Kybernetická bezpečnost PZS

Prakticky, přiměřeně, bez strašení

Michal Beneš

CEO s-boost
benes@s-boost.cz

Východiska bezpečnosti

HROZBY

Překonání fyzického perimetru
Využití zranitelnosti technologie
Politické změny
Insider (cílené zaměstnání, vydírání)
Napadení dodavatele
Válka

ZRANITELNOSTI

Zabezpečení technologií
Vzdálený přístup
IT / OT konvergence
Admin účty
Cloudové technologie
Vstup do budov

AKTIVA

Lidé
Průmyslové technologie
Informace, data
Lokality a budovy
HW, SW

DOPADY

Finanční ztráta
Ohrožení lidských životů
Dopady do životního prostředí
Ztráta důvěry
Sankce a soudní řízení
Ztráta aktiv

BEZPEČNOST

FYZICKÁ	PERSONÁLNÍ	IT / OT	INFORMAČNÍ
Areály Budovy Technologické celky	Interní pracovníci Externí pracovníci	Průmyslové technologie Informační technologie Informační systémy Komunikační sítě	Osobní údaje Strategické informace Obchodní informace Utajované informace

KONTINUITA ČINNOSTI PODNIKU

Naplnění očekávání vlastníků
Dlouhodobý růst
Odpovědné chování
Reputace
Finanční prosperita

Koncept bezpečnosti

Bezpečnostní politiky a bezpečnostní dokumentace

Bezpečnostní role a orgány				
	Manažer KB	Auditor KB	OT technik	VŘKB
	Architekt KB	Garant aktiva	IT technik	IRT

Nástroje zajištění bezpečnosti

FYZICKÁ	PERSONÁLNÍ	IT / OT	INFORMAČNÍ
Ostraha Zabezpečení perimetru EZS, kamery, PCO Poučený zaměstnanec Řízení vstupu	Výběr zaměstnanců Motivace Školení Testování Řízení přístupu	Konfigurace technologií Řízení oprávnění a přístupu Bezpečnostní monitoring Návnady Poučený zaměstnanec Testování a fixace zranitelností	Klasifikace informací Dostupnost, integrita, důvěrnost Řízení přístupu k datům Sledování pohybu dat Šifrování dat

Sledování, testování, vyhodnocování, zpětná vazba, zlepšování

Soulad s legislativními požadavky a platnými směrnicemi

Kyberbezpečnost – na co se zaměřit

30 dnů	60 dnů	90 dnů a více
Prověřit aktuálnost a nastavení EDR a VPN	Zpracovat evidenci hlavních aktiv	Zpracování BIA
Zavést u vnějších aplikací 2-faktor	Obeslat klíčové dodavatele s podpisem dodatků	Zpracovat DRP
Udělat pořádek v identitách (uživatelských účtech)	Zpracovat IRP	Zpracovat BCP
Ověřit nastavení zálohování a restore	Provést penetrační testy na klíčové služby do externího perimetru	Prediktivní údržba a obnova aktiv
Omezit užití USB	Zahájit implementaci monitoringu a log managementu	Řešení zastupitelnosti aktiv
Provést externí test zranitelnosti	Zahájit školení klíčových adminů	Zahájit zavedení DLP
Provést interní testy zranitelnosti	Zahájit školení uživatelů	Zahájit analýzu rizik
	Jmenovat odpovědné osoby - garanty	Zavést patch mamagement a řízení obnovy

Digitalizace řízení

Poznej svá aktiva a architekturu

Pečuj o svá aktiva bezpečně a ekonomicky

Věnuj se compliance z praktického hlediska

IT a OT autodiscovery + CMDB

Technický informační systém

GRC nástroj

MANAŽERSKÝ KOKPIT – Integrace, reporting a automatizace

TOGAF

ITIL

IT4IT

CYBER LAW

Digitalizace řízení

Modul Řízení regulace	Modul Řízení aktiv	Modul Datová integrace
Bezpečnostní Intel (monitoring hrozeb)	Evidence a životní cyklus aktiv (OT, dle potřeb i IT)	Integrace na ERP (Evidence majetku)
Monitoring a analýza stavu regulatorních požadavků	Systematizace aktiv, typová aktiva	Integrace na TIS
Řízení nápravných opatření	Prediktivní údržba a obnova aktiv	Integrace na CMDB
Řízení aktiv a rizik, typová rizika	Řešení havarijních situací Disaster Recovery	Autodiscovery SW pro infrastrukturu OT
Řízení bezpečnostní dokumentace	Správa bezpečnostních prvků aktiv (firmware, dokumentace...)	Případné další IS s informacemi o majetku a technologiích
Řízení dodavatelů	Monitoring zranitelností aktiv	
Komunikace s regulačními orgány	Řešení zastupitelnosti aktiv Business Continuity	