Microsoft Services Premier Support

Implementace Zákona o kybernetické bezpečnosti

Organizační opatření

Microsoft

Vyhláška k ZKB 181/2014 Sb.	Předmět	Řešení
§4 Řízení rizik, *odst. 4* – povinná osoba „zvažuje hrozby“	Písm. **c)** zneužití identity jiné fyzické osoby	DIF – Dynamic Identity Framework Assessment
	d) užívání SW v rozporu s licenčními podmínkami	SAM – Software Asset Management
	f) škodlivý kód	SERA – Security Error Reporting & Analysis
	k) trvale působící hrozby (APT)	PADS – Persistent Adversary Detection Services
§4 Řízení rizik, *odst. 5* – povinná osoba „zvažuje zranitelnosti“	**b)** nedostatečné bezpečnostní povědomí uživatelů a administrátorů **c)** nedostatečná údržba informačního systému **d)** nevhodné nastavení přístupových oprávnění **f)** nedostatečné monitorování činnosti uživatelů a administrátorů	MSRA – Microsoft Security Risk Assessment SUM – Software Update Management
§8 Řízení aktiv	*Odst. 1.* **c)** hodnotí důležitost primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti a zařadí je do jednotlivých úrovní minimálně v rozsahu podle přílohy č. 1 k této vyhlášce	Metodika Microsoft pro označení primárních aktiv do 4 úrovní (HBI / MBI / LBI / Public)
	Odst. 2. **a)** identifikuje a eviduje podpůrná aktiva **c)** určí vazby mezi primárními a podpůrnými aktivy a hodnotí důsledky závislostí mezi primárními a podpůrnými aktivy	CCM – Change & Configuration Management (volitelně s využitím System Center), SMAP – Service Mapping
	Odst 3. **a)** Bod 2. stanoví pravidla pro manipulaci… s aktivy podle jejich úrovně, včetně pravidel pro bezpečné sdílení a přenášení aktiv; Bod 3. Stanoví přípustné způsoby používání aktiv **b)** Zavede pravidla ochrany odpovídající úrovni aktiv	Stanovení pravidel pro nasazení zabezpečovacích mechanismů – např. RMS pro Outlook / MS Office, Bitlocker šifrování pro paměťová média, zabezpečené přenosy dat, el. podpis pro vyšší úrovně zabezpečení aktiv

Vyhláška k ZKB 181/2014 Sb.	Předmět	Řešení
§10 Řízení provozu a komunikací, *odst. 3* – provozní pravidla a postupy	a) práva a povinnosti osob zastávajících bezpečnostní role, administrátorů a uživatelů	RKM – Roles and Knowledge Management
	b) postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů	RES – Recovery Execution Services (Windows Server, Cluster AD, Exchange, Sharepoint, SQL) Remediation Side-by-Side
	c) postupy pro sledování kybernetických bezpečnostních událostí a pro ochranu přístupu k záznamům o těchto činnostech	V rámci Proactive Monitoring with System Center Operations Manager
	e) postupy řízení a schvalování provozních změn	CCM - Change and Configuration Management
§ 11 Řízení přístupu a bezpečné chování uživatelů, *odst. 1* a *odst. 3*	*Odst. 1* – Přidělení jednoznačného identifikátoru každému uživateli.	ESAE – Enhanced Security Administrative Environment
	Odst. 3 – Oprávněná osoba a) přidělí přistupujícím aplikacím samostatný identifikátor,	DIF – Dynamic Identity Framework Assessment
	b) omezí přidělování administrátorských oprávnění,	Technologie pro identity management (Microsoft Active Directory, AD Federation Services, a Forefront Identity Manager)
	c) přiděluje a odebírá přístupová oprávnění v souladu s politikou řízení přístupu,	
	d) provádí pravidelné přezkoumání nastavení přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách nebo rolích,	
	e) využívá nástroj pro ověřování identity uživatelů podle § 18 a nástroj pro řízení přístupových oprávnění podle § 19	
	f) zavede bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení, případně i bezpečnostní opatření spojená s využitím technických zařízení, kterými povinná osoba nedisponuje	Enterprise Mobility Blueprint Enterprise Mobility Suite – Azure AD Premium, Intune, RMS WPhone 8.1, Android, iOS
§ 12 Akvizice, vývoj a údržba, *odst. 2*	b) zajistí bezpečnost vývojového prostředí a zajistí ochranu používaných testovacích dat	SDL – Security Development Lifecycle
	c) provádí bezpečnostní testování změn informačního systému kritické informační infrastruktury nebo komunikačního systému kritické informační infrastruktury před jejich zavedením do provozu	Používán interně pro veškerý SW Microsoft Zákazníkům je poskytována metodika, analýza a školení

Vyhláška k ZKB 181/2014 Sb.	Předmět	Řešení
§ 13 Zvládání kybernetických bezpečnostních událostí a incidentů	a) přijme nezbytná opatření, která zajistí oznamování kybernetických bezpečnostních událostí ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a o oznámeních vede záznamy, b) připraví prostředí pro vyhodnocení oznámených kybernetických bezpečnostních událostí a kybernetických bezpečnostních událostí detekovaných technickými nástroji podle § 21 až 23, provádí jejich vyhodnocení a identifikuje kybernetické bezpečnostní incidenty e) dokumentuje zvládání kybernetických bezpečnostních incidentů	Procesně – Incident Management V rámci technologií Microsoft System Center (Service Manager, Operations Manager)
	c) provádí klasifikaci kybernetických bezpečnostních incidentů, přijímá opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu, provádí hlášení kybernetického bezpečnostního incidentu podle § 32 a zajistí sběr věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu d) prošetří a určí příčiny kybernetického bezpečnostního incidentu, vyhodnotí účinnost řešení kybernetického bezpečnostního incidentu a na základě vyhodnocení stanoví nutná bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu	SERA – Security Error Reporting & Analysis PADS – Persistent Adversary Detection Services IR&R – Incidence Response & Recovery Service
§ 14 Řízení kontinuity činností	*Odst. 1*, písm. b) cíle řízení kontinuity činností formou určení 1. minimální úrovně poskytovaných služeb 2. doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb 3. bodu obnovení dat jako termínu, ke kterému budou obnovena data po kybernetickém bezpečnostním incidentu	Operations Consulting – Service Level Management ITSCM – IT Service Continuity Management
	Odst. 2, písm. b) stanoví, aktualizuje a pravidelně testuje plány kontinuity činností informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury	RES – Recovery Execution Services (Windows Server, Cluster AD, Exchange, Sharepoint, SQL)

Vyhláška k ZKB 181/2014 Sb.	Předmět	Řešení
§ 15 Kontrola a audit kybernetické bezpečnosti	*Odst. 3* – pro informační systém kritické informační infrastruktury a komunikační systém kritické informační infrastruktury provádí kontrolu zranitelnosti technických prostředků pomocí automatizovaných nástrojů a jejich odborné vyhodnocení a reaguje na zjištěné zranitelnosti	RAP as a Service for Microsoft Security (Security Healthcheck) Active Directory Security Assessment

Technická opatření

Microsoft

§ 17 Nástroj pro ochranu integrity komunikačních sítí	*Odst. 1* a) řízení bezpečného přístupu mezi vnější a vnitřní sítí c) kryptografické prostředky (§ 25) pro vzdálený přístup, vzdálenou správu nebo pro přístup pomocí bezdrátových technologií	Direct Access (součást OS Windows) a UAG (Unified Access Gateway) a jeho nástupce Windows Server 2012 R2 Federace identit ADFS
	Odst. 1 b) segmentaci zejména použitím demilitarizovaných zón jako speciálního typu sítě používaného ke zvýšení bezpečnosti aplikací dostupných z vnější sítě a k zamezení přímé komunikace vnitřní sítě s vnější sítí *Odst. 2* využívá nástroje pro ochranu integrity vnitřní komunikační sítě, které zajistí její segmentaci	NAP (Network Access Protection) – součást OS Windows
§ 18 Nástroj pro ověřování identity uživatelů	Řešení kompletně splňuje	Microsoft Active Directory jako součást OS Windows
§ 19 Nástroj pro řízení přístupových oprávnění	Řešení kompletně splňuje	Forefront Identity Manager a prostředky OS Windows
§ 20 Nástroj pro ochranu před škodlivým kódem	b) serverů a sdílených datových úložišť a c) pracovních stanic, přičemž provádí pravidelnou aktualizaci nástroje pro ochranu před škodlivým kódem, jeho definic a signatur	System Center Endpoint Protection – součást Core CAL (EA) Windows Defender jako součást OS Windows

Vyhláška k ZKB 181/2014 Sb.	Předmět	Řešení
§ 21 Nástroj pro zaznamenávání činností KII a VIS systémů, jejich uživatelů a administrátorů	Řešení kompletně splňuje	System Center Audit Collection Services a součásti OS Windows
§ 22 Nástroj pro detekci kybernetických bezpečnostních událostí	*Odst. 2*, písm. b) serverů patřících do informačního systému kritické informační infrastruktury a komunikačního systému kritické informační infrastruktury	System Center Endpoint Protection, SERA – Security Error Reporting & Analysis
§ 23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí	Je možné pokrýt všechny požadavky (Microsoft nenabízí SIEM)	System Center a SQL Reporting Services
§ 24 Aplikační bezpečnost	*Odst. 1* – bezpečnostní testy zranitelnosti aplikací, které jsou přístupné z vnější sítě, a to před jejich uvedením do provozu a po každé zásadní změně bezpečnostních mechanismů.	SDL (Security Development Lifecycle) – Application vulnerability assessment
§ 25 Kryptografické prostředky	Symetrické algoritmy: AES 128 nebo 256 bit Asymetrické algoritmy: DSA, EC-DSA, RSA 2048 bit Hash funkce SHA-2 / SHA-256 a vyšší	Součásti OS Windows jako Bitlocker, EFS, RMS, IPSec, KMS, atd., Windows Phone
§ 26 Nástroj pro zajišťování úrovně dostupnosti	*Odst. 2* – a) dostupnost informačního systému KII… c) zálohování důležitých technických aktiv informačního systému KII a kom. systému KII 1. využitím redundance v návrhu řešení a 2. zajištěním náhradních technických aktiv v určeném čase.	System Center Operations Manager Data Protection Manager, Windows Cluster, Cold Backup Windows Azure, StorSimple