axians

The best of ICT with a human touch

Hodnocení stavu kybernetické bezpečnosti a strategie

Je strategický plán pro udržení bezpečné a odolné infrastruktury prostřednictvím identifikace, hodnocení a stanovení priorit rizik.

Klíčové oblasti

- Endpoint Security
- Identity Management
- Network Security
- Security Monitoring & Detection
- Additional Security Services Security

Co získáte?

- **Ucelený pohled na kybernetickou bezpečnost** ve Vaší organizaci
- Hodnocení hlavních oblastí kybernetické bezpečnosti
- **Identifikace slabých míst** doporučení pro jejich odstranění
- **Strategický dokument** a určení priorit pro další rozvoj bezpečnosti
- Nezávislý vhled/názor nezatížený „profesní slepotou“ s minimálním usilím a v krátkém čase

Proč je to důležité?

- Abyste nemuseli trávit mnoho času na oblastech, které mají menší význam z pohledu bezpečnosti / zaměřit svůj čas na věci, které jsou důležité
- Umožní Vám to systematický přístup k otázkám kybernetické bezpečnosti
- Získáte manažerský podklad pro další rozhodování
- Identifikujete si nejvíce rizikové místa, na která se musíte zaměřit
- Získáte širší vhled do problematiky bezpečnostních řešení, technologií a trendů
- Získáte podklady a přehled o finančních nákladech daných oblastí

	BEZPEČNOSTNÍ ÚROVNĚ				
	Úroveň 1 Základní	**Úroveň 2** Mírně pokročilá	**Úroveň 3** Středně pokročilá	**Úroveň 4** Řízená	**Úroveň 5** Vyspělá
Ochrana koncových zařízení Endpoint Security	Basic Antivirus protection Emailová ochrana / Filtrování spamů	Pravidelné zabezpečování (hardening) Audity koncových zařízení Šifrování mobilních zařízení Vzdálený přístup (VPN)	Ochrana a správa mobilních zařízení (MDM)	Pokročilá ochrana koncových zařízení (EDR) Zabezpečený vzdálený přístup k aplikacím (ZTNA)	Prevence ztráty dat
Správa identit Identity Management	Základní správa identit užitelů Správa zařízení v síti	MFA pro veřejně dostupné a cloudové služby Audit nastavení Active Directory Základní multifaktorové ověření	Řízení přístupu na základě rolí (RBAC)	Správa privilegovaných účtů (PAM) Korporátně/centrálně spravovaná multifaktorová autentizace	Správa přístupu a identit (IAM)
Síťová bezpečnost Network Security	Zabezpečení DNS komunikace	Implementace Proxy Serveru Základní segmentace sítě (základní ACL)	Pokročilá segmentace sítě založená na vyhodnocení rizik/hrozeb Aplikační firewall Next-gen Business class Firewall (perimeter + internal)	Řízení přístupu k síti Flow security monitoring	Systém prevence průniku
Bezpečnostní monitoring a detekce MDR	Provozní dohled	Skenování zranitelností Centrální logování událostí	Zavedení procesu řízení zranitelností Pravidelné hodnocení úrovně bezpečnosti na roční bázi	Logování bezpečnostních událostí - Log Management Systém pro správu bezpečnostních informací a událostí (SIEM) Plán zvládání Incidentů (Incident management) Bezpečnostní monitoring (SOC)	Threat Intelligence Prediktivní bezpečnostní technologie Bezpečnostní orchestrace, automatizace a reakce (SOAR) Systémy detekcí anomálií Systémy detekce chování uživatelů
Přidružené bezpečnostní služby Additional Security Services	Zálohování dat	Pravidelné školení zaměstnanců Penetrační testování	Skenování veřejných zdrojů - DarkWeb (OSINT)	Cloud Security Posture Management (CSPM) nástroje	Governance Risk Compliance (GRC) nástoje

Realizace projektu

1 PŘÍPRAVA

Úvodní schůzka

Poskytnutí dokumentace

2 HODNOCENÍ

Analýza dokumentace

Pohovory s odpovědnými osobami

3 NÁSLEDNÉ ZPRACOVÁNÍ

Zpracování zprávy

Identifikace Quick Wins s nízkými náklady

Návrh strategických opatření

4 PREZENTACE

Prezentace závěrečné zprávy a doporučení

Kontakt:

Kryštof Oczadlý
Head of Sales
tel.: +420 720 761 981
e-mail: krystof.oczadly@axians.com

David Tůma
Sales Manager
tel.: +420 731 441 783
e-mail: david.tuma@axians.com

VINCI ENERGIES