# Kybernetická bezpečnost s CRA: Komplexní ochrana pro digitální éru

**29.1.2026 - | České Radiokomunikace**

**"Téměř každý den si přečteme, nebo se doslechneme o novém typu kybernetického útoku, nebo dalším napadeném systému veřejné služby. Kybernetické útoky jsou stále sofistikovanější a jejich počet každoročně roste. Ale terčem dnes nejsou pouze velké nadnárodní korporace – ohrožena může být jakákoli organizace fungující v digitálním prostředí. Nedostatečné zabezpečení může vést k závažným škodám, od úniku citlivých dat a finančních ztrát až po poškození reputace. S odborníky z CRA získáte silného partnera, který zajistí, že vaše organizace bude chráněná, odolná a připravená na budoucnost a zároveň vás bezpečně provede požadavky nové legislativy." Martin Pavelka, Product manager – Security & Managed Services**

I pro vás je kybernetická bezpečnost prioritou

V digitální éře čelí firmy nejen technologickým výzvám, ale i legislativním povinnostem. Nový Zákon o kybernetické bezpečnosti (264/2025 Sb.), vycházející ze Směrnice EU NIS2, ukládá organizacím povinnost zajistit plný soulad a posílit svou obranu proti stále sofistikovanějším kybernetickým hrozbám.

V CRA poskytujeme komplexní odbornou pomoc, která pokryje celý cyklus kybernetické bezpečnosti vaší organizace, a zajistíme, že vaše aktivity zůstanou chráněny a dostupné za všech okolností.

## Compliance management: Analýza a poradenství

Pro efektivní řešení a dosažení souladu s novou legislativou je klíčové znát aktuální stav vaší firmy z pohledu kybernetické bezpečnosti. CRA zajistí ucelený balíček služeb Analýza stavu kybernetické bezpečnosti, který vám pomůže definovat cílový stav v souladu s aktuálními legislativními požadavky a standardy. Compliance management od CRA obsahuje:

### Základní analýza stavu kybernetické bezpečnosti

Získáte situační mapu popisující stav informační a kybernetické bezpečnosti vaší organizace – jasný přehled o tom, kde stojíte a kde jsou vaše zranitelné body.

### GAP analýza

Popíšeme současný a cílový stav a navrhneme konkrétní opatření nezbytná pro dosažení požadované úrovně kybernetické bezpečnosti. Diferenční analýza vám ukáže, co je potřeba udělat a v jakém pořadí.

### Analýza rizik

Komplexní zpráva o analýze rizik včetně BIA (Business Impact Analysis) a zmapování míry naplnění požadavků ISO/IEC 27xxx vám pomůže identifikovat kritická aktiva a potenciální dopady kybernetických incidentů.

### Penetrační testování a skenování zranitelností

Identifikujeme známé zranitelnosti a navrhneme konkrétní doporučení, jak je řešit. Služba slouží také k ověření, zda jsou vaši zaměstnanci dostatečně znalí kybernetické bezpečnosti prostřednictvím simulovaných phishingových a smishingových útoků.

### Virtuální CISO

Získáte odborníka ve formě manažera kybernetické bezpečnosti, který zastane chybějící roli ve vaší firmě a pomůže v celé řadě oblastí kybernetické bezpečnosti – od tvorby bezpečnostních politik až po řízení incidentů.

Chci analyzovat stav Kybernetické bezpečnosti

## Managované služby: Ochrana v rukou profesionálů

Managované služby, založené na outsourcingu, představují ideální řešení pro zvýšení kybernetické bezpečnosti, zejména pokud organizace nemá dostatek interních zdrojů nebo know-how. Celá správa je v rukou profesionálů CRA, což vám vašemu IT oddělení soustředit se na vaše vlastní podnikání a přináší úsporu finančních i lidských zdrojů.

### Managed Firewall a SD-WAN: Bezpečné propojení poboček

Komplexní řešení síťové bezpečnosti prostřednictvím virtuálních nebo fyzických zařízení. Profesionální zabezpečení privátní sítě prostřednictvím firewallu, IPS, filtrování webového obsahu, antiviru, antispamu a kontroly aplikací.

### Proč je tato kombinace výhodná?

Zařízení **FortiGate**, která tvoří základ služby Managed Firewall, nativně podporují řadu rozšíření a doplňkových funkcí, včetně SD-WAN. Funkce firewallu (IPS, antivir, VPN) jsou úzce integrovány s funkcionalitou SD-WAN pro inteligentní a dynamické směrování provozu.

SD-WAN propojuje infrastrukturu do jedné bezpečné privátní sítě, zatímco firewall poskytuje pokročilé bezpečnostní funkce. Doplněním o **FortiAnalyzer** získáte centralizovaný přehled, dlouhodobou archivaci a pokročilou analýzu bezpečnostních událostí napříč celou sítí.

Naše řešení umožňují centrální správu, jednotnou orchestraci a koordinaci bezpečnostních politik i přehledný reporting, což zjednodušuje řízení bezpečnosti v jakékoli organizaci – od menších týmů až po rozsáhlé distribuované prostředí.

### DDoS ochrana: Nepřetržitá dostupnost služeb

Distribuované útoky typu Denial of Service (DDoS) patří stále mezi největší hrozby, které vedou k nedostupnosti služeb. To organizacím způsobuje značné finanční ztráty a poškození reputace.

### Jak naše DDoS ochrana funguje?

Služba je postavena na špičkové technologii od společnosti **NetScout** a představuje robustní, nepřetržitou a inteligentně automatizovanou ochranu vaší konektivity.

Technologie nepřetržitě monitoruje provoz (24/7) a identifikuje anomálie. V případě útoku se spouští

automatická nebo manuální mitigace, neboli čištění provozu. Podezřelý provoz je přesměrován přes Scrubbing centrum CRA, kde je škodlivý provoz eliminován, zatímco legitimní provoz je bezpečně doručen k cíli.

**Zásadní výhodou** je nepřetržitý přístup k vašim online službám a aplikacím i během pokusů o DDoS útok, čímž minimalizujeme riziko výpadků, provozních komplikací a souvisejících finančních ztrát.

## Network Access Control (NAC): Váš síťový vrátný a strážce pravidel

Služba **NAC** představuje pokročilý nástroj pro řízení přístupu do sítě organizace, který zajišťuje, že se k citlivým datům a systémům připojují pouze autorizovaná a zabezpečená zařízení a uživatelé. Naše řešení je postaveno na platformě **ClearPass** od společnosti Aruba Networks, která patří mezi nejdůvěryhodnější technologie v síťové bezpečnosti.

## Proč je NAC klíčový?

Zneužití nezabezpečených síťových přístupů je jedním z nejčastějších vektorů útoku. Pokud chybí kontrola, organizace riskuje vniknutí neautorizovaných zařízení, ale i nesoulad s legislativou (ZoKB/NIS2).

**Jak funguje? Na principu 3 kroků:**

1. **Identifikace a ověření:** Každý pokus o připojení (kabel, Wi-Fi, VPN) je automaticky rozpoznán – zařízení, uživatel, typ OS, poloha. Služba vyhodnocuje kontext zařízení, tzn. kdo je uživatel, jaké je zařízení, kde a kdy se připojuje.
2. **Vyhodnocení a rozhodnutí:** Na základě definovaných politik systém dynamicky rozhoduje, zda má být přístup povolen (a s jakou segmentací), nebo zda má být odepřen či omezen (karanténa). Zajišťuje i tzv. Posture Check neboli zdravotní kontrolu zařízení – kontroluje aktivní firewall, antivirový software a aktualizace.
3. **Dynamické řízení a reakce:** Systém v reálném čase uděluje nebo mění přístupová práva, segmentuje síť a dokáže automaticky reagovat na incidenty. To se děje například odpojením zařízení nebo přesunutím do karantény, a to bez nutnosti manuálního zásahu.

**Klíčové výhody:**

- **Segmentace sítě:** Omezení volného pohybu hrozeb v síti, čímž se minimalizují škody při kompromitaci
- **Podpora Compliance:** Pomáhá organizacím splnit regulatorní požadavky (NIS2, GDPR, DORA)
- **BYOD a Guest Access Management:** Automatizuje a zabezpečuje připojení osobních zařízení uživatelů a poskytuje zabezpečený přístup pro hosty
- **Zlepšení bezpečnosti:** Zabraňuje neautorizovanému přístupu a šíření hrozeb, přičemž přístup dostane jen ten, kdo má právo

Kontakt pro více informací o managovaných službách

**Klid na práci a jistota**

Zákon č. 264/2025 Sb. o kybernetické bezpečnosti je nyní účinný, a potřeba aktivní a komplexní ochrany digitální infrastruktury je tak aktuálnější než kdy dříve. Kybernetická bezpečnost přitom nepředstavuje jen nutný náklad, ale strategickou investici do stability, dostupnosti a důvěryhodnosti vašich služeb.

Služby kybernetické bezpečnosti od CRA vám pomohou systematicky řídit rizika, chránit klíčová aktiva a zajistit soulad s novou legislativou – od odborných analýz přes preventivní ochranu až po nepřetržitý dohled a reakci na incidenty.

https://www.cra.cz/tiskove-centrum/bezpecnost/kyberneticka-bezpecnost-s-cra-komplexni-ochrana-pro-digitalni-eru