Datum: 22. dubna 2025

KYBERNETICKÉ OPERAČNÍ CENTRUM

POPIS SLUŽEB A ČINNOSTÍ KOC

Úvod

Kybernetické operační centrum (dále jen KOC) je oddělení zařazené do Odboru kanceláře ředitele Krajského úřadu Jihomoravského kraje. Jeho hlavním úkolem je zabezpečovat činnosti bezpečnostního dohledového centra, a tím minimalizovat rizika spojená s kybernetickými hrozbami, zejména ztrátou, zneužitím nebo odcizením dat. Služby bezpečnostního dohledového centra jsou kromě sítě KrÚ JMK poskytovány také vybraným příspěvkovým organizacím kraje (dále jen PO).

Krajský úřad Jihomoravského kraje je podle zákona č. 181/2014 Sb., zákona o kybernetickébezpečnosti a o změně souvisejících zákonů (dále jen „ZoKB“), povinnou osobou. Z tohoto důvodu je úřad povinen implementovat opatření, která tento zákon a prováděcí vyhláška stanovují. Dle § 5 ZoKB je povinná osoba povinna zavést v něm vyjmenovaná bezpečnostní opatření.

SLA (Service Level Agreement) jednotlivých služeb

Tato část definuje rozsah, úroveň a parametry poskytovaných služeb. Veškeré služby jsou pro připojené PO poskytovány bezplatně. Nicméně na straně PO mohou vzniknout související náklady, ať už personální nebo jiné. Poskytované služby zahrnují licenční poplatky, poplatky za údržbu (maintenance), servis dodaných technologií a dohled zajišťovaný bezpečnostním dohledovým centrem ve specifikovaném rozsahu.

Dostupnost služby

Veškeré technologie jsou v nepřetržitém provozu s výjimkou plánovaných servisních odstávek, na které je zákazník vždy s předstihem upozorněn. Aktivní dohled probíhá v minimálním rozsahu během pracovních dnů, konkrétně v režimu 8x5 (pondělí–pátek, 8:00–16:00). Alerty, které vzniknou mimo pracovní dobu, jsou zaznamenány a vyhodnoceny následně během doby aktivního dohledu.

Poskytované služby

Sběr, zpracování a ukládání logů

Kolektor (server v majetku JMK) – shromažďování logů z prostředí zákazníka z definovaných zdrojů a jejich přeposílání do KOC.

- Logy jsou sbírány a archivovány po dobu 12 měsíců, s možností individuálního nastavení pro každou připojenou PO
- Sjednocení ukládaných logů do strukturované podoby Event Managementu (parsing)
- Vyhledávání
- Analytika
- Auditní stopa – logy jsou ukládány v souladu s VoKB v nezměněné podobě (tzv. RAW)

Security Information and Event Management (SIEM)

- Kontinuální automatizovaná analýza a vyhodnocení logů a alertů, detekce incidentů pomocí analytických nástrojů
- V rámci služby pravidelně vykonávaná analýza logů, dat o síťové komunikaci a ostatních zdrojů dat za účelem odhalení neznámých hrozeb a neznámých bezpečnostních problémů, tzv. Threat Hunting
- Zákaznické korelace – pro účely specifických výstupů lze definovat speciální korelace

Endpoint Detection and Response (EDR)

- Služba zajišťuje vizibilitu (viditelnost) do dějů probíhajících na koncových zařízeních a analýzu získaných dat způsobem průběžného monitoringu nebo Threat Huntingu
- Tato služba umožňuje automatizovanou reakci na detekované incidenty, například odpojení podezřelé stanice. Přesná specifikace oprávnění k izolaci stanice musí být přesně definována samostatnou dohodou.
- Součástí služby je instalace virtuálního serveru pro management EDR na server KOC
- Podmínkou pro využívání je vlastní antivirové řešení od společnosti ESET

Provozní monitoring

- Tato služba umožňuje sledovat technologie z pohledu dostupnosti. Provozní monitoring komponent dohledového centra lze rozšířit o monitoring klíčových technologií zákazníka

Ticketing

- Komunikace (hlášení událostí, incidentů, požadavků na změnu apod.) je vedena přes zabezpečený kanál ticketovacího systému. Je zajištěna auditní stopa včetně časového řetězce událostí

Centrální Dashboard a Reporting

- CyberCopter – grafy, tabulky, dashboard s možností individuálního přizpůsobení pro zákazníka jako přehled nad službou
- Pravidelný reporting o využívání služby, nálezech a KPI parametrech s periodou 1xměsíčně

NETBOX dokumentace a IPAM

NetBox je softwarové řešení pro modelování a dokumentaci moderních sítí, které efektivně umožňuje správu IP adres (IPAM). Jedná se o otevřenou webovou aplikaci pro správu síťové infrastruktury. Dokumentace sítí připojených PO je vedena v tomto systému. Přístup ke správě je umožněn IT pracovníkům připojených PO.

Vulnerability Management, hardening

- Opakované testy zranitelností
- Součástí služby je vyžívání a úprava existujících detekčních metod a pravidel na základě volně dostupných nebo placených zdrojů informací o hrozbách, tzv. Threat Intelligence na technické úrovni (zpracování indikátorů kompromitace, tzv. IoC – Indicators of Compromise