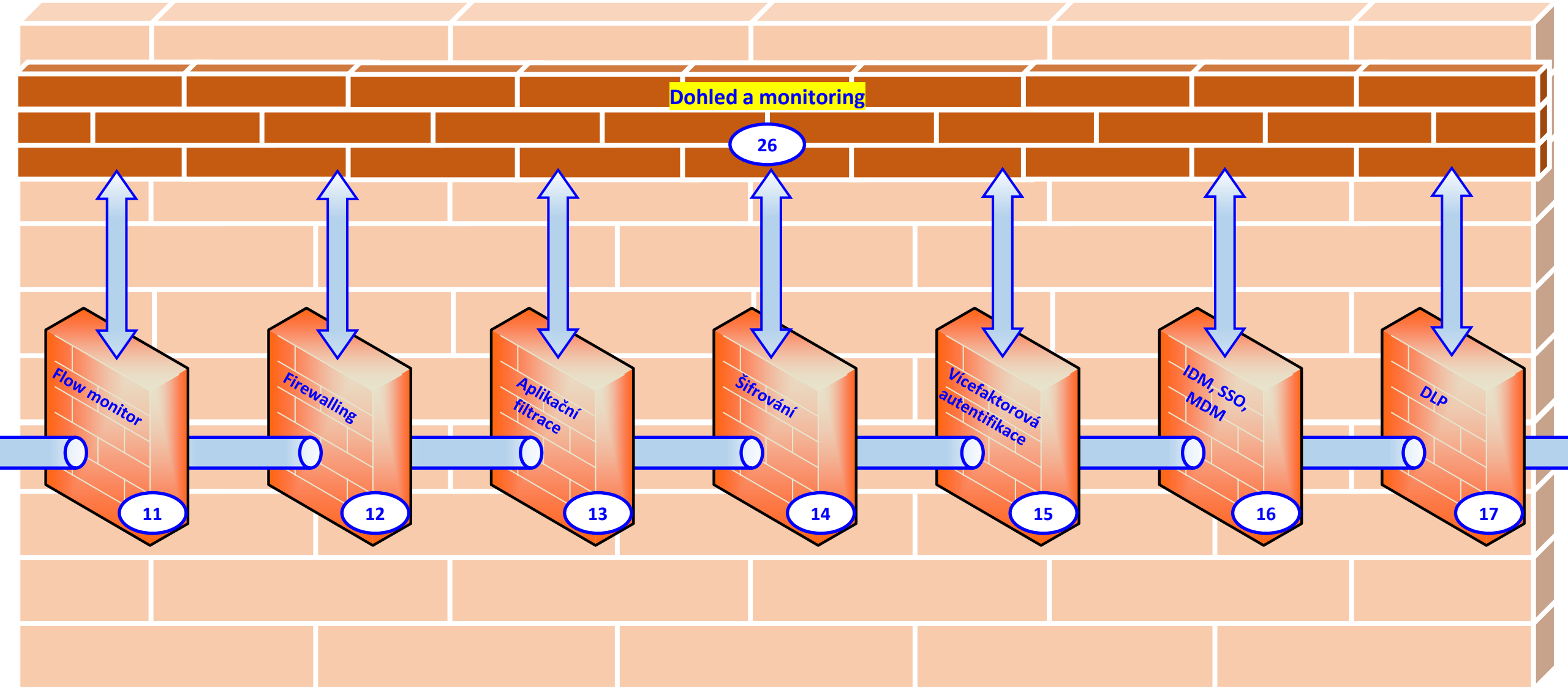
11-25

51-53

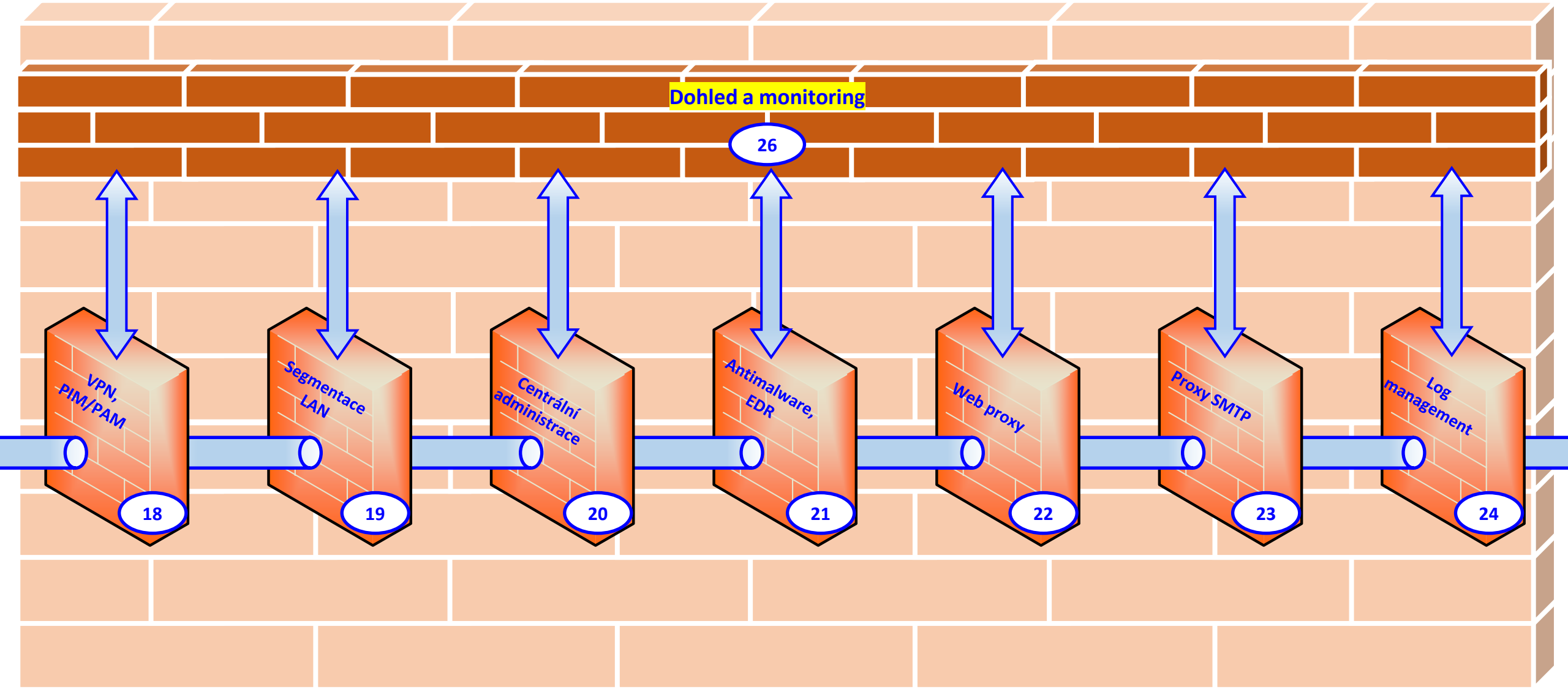
Dohled a monitoring

26

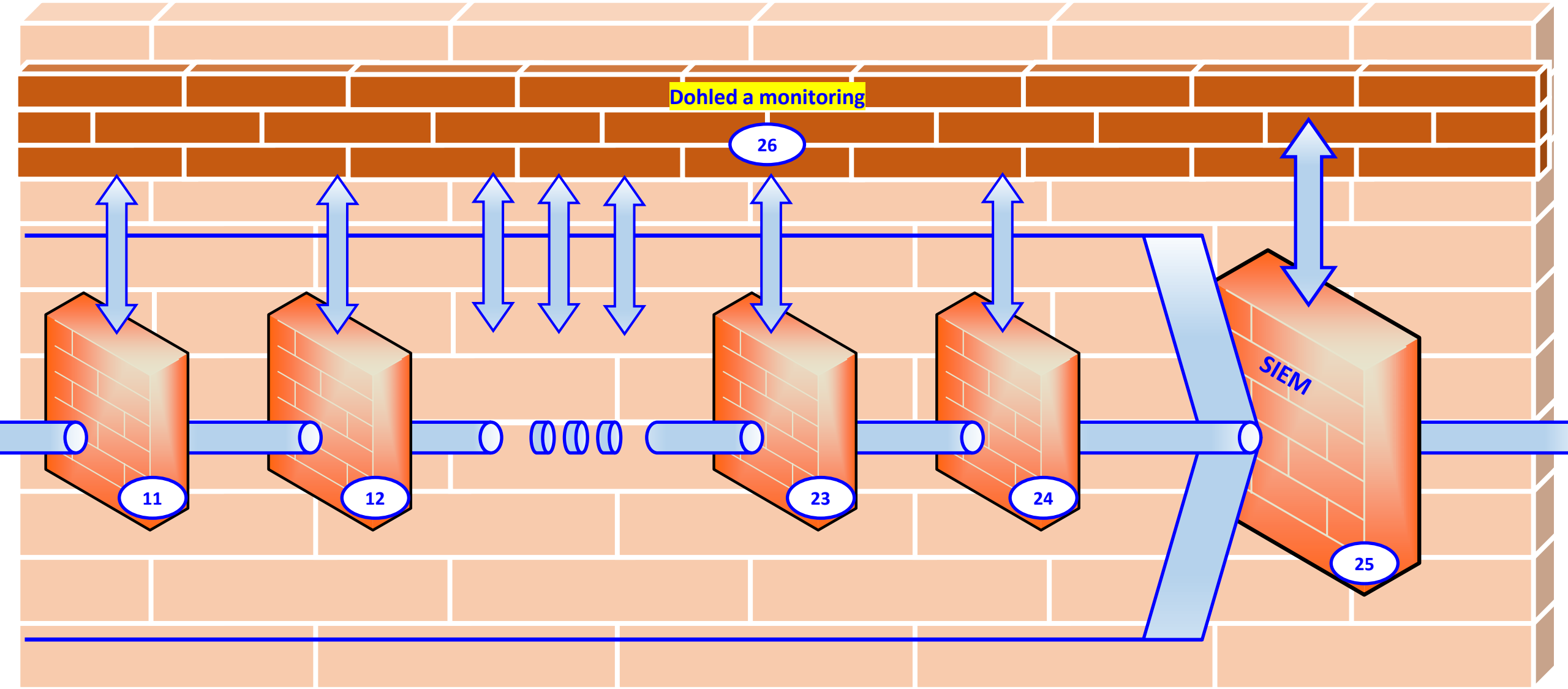
IT SECURITY NA ÚROVNI A V PERIMETRU 1. část



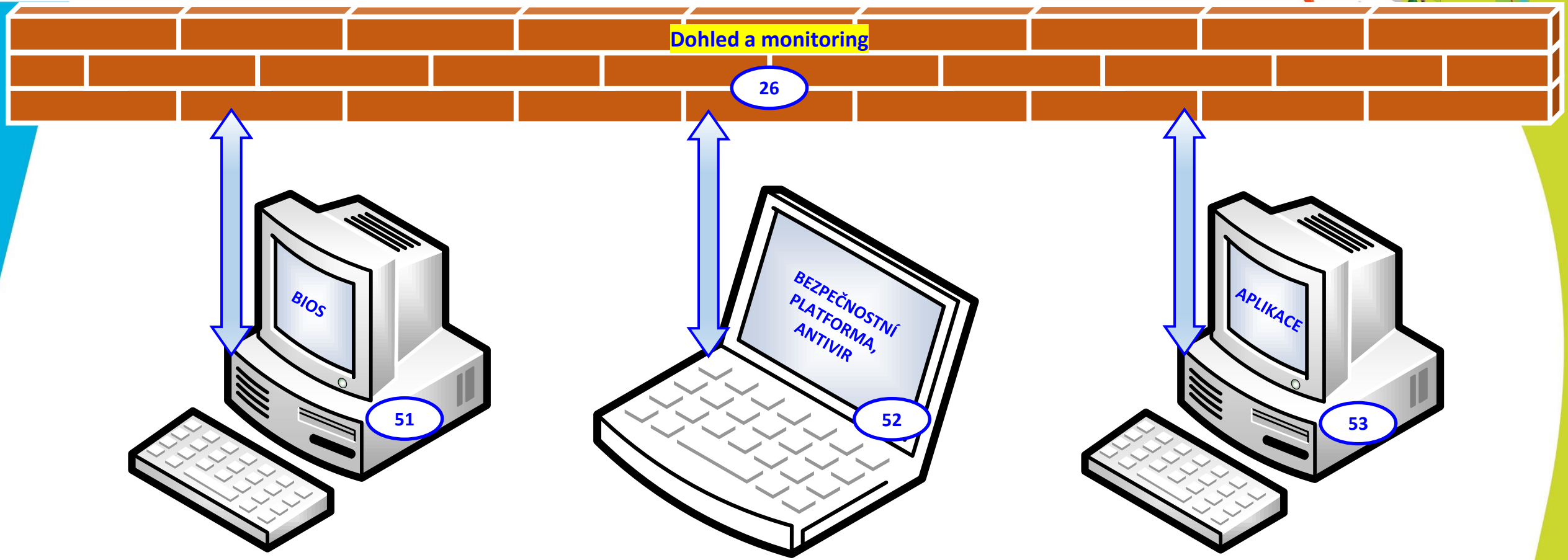
IT SECURITY NA ÚROVNI A V PERIMETRU 2. část



IT SECURITY NA ÚROVNI A V PERIMETRU



IT Security – technologie – na endpoints



51 – SECURITY NA ÚROVNI BIOS

52 – BEZPEČNÁ PLATFORMA, ANTIVIR

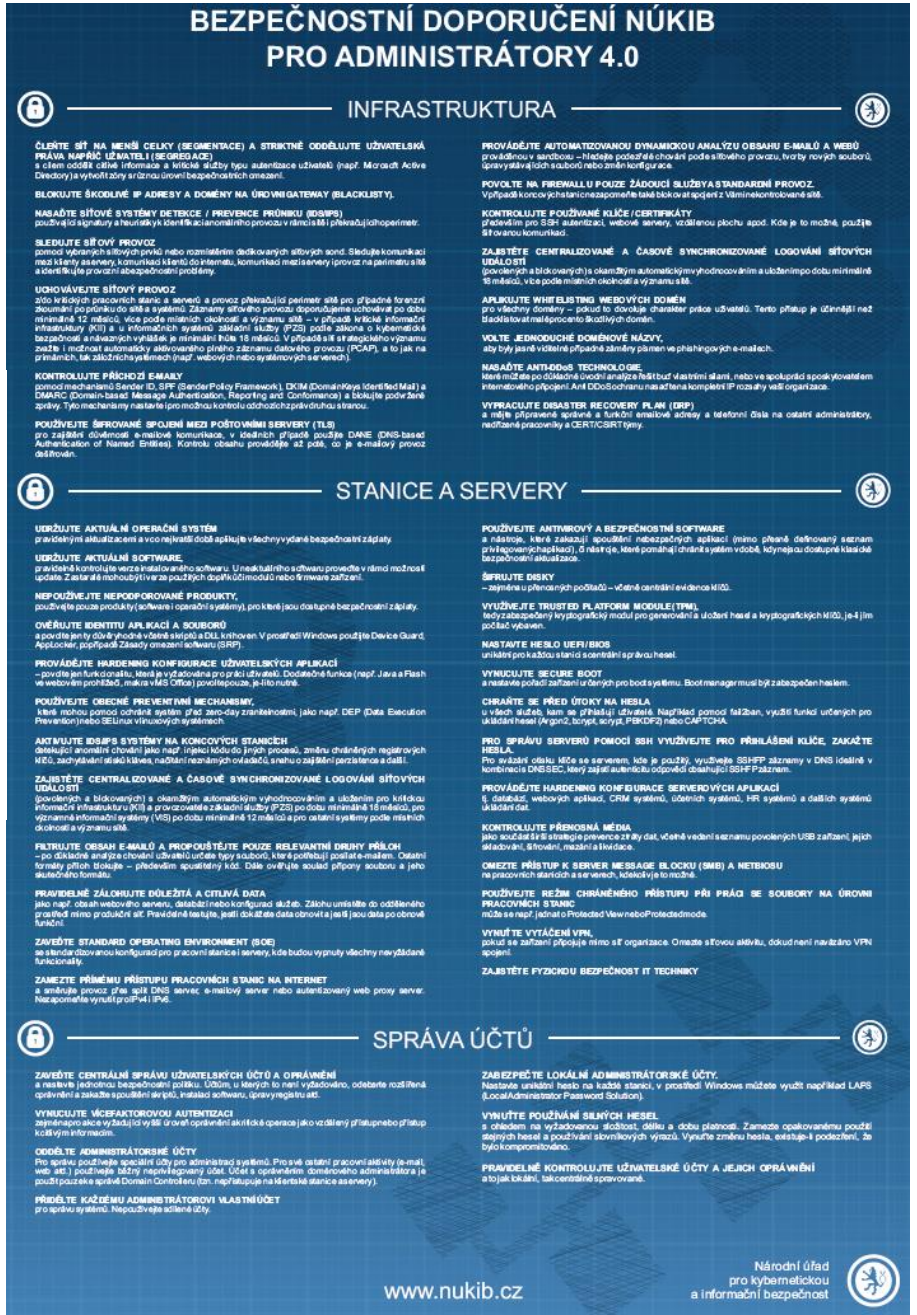
53 – SECURITY NA ÚROVNI APLIKACÍ

IT Security – technologie – doporučení NÚKIB

Celkem 47 nejrůznějších pravidel.

- 15 doporučení pro infrastrukturu.
- 25 doporučení pro stanice a servery.
- 7 doporučení pro správu účtů.

Naše řešení odpovídá na každé jedno z nich!



BEZPEČNOSTNÍ DOPORUČENÍ NÚKIB
PRO ADMINISTRÁTORY 4.0

INFRASTRUKTURA

ČLEŇTE SÍŤ NA MENŠÍ CELKY (SEGMENTACE) A STRIKTNĚ ODDĚLUJTE UŽIVATELSKÁ PRÁVA NAPŘÍČ UŽIVATELI (SEGREGACE)
s cílem oddělit citlivé informace a kritické služby typu autentizace uživatelů (např. Microsoft Active Directory) a vytvořit zóny s různou úrovní bezpečnostních omezení.

BLOKUJTE ŠKODLIVÉ IP ADRESY A DOMÉNY NA ÚROVNI GATEWAY (BLACKLISTY).

NASAĎTE SÍŤOVÉ SYSTÉMY DETEKCE / PREVENCE PRŮNIKU (IDS/IPS)
používající signatury a heuristických identifikacích anomálního provozu v rámci sítě překračující/chránící perimetr.

SLEDUJTE SÍŤOVÝ PROVOZ
pomocí vybraných síťových prvků nebo rozmístěním dedikovaných síťových sond. Sledujte komunikaci mezi klienty a servery, komunikaci klientů do internetu, komunikaci mezi servery i provoz na perimetru sítě a identifikujte provozní a bezpečnostní problémy.

UCHOVÁVEJTE SÍŤOVÝ PROVOZ
zdrojů kritických pracovních stanic a serverů a provoz překračující perimetr sítě pro případné forenzní zkoumání po průniku do sítě a systémů. Záznamy síťového provozu doporučujeme uchovávat po dobu minimálně 12 měsíců, více podle místních okolností a významu sítě – v případě kritické informační infrastruktury (KII) a u informačních systémů základní služby (PZS) podle zákona o kybernetické bezpečnosti a návazných vyhlášek je minimální lhůta 18 měsíců. V případě sítě strategického významu zvažte i možnost automatický aktivovaného plného záznamu datového provozu (PCAP), a to jak na primárních, tak záložních systémech (např. webových nebo systémových serverech).

KONTROLUJTE PŘÍCHOZÍ E-MAILY
pomocí mechanismů Sender ID, SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) a DMARC (Domain-based Message Authentication, Reporting and Conformance) a blokujte podvržené zprávy. Tyto mechanismy nastavte i pro možnou kontrolu odchozích zpráv z vlastní strany.

POUŽÍVEJTE ŠIFROVANÉ SPOJENÍ MEZI POŠTOVNÍMI SERVERY (TLS)
pro zajištění důvěrnosti e-mailové komunikace, v dalších případě použijte DANE (DNS-based Authentication of Named Entities). Kontrolu obsahu provádějte až poté, co je e-mailový provoz dešifrován.

PROVÁDĚJTE AUTOMATIZOVANOU DYNAMICKOU ANALÝZU OBSAHU E-MAILŮ A WEBŮ
provádějící v sandboxu – hledejte podezřelé chování podle síťového provozu, tvorby nových souborů, úpravy stávajících souborů nebo změn konfigurace.

POVOLTE NA FIREWALLU POUZE ŽÁDOUCÍ SLUŽBY A STANDARDNÍ PROVOZ.
V případě korcových stanic nezapomeňte také blokovat spojení z VLAN nekontrolované sítě.

KONTROLUJTE POUŽÍVANÉ KLÍČE / CERTIFIKÁTY
především pro SSH autentizaci, webové servery, vzdálenou plochu apod. Kde je to možné, použijte šifrovanou komunikaci.

ZAJISTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ
(povolených a blokovaných) s okamžitým automatickým vyhodnocováním a uložením po dobu minimálně 18 měsíců, více podle místních okolností a významu sítě.

APLIKUJTE WHITELISTING WEBOVÝCH DOMÉN
pro všechny domény – pokud to dovoluje charakter práce uživatelů. Tento přístup je účinnější než blacklistování malé procento škodlivých domén.

VOLTE JEDNODUCHÉ DOMÉNOVÉ NÁZVY,
aby byly jasně viditelné případné záměny písmen ve phishingových e-mailech.

NASAĎTE ANTI-DDoS TECHNOLOGIE,
které můžete po důkladné úvodní analýze řešit buď vlastními silami, nebo ve spolupráci s poskytovatelem internetového připojení. Ani DDoS ochranu nasaďte kompletní IP rozsahy vaší organizace.

VYPRACUJTE DISASTER RECOVERY PLAN (DRP)
a mějte připravené správné a funkční emailové adresy a telefonní čísla na ostatní administrátory, nadřízené pracovníky a CERT/CSIRT týmy.

STANICE A SERVERY

UDRŽUJTE AKTUÁLNÍ OPERAČNÍ SYSTÉM
pravidelnými aktualizacemi a co nejrychlejší době aplikujte všechny vydané bezpečnostní záplaty.

UDRŽUJTE AKTUÁLNÍ SOFTWARE.
pravidelně kontrolujte verze instalovaného software. U neaktuálního software proveďte v rámci možností update. Zastaralé mohou být i verze použitých doplňků/modulů nebo firmware zařízení.

NEPOUŽÍVEJTE NEPODPOROVANÉ PRODUKTY,
používejte pouze produkty (software i operační systémy), pro které jsou dostupné bezpečnostní záplaty.

OVĚŘUJTE IDENTITU APLIKACÍ A SOUBORŮ
a povolte jen ty důvěryhodné včetně skriptů a DLL knihoven. V prostředí Windows použijte Device Guard, AppLocker, popřípadě Zásady omezení softwaru (SRP).

PROVÁDĚJTE HARDENING KONFIGURACE UŽIVATELSKÝCH APLIKACÍ
– povolte jen funkcionalitu, která je vyžadována pro práci uživatelů. Dodatečné funkce (např. Java a Flash ve webovém prohlížeči, makra v MS Office) povolte pouze, je-li to nutné.

POUŽÍVEJTE OBECNÉ PREVENTIVNÍ MECHANISMY,
které mohou pomoci odhalit systém před zero-day zranitelnostmi, jako např. DEP (Data Execution Prevention) nebo SELinux virtualizovaných systémech.

AKTIVUJTE IDS/IPS SYSTÉMY NA KONCOVÝCH STANICÍCH
detekující anomální chování jako např. injekci kódu do jiných procesů, změnu chráněných registrových klíčů, zachytávání stisků kláves, načítání neznámých ovladačů, snahu o zajištění perzistence a další.

ZAJISTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ
(povolených a blokovaných) s okamžitým automatickým vyhodnocováním a uložením pro kritickou informační infrastrukturu (KII) a provozovatele základní služby (PZS) po dobu minimálně 18 měsíců, pro významné informační systémy (VIS) po dobu minimálně 12 měsíců a pro ostatní systémy podle místních okolností a významu sítě.

FILTRUJTE OBSAH E-MAILŮ A PROPOUŠTĚJTE POUZE RELEVANTNÍ DRUHY PŘÍLOH
– po důkladné analýze chování uživatelů určete typy souborů, které potřebují posílat e-mailem. Ostatní formáty příloh blokujte – především spustitelný kód. Dále ověřujte soulad přípony souboru a jeho skutečného formátu.

PRAVIDELNĚ ZÁLOHUJTE DŮLEŽITÁ A CITLIVÁ DATA
jako např. obsah webového serveru, databází nebo konfigurací služeb. Zálohu umístěte do odděleného prostředí mimo produkční síť. Pravidelně testujte, jestli dokážete data obnovit a jestli jsou data po obnově funkční.

ZAVEĎTE STANDARD OPERATING ENVIRONMENT (SOE)
se standardizovanou konfigurací pro pracovní stanice i servery, kde budou vypnuty všechny nevyžádané funkcionality.

ZAMEZTE PŘÍMÉMU PŘÍSTUPU PRACOVNÍCH STANIC NA INTERNET
a směrujte provoz přes split DNS server, e-mailový server nebo autentizovaný web proxy server. Nezapomeňte vynutit pro IPv4 i IPv6.

POUŽÍVEJTE ANTIVIROVÝ A BEZPEČNOSTNÍ SOFTWARE
a nástroje, které zakazují spouštění nebezpečných aplikací (mimo přesně definovaný seznam privilegovaných aplikací), či nástroje, které pomáhají chránit systém v době, kdy nejsou dostupné klasické bezpečnostní aktualizace.

ŠIFRUJTE DISKY
– zejména u přenosných počítačů – včetně centrální evidence klíčů.

VYUŽÍVEJTE TRUSTED PLATFORM MODULE (TPM),
čipy zabezpečený kryptografický modul pro generování a uložení hesel a kryptografických klíčů, je-li jím počítač vybaven.

NASTAVTE HESLO UEFI/BIOS
unikátní pro každou stanici s centrální správou hesel.

VYNUCUJTE SECURE BOOT
a nastavte pořadí zařízení určených pro boot systému. Boot manager musí být zabezpečen heslem.

CHRAŇTE SE PŘED ÚTOKY NA HESLA
u všech služeb, kam se přihlašují uživatelé. Například pomocí fail2ban, využití funkcí určených pro ukládání hesel (Argon2, bcrypt, scrypt, PBKDF2) nebo CAPTCHA.

PRO SPRÁVU SERVERŮ POMOCÍ SSH VYUŽÍVEJTE PRO PŘIHLÁŠENÍ KLÍČE, ZAKAŽTE HESLA.
Pro svázání otisku klíče se serverem, kde je použitý, využívejte SSHFP záznamy v DNS (ideálně v kombinaci s DNSSEC), který zajistí autenticitu odpovědi obsahující SSHFP záznam.

PROVÁDĚJTE HARDENING KONFIGURACE SERVEROVÝCH APLIKACÍ
(j. databází, webových aplikací, CRM systémů, účetních systémů, HR systémů a dalších systémů ukládání dat.

KONTROLUJTE PŘENOSNÁ MÉDIA
jako součást širší strategie prevence ztráty dat, včetně vedení seznamu povolených USB zařízení, jejich skladování, šifrování, mazání a likvidace.

OMEZTE PŘÍSTUP K SERVER MESSAGE BLOCKU (SMB) A NETBIOSU
na pracovních stanicích a serverech, kdekoliv je to možné.

POUŽÍVEJTE REŽIM CHRÁNĚNÉHO PŘÍSTUPU PŘI PRÁCI SE SOUBORY NA ÚROVNI PRACOVNÍCH STANIC
může se např. jednat o Protected View nebo Protected mode.

VYNUŤTE VYTÁČENÍ VPN,
pokud se zařízení připojuje mimo síť organizace. Omezte síťovou aktivitu, dokud není navázáno VPN spojení.

ZAJISTĚTE FYZICKOU BEZPEČNOST IT TECHNIKY

SPRÁVA ÚČTŮ

ZAVEĎTE CENTRÁLNÍ SPRÁVU UŽIVATELSKÝCH ÚČTŮ A OPRÁVNĚNÍ
a nastavte jednotnou bezpečnostní politiku. Účtům, u kterých to není vyžadováno, odeberte rozšířená oprávnění a zakažte spouštění skriptů, instalaci software, úpravy registrů atd.

VYNUCUJTE VÍCEFAKTOROVOU AUTENTIZACI
zejména pro akce vyžadující vyšší úroveň oprávnění a kritické operace jako vzdálený přístup nebo přístup k citlivým informacím.

ODDĚLTE ADMINISTRÁTORSKÉ ÚČTY
Pro správu používejte speciální účty pro administraci systémů. Pro své ostatní pracovní aktivity (e-mail, web atd.) používejte běžný neprivilegovaný účet. Účet s oprávněním doménového administrátora je použít pouze ke správě Domain Controllerů (tzn. nepřistupuje na klientské stanice a servery).

PŘIDĚLTE KAŽDÉMU ADMINISTRÁTOROVI VLASTNÍ ÚČET
pro správu systémů. Nepoužívejte sdílené účty.

ZABEZPEČTE LOKÁLNÍ ADMINISTRÁTORSKÉ ÚČTY.
Nastavte unikátní heslo na každé stanici, v prostředí Windows můžete využít například LAPS (Local Administrator Password Solution).

VYNUŤTE POUŽÍVÁNÍ SILNÝCH HESEL
s ohledem na vyžadovanou složitost, délku a dobu platnosti. Zamezte opakovanému použití stejných hesel a používání slovníkových výrazů. Vynuťte změnu hesla, existuje-li podezření, že bylo kompromitováno.

PRAVIDELNĚ KONTROLUJTE UŽIVATELSKÉ ÚČTY A JEJICH OPRÁVNĚNÍ
a to jak lokální, tak centrálně spravované.

www.nukib.cz

Národní úřad pro kybernetickou a informační bezpečnost

TechData

IT Security – jak jí dosáhnout - zavést, udržovat a rozvíjet

E T A P Y

Analýza organizace – zaměření, potřeby, stav, analýza rizik, …

Tvorba a verifikace Systém managementu ITSEC (ISMS)

Detailní analýza ICT – architektura, technologie, ISs, …

Návrh a verifikace ucelené, smysluplné, účelné a efektivní technologie ITSEC jako celku

Implementace Systému řízení ITSEC a technologie ITSEC ve vzájemné integraci

Provoz Systému řízení ITSEC a technologie ITSEC ve vzájemné integraci (PDCA), předcházení a řešení bezpečnostních událostí a incidentů, …

Rozvoj Systému řízení ITSEC a technologie ITSEC ve vzájemné integraci (PDCA)

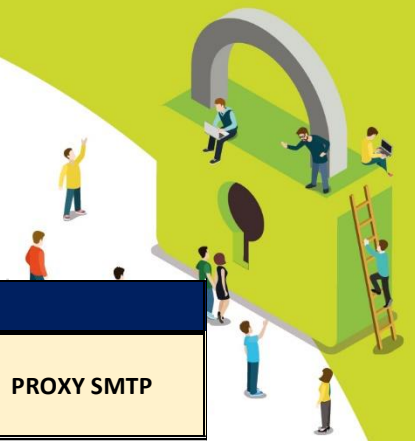
TechData

IT SECURITY SOLUTIONS TECH DATA

IT SECURITY (ITSEC)

NÁZEV komponenty ITSEC	Počet wendors pokrývající komponenty ITS (portólio TD)	ITSEC technologie TD												
		Palo Alto Networks	Barracuda Networks	IBM	Cisco	Microsoft	VMware	HPE	ORACLE	DELL	BROADCOM	SonicWall	Micro Focus	SOPHOS	Zyxel
SCRUBBING	5			X	X					X		X		X	
	6		X	X	X	X					X	X			
FLOW MONITOR	9	X		X	X		X	X		X	X	X			X
	6	X		X	X	X						X			X
FIREWALLING	8	X	X		X		X	X				X		X	X
	8	X	X	X	X	X						X		X	X
APLIKAČNÍ FILTRACE	11	X	X	X	X	X	X	X		X	X	X			X
	4	X	X			X						X			
ŠIFROVÁNÍ	9	X	X	X	X	X	X			X	X	X		X	
	8	X	X		X	X		X		X		X		X	
VÍCEFAKTOROVÁ AUTENTIFIKACE	7				X		X	X		X	X	X			X
	6			X	X	X					X	X			X
IDM, SSO, MDM	6			X	X	X	X		X		X				
	1			X											
DLP	5	X		X		X	X				X				
	4	X				X		X			X				
VPN, PIM/PAM	10	X	X	X	X		X	X			X	X		X	X
	6	X	X	X		X						X			X
SEGMENTACE LAN	11	X	X	X	X	X	X	X		X		X			X
	4	X	X									X			X
CENTRÁLNÍ ADMINISTRACE	9	X	X	X	X			X		X	X	X			X
	7	X	X			X		X				X			X
ANTIMALWARE, EDR	9	X	X	X	X	X	X				X	X		X	
	7	X	X	X				X			X	X		X	
WEB PROXY	9	X	X	X	X	X	X					X			X
	5	X	X		X	X		X							
PROXY SMTP	8	X	X		X	X					X	X			X
	5	X	X		X						X	X			
LOG MANAGEMENT	9	X	X	X	X		X	X				X			X
	6	X		X				X				X			X
SIEM	6	X		X			X			X		X			
	4	X		X								X			
DOHLED A MONITORING, SD	6	X		X	X		X	X							
	4	X		X				X							
ITSEC BIOS	6	X					X	X		X		X			
	3	X										X			
BEZPEČNOSTNÍ PLATFORMA, ANTIVIR	8	X		X		X	X				X	X			
	5	X	X	X								X			
ITSEC APLIKACÍ	7	X		X	X	X	X				X	X			
	5	X			X						X	X			

Příklad nasazení IT Security Solution TD



Produkt	kód ITSEC	NÁZEV komponenty ITSEC					
Palo Alto Networks NGFW	12 FIREWALLING	13 APLIKAČNÍ FILTRACE	14 ŠIFROVÁNÍ	18 VPN, PIM/PAM	19 SEGMENTACE LAN	22 WEB PROXY	23 PROXY SMTP
Palo Alto Networks CORTEX XDR	11 FLOW MONITOR	20 CENTRÁLNÍ ADMINISTRACE	21 ANTIMALWARE, EDR	52 BEZPEČNOSTNÍ PLATFORMA, ANTIVIR	53 ITSEC APLIKACÍ		
BROADCOM Symantec Endpoint Security	51 ITSEC BIOS	52 BEZPEČNOSTNÍ PLATFORMA, ANTIVIR	53 ITSEC APLIKACÍ				
Cisco DUO Security	15 VÍCEFAKTOROVÁ AUTENTIFIKACE	16 IDM, SSO, MDM					
IBM Qradar	24 LOG MANAGEMENT	25 SIEM					
BROADCOM CA SDM	26 DOHLED A MONITORING, SD						
Operátor	1 SCRUBBING						
	17 DLP						

paloalto® NETWORKS

TechData

IT Security Solutions

Tech Data

Ing. Miroslav Tůma, Ph.D.
IT Security Specialist
miroslav.tuma@techdata.com
+420 603 457 377

… děkuji za pozornost a Váš čas