Resilience správy dokumentů ve světle proměny bezpečnostních hrozeb

Mgr. Zbyšek Stodůlka

Konference ISSS 2022, Hradec Králové

Správa dokumentů – proměny hrozeb

iDNES.cz / ZPRAVODAJSTVÍ Domácí Zahraničí Krimi Kraje Ekonomika Kultura Finance

V karv… dokum…

27. července 2…

Zaměstnanc… chybí dvě de… snaze vypáti… Úřad pro och…

V karvinských láz… pacientů. Za poch…

Aktuálně.cz MENU UKRAJINA ZPRÁVY NÁZORY SPORT VIDEO LIFESTYLE AKTUÁLNĚ+

Jedna z třiceti. Policie odkládá žaloby NKÚ, úřad…

Marek P… 28. 6. 20…

Jen mizivou… Nejvyšší ko… třicet, ale p… člověka. Bo… říká v rozho… Miloslav Ka…

DOMOV

Kde se nacházíte: iROZH…

Hackeři se … zahraničí, …

Počítače minis… středu Deník N… doby krátce př… úřadu, ale citli… vyšetřování je … na elektronick… nich podle Bezp… rozvědky.

Praha 19.25 31. č…

iROZHLAS

Česká justice

V případu brněnské… spisu, musí se najít č…

DALŠÍ ČLÁNKY AUTORA

iDNES.cz / ZPRAVODAJSTVÍ Domácí Zahraničí Krimi Kraje Ekonomika Kultura Finance Revue

Hackeři na počítačích magistrátu zašifrovali data a žádali dva miliony

13. dubna 2021 16:45

Policie po necelém týdnu zveřejnila první bližší informace o způsobu provedení a okolnostech masivního útoku hackerů, který ochromil olomoucký magistrát. Jak se ukázalo, doposud neznámým útočníkům šlo o peníze.

Ilustrační foto | foto: AP

Případu se věnují krajští kriminalisté odboru analytiky a kybernetické kriminality, kteří zatím vše vedou jako trestný čin neoprávněného přístupu

Reklamu zavřela společnost Google

Správa dokumentů

Principy FAIR:

F – findable (dohledatená)
A – accesible (přístupná)
I – interoperable (strojovně zpracovatelná)
R – reusable (znovu použitelná)

R – resilient (odolná)

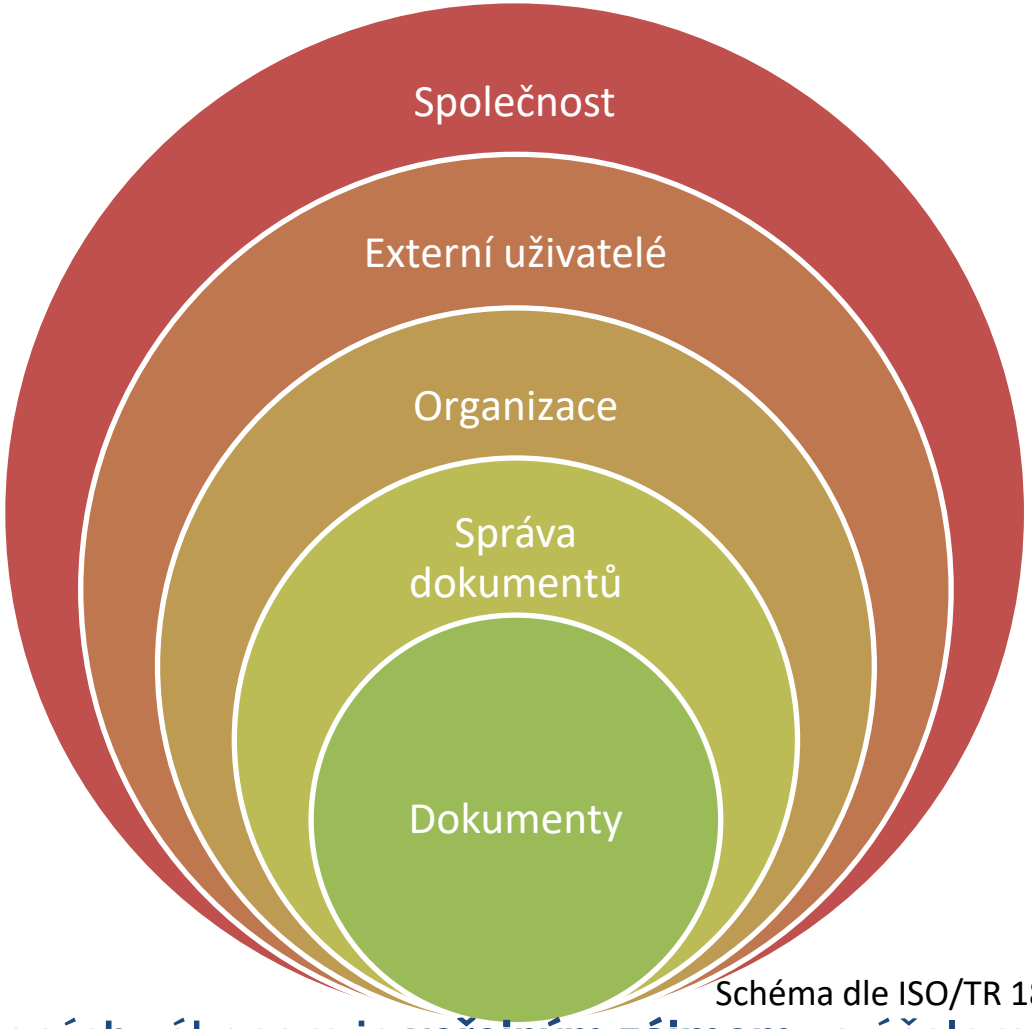


Schéma dle ISO/TR 18128:2014

Uchování informací i **jejich ochrana** za podmínek stanovených zákonem je **veřejným zájmem** za účelem řízení, kontroly, doložení právních závazků a povinností, zabránění zneužití, znovuvyužití, výzkumu atd.

Správa dokumentů nebo informací?

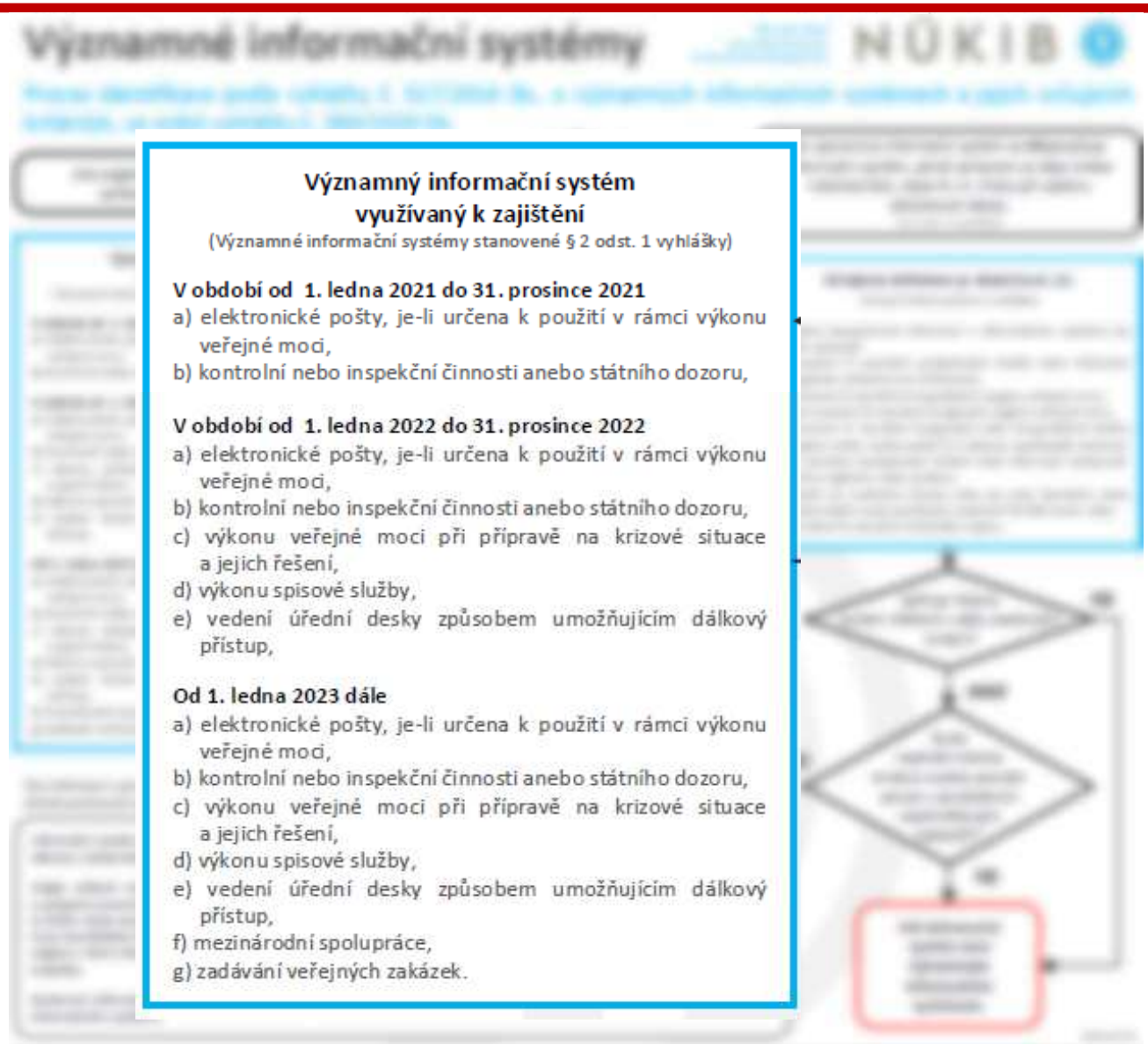
Chybou redukovat jen na dokumenty evidované v eSSL - viz.:

- „dokumentem každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena“ (§ 2 písm. e) zák. 499/2004 Sb.)
- „archiváliı (je) takový dokument, který byl vzhledem k době vzniku, obsahu, původu, vnějším znakům a trvalé hodnotě dané politickým, hospodářským, právním, historickým, kulturním, vědeckým nebo informačním významem vybrán ve veřejném zájmu k trvalému uchování… (§ 2 písm. f) zák. 499/2004 Sb.)

- listina
- audiovizuální soubor (např. vystoupení ministra na TK, video z policejní akce aj.)
- informační systém, rejstřík, databáze
- e-mailový účet, týmový instant messaging
- videokonference
- prezentace institucí a jejích představitelů na internetu vč. sociálních sítí (např. i s ohlasy veřejnosti)
- prostorová data (např. na mapovém portálu)
- zdravotnická dokumentace
- televizní a rozhlasové vysílání

…

Významný informační systém



Významný informační systém využívaný k zajištění

(Významné informační systémy stanovené § 2 odst. 1 vyhlášky)

V období od 1. ledna 2021 do 31. prosince 2021

a) elektronické pošty, je-li určena k použití v rámci výkonu veřejné moci,
b) kontrolní nebo inspekční činnosti anebo státního dozoru,

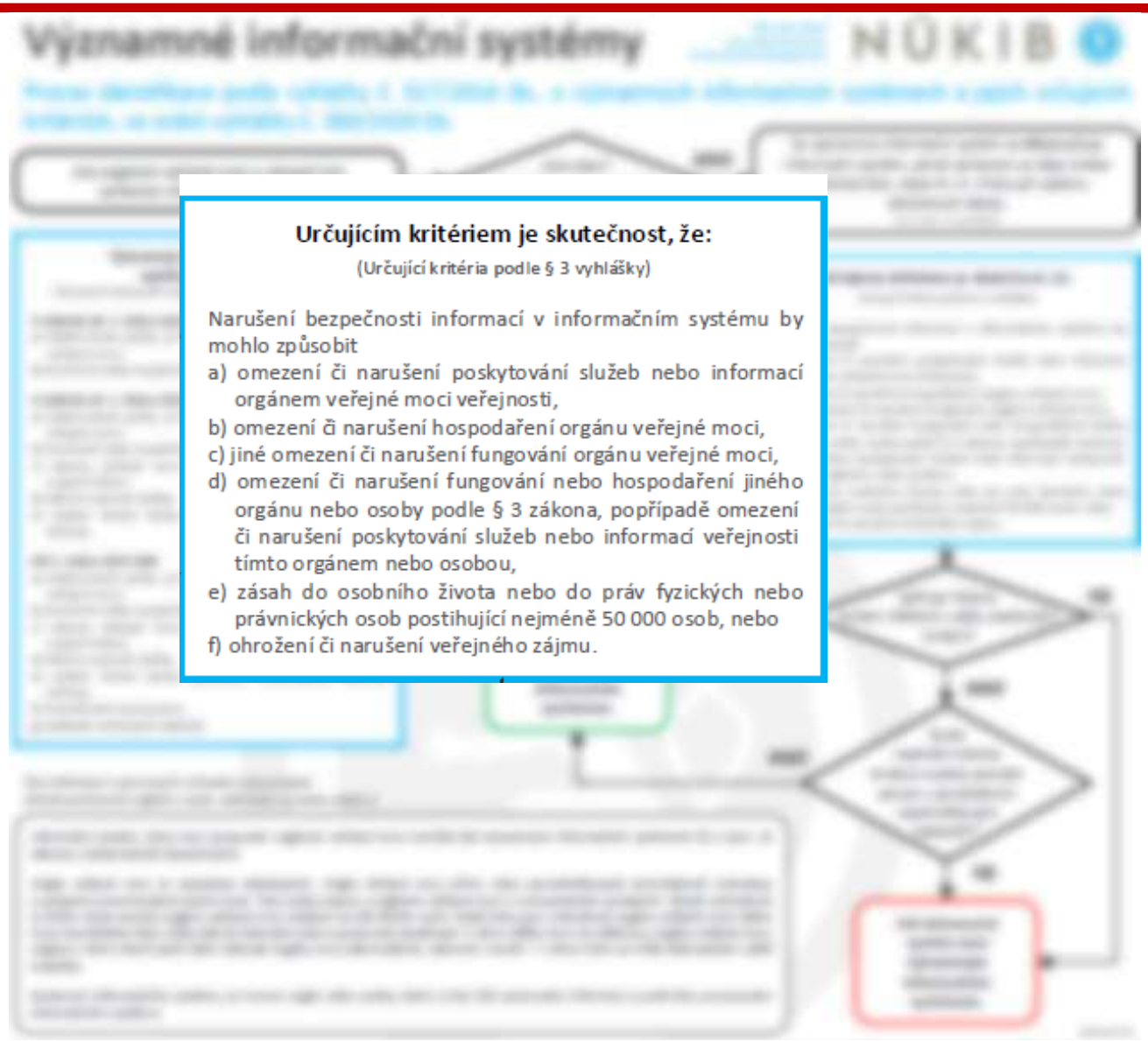
V období od 1. ledna 2022 do 31. prosince 2022

a) elektronické pošty, je-li určena k použití v rámci výkonu veřejné moci,
b) kontrolní nebo inspekční činnosti anebo státního dozoru,
c) výkonu veřejné moci při přípravě na krizové situace a jejich řešení,
d) výkonu spisové služby,
e) vedení úřední desky způsobem umožňujícím dálkový přístup,

Od 1. ledna 2023 dále

a) elektronické pošty, je-li určena k použití v rámci výkonu veřejné moci,
b) kontrolní nebo inspekční činnosti anebo státního dozoru,
c) výkonu veřejné moci při přípravě na krizové situace a jejich řešení,
d) výkonu spisové služby,
e) vedení úřední desky způsobem umožňujícím dálkový přístup,
f) mezinárodní spolupráce,
g) zadávání veřejných zakázek.

Významný informační systém



Zranitelnosti a hrozby – interní a externí (dle vyhl. č. 82/2018 Sb.)

- Zranitelnosti

1. nedostatečná údržba informačního a komunikačního systému,
2. zastaralost informačního a komunikačního systému,
3. nedostatečná ochrana vnějšího perimetru,
4. nedostatečné bezpečnostní povědomí uživatelů a administrátorů,
5. nedostatečná údržba informačního a komunikačního systému,
6. nevhodné nastavení přístupových oprávnění,
7. nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
8. nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,
9. nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,
10. nedostatečná ochrana aktiv,
11. nevhodná bezpečnostní architektura,
12. nedostatečná míra nezávislé kontroly,
13. neschopnost včasného odhalení pochybení ze strany zaměstnanců.

- Hrozby

1. porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,
2. poškození nebo selhání technického anebo programového vybavení,
3. zneužití identity,
4. užívání programového vybavení v rozporu s licenčními podmínkami,
5. škodlivý kód (například viry, spyware, trojské koně),
6. narušení fyzické bezpečnosti,
7. přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,
8. zneužití nebo neoprávněná modifikace údajů,
9. ztráta, odcizení nebo poškození aktiva,
10. nedodržení smluvního závazku ze strany dodavatele,
11. pochybení ze strany zaměstnanců,
12. zneužití vnitřních prostředků, sabotáž,
13. dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,
14. nedostatek zaměstnanců s potřebnou odbornou úrovní,
15. cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,
16. zneužití vyměnitelných technických nosičů dat,
17. napadení elektronické komunikace (odposlech, modifikace).

Identifikace a analýza rizik

- identifikace primárních a podpůrných aktiv v organizaci (služby, informace/data) vč. technického, komunikačního a programového vybavení
- identifikace, analýza, vyhodnocení rizik a jejich zvládání v oblastech:
  - důvěrnosti aktiv
  - integrity aktiv
  - dostupnosti aktiv
- součástí hodnocení i politika řízení kontinuity činností (angl. business continuity) včetně minimální úrovně poskytovaných služeb, doby obnovení chodu a bodu obnovení dat (plány kontinuity vč. havarijních plánů)
- srv. kap. 7 NSESSS – Kontrola a bezpečnost (Přístup, Transakční protokol, Záloha a obnova, Škodlivý kód) – kdo v organizaci zodpovídá, kdo zajišťuje, kdo pravidelně kontroluje, ev. zda outsourcing není zpoplatněn tak, že je fakticky v případě incidentu většího rozsahu obnova finančně nedostupná (!)
- srv. také ISO TR 18128:2014 - Risk assessment for record processes and systems (včetně možných otázek při identifikaci rizik)

Správa dokumentů - dříve

Útvary organizace

Posouzení významu dokumentů pro výkon agendy, postup dle vnitřních předpisů

Metodik spisové služby

koordinace a tvorba vnitřních předpisů (např. spisový řád)

Spisovna

Archiv

úřad pro ochranu osobních údajů
the office for personal data protection

Správa dokumentů – současný informační management

Pověřenec pro ochranu osobních údajů

Záznamy o činnostech zpracování (čl. 30 GDPR), implementace ochrany OÚ do vnitřních předpisů (např. doba uchovávání – tj. skartační lhůty), hlášení porušení zabezpečení osobních údajů

Útvar organizace (garant agendy)

Poskytovatel IT infrastruktury (interní/externí)

úřad pro ochranu osobních údajů
the office for personal data protection

OTEVŘENÁ DATA

NÚKIB

Manažer kybernetické bezpečnosti (vč. architekta, řídícího výboru atd.)

Analýza rizik ve spolupráci s garanty aktiva, implementace opatření, hlášení kybernetického bezpečnostního incidentu

Spisovna

NA RP Národní archivní portál

Koordinátor otevírání dat

Identifikace datových sad (publikaci kurátor dat), koordinace s dodavatelem IT řešení (např. transformace dat, API, anonymizace/ pseudonymizace atd.)

Metodik správy dokumentů

Řízení správy dokumentů v organizaci, architektura správy dokumentů ve spolupráci s poskytovatelem IT infrastruktury a dodavatelem IT řešení, správa rolí a identit v eSSL/ISSD, koordinace a tvorba vnitřních předpisů, kontrola jejich aplikace

Dodavatel IT řešení (např. eSSL/agendového IS atd.)

Závěr

- zpracování analýzy rizik v rámci hlášení VIS dle ZoKB je možné využít k zvýšení zájmu o řízení správy dokumentů u vedení organizací (obdobně 2016 s účinností GDPR) a ke zmapování zdrojů dokumentů (informací) napříč organizací včetně podchycení jejich životního cyklu
- napříč veřejnou správou (i u organizací stejného významu) enormní rozdíly v personálním zajištění správy dokumentů vč. absence kvalifikačních kritérií (vedení spisové evidence a příprava SŘ od 4. PT, kompletní zajišťování spisové služby od 6. PT, tvorba spisového řádu od 8. PT, návrhy a zadání eSSL 10. PT, architektura eSSL a ISSD 11. PT) – srv. požadavky ZoKB – správa dokumentů musí být partnerem
- ztrátou/neuchováním dokumentu (informace) ve veřejné správě dochází k narušení veřejného zájmu (kontrola činnosti státem či občany, nemožnost dalšího využití atd.) – přestupek dle § 74 odst. 6 zák. 499/2004 Sb.
- k aplikaci § 9 odst. 2 vyhl. č. 259/2012 Sb. (ztráta/neuchování dokumentu vč. ztráty čitelnosti) stanovisko v InfoListu NA č. 29/18 (čá. 3/2018), nutná rekonstrukce informace (viz. judikáty NSS) – dnes většina přestupků zjištěna vnější kontrolou nebo na základě podnětu, v oblasti hlášení narušení nebo ztráty nutná interoperabilita mezi správními úřady na úseku správy informací ve veřejné správě: ÚOOÚ – osobní údaje, NÚKIB – bezpečnost informací, státní archivy – uchování dokumentů (informací)

Díky za Vaši pozornost!

zbysek.stodulka@nacr.cz