

DOTAZNÍK PRO NASAZENÍ ŘÍZENÍ PŘÍSTUPU A MONITORINGU POČÍTAČOVÉ SÍTĚ VČETNĚ SEGMENTACE

Prosíme vyplňte:

1. Fyzická infrastruktura (kabeláž)				Poznámky:
Půdorysné výkresy budov s vyznačením datových zásuvek?	Ano	Ne	Nevím	
Měřicí protokoly od kabelových tras?	Ano	Ne	Nevím	
Dostatečný počet přípojných míst pro koncová zařízení?	Ano	Ne	Nevím	
Rozbočené datové zásuvky, typicky malý switch mimo datový rozvaděč?	Ano	Ne	Nevím	

2. Aktivní prvky				
Schéma fyzického zapojení akt. prvků?	Ano	Ne	Nevím	
Dostatečné propustnost páteřních spojení mezi akt. prvky?	Ano	Ne	Nevím	
Používáte v síti VLANy?	Ano	Ne	Nevím	
Dostatečný počet portů na akt. prvcích?	Ano	Ne	Nevím	
Seznam typů akt. prvků, ideálně Part Number?	Ano	Ne	Nevím	
Znáte IP adresy akt. prvků?	Ano	Ne	Nevím	
Nainstalovaný SW pro centrální správu akt. prvků a klíčových zařízení?	Ano	Ne	Nevím	
HW Firewall s podporou pokročilých technik detekce podezřelého datového provozu?	Ano	Ne	Nevím	

3. Bezdrátová infrastruktura				
Půdorysné výkresy budov s vyznačením WiFi přístupových bodů?	Ano	Ne	Nevím	
Dostatečné pokrytí kvalitním bezdrátovým signálem - měřicí protokol?	Ano	Ne	Nevím	
Bezdrátová síť řízená centrálním prvkem - kontrolérem?	Ano	Ne	Nevím	
Seznam typů AP a kontroléru, ideálně Part Number?	Ano	Ne	Nevím	
Požadujete návrh a instalaci WiFi?	Ano	Ne	Nevím	

4. Serverová infrastruktura				
Logické schéma zapojení serverů, případně diskových polí?	Ano	Ne	Nevím	
Dostatečný výpočetní výkon, paměť a diskový prostor?	Ano	Ne	Nevím	
Požadujete návrh na rozšíření serverového řešení?	Ano	Ne	Nevím	
Používáte záložní zdroje napájení (UPS / motorgenerátor)?	Ano	Ne	Nevím	
Používáte UPS pro automatické, korektní vypnutí serverů?	Ano	Ne	Nevím	

5. Virtualizace				
Typ virtualizace (Vmware, Hyper-V, KVM,...)?	Ano	Ne	Nevím	
Je výkon i kapacita dostatečná pro instalaci dalších virtuálních strojů?	Ano	Ne	Nevím	
Víte jaké síťové služby pro uživatele zajišťují vaše fyzické a virtuální servery?	Ano	Ne	Nevím	

6. Zálohování

Pravidelné, automatizované zálohování dat uložených na serverech včetně konfigurací?	Ano	Ne	Nevím	
Mají uživatelé na PC, důležitá data, lokálně uložená, která nejsou zálohovaná?	Ano	Ne	Nevím	
HW pro zálohování (NAS, pásková knihovna,...)?	Ano	Ne	Nevím	
HW fyzicky umístěn v jiné lokalitě?	Ano	Ne	Nevím	
HW logicky oddělen od produkčních serverů (VLAN)?	Ano	Ne	Nevím	
SW pro zálohování (Veeam,...)?	Ano	Ne	Nevím	
Je zdokumentované zálohovací schéma?	Ano	Ne	Nevím	
Existuje postup a plán obnovy dat v případě fatálního bezpečnostního incidentu (DRP)?	Ano	Ne	Nevím	

7. OS serverů

Používané typy OS včetně verze (Win 2012, 2016, 2019, Debian, CentOS, SuSE,...)?	Ano	Ne	Nevím	
Dostatečný počet uživatelských licencí na všechny OS serverů?	Ano	Ne	Nevím	
AntiSPAM na poštovním serveru nebo FW?	Ano	Ne	Nevím	

8. Cloudové služby

Cloudové služby na serveru ve vlastnictví?	Ano	Ne	Nevím	
Cloudové služby u poskytovatele těchto služeb (Microsoft (Office365), Google...)?	Ano	Ne	Nevím	
Jaké služby využíváte? (sdílení souborů, kancelářský SW,...)	Vyjmenujte:			
Napojeny na lokální LDAP např. AD?	Ano	Ne	Nevím	

9. Pracovní stanice

Jiné verze OS než Windows 10 Profesional?	Ano	Ne	Nevím	
Plán upgrade na Windows 10 Profesional?	Typ, verze, počet:			
Dostatečný počet uživatelských licencí na desktopový OS a instalované aplikace?	Ano	Ne	Nevím	
PC jsou naimportované do AD?	Ano	Ne	Nevím	
Uživatelé mají administrátorský přístup k lokálnímu OS?	Ano	Ne	Nevím	
Nainstalovaný a centrálně spravovaný antivirus?	Ano	Ne	Nevím	
Klient pro pokročilé detekce anomálií (sandboxing,...)?	Ano	Ne	Nevím	
Používáte tenké klienty pro využívání terminálových služeb?	Ano	Ne	Nevím	

10. Ostatní zařízení v poč. síti

Soukromá zařízení?	Ano	Ne	Nevím	
Síťové tiskárny?	Ano	Ne	Nevím	
IP telefonie?	Ano	Ne	Nevím	
Měření a regulace (MaR)?	Ano	Ne	Nevím	
Zabezpečovací a zhasací systém?	Ano	Ne	Nevím	
Stravovací terminály?	Ano	Ne	Nevím	
Vzdálené otevírání dveří?	Ano	Ne	Nevím	
Další?	Vyjmenujte:			

11. Řízení přístupu do LAN a WLAN

Využívají všichni uživatelé k přihlášení na PC účet v LDAP typicky Active Directory (AD)?	Ano	Ne	Nevím	
Využíváte nějaké funkce radius serveru?	Ano	Ne	Nevím	

12. Monitoring datových toků

Monitorujete datové toky v poč. síti typy pomocí flowmon sondy?	Ano	Ne	Nevím	
Užíváte nějaký systém pro detekci anomálního chování poč. sítě?	Ano	Ne	Nevím	

13. Centrální správa identity

Využíváte centrální správu identity (IDM) v různorodých informačních systémech a LDAP?	Ano	Ne	Nevím	
--	-----	----	-------	--

14. Vzdálený přístup (VPN)

Vzdálený přístup do lokální poč. sítě pouze přes VPN bez výjimek?	Ano	Ne	Nevím	
Kdo má přístup přes VPN zaměstnanci / IT personál, zákazníci, dodavatelé?	Vyjmenujte:			
Přístup z veřejné sítě na vzdálenou plochu (RDP) některého serveru bez VPN?	Ano	Ne	Nevím	
Nasdílené disky některého serveru nebo NAS na veřejnou IP adresu?	Ano	Ne	Nevím	
Pro ověření pouze jméno a heslo?	Ano	Ne	Nevím	
Napojení na LDAP typicky Active Directory (AD)?	Ano	Ne	Nevím	

15. Centrální správa logů

Provádíte sběr syslogových zpráv z klíčových zařízení a systémů na syslog server?	Ano	Ne	Nevím	
Provádíte nad syslogy pokročilé analýzy případně korelace?	Ano	Ne	Nevím	

16. Servisní podpora a profylaxe

Pravidelné testy výpadku napájení?	Ano	Ne	Nevím	
Pravidelné testy obnovy zálohovaných dat?	Ano	Ne	Nevím	
Pravidelný upgrade firmware HW komponent serverů, akt. prvků, FW?	Ano	Ne	Nevím	
Pravidelné aktualizace serverových OS, minimálně bezpečnostní?	Ano	Ne	Nevím	
Pravidelné aktualizace desktopových OS, minimálně bezpečnostní?	Ano	Ne	Nevím	
Serverové OS včetně virtualizace pod supportem výrobce?	Ano	Ne	Nevím	
Zálohovací SW pod supportem výrobce?	Ano	Ne	Nevím	
HW pod supportem výrobce (servery, disk. pole, NASky, switchy, firewally, WiFi,...)?	Ano	Ne	Nevím	
Uzavřená servisní smlouva na pravidelné kontroly a odbornou pomoc?	Ano	Ne	Nevím	

17. Vzdělávání

Pravidelné vzdělávání uživatelů v oblasti počítačové bezpečnosti?	Ano	Ne	Nevím	
---	-----	----	-------	--