Informačná bezpečnosť a GDPR z pohľadu tvorcu knižnično-informačného systému

S nárastom počtu technologických zariadení, ktoré nás postupne obklopujú, si stále častejšie kladieme otázky týkajúce sa bezpečnosti či ochrany – bezpečnosti dát, ochrany našich osobných údajov, bezpečnosti informačných systémov, bezpečnosti našej komunikácie, bezpečnosti technológií, ktoré používame a ďalšie otázky, ktoré súvisia s našou každodennou interakciou s týmito zariadeniami a technológiami. Informačná bezpečnosť je oblasťou poznania, ktorá obsahuje pojmy „Počítačová bezpečnosť"[1] a „Bezpečnosť systémov na spracovanie informácií."[2]

Otázkou je, či a akým spôsobom sa táto oblasť dotýka aj knižníc a informačných systémov, ktoré knižnice používajú k automatizácii vlastných procesov, od obstarávania fondov, zabezpečenie služieb, až po ich sprostredkovanie používateľom. Informácie o zdrojoch poznania sú predsa verejne dostupné, alebo by aspoň mali byť voľne dostupné. Tak prečo riešiť počítačovú bezpečnosť v knižniciach? Na tieto, ale aj viaceré ďalšie otázky spojené hlavne s ochranou osobných údajov, sa pokúsime odpovedať v nasledujúcich riadkoch. Oboznámime sa so základnou terminológiou, zhrnieme si základné ciele, ktoré aplikovaním počítačovej bezpečnosti do našej činnosti sledujeme, ale aj nevyhnutné kroky a opatrenia, ktoré k tomu musíme vykonať. Zároveň upozorníme aj na niektoré riziká, na ktoré by sme v tejto súvislosti nemali zabúdať. Keďže uplynul takmer rok od chvíle, kedy bolo v krajinách Európskej únie zavedené do praxe Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov[3], známe pod akronymom „GDPR", tak sa pokúsime zhodnotiť tento process z pohľadu tvorcu knižnično-informačného systému. Čo je nevyhnutné v systéme implementovať, aby bol v súlade s týmto nariadením a čo je ešte možné pri dodržaní nariadenia GDPR v systéme automatizovať.

Knižnice si dnes bez počítačov, ale aj množstva iných prostriedkov, zariadení či služieb z oblasti informačných a komunikačných technológií nevieme ani len predstaviť. Druhá polovica minulého storočia, kedy sa tieto technológie začali masívnejšie zavádzať aj v pamäťových a fondových inštitúciach, a v knižniciach obzvlášť, bola zároveň počiatkom nového prerodu knižníc. Z pôvodných klasických knižníc, kde prevládali knihy a iné zdroje poznania v klasickej papierovej podobe sú dnes tzv. „heterogénne" prípadne aj čisto „digitálne" knižnice. Knižnice, v ktorých vedľa klasických kníh fungujú viaceré technológie a informačné systémy, a ktoré sú dnes súčasťou prakticky každej organizácie, ako aj väčšiny domácností. Informačný systém pre knižnice (KIS) tu predstavuje hlavný informačný systém, ktorého úlohou je čo najefektívnejšie automatizovať procesy v knižniciach. Nejde v nich však už len o automatizáciu procesov obstarávania a vypožičiavania dokumentov. Súčasné informačné systémy v knižniciach musia v sebe integrovať rôzne technológie, na ktoré sú používatelia zvyknutí z bežného života, ako aj viaceré informačné systémy.

Naviac, tieto systémy sa pomerne rýchlo menia, lebo musia vedieť reagovať na neustále zmeny technológií, ako aj meniace sa požiadavky a očakávania používateľov. Ak hovoríme o efektívnej automatizácii procesov, tak je zrejmé, že z hľadiska práce s informačnými systémami veľmi vítame, ak nám tieto umožňujú dáta vložiť len raz a vzájomne si ich zdieľať či viacnásobne používať a znova využívať. Toto však na druhej strane predstavuje aj veľké riziko. Riziko toho, že by mohlo prísť napríklad k neoprávnenému prístupu k dátam či k ich modifikáci alebo k zneužitiu, prípadne ich prostredníctvom získavať iné dáta a podobne. Preto aj pri tejto práci, pri práci s technológiami, rovnako, ako aj pri akejkoľvek inej činnosti, musíme dbať na bezpečnosť a tiež elimináciu možných rizík, ktoré dáta v elektronickej, ale aj papierovej podobe so sebou prinášajú. Keďže hovoríme o IKT, tak sa jedná o informačnú alebo tiež počítačovú bezpečnosť. No a čo to vlastne počítačová či informačná bezpečnosť je? Čo si pod ňou môžeme predstaviť a čo je jej cieľom? Nie je úplne jednoduché ju zadefinovať, ale Interná správa NIST NISTIR 7298 (Slovník kľúčových pojmov v informačnej bezpečnosti) ju v máji 2013 definoval takto: „**Opatrenia a riadenie, ktoré zabezpečujú dôvernosť, integritu, a dostupnosť aktív informačného systému vrátane hardvéru, softvéru, firmvéru a informácií, ktoré sa spracovávajú, uchovávajú a komunikujú."[4]**

Ako môžeme vidieť, táto definícia zavádza tri veľmi dôležité nové pojmy pre označenie cieľov, ktoré vždy stoja v centre počítačovej bezpečnosti. Jedná sa o dôvernosť (confidentiality), integritu (integrity) a dostupnosť (availability), spoločne tiež označované skratkou CIA. Tieto termíny zároveň predstavujú základné bezpečnostné ciele pre údaje a informačné a výpočtové služby. Dôvernosť a integrita pritom môžu byť chápané na dvoch úrovniach – zastrešujú samostatné čiastkové koncepty.

Dôvernosť si kladie za cieľ zachovanie oprávnených obmedzení prístupu a zverejňovania informácií, vrátane prostriedkov na ochranu osobného súkromia a chránených informácií. Teda myslíme tým jednak dôvernosť údajov a tiež ich privátnosť.

[1] Interná správa NIST NISTIR 7298 (Slovník kľúčových pojmov v informačnej bezpečnosti), 2013.

[2] STALLINGS, W., BROWN, L.: Computer Security Principles and Practice. Fourth Edition. Pearson Education, Inc. 2018. ISBN 9781292220611.

[3] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov. Portál EUR-Lex. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/ALL/?uri=CELEX%3A32016R0679

[4] NIST NISTIR 7298, 2013.

Pričom dôvernosť údajov má za cieľ zabezpečiť, aby súkromné alebo dôverné informácie neboli sprístupnené ani dostupné neoprávneným osobám. Na druhej strane privátnosť zasa zabezpečuje to, že jednotlivci sú tí, ktorí priamo riadia a ovplyvňujú to, aké informácie súvisiace s nimi môžu byť zhromaždené a uložené, ale aj to, kto a komu ich môže sprístupniť.

Integrita je zasa chápaná ako ochrana proti nesprávnej modifikácii alebo zničeniu informácie vrátane zaistenia neodmietnutia a autenticity informácie, pričom strata integrity je neoprávnená modifikácia alebo zničenie informácie. Integrita môže byť chápaná na dvoch úrovniach, ako integrita údajov, ktorá zabezpečuje, že informácie a program sa menia len stanoveným a oprávneným spôsobom. Na druhej strane integrita systému zabezpečuje, že systém vykonáva zamýšľanú funkciu nenarušeným spôsobom, bez zámernej alebo neúmyselnej neoprávnenej manipulácie so systémom.

No a posledným z vyššie uvedených troch termínov je dostupnosť.

Dostupnosť zabezpečuje, aby systémy fungovali okamžite a aby služba nebola oprávneným používateľom odmietnutá. Okrem týchto troch pojmov sa v súvislosti s definovaním cieľov počítačovej bezpečnosti stretávame s viacerými ďalšími, ktoré nám umožňujú konkrétnejšie zadefinovať ciele vlastnej bezpečnostnej politiky.

Najčastejšie sú to pojmy **„Autenticita" a „Účtovateľnosť" (zodpovednosť)**. Pod autenticitou chápeme predovšetkým to, že používateľ je ten, za ktorého ho považujeme, ako aj to, že každý vstup do systému pochádza z dôveryhodného zdroja. Ide teda o schopnosť systému overiť pôvod, alebo originalitu údajov, ako aj výsledok overenia, teda dôveryhodnosť, rovnako aj dôvera v platnosť prenosu, správy, alebo pôvodcu správy.

Zúčtovateľnosť je zasa chápaná ako bezpečnostný cieľ, ktorý vytvára požiadavku na to, aby sa činnosti danej entity mohli jednoznačne dosledovať. To podporuje neodmietnutie, odstrašovanie, izoláciu porúch, detekciu a prevenciu narušenia a následné zotavenie a právne kroky. Z hľadiska bezpečnosti musíme byť vždy schopní dosledovať to, kto porušenie bezpečnosti spôsobil. Teda dosledovať porušenie bezpečnosti entite, ktorá je za porušenie bezpečnosti zodpovedná.

Na druhej strane si systémy musia viesť záznamy o svojej činnosti, aby umožnili neskoršiu **forenznú analýzu** na dosledovanie narušenia bezpečnosti alebo na pomoc pri transakčných sporoch.

Z uvedeného vyplýva, že informačná bezpečnosť má multilaterárny charakter. Jej cieľom je, zabezpečenie súladu požiadaviek zo strany vlastníkov informačných systémov s potrebami ich používateľov práv fyzických a právnických osôb, ktorých a o ktorých sú údaje v systémoch spracovávané. Ak sa na problém informačnej bezpečnosti pozrieme z pohľadu používateľov, tak k najdôležitejším faktorom pri spracovaní informácií patria účel a obsah informácií, presnosť, aktuálnosť, autenticita, usporiadanie a kvalita informácií.

Na druhej strane z pohľadu prevádzkovateľov a vlastníkov je najdôležitejší spoľahlivý prístup k informačným zdrojom s online prístupom, ich zabezpečenie pred únikom informácií, neoprávneným použitím a narušením integrity údajov, ako aj autorita a dobré meno vlastníka systému.

K znehodnoteniu týchto systémov a údajov, ktoré sa v nich nachádzajú, môže prísť rôznymi spôsobmi a pod vplyvom viacerých činiteľov. Patria medzi nich napríklad prírodné katastrofy alebo iné prírodné vplyvy. Najčastejšie však medzi nich patrí zlyhanie ľudského faktora alebo technické poruchy. Ťažko predvídateľné nebezpečenstvo predstavujú predovšetkým cieľavedomé útoky na systém, medzinárodný terorizmus, škodlivý softvér, alebo počítačová kriminalita. Ďalšie vážne bezpečnostné problémy sú spojené s informačnou a komunikačnou infraštruktúrou, ktorej základom je internet a jeho služby. S prenosom dát prostredníctvom internetovej siete sa spájajú vážne bezpečnostné problémy, napr. pri využívaní elektronickej pošty či prenose súborov. Nezabezpečenie informačných systémov, informácií a dát tak môže spôsobiť únik dát, ich zneužitie, nenahraditeľné straty, a tým aj narušenie dôveryhodnosti systému, organizácie, ale aj štátu. Preto je nesmierne dôležité venovať tejto problematike primeranú pozornosť, a to na všetkých úrovniach od jednotlivca cez organizácie, krajiny a tiež na medzinárodnej úrovni. Pre definovanie základných cieľov počítačovej bezpečnosti si väčšinou postačíme s vyššie uvedenými pojmami. Oveľa komplikovanejšie je to s mechanizmami použitými pre dosiahnutie týchto cieľov.

Vysvetlenie všetkých pojmov, ktoré k tomu budeme potrebovať môžeme nájsť v dokumente známom pod označením IETF RFC 2828[5]. Tento „slovník" obsahujúci „RFC"– Request for Comments 282 bol vytvorený a naďalej je aj aktualizovaný otvorenou pracovnou skupinou, ktorá v úzkej spolupráci s konzorciom W3C a organizáciou ISO/IEC, vytvára a propaguje internetové štandardy týkajúce sa prevažne protokolu TCP/IP (*https://www.ietf.org/*).

Vzhľadom na to, že štát je garantom kritických procesov v oblasti technológií a má za úlohu starať sa o celkovú úroveň konkurencieschopnosti krajiny, a tak chrániť národné bohatstvo ukryté v dátach (súčasťou ktorého sú aj znalosti a informácie), musí sa snažiť o čo najlepšie nastavenie kritérií úrovne bezpečnosti. Dosahy podcenenia úlohy bezpečnosti IT môžu byť pre štát v určitých oblastiach zničujúce. Jeho povinnosťou je preto zabezpečiť ochranu informácií pred zneužitím a minimalizáciu následkov v prípade ich zneužitia. To je dôvod, ktorý vedie štáty, vlády a organizácie vyspelých krajín uvedomujúce si dôležitosť informačnej bezpečnosti, aby vytvorili rôzne inštitúcie či inštitucionálne systémy, ktoré majú za úlohu zabezpečovanie ochrany informácií, napríklad Európsku agentúru pre bezpečnosť informačných sietí, tiež Skupinu vysokých zástupcov pre otázky správy internetu a Jednotku pre riešenie počítačových incidentov. Určili si strategické ciele a prijímajú opatrenia na ich splnenie, z ktorých dnes už viaceré aj realizujú. Veľký prínos v tejto oblasti nemožno uprieť ani **(General Data Protection Regulation)**, teda Nariadeniu Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri

[5] Shiery, R. et al. 2000. IETF RFC 2828 – Internet Security Glossary, The Internet Society. 212 pp.

spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa ruší smernica 95/46/ES (Všeobecné nariadenie o ochrane údajov). V súvislosti s týmto nariadením v roku 2018 vošli do platnosti na úrovni každej krajiny usmernenia, ktoré toto nariadenie upravujú s ohľadom na špecifiká a potreby krajiny.

Na Slovensku v tomto roku vošiel do platnosti nový Zákon o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov č. 95/2019 Z. z.[6] Tento zákon sa vzťahuje na všetky informačné technológie a infraštruktúry vo verejnej správe, ako aj na ich správu, to znamená – na všetky informačné systémy. Dnes všetky knižnice už majú, alebo by mali mať skúsenosti so zabezpečením a ochranou osobných údajov v súlade s GDPR. Našim cieľom je preto priblížiť tu aj zosúladenie požiadaviek GDPR z pohľadu informačného systému, konkrétne z pohľadu tvorcov takéhoto informačného systému.

Bezpečnosť (knihovníckych) informačných systémov

Osobné údaje patria k najcitlivejším informáciám a dotýkajú sa každého človeka. Čo však predstavujú z pohľadu informačného systému (IS)? Čo všetko a na akých úrovniach musí zabezpečiť dodávateľ informačného systému? Zámerne uvádzame –dodávateľ informačního systému, pretože to nemôže urobiť nikto iný. Žiadne univerzálne riešenie tohoto druhu neexistuje a nie je možné ho vytvoriť. Ako sa s tým všetkým vysporiadať? To sú otázky, ktoré si určite položili a stále si kladú viacerí dodávatelia IS, spracovatelia či inštitúcie. Máme za sebou prvý rok účinnosti európskeho Všeobecného nariadenia na ochranu osobných údajov, známejšieho viac pod skratkou GDPR. Môžeme si teda položiť otázku, aký dopad malo zavedenie tohto nariadenia na bezpečnosť informačných systémov?

Z nášho pohľadu určite pozitívny. Každá organizácia sa musela svojím spôsobom vysporiadať s jeho zapracovaním do svojich procesov a systémov, zmapovať toky dát, doplniť dokumentácie, ošetriť zmluvné vzťahy so svojimi dodávateľmi – spracovateľmi. Na dodávateľov informačných systémov doľahol tlak na urýchlené doriešenie starých hriechov v ich systémoch, doplnenie chýbajúcich funkcionalít, prispôsobenie architektúry, ale predovšetkým na dokonalejšie zabezpečenie dát a prevenciu incidentov.

Princípy ochrany informačných systémov (IS):

Jedným z prínosov GDPR je odporúčanie základných princípov ochrany, medzi ktoré patrí:

- Ochrana dát ako základná požiadavka na design systému
- Minimalizácia spracovania
- Evidencia spracovania
- Zabezpečenie integrity a aktuálnosti dát
- Dostupnosť a zamedzenie straty dát
- Detekcia a riešenie incidentov

Knižničný informačný systém musí zaistiť ochranu dát a bezpečné uloženie osobných údajov. Jedným z predpokladov je dobre navrhnutá a spoľahlivo fungujúca sieťová infraštruktúra (firewall, antivírus, monitoring hardwaru a softwarových služieb, včasné aktualizácie a odstraňovanie zraniteľností), databáza, systém zálohovania, aplikačná vrstva, komunikačné protokoly). Pri prevádzkovaní KIS formou hostingovej (cloudovej) služby je to starosťou spracovateľa, pri inštalácii KIS na vlastnom zariadení si musí knižnica zabezpečiť aj celú infraštruktúru vlastnými silami, alebo formou outsourcingu – teda služby.

Ochrana dát na úrovni návrhu IS

Počítať s ochranou osobných údajov je potrebné už od chvíle návrhu praktického riešenia ich spracovania v IS. Tento princíp sa najlepšie uplatní pri návrhu nových systémov, modulov a funkcionalít do informačného systému. Celý rad účinných opatrení je však možné aplikovať aj do existujúcich riešení.

Medzi účinné technické opatrenia patrí:

1. Bezpečné uloženie, šifrovanie

Hoci nariadenie GDPR priamo neurčuje šifrovanie dát ako povinné, stalo sa napriek tomu najviac odporúčaným variantom zabezpečenia osobných údajov uložených v databáze KIS.

Malo by byť samozrejmosťou ukladanie loginov (prihlasovacích údajov), hesiel, rolí, prístupových práv a pod. do šifrovanej časti databázy. Ostatné osobné údaje používateľov je tiež vhodné chrániť šifrovaním, a to vrátane záznamov v chronológii zmien v zálohách KIS.

Hashovanie

Na rozdiel od šifrovania, ktoré dovoľuje zašifrované dáta pri použití príslušných kľúčov znovu dešifrovať do čitateľnej podoby, je hashovanie výlučne jednosmerný proces. Preto sa využíva pre ukladanie hesiel. Do databázy sa nikdy neukladá samotné

[6] Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov. Dostupné na: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2019/95/20190501

heslo, ale len jeho jedinečný kryptický odtlačok, hash, z ktorého nie je možné v žiadnom prípade heslo spätne rekonštruovať. Je dôležité, aby dosiaľ v praxi veľmi rozšírené, ale zastarané a dnes už prelomiteľné hashovanie MD5, bolo v KIS nahradené bezpečnými algoritmami SHA-512, prípadne bcrypt nebo scrypt.

2. Zabezpečenie komunikácie

Kľúčový pre komunikáciu medzi webovým prehliadačom, klientom KIS a serverom KIS, je komplexný prechod z voľne čitateľného http protokolu na šifrovaný protokol https. Osobné údaje používateľov KIS tak sú chránené proti „odpočúvaniu". Niektoré systémy pôvodne vyžadovali protokol https len na prihlásenie do konta používateľa v online katalógu. To už dnes nestačí, štandardom je kompletne šifrovaná komunikácia všetkých komponentov KIS – celého online katalógu, „tučného" i „tenkého" klienta, nástrojov pre správcu, integračných API.

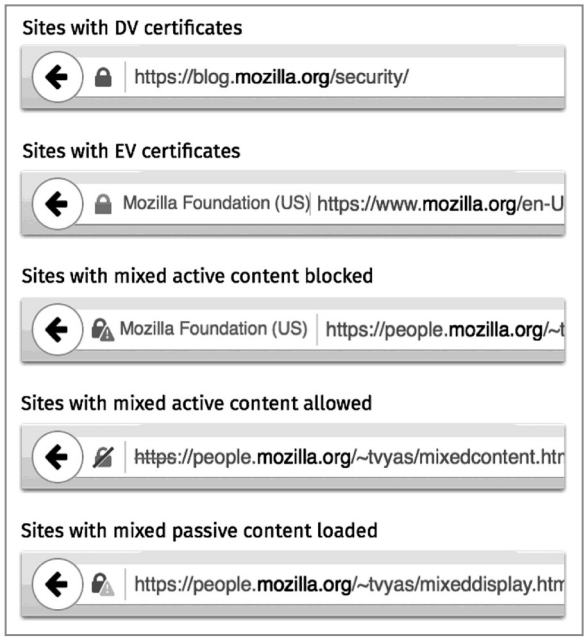
Určitou prekážkou v prechode webových katalógov na protokol https, obzvlášť pre malé knižnice, bol dovtedy nie úplne jednoduchý postup pri získavaní certifikátov overených dôveryhodnou autoritou. Bolo nutné ich zakúpiť, správne nainštalovať a pravidelne obnovovať. Táto prekážka už bola prekonaná, jednoduchší prístup k certifikátom pre kohokoľvek je v súčasnosti možný vďaka zdarma dostupným „Let's Encrypt" certifikátom[7] a vďaka skriptom pre ich automatizované obnovovanie.

Pre väčšie univerzitné siete, ktoré bežne mávajú zavedenú centrálnu správu certifikátov, je relevantné, aby KIS obsahoval podporu pre reverzné https proxy. V tomto režime prebieha vonkajšia komunikácia prostredníctvom protokolu https, dovnútra na webový server je následne preklopená na http, ale do stránok vložené skripty, obrázky a ďalšie prvky musia byť odkazované cez https protokol.

Ďalším nevyhnutným krokom je zmena nastavení webových aplikačných serverov z šifrovania SSL na jeho bezpečnejšieho nástupcu TLS. Dôležité je sledovanie a prípadné aplikovanie nových technológií, ako napríklad HSTS – vynútenie https, dokáže zabrániť presmerovaniu na http, HPKP – dokáže zabrániť výmene certifikačných autorít.

3. Bezpečná práca s prehliadačom

Najčastejším pracovným nástrojom používateľa pri používaní webového katalógu KIS je webový prehliadač. Nové verzie webových prehliadačov sa snažia používateľa chrániť pred nezabezpečenými stránkami, cez ktoré by mohlo dôjsť k úniku citlivých osobných informácií. V adresnom riadku napríklad graficky zvýrazňujú zabezpečené stránky, aj tie potenciálne nebezpečné, rozlišujú úrovne certifikátov DV, OV, EV (Domain, Organization, Extended Validation), stále viac aktívne blokujú nezabezpečené stránky.



Vidíme tu priestor aj pre verejné knižnice zapojiť sa do vzdelávania používateľov, učiť ich, ako správne a bezpečne používať webové technológie.

Definícia prístupových práv

Personálne a organizačné opatrenia slúžia na to, aby zabezpečili prístup každého jednotlivého zamestnanca, správcu údajov k určitým konkrétnym údajom. Určujú teda toky dát. Na to musí byť KIS pripravený dostatočnou ponukou možností definície pracovných rolí a prístupových práv. Mal by poskytovať čo najväčšiu granularitu nastavení nielen na úrovni databázových tabuliek a logických databáz (na úrovni riadkov), ale až na jednotlivé položky (stĺpce). Z pohľadu toku dát zase práva k spusteniu vybraných aplikačných modulov, prípadne až na úroveň jednotlivých funkcií.

Minimalizácia spracovania – „Data protection by default"

Medzi hlavné zásady GDPR patrí minimalizácia údajov[8]. Informačné systémy majú zabezpečiť, aby v základnom nastavení určitej služby boli spracovávané len tie osobné údaje, ktoré sú nevyhnutné pre jej poskytovanie. V KIS sa to týka napríklad štandardných pracovných formulárov na evidenciu používateľov.

Technickým riešením môže byť aj anonymizácia a pseudonymizácia osobných údajov. V prípade anonymizácie nesmú byť osobné údaje spojiteľné s konkrétnym človekom, typické využitie je anonymizovaná história výpožičiek využívaná ako podklad pre štatistiky, určovanie trendov, odporúčanie literatúry a podobne.

---

[7] Open Web Application Security Project, OWASP, Global AppSec, AppSec Days, AppSec California, SnowFROC, LASCON, and the OWASP logo are trademarks of the OWASP Foundation. Dostupné na: https://letsencrypt.org/about/ https://www.abetterinternet.org/about/

[8] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016, Článok 5. Osobné údaje musia byť: ... c) primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú („minimalizácia údajov");

U pseudonymizácie sa jedná o ukrytie identity pomocou kódu – kľúč spojujúci kódy s osobnými dátami jednotlivcov sa uchováva zvlášť.

KIS v súlade s GDPR poskytuje používateľom možnosť požiadať o výmaz jeho osobných údajov v systéme, ale aj vysporiadanie záväzkov a splnenie podmienok pre ukončenie registrácie. To zahŕňa nezvratný výmaz osobných údajov, anonymizáciu výpožičkových údajov, návštevných a platobných transakcií a vymazanie chronológie. Aktívni používatelia môžu kedykoľvek požiadať o výmaz (anonymizáciu) histórie ich výpožičiek. A to buď jednorázovo, alebo priebežne automaticky počas celej doby platnosti registrácie. V tomto prípade si zvyčajne knižnice stanovujú určitú ochrannú lehotu na riešenie reklamácií a vysporiadanie záväzkov.

Evidencia spracovania osobných údajov:

Spracovateľ dát musí uschovať a tiež dokázať doložiť kompletnú históriu zmien a prístupov k dátam. To znamená, že KIS musí podporovať ukladanie zmien do chronológie, vrátane používateľa, ktorý zmenu zrealizoval. Rovnako tak prevádzkové logovanie všetkých operácií v systéme (napr. výpožičky, platby, evidencie návštev, generovanie upomienok, zasielanie newslettrov – noviniek). GDPR rozšírilo nároky na evidenciu navyše o logovanie prístupov k osobným údajom, t. z. nutnosť evidovať aj každé jedno zobrazenie záznamu používateľa, spustenie výstupu, exportu, a ďalšie operácie.

Dostupnosť a zamedzenie straty dát:

Udržanie informačných systémov v bezproblémovej prevádzke a ochrana dát pred stratou, útokom alebo ich poškodením v prípade havárie sa rieši v rámci informačných systémov variabilne na viacerých úrovniach. Na začiatku by mala byť realizovaná analýza potenciálnych rizík a určenie závažnosti prípadných následkov (útoku, katastrofy) a strát. Od toho sa odvíja výška investícií do zodpovedajúcej infraštruktúry produkčného a zálohovacieho prostredia. Konkrétne sa v oblasti KIS používa:

- Duplicita hardwaru – viacero fyzických serverov, sieťových prvkov, zdvojené komponenty, záložné napájanie;
- Geografické rozdelenie minimálne do 2 dátových centier, zálohovaná sieťová a internetová konektivita;
- Virtualizácia aplikačných serverov a diskových polí, s možnosťou rýchleho presunu virtuálnych strojov medzi fyzickými servermi;
- Zálohovanie virtuálnych serverov na inú lokalitu;
- Tieňovanie databázy na záložný mirror/shadow server (voliteľne), prípadne využitie distribuovanej databázy;
- Automatické online zálohovanie databázy podľa vopred stanoveného plánu záloh;
- Cyklické ukladanie databázových transakčných denníkov (žurnálov) pre zaistenie prípadnej obnovy od poslednej zálohy až po moment výpadku;
- „Write image" žurnál pre automatické zotavenie systému po neplánovanom reštarte databázy;
- Plánované kontroly integrity;
- Offline režim aplikačného klienta, ktorý umožňuje realizovať základné operácie aj pri dlhšie trvajúcej strate konektivity IS s aplikačným serverom. Po obnovení konektivity dôjde k synchronizácii dát so serverom.

Detekcia a riešenie incidentov:

1. Sieťová infraštruktúra

Dôležitým prvkom ochrany vnútornej siete by mal byť firewall s proaktívnou detekciou útokov a pokusov o prienik do systému. Pred hackerskými nástrojmi, hľadajúcimi „dieru" (zraniteľnosť) v systéme technikou skenovania otvorených portov, je potrebné sa brániť defaultným uzatvorením všetkých portov a povolením len tých, ktoré potrebujú používané služby KIS. Vhodný je tiež permanentne aktívny monitoring hardwaru i softwarových služieb, napríklad nástrojmi Nagios alebo PRTG.

2. Aplikačná bezpečnosť

Na neustály vývoj hackerských techník a nástrojov, nové typy útokov je vhodné reagovať pravidelnou realizáciou penetračných testov a následných opatrení, napríklad podľa metodiky OWASP Top 10[9].

Pre spätnú analýzu incidentov a problémových alebo sporných situácií je vždy vhodné mať zavedený systém auditu a logovania všetkých aktivít, prístupov a zmien v KIS.

[9] OWASP Top 10 ceritifikacna autorit - https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project

3. Reakcia na bezpečnostné incidenty

Všeobecný odporúčaný postup (pre väčšie organizácie):

1. Vyhodnotiť dopady a závažnosť udalosti, následne môže alebo nemusí prísť k eskalácii úloh smerujúcich na tím kybernetického zabezpečenia/ochrany dát.
2. Zrealizovať technické alebo forenzné vyšetrovanie a určiť stratégiu na zamedzenie šírenia škôd, obmedzenie dopadu incidentu a alternatívne riešenie.
3. Začať oznamovací proces (v súlade s GDPR).
4. Vytvoriť plán obnovy na zmiernenie dopadov. Je nutné okamžite realizovať krízové kroky na zamedzenie šírenia problému, napríklad umiestniť postihnuté systémy do karantény. Je možné naplánovať dlhodobé kroky nápravy, ktoré je možné realizovať, až keď pominie bezprostredné riziko.
5. Vytvoriť následnú analytickú správu, ktorá uvádza podrobnosti incidentu a ktorej cieľom je revidovať zásady, procesy a postupy, aby sa udalosť nemohla opakovať.

Záver

A čo povedať záverom? Bezpečnosť informačných systémov je komplex procesov na rôznych úrovniach s cieľom ochrániť to najcenejšie – „dáta". Je zrejmé, že pracovné postupy v jednotlivých knižniciach, ako aj kdekoľvek inde, sa môžu vzájomne odlišovať, čo vyplýva z viacerých faktorov. Rovnako môžeme povedať, že vyšší stupeň automatizácie týchto procesov so sebou prináša zároveň aj elimináciu rizík. Samozrejme si to vyžaduje kvalitnú analýzu jednotlivých postupov a zapracovanie vyššie uvedených prvkov bezpečnosti v každom kroku, kde systém zabezpečuje prístup k dátam, vrátane dát, ktoré sú do systému vkladané už na úrovni prihlasovania sa do systému. Automatizáciou dokážeme tiež eliminovať riziká, nakoľko je známe, že automatizácia eliminuje ľudskú chybovosť.

Naviac, správna automatizácia prácu uľahčuje, pričom klasická evidencia dát so sebou prináša nevyhnutnosť zaviesť ďalšiu evidenciu, čo je práca naviac. Dôležité je uvedomiť si fakt, že všetko, o čom sme hovorili vyššie, je proces, ktorý nikdy nekončí a ostražitosť v tomto smere je stále dôležitejšia ako kedykoľvek predtým. Technológie, s ktorými sa spája, podobne ako čokoľvek iné, majú dve strany, vedia byť veľmi nápomocné a užitočné, ale na druhej strane neskutočne nebezpečené, a to, čo „včera" bolo nereálne a nepredstaviteľné, „dnes" je úplne automatické. Preto by malo byť v záujme každého z nás, aby sme bezpečnosť mali na pamäti pri každom našom kroku. Ako sa k tomu staviate?

Zoznam použitej literatúry:

O'BRIEN, R. (2016). Privacy and security: The new European data protection regulation and it's data breach notification requirements. *Business Information Review*, *33*(2), 81–84. *https://doi.org/10.1177/0266382116650297*

BAILEY, J. (2018). Data Protection in UK Library and Information Services: Are We Ready for GDPR? *Legal Information Management*, 18(1), 28-34. doi:10.1017/S1472669618000063

Ing. Nadežda Andrejčíkov, PhD.
andrejcikova@cosmotron.cz

Ing. Libor Piškula
piskula@cosmotron.cz
(Cosmotron Bohemia, s. r. o.)

Mgr. Henrieta Gabrišová, PhD.
henrieta.gabrisova@stuba.sk
(Slovenská informatická knižnica, STU)