Metodický pokyn
pre kategorizáciu citlivosti údajov z dôvodu bezpečnosti
(verzia 1.0)

Tento dokument bol vypracovaný na základe potreby rozlíšiť, ktoré údaje o informačno-komunikačných technológiách (ďalej len „IKT“) resp. informačných systémoch je vhodné pokladať za citlivé z dôvodu možnosti narušenia bezpečnosti. V praxi sa často krát vyskytujú diametrálne odlišné hodnotenia, niektoré organizácie idú až do extrémnych prípadov.

Cieľom dokumentu je preto poskytnúť najmä pomoc pri vytváraní vnútorných klasifikácií údajov, ako aj postupov pre poskytovanie informácií v zmysle zákona č. 211/2000 Z. z. o slobodnom prístupe k informáciám a o zmene a doplnení niektorých zákonov (zákon o slobode informácií) v znení neskorších predpisov (ďalej len „zákon č. 211/2000 Z. z.“). Dokument poskytuje metodické usmernenie najmä pre znenie § 21c, písm. h) tohto zákona.

Metodický pokyn nadväzuje na bezpečnostné štandardy, určené výnosom MF SR č. 312/2010 Z. z. o štandardoch pre informačné systémy verejnej správy (ďalej len „výnos“), kde je definovaná „bezpečnostná politika“, ako aj na požiadavky zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení neskorších predpisov (ďalej len „zákon č. 428/2002 Z. z.“), kde je zavedený pojem „bezpečnostný projekt“. Uvedené bezpečnostné dokumentácie sa výrazne prelínajú, pričom bezpečnostný projekt má zúžený záber iba na ochranu osobných údajov. Metodický pokyn sa v určitom rozsahu týka aj zákona č. 45/2011 Z. z. o kritickej infraštruktúre, kde sú rámcovo definované citlivé informácie o kritickej infraštruktúre, kde sú jedným zo sektorov aj informačné a komunikačné technológie.

Metodický pokyn vznikol spoločnou prácou pracovnej skupiny pri Komisii pre štandardizáciu informačných systémov verejnej správy, s aktívnym zapojením štátnych orgánov ako Ministerstvo spravodlivosti SR, Úrad na ochranu osobných údajov SR a Ministerstvo hospodárstva SR, ale aj odborných organizácií ako Spoločnosť pre otvorené informačné technológie a IT asociácia Slovenska.

Ambíciou usmernenia nie je zaoberať sa legislatívou upravovanými procesnými postupmi zverejňovania informácií, ale klasifikovať údaje na „zverejniteľné“ a „nezverejniteľné“. Využívanie príslušnej legislatívy z dôvodu transparentnosti a verejnej kontroly by však nemalo znižovať ochranu majetku štátu a informácií a aktív, zverených občanmi jednotlivým organizáciám verejnej správy.

V prípade vecných otázok alebo pripomienok k zneniu metodického pokynu je možné obrátiť sa Ministerstvo financií SR buď prostredníctvom webového sídla www.informatizacia.sk alebo na kontaktnú adresu [redacted].

OBSAH

1. Základná kategorizácia

Základná kategorizácia citlivých údajov o IKT rozlišuje dve úrovne:

- **zverejniteľné údaje (Z)** – údaje, ktorých zverejnenie neohrozuje IKT, a preto ich je možné kedykoľvek zverejniť.
- **nezverejniteľné údaje (NZ)** – údaje, ktoré nie je vhodné zverejniť v žiadnom prípade, pretože zverejnenie nesie riziko okamžitého alebo neskoršieho pokusu o narušenie informačnej bezpečnosti. Pre nezverejniteľné údaje môže existovať podmienka, za splnenia ktorej sa stanú zverejniteľnými.

Zverejniteľnosťou sa rozumie aj sprístupňovanie či iný terminologický ekvivalent získania danej informácie, rozdiel je iba v legislatívno-právnej potrebnosti explicitného vyžiadania.

Navrhovaná kategorizácia samozrejme môže byť vo vnútornom prostredí organizácie ďalej rozšírená napr. podľa bezpečnostnej politiky organizácie (napr. na chránené, služobné).

V súvislosti so zverejňovaním pripomíname aj základné zásady:

- na základe práva na informácie zakotveného v čl. 26 Ústavy SR je základným právom umožnenie prístupu občanov k informáciám (údajom), pričom orgány verejnej moci majú poskytovať informácie o svojej činnosti primeraným spôsobom podľa podmienok a postupov ustanovených v zákone,
- čl. 19 Ústavy SR ďalej zakladá právo na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života a ochranu pred neoprávneným zhromažďovaním, zverejňovaním alebo iným zneužívaním údajov o svojej osobe, kam patrí väčšina údajov spravovaná štátom, naplnenie tohto článku má byť zohľadňované zákonmi,
- podmienky a postupy zverejňovania a sprístupňovania sú stanovené najmä zákonom č. 211/2000 Z. z., kde je zároveň určené, že „ak časť požadovaných údajov nie je možné sprístupniť (napr. časť dokumentu, niektoré súbory, niektoré typy údajov z tabuľky, osobné údaje), sprístupnia sa ostatné údaje po ich odstránení (vymazaní, vylúčení a pod.)“ (tzv. anonymizácia),
- sprístupňovanie sa v zmysle zákona týka už existujúcich informácií, nové nie je preto povinnosť vypracovávať nové informácie (napr. analytické materiály, názory, stanoviská atď.) =odkaz na zákon,

- ohrozenie nosiča informácie t.j. miesta, kde je informácia vo forme údaja uložená, je zároveň ohrozením samotnej informácie.

2. Osobné údaje vo vzťahu k IKT

Ochrana osobných údajov je problematikou, ktorá úzko súvisí a ktorou je potrebné sa zaoberať aj v rámci bezpečnosti informačných systémov. Zákon č. 428/2002 Z. z. neupravuje konkrétny zoznam údajov, ktoré sú považované za osobné údaje; v súlade s ustanovením § 3 poskytuje demonštratívny výpočet charakteristík určujúcich fyzickú osobu. V zmysle tohto ustanovenia je potrebné individuálne a v každom prípade jednotlivo taktiež rozlišovať, či rôzne údaje o IKT, majú zároveň aj charakter osobného údaju v zmysle uvedeného § 3 zákona č. 428/2002 Z. z. Rovnako je dôležité aj to, že po priradení určitej informácie k osobnému údaju, ktorá sama o sebe nemá charakter osobného údaju, sa takáto informácia môže stať tiež osobným údajom, ak vedie k lepšej identifikácii konkrétnej fyzickej osoby, napr. údaje o používanom softvéri sa priradia ku konkrétnemu zamestnancovi orgánu verejnej správy identifikovanému menom, priezviskom a zamestnaneckou príslušnosťou k danému orgánu ako svojmu zamestnávateľovi.

Osobné údaje a zároveň údaje o IKT sú, resp. môžu byť napr.: prihlasovacie meno užívateľa informačného systému, logy (prihlasovanie / odhlasovanie užívateľa), rôzne súbory na pamäťových médiách, vlastné údaje databáz a registrov (t.j. používateľské údaje), nastavenie prístupových práv používateľov informačných systémov, ako aj ďalšie IKT, ktoré môžu mať určitú vypovedaciu schopnosť vedúcu k identifikácii konkrétnej fyzickej osoby.V prílohe č. 1 je uvedený krátky príklad takéhoto posúdenia.

Bezpečnosť spracúvaných osobných údajov v informačných systémoch je jednou z kľúčových podmienok garantovania ústavného práva pred neoprávneným zhromažďovaním, zverejňovaním alebo iným neoprávneným nakladaním údajov o fyzickej osobe - jednotlivcovi. Každý subjekt, ktorý má v zmysle zákona č. 428/2002 Z. z. postavenie prevádzkovateľa alebo sprostredkovateľa spracúvajúceho osobné údaje, je preto pri spracúvaní osobných údajov v informačnom systéme povinný vytvoriť také podmienky jeho fungovania, ktoré zaručia ochranu osobných údajov pred ich náhodným ako aj nezákonným poškodením a zničením, náhodnou stratou, zmenou, nedovoleným prístupom a sprístupnením ako aj pred akýmikoľvek inými neprípustnými formami spracúvania. Za týmto účelom je povinný prijať primerané technické, organizačné a personálne opatrenia (najmä vo forme bezpečnostného projektu a prijatých bezpečnostných opatrení).

Daný subjekt by nemal pri sprístupňovaní údajov v súvislosti s IKT sprístupňovať rozsah a spôsob technických, organizačných a personálnych opatrení potrebných na eliminovanie a minimalizovanie hrozieb a rizík pôsobiacich na informačný systém, v ktorom sa spracúvajú osobné údaje, keďže ich sprístupnením sa môže vytvoriť bezpečnostné riziko, ktoré ohrozí ochranu osobných údajov garantovanej samotnou Ústavou SR.

Táto metodika sa zaoberá určením citlivosti z pohľadu informačnej bezpečnosti, ktorá zahŕňa celkovú ochranu údajov ako takých (s výnimkou utajovaných údajov), pričom osobné

údaje tvoria podmnožinu týchto údajov s osobitne upravovanými pravidlami ochrany. Osobné údaje je preto potrebné vnímať z hľadiska špecifickej komplexnej bezpečnosti, ktorá je predmetom právnej úpravy osobitného zákona.

3. Ostatné typy údajov vo vzťahu k IKT

Obdobne ako pri osobných údajoch, klasifikácia citlivosti v tejto metodike sa nenavrhuje z pohľadu autorského práva, obchodného či bankového tajomstva a podobne, ale iba z pohľadu bezpečnosti, aj keď uvedené faktory môžu zverejnenie významne ovplyvniť. Súčasťou nie sú ani utajované skutočnosti.

4. Údaje o IKT

4.1 Podmienka zverejniteľnosti

Podmienky pre zverejniteľnosť údajov môžu byť rôzne a po odbornom zvážení by o nich mala rozhodovať príslušná organizácia. V prípade, že má organizácia zavedenú adekvátnu a funkčnú organizáciu bezpečnosti (vyplývajúcu z bezpečnostnej politiky), o posudzovaní zverejniteľnosti by mala rozhodovať niektorá z bezpečnostných rolí celého systému (napr. bezpečnostný manažér alebo metodik bezpečnosti). Podmienky zverejniteľnosti môžu byť najmä nasledovné:

- uplynul určitý čas (uvedené kritérium je potrebné používať s rozvahou, nakoľko nemusí znamenať, že riziko ohrozenia pominulo),
- údaj už nie je relevantný a existujúce („živé“) IKT neohrozí,
- údaj sa týka nefunkčných („neživých“) alebo nepoužívaných IKT,
- atď.

Konkrétna podmienka je v ďalšej kapitole vždy uvedená pri relevantnom type údaja.

V metodike sa používa pojem „neaktuálny“, čím sa rozumie údaj, ktorý už nie je vo vzťahu ku konkrétnemu IKT platný (relevantný) a zároveň významne neohrozuje ani iné IKT (napr. tým, že sa používa v obdobnom znení alebo zahŕňa nezverejniteľné údaje o iných IKT)

Ambíciou metodického pokynu nie je nahrádzať tento rozhodovací proces, MF SR však môže v prípade pochybností v konkrétnom prípade poskytnúť poradenstvo. Kontaktná adresa na tento účel je [redacted].

4.2 Zoznam typov údajov o IKT

V tejto kapitole sa nachádza zoznam typov údajov, pričom indikácia zverejniteľnosti je uvádzaná pri každom type údaju osobitne.

Organizácia môže v konkrétnej situácii rozhodnúť aj o sprístupnení údajov z kategórie nezverejniteľné, avšak až po osobitnom preskúmaní, či bezpečnosť IKT nebude skutočne narušená alebo významne ohrozená. V prípade nejasností môže gestor informačnej bezpečnosti, ktorým je Ministerstvo financií SR, poskytnúť pomocné stanovisko.

a) heslá a ich ekvivalenty (napr. privátne (súkromné) kľúče atď.) – NZ – sú to vysoko citlivé údaje, zneužitie, ktorých môže mať za následok značné škody, a to aj v už neplatnom (neaktuálnom) stave

b) bežná dokumentácia o IKT

   - používateľská dokumentácia[1)] (návod na používanie informačného systému používateľmi, aplikácie, softvéru) – Z,
   - administrátorská dokumentácia[2)] (návod na správu a prevádzku informačného systému, aplikácie, softvéru) – Z,

c) bezpečnostná dokumentácia

   - všeobecný obsah bezpečnostnej politiky[3)],
     - bezpečnostné ciele – Z, spôsoby vyhodnocovania bezpečnostných cieľov – Z,
     - úlohy vedenia organizácie v oblasti informačnej bezpečnosti – Z,
     - pozície (role) organizácie pre manažment informačnej bezpečnosti, kompetencie a úlohy jednotlivých pozícií – Z,
     - povinnosť na zaistenie nenarušenia informačnej bezpečnosti (vyhlásenie resp. záväzok organizácie) – Z,
     - zhodnotenie súladu bezpečnostnej politiky s platnými všeobecne záväznými právnymi predpismi, vnútornými predpismi organizácie a zmluvnými záväzkami a určenie príslušných požiadaviek na informačné systémy (príslušnými požiadavkami sa rozumejú metódy, nie konkrétne pravidlá pre konkrétne systémy) – Z,
     - spôsob vedenia a aktualizácie dokumentácie o IKT, zoznam dokumentov na zaistenie informačnej bezpečnosti – Z,
     - rozsah a úrovne ochrany (štandardizovaná klasifikácia požiadaviek na ochranu, metodika) – Z,
     - periodicita monitorovania bezpečnosti (najmä z pohľadu činnosti administrátorov, manažérov bezpečnosti) – Z,
     - periodicita a postup pri revízii bezpečnostnej politiky, dôvody mimoriadnych revízií – Z,
   - bezpečnostný audit

[1)] § 41 písm. e) prvý bod výnosu č. 312/2010 Z. Z. o štandardoch pre informačné systémy verejnej správy
[2)] § 41 písm. e) prvý bod výnosu č. 312/2010 Z. Z. o štandardoch pre informačné systémy verejnej správy
[3)] § 28 písm. a) výnosu č. 312/2010 Z. Z. o štandardoch pre informačné systémy verejnej správy

- pravidlá používania IKT na súkromné účely (v rozsahu či je to možné alebo nie, prípadne ďalšie základné informácie typu ktorým zamestnancom je to umožnené, neobsahuje však konkrétne ochranné postupy a opatrenia) – Z,
- pravidlá pre prenos IKT a údajov mimo priestory organizácie – NZ, zverejnenie by bolo priamym návodom na obídenie ochranných opatrení,
- pravidlá vyraďovania IKT – Z,
- pravidlá a metódy trvalého vymazávania údajov – NZ, znalosť tejto informácie je priamym návodom na uskutočnenie obnovy a získanie nezverejniteľných informácií (napr. z vyradených IKT),

o politika pre správu rizík (obvykle súčasťou bezpečnostnej politiky)

- používaná metodika – Z,
- organizačné postupy – v rámcovom rozsahu, ktorá pozícia navrhuje riziká a ktorá ich schvaľuje Z, v podrobnom rozsahu ako určenie, ktorá osoba má konať a za akých podmienok NZ, znalosť tejto informácie môže poskytnúť účinný spôsob vyhnutia sa ochranným postupom,
- analýza rizík pre jednotlivé aktíva – NZ pokiaľ je aktuálna (t.j. príslušné riziká stále existujú), v prípade neaktuálnosti (pre akékoľvek IKT) Z,
- určenie ochrany aktív na základe analýzy rizík – NZ, znalosť ochranných postupov významne uľahčuje vyhnutie sa im,

o politika prístupu

- definície všeobecných (štandardizovaných) pozícií (rolí) a príslušných oprávnení – Z,
- pravidlá pre možnosti vzdialeného prístupu t.j. prístupu z externých priestorov – postupy pridelenia vzdialeného prístupu – Z, prístupové heslá, technické a ostatné bezpečnostné opatrenia – NZ,
- pravidlá pre správu a pripájanie mobilných zariadení (notebooky, mobilné telefóny, USB a podobne) – Z,
- politika vytvárania hesiel – NZ, zverejniteľné sú všeobecné odporúčania ako správne vytvárať heslá, avšak znalosť konkrétnych požiadaviek na základe technických podmienok konkrétneho systému výrazne uľahčuje možný útok,

o politika zálohovania (obvykle súčasťou bezpečnostnej politiky)

- klasifikácia (typy) záloh, všeobecné frekvencie zálohovania (v rozsahu všeobecnej metodiky zálohovania bez konkrétnych nastavení) – Z,
- miesta ukladania záloh – NZ, znalosť výrazne zvyšuje možnosť krádeže alebo vyradenia obnovy,

skripty, pluginy a aplikácie, pravidlá pre sťahovanie súborov z internetu, antispamové pravidlá, periodicita zamknutia obrazovky, zaheslovanie prístupu do BIOSu, zobrazovanie prípon súborov, povolenie bootovania z médií, no LM hash) - NZ,

- šifrovacie / kryptologické mechanizmy (používané typy, konkrétne nastavenia) – NZ,
- zdôvodnenie potreby nákupu softvéru a aplikácií – Z,
- zoznamy (počty a názvy) reálne využívaného a nevyužívaného softvéru a aplikácií – Z,

f) údaje o používateľoch konkrétnych informačných systémov, aplikácií, softvéru a hardvéru

- počet používateľov – Z,
- typy pozícií (rolí) alebo okruhov (skupín) používateľov – Z,
- údaje o riadení prístupu, napr. podmienky pre vytvorenie účtu, schvaľovacie postupy, mechanizmy prideľovania oprávnení (obvykle obsahom bezpečnostnej politiky) – Z,
- výpisy prihlasovacích mien, zoznamy používateľských a administrátorských účtov) – NZ, znalosť nastavení významne zvyšuje možnosť cielenia útoku,
- mená používateľov a ich priradenie ku konkrétnemu hardvéru alebo softvéru a aplikáciám (napr. „čo má nainštalované zamestnanec X?“) – NZ, významne uľahčuje útoky cez sociálne inžinierstvo,
- mená používateľov a ich priradenie do rolí alebo výpis konkrétnych oprávnení čítania, zápisu, spúšťania atď. – Z len za podmienky splnenia požiadaviek na ochranu osobných údajov, inak NZ,

g) údaje o servisných službách (typu Service Licence Agreement) – (iba v zdokumentovanom rozsahu, nevytvárajú sa informácie navyše) – Z alebo NZ v súlade s pravidlami pre zverejňovanie zmlúv podľa zákona 211/2000 Z. z.,

h) údaje špecifikované nepriamo alebo pomocou adresácie ich nosiča – pamäťového média (napr. pevných diskov, C[redacted], D[redacted], USB)

- v adresnom tvare (zadané menom alebo rozsahom, napr. „zašlite súbor bezpecnostna_politika.pdf“) – Z v rozsahu súborov a informácií, ktoré sú podľa tejto metodiky zverejniteľné a neporušujú ani iné požiadavky zverejniteľnosti (napr. obchodné tajomstvo, ochranu osobných údajov), inak NZ,
- v neadresnom tvare, ktorého výstupom sú súbory (napr. „zašlite celý obsah priečinka XY z disku vášho zamestnanca YX“ alebo „zašlite obsah diskety X“) – Z v rozsahu súborov a informácií, ktoré sú podľa tejto metodiky zverejniteľné a neporušujú ani iné požiadavky zverejniteľnosti (napr. obchodné tajomstvo, ochranu osobných údajov), inak NZ,