## Metodika pre spoločné postupy a podporu (hotline) za účelom zabezpečenia prevencie a pripravenosti proti narušeniu informačných aktív kritickej infraštruktúry.

1. **Úvod**

Častý výskyt počítačových bezpečnostných incidentov, ako aj neschopnosť zabezpečiť efektívnu ochranu voči nim významne narúša dôveru verejnosti voči štátu, a to najmä v súvislosti s poskytovaním jeho elektronických služieb verejnosti. Na ucelené riešenie tejto problematiky v Slovenskej republike (ďalej len „SR“) sú zamerané aj úlohy Akčného plánu ku Koncepcii kybernetickej bezpečnosti SR na roky 2015 – 2020 (ďalej len „Akčný plán“) schváleného uznesením vlády SR č. 93/2016 v marci tohto roku. Úlohy Akčného plánu sú prioritne zamerané na oblasti vytvárania bezpečného prostredia, vytvárania povedomia a kompetentnosti a na rozširovanie národnej a medzinárodnej spolupráce a kompetentnosti SR.

1. **Cieľ plnenia úlohy**

Cieľom plnenia úlohy „Metodika pre spoločné postupy a podporu (hotline) za účelom zabezpečenia prevencie a pripravenosti proti narušeniu informačných aktív kritickej infraštruktúry“ je identifikovať požiadavky na efektívne riešenia incidentov na úrovni organizácie, rezortu/sektora a navrhnúť  spoločné postupy na národnej úrovni za účelom zabezpečenia prevencie a pripravenosti proti narušeniu informačných aktív (primárnych a sekundárnych) definovaných podľa metriky, ktorá bude obsiahnutá v pripravovanom návrhu zákona o kybernetickej bezpečnosti.

Súčasťou úlohy je vytvorenie centrálneho registra s relevantnými informáciami pre potreby riešenia významných bezpečnostných incidentov v rozsahu kritickej informačnej infraštruktúry v SR, vrátane verejnej správy.

1. **Postupnosť realizácie úlohy**

Postupnosť realizácie bola navrhnutá do troch etáp, a to:

1. vytvorenie registra relevantných subjektov, aktualizácia evidencie údajov CSIRT.SK, resp. aj iných relevantných organizácií pre tento register,
2. pilotná prevádzka systému, vrátane zabezpečovanie procesu priebežnej aktualizácie údajov.
3. Vyhodnotenie pilotnej prevádzky a v spolupráci so súčinnostnými subjektami a vypracovanie návrhu *Metodiky pre spoločné postupy a podporu (hotline) za účelom zabezpečenia prevencie a pripravenosti proti narušeniu informačných aktív kritickej infraštruktúry“*
4. **Realizácia**

Riešenie úlohy je realizované rozpočtovou organizáciou DataCentum/CSIRT.SK v pôsobnosti MF SR. V rámci plnenia úlohy bola vypracovaná pracovná verzia dokumentu, ktorý rámcovo popisuje potrebné činnosti na zabezpečenie pripravenosti a prevencie bezpečnostných incidentov, ako aj nutné požiadavky na národné jednotné kontaktné miesta typu CSIRT/CERT, ktoré majú byť zodpovedné za implementáciu procesov prevencie bezpečnostných incidentov, ako aj riešenie rozsiahlych bezpečnostných incidentov a koordináciu riešenie incidentov na nadrezortnej/nadsektorovej úrovni.

Vzhľadom na interkonektivitu IS v kybernetickom priestore ako aj rozsahu a typu hrozieb identifikovaných pri zabezpečení organizácií a riešení bezpečnostných incidentov sme došli k záveru, že je potrebné metodicky riešiť nielen informačné aktíva definované v zákone o kybernetickej bezpečnosti ale aj ostatné informačné aktíva. Z tohto dôvodu navrhovaná metodika rieši spoločné postupy a podporu za účelom zabezpečenia prevencie a pripravenosti systematicky. Navrhovaná ***Metodika prevencie a pripravenosti organizácie pre systematické zabezpečenie informačnej bezpečnosti*** sa skladá s nasledujúcich častí :

* 1. Spoločné postupy. V rámci spoločných postupov boli identifikované a navrhnuté postupy v závislosti od požiadaviek na úroveň zabezpečenia na úrovni organizácie , rezortu /sektora a národnej úrovni za účelom prípravy na riešenie bezpečnostných incidentov a prípravy spôsobilostí za účelom zvýšenia obranyschopnosti voči kybernetickým útokom.
  2. Bezpečnostné tímy. V tejto časti metodika popisuje úlohy bezpečnostných tímov v organizáciách, požiadavky na materiálne, technické a personálne zabezpečenie v závislosti na úrovni požiadaviek na úroveň zabezpečenia. V tejto časti metodika popisuje pre ktoré organizácie je potrebné prevádzkovať bezpečnostný tím.
  3. Tímy CSIRT. V tejto časti metodika popisuje úlohy tímov CSIRT v organizáciách, požiadavky na materiálne, technické a personálne zabezpečenie v závislosti na úrovni požiadaviek na úroveň zabezpečenia. V tejto časti metodika popisuje pre ktoré organizácie je potrebné prevádzkovať tím typu CSIRT.
  4. Bezpečnostné opatrenia. V tejto časti metodika popisuje navrhované bezpečnostné opatrenia, ktoré je potrebné implementovať na systematické zabezpečenie informačnej bezpečnosti v rámci organizácie. Opatrenia boli zvolené na základe výsledkov penetračných testov a analýzy kybernetických útokov na Slovensku aj v zahraničí.
  5. Posúdenie bezpečnosti. V tejto časti metodika popisuje navrhované spôsoby a rozsahy posudzovania úrovne informačnej bezpečnosti v organizácií resp. na úrovni rezortu/ sektora a národnej úrovni.

V rámci návrhu metodiky boli identifikované oblasti, ktoré je potrebné zabezpečiť na úrovni:

1. Organizácie
2. Sektora / Rezortu
3. Národnej úrovni

V rámci návrhu metodiky boli identifikované oblasti, ktoré je potrebné zabezpečiť na úrovni organizácie :

1. Organizačne, materiálne a personálne zabezpečenie riešenia informačnej bezpečnosti v organizácií vrátane zabezpečenia spôsobilostí riešenia bezpečnostných incidentov v rámci organizácie.
2. Implementáciu štruktúry riadenia informačnej bezpečnosti na rezortnej, sektorovej a národnej úrovni
3. Implementáciu systému riadenia informačnej bezpečnosti v organizácií (vrátane analýzy bezpečnostných rizík) a implementáciu bezpečnostných opatrení za účelom vytvorenia bezpečnostného baseline v organizácií.
4. Pravidelné vykonávanie kontrolných činností (auditov bezpečnosti vrátane penetračných testov)

Vzhľadom na štruktúru Internetu, typy a rozsahy hrozieb a potrebné odborné spôsobilosti na ich zvládanie je potom na národnej / vládnej úrovni ďalej potrebné zabezpečiť:

1. Vytvorenie spôsobilostí poslednej inštancie na národnej a vládnej úrovni
2. Vytvorenie spôsobilostí na analytické a proaktívne činnosti
3. Vydávanie štandardov v oblasti informačnej bezpečnosti
4. Vydávanie postupov na bezpečnú konfiguráciu jednotlivých technológií (tzv. hardening guidov)
5. Školenia zamestnancov – špecialistov v oblasti informačnej bezpečnosti

Navrhovaná metodika ďalej do väčšej úrovne detailu rozoberá :

1. Predpoklady pre riešenie bezpečnostných incidentov
2. Riešenie bezpečnostných incidentov na úrovni organizácie / rezortu /sektora a národnej úrovni
3. Tvorba bezpečnostných a CSIRT tímov
4. Požiadavky na zabezpečenie infraštruktúry organizácie.
5. Základná úroveň overovania úrovne informačnej bezpečnosti v organizáciách

Navrhnuté procesy sú v súčasnosti čiastočne skúšobne implementované na operatívnej úrovni v organizácii DataCentrum/CSIRT.SK zriadenej MF SR a v nasledujúcom období budú tieto procesy zovšeobecnené formou návrhu metodiky a prediskutované odbornou komunitou relevantných a súčinnostných subjektov.