Zabezpečení kybernetické bezpečnosti

Kód:	FSv_PD_2023_05_V01
Druh:	Příkaz děkana
Č. j.:	CVUT00021748/2023
Oblast normy:	ISMS
Organizační závaznost:	FSv
Garant:	11375 vedoucí VIC Ing. Tomáš Líbenek
Vydavatel:	prof. Ing. Jiří Máca, CSc. děkan
Počet stran:	4
Počet příloh:	0
Rozdělovník:	Martina Vavřinová (B-11000-DEKAN-SEKRETARKA)
Dotčené osoby:	všichni (B-11000-SUMA-OSOBA-CVUT)
Forma zveřejnění:	intranet
Nahrazuje:	Opatření děkana č. 12/2022
Datum vydání:	04.12.2023
Účinnost:	04.12.2023 – do zrušení
Platnost:	04.12.2023 – do zrušení
Další informace:	
Podpis vydavatele:	

v.r.

prof. Ing. Jiří Máca, CSc.

děkan fakulty

Přehled změn

Nejsou.

Seznam příloh

Nejsou.

Seznam souvisejících dokumentů

Nejsou.

V souladu s čl. 18 odst. 4 Statutu Fakulty stavební Českého vysokého učení technického v Praze vydávám tento příkaz:

Článek 1
Základní ustanovení

Tímto příkazem se ukládá všem katedrám a pracovištím FSv přijmout a implementovat organizační a technická opatření k minimalizaci kybernetické hrozby a výskytu kybernetického incidentu v komunikační a informační infrastruktuře FSv nebo ČVUT v Praze.

Článek 2
Organizační opatření

2.1 Zařízení, připojená do pevné datové sítě FSv, budou centrálně evidována v Informačních systémech provozovaných Výpočetním a informačním centrem FSv (dále jen „VIC FSv") (dále jen „IS VIC FSv"). U zařízení budou evidovány jeho síťové identifikátory, typ zařízení, operační systém, inventární číslo, umístění, organizační jednotka a odpovědná osoba s platným vztahem k FSv.

2.2 VIC FSv bude periodicky informovat odpovědné osoby a sekretariáty kateder a pracovišť FSv o zjištěných nesouladech v IS VIC FSv s výzvou k jejich nápravě.

2.3 Odpovědná osoba zodpovídá zejména za:

a) udržování aktuálních informací v IS VIC FSv,
b) aplikaci tohoto pokynu na všech svěřených zařízeních,
c) zajištění všech dostupných kroků k odstranění zranitelností na svěřených zařízeních a na software na nich nainstalovaných.

2.4 Bude probíhat periodické školení zaměstnanců a partnerů fakulty v tématech kybernetické bezpečnosti, a to ve dvou stupních:

a) prezenční školení, určené pro vedoucí a manažerské pracovníky fakulty, kateder a středisek, dále zaměstnancům pracovišť, a řešitelům grantů, které jsou z hlediska kybernetické bezpečnosti významné,
b) online školení, určené pro všechny ostatní pracovníky a vybrané partnery fakulty.

O zařazení do konkrétní skupiny rozhoduje tajemník fakulty.

2.5 VIC FSv provozuje stránku na webovém Portálu FSv, kde souhrnně informuje a podrobněji vysvětluje fakultní opatření ke kybernetické bezpečnosti, je-li to relevantní.

Článek 3
Technická opatření

3.1 V datové síti FSv je zakázáno provozovat výrobcem nepodporovaná zařízení, případně výrobcem nepodporovaný software na těchto zařízeních nainstalovaný.

3.2 Je zakázáno pořizovat a v datové síti FSv provozovat zařízení od výrobců, před kterými vydal varování Národní úřad pro kybernetickou a informační bezpečnost.

3.3 Na všech zařízeních připojených do datové sítě FSv musí být nainstalované centrálně provozované a monitorované bezpečnostní řešení VIC FSv.

3.4 Tzv. Dočasný přístup do datové sítě FSv (WG server) není podporován. Všechny počítače, které přistupují do datové sítě FSv pomocí pevného připojení musí být registrovány v IS VIC FSv.

3.5 Na zařízení v pevné datové síti FSv je blokován veškerý příchozí provoz z datových sítí mimo FSv. Odchozí provoz zůstane beze změny.

3.6 Vzdálený přístup na zařízení v datové síti FSv je možný pouze přes VPN provozovanou ČVUT nebo FSv. Pro přístup na zařízení s operačním systémem MS Windows je možné použít pouze Vzdálenou plochu a pro operační systém Linux protokol SSH. Všechny ostatní metody (TeamViewer, VNC apod.) jsou zakázány a blokovány.

3.7 Servery ve správě kateder musí být v evidenci v IS VIC FSv označeny jako servery, připojeny přes vyhrazený adresní prostor a musí na nich být umístěn EDR software, spravovaný a monitorovaný VIC FSv nebo VIC ČVUT.

3.8 Lokální datová pole (NAS) ve správě kateder musí být v evidenci v IS VIC FSv označena jako NAS, musí být připojena přes vyhrazený adresní prostor a musí se řídit pro ně definovanou bezpečnostní politikou.

3.9 Pracovníci, kteří ke své práci používají virtualizační platformu Tenkého klienta, ji musí používat výhradně, a to i pro práci z domova. Není dovoleno si pracovní data kopírovat na jiná, soukromá nebo služební zařízení, případně si na ně instalovat software potřebný pro práci. Veškerá činnost se bude odehrávat ve virtuálním prostředí pomocí vzdáleného připojení.

3.10 VIC FSv je oprávněn odpojit od datové sítě zařízení:

a) u kterého odpovědná osoba nereaguje na výzvy VIC FSv,
b) u kterého není známá odpovědná osoba, nebo byl ukončen její vztah k FSv,
c) u kterého byla zjištěna závažná bezpečnostní hrozba, o této situaci je informována odpovědná osoba daného zařízení, spolu s návrhem na řešení,
d) které nesplňuje požadavky plynoucí z tohoto pokynu a nemá udělenu výjimku.

3.11 Výjimky z technických opatření č. 3.1, 3.2, 3.3 a 3.5 jsou možné. Tyto výjimky jsou evidovány v IS VIC FSv a schvalovány pověřenými pracovníky VIC FSv. Smyslem výjimek je zejména umožnit provoz veřejně provozovaných služeb (webové servery atp.), umožnit provoz zařízení, které poskytují unikátní službu nebo z technických důvodů je nelze uvést do souladu s opatřeními, ale jejich užitná hodnota převyšuje riziko plynoucí z jejich používání. Výjimku není možné poskytnout bez přijmutí technických opatření pro snížení tohoto rizika.

Článek 4
Závěrečná ustanovení

4.1 Tímto příkazem se zrušuje Opatření děkana č. 12/2022.

4.2 Opatření na uvedení současného stavu do souladu s tímto příkazem budou realizována neodkladně, nicméně budou probíhat postupně a v gesci VIC FSv.

4.3 Nejpozději v červnu 2024 dojde k vyhodnocení dosavadního stavu zavádění opatření.

4.4 Tento příkaz nabývá účinnosti dnem 4. 12. 2023.

prof. Ing. Jiří Máca, CSc.
děkan fakulty