ZKRATKY A POJMY

V této instrukci jsou použity následující zkratky a pojmy:

Aktivum - obecně cokoliv, co má pro organizaci nebo i jednotlivce hodnotu, v případě této politiky a návazných předpisů pojem označuje informační aktiva resp. aktiva s nimi související, která se dělí na primární aktiva a podpůrná aktiva.

Bezpečnostní incident - jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, které mohou s vysokou pravděpodobností kompromitovat činnost organizace nebo ohrožovat bezpečnost informací.

Bezpečnostní událost - identifikovaný stav systému, služby nebo sítě, který signalizuje možné porušení bezpečnostní politiky nebo selhání bezpečnostních opatření, popř. jinou předtím nepoznanou situaci, která může být významná z pohledu bezpečnosti informací.

Bod obnovy dat (Recovery Point Objective - RPO) - místo v čase, ke kterému musí být obnovena data po selhání.

Centrálním úložištěm bezpečnostních logů je myšlen centrální systém shromažďující a případně dále zpracovávající záznamy potenciálně související s kybernetickými bezpečnostními událostmi. Počet těchto systémů v prostředí resortu justice není v této politice určen.

Doba obnovy chodu (Recovery Time Objective - RTO) - časové období, během kterého musí být po havárii obnovena minimální úroveň funkčnosti systému.

Dostupnost informací (aktiva) - informace musí být dostupné oprávněným osobám tehdy, když je potřebují.

Důvěrnosti informací (aktiva) - informace mají být dostupné jen tomu, kdo je k tomu oprávněn a potřebuje je znát ke své práci.

Externí síť - komunikační síť, která není pod správou resortu spravedlnosti nebo justiční složky.

Garant aktiva (GA) - fyzická osoba pověřená justiční složkou k zajištění rozvoje, použití a bezpečnosti aktiva.

Havarijní plán (Disaster Recovery Plan - DRP) - Plán pro záložní postupy, odezvu na nepředvídanou událost a obnovu po havárii.

Hrozba - potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození informačního systému nebo organizace.

Informační a komunikační technologie (ICT) - veškeré informační technologie používané pro komunikaci a práci s informacemi.

Informační technologie - každý elektronický přístroj schopný zpracovávat nějaké informace (neboli provádět algoritmus), tedy přijmout nějaká vstupní data, samostatně s nimi provést nějaké operace a vydat příslušná data výstupní (popřípadě část této technologie).

Informační systém (IS) - celek složený z počítačového hardwaru a souvisejícího softwaru spolu s lidmi a procesy, a navržený ke sběru, zpracování a šíření informací potřebných k plánování, rozhodování a řízení.

Informační systém kritické informační infrastruktury (KII) - informační systém, který je prvkem nebo systémem prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti (termín definovaný zákonem č. 181/2014 Sb. o kybernetické bezpečnosti).

Integrita informací (aktiva) - informace mohou být měněny pouze oprávněnými osobami nebo na pokyn oprávněných osob a řízeným způsobem.

Interní síť - komunikační síť, která je pod správou resortu spravedlnosti nebo justiční složky.

MKB - Manažer kybernetické bezpečnosti.

Opatření (Bezpečnostní opatření) - ochranná opatření pro zajištění bezpečnostních požadavků kladených na systém. Mohou mít různý charakter.

Plán kontinuity činnosti (Business Continuity Plan - BCP) - Dokumentovaný soubor postupů a informací, který je vytvořen a udržován v pohotovosti pro užití při incidentu za účelem umožnění organizaci uskutečňovat své kritické činnosti na přijatelné, předem stanovené úrovni.

Podpůrné aktivum - technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému.

Politika systému řízení bezpečnosti informací (nebo také „politika systému řízení“) - Jedná se o systém řízení popsaný v druhé části této instrukce.

Pracovník - uživatel nebo správce.

Primární aktivum - informace nebo služba, kterou zpracovává nebo poskytuje informační systém.

Privilegovaná oprávnění - oprávnění překračující svým rozsahem oprávnění standardních uživatelů.

Riziko - možnost, že určitá hrozba využije zranitelnosti informačního systému a způsobí poškození aktiva.

SLA (Service Level Agreement) - dohoda o úrovni poskytovaných služeb - dohoda mezi poskytovatelem služby a jejím konzumentem definující rozsah, úroveň a intenzitu poskytovaných služeb.

Soukromý klíč - jeden z páru klíčů používaných v asymetrické kryptografii, který musí být chráněný a používaný pouze jednou osobou.

Správce - fyzická osoba pověřená Garantem aktiva zajišťující správu, provoz, použití, údržbu a bezpečnost technického aktiva (administrátor); ve většině případů označuje zaměstnance justičních složek nebo pracovníka smluvního partnera, který má přístup k informačním službám, informacím nebo jiným aktivům justičních složek, přičemž má přidělený rozsah oprávnění překračující svým rozsahem oprávnění uživatelů. V předpisu Vnitřní kancelářský řád pro okresní, krajské a vrchní soudy je správce označován pojmem informatik.

Standardní informační systém (SIS) - informační systém, který není určen prvkem kritické informační infrastruktury (KII) nebo významným informačním systémem (VIS).

Tajný klíč - klíč symetrické kryptografie používaný pro šifrování i dešifrování.

Technické aktivum - technické vybavení, komunikační prostředky a programové vybavení informačního systému a objekty, ve kterých je tento systém umístěn.

Uživatel - fyzická nebo právnická osoba anebo orgán veřejné moci, který využívá primární aktiva; ve většině případů zahrnuje zaměstnance justičních složek nebo pracovníka smluvního partnera, který má přístup k informačním službám, informacím nebo jiným aktivům justičních složek, přičemž má přidělený běžný rozsah oprávnění přístupu.

Vedení resortu - tímto pojmem se rozumí ministr nebo ministryně.

Vedoucí justiční složky - vedoucí dané organizační složky resortu justice.

Veřejný klíč - jeden z páru klíčů používaných v asymetrické kryptografii určený ke zveřejnění (většinou obsažen v certifikátu uživatele nebo serveru).

Významný informační systém (VIS) - informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci (termín definovaný zákonem č. 181/2014 Sb. o kybernetické bezpečnosti).

Zástupce vedení resortu - osoba zastupující vedení resortu pro oblast bezpečnosti informací.

Zranitelnost - slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.