Informačná bezpečnosť

Ing. Eva Oláhová, PhD.
CIT FEM SPU v Nitre

Obsah

1. Úvod do informačnej bezpečnosti

Informačná bezpečnosť súvisí so zabezpečením informáciami v procesoch spracovania, uchovávania, používania, distribúcie a ich konečnej likvidácie. V súčasnosti Internet obsahuje obrovské množstvo informácií rozličného charakteru a významu. Ide napríklad o informácie organizácií a firiem (výrobnotechnické znalostí, finančné údaje, informácie o zákazníkoch), ale aj informácie, ktoré o sebe zverejňuje jednotlivec prostredníctvom internetových služieb a interakcii s nimi. Časť týchto informácií je neverejná, množstvo informácií je však verejne publikovaných a dostupných.

Trendom súčasnosti je prevaha digitálneho spracovania informácií organizácií a podnikov prostredníctvom informačných a komunikačných technológií (IKT). Podľa prieskumu spoločnosti AirSlate (2024) 75 % organizácií už spracúva všetky svoje dokumenty digitálne, respektíve minimalizuje používanie papiera. Digitálne spracovanie informácií zvýšilo efektívnosť ich spracovania, negatívom je možná zraniteľnosť organizácie pri ich krádeži, resp. zničení. Dôsledkom krádeže/poškodenia môže byť strata dobrého mena a dôvery zákazníkov, alebo narušenie činnosti organizácie, resp. verejných služieb (napr. výpadok riadiaceho systému dopravy, služieb e-health, e-government, univerzitného informačného systému). Preto je z hľadiska bezpečnosti dôležitým faktorom chodu organizácií spoľahlivé fungovanie vybudovanej informačnej a komunikačnej infraštruktúry, ktorá vzhľadom na existenciu vo virtuálnom kybernetickom priestore často presahuje hranice štátu. Internet je verejne dostupnou celosvetovou sieťou vzájomne prepojených počítačových sietí s nepretržitou vzájomnou komunikáciou a množstvom spracovávaných informácií uložených v osobných počítačoch, notebookoch, mobilných telefónoch, cloudových úložiskách, kde sú vystavené možným bezpečnostným hrozbám. ***Bezpečnosť uložených informácií každého počítača je podmienená úrovňou bezpečnosti iného počítača, ku ktorému sú pripojené.*** (Whitman a Mattord, 2012).

1.1. Definícia pojmu informačná bezpečnosť

Vo všeobecnosti je bezpečnosť stav bez nebezpečenstva, tj. ochrana pred protivníkmi. Informačná bezpečnosť sa zameriava na ochranu informácií v akejkoľvek forme. Existuje viacero definícií informačnej bezpečnosti, napríklad:

- Informačná bezpečnosť je súbor pravidiel, postupov pre ochranu ***informácií v tlačenej a digitálnej podobe*** pred neoprávneným prístupom, použitím, zverejnením, úpravou, kontrolou, zaznamenaním alebo zničením.
- ***Medzinárodná norma ISO/IEC 27002 (2005)*** definuje informačnú bezpečnosť ako zachovanie ***dôvernosti, integrity a dostupnosti*** informácií. Je to ochrana informácií pred celým radom hrozieb s cieľom zabezpečiť kontinuitu podnikania, minimalizovať obchodné riziko a maximalizovať návratnosť investícií a obchodných príležitostí.
- ***Inštitút SANS*** - informačná bezpečnosť sa týka ***procesov a metodík***, ktoré sú navrhnuté a implementované ***na ochranu tlačených, elektronických alebo akýchkoľvek iných foriem dôverných, súkromných a citlivých informácií a údajov*** pred neoprávneným prístupom, použitím, zneužitím, zverejnením, zničením, pozmenením alebo prerušením.
- ***Európsky parlament a Rada EÚ*** - bezpečnosť sietí a informačných systémov je ***schopnosť sietí a informačných systémov*** odolávať na určitom stupni spoľahlivosti akémukoľvek

konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov.

1.2. Model informačnej bezpečnosti

V zmysle základnej definície informačnej bezpečnosti bol definovaný základný model informačnej bezpečnosti. Model vychádza z charakteristík informácií, ktoré sú pre bezpečnosť dôležité a ich narušenie je kritické. Model sa označuje ako ***triáda CIA*** alebo ***trojuholník CIA*** (Obrázok 1) a bol prvým priemyselným štandardom pre oblasť bezpečnosti v období sálových počítačov.

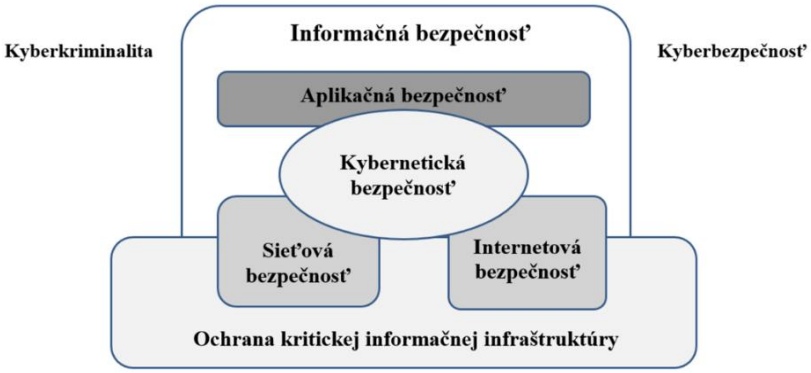
Obrázok 1 Model CIA
Zdroj: Gerensner (2020)

Model popisuje tri základné charakteristiky informácií:

- **Confidentiality** (dôvernosť) znamená, že informácie nie sú prístupné neoprávneným osobám alebo systémom. Dôvernosť zaručuje, že iba používatelia, ktorí majú príslušné práva a oprávnenia majú k informáciám prístup.
- **Integrity** (integrita) znamená, že informácie sú v pôvodnej forme a v pôvodnom stave, sú úplné a bez narušenia (neboli zmenené, zmanipulované alebo poškodené). Integrita informácií je podstatnou vlastnosťou informačných systémov, pretože ak si používatelia nemôžu overiť „pravosť“ informácií, nemajú pre nich žiadnu hodnotu.
- **Availability** (dostupnosť) znamená zabezpečenie včasného a spoľahlivého prístupu k informáciám, schopnosť mať k dispozícii informácie keď sú potrebné. Umožňuje autorizovaným používateľom/počítačovým systémom prístup k informáciám bez prekážok a ich prijímanie v požadovanom formáte a čase.

1.3. Informačná a kybernetická bezpečnosť

V praxi sa pojem informačná bezpečnosť často zamieňa s pojmom kybernetická bezpečnosť. I keď sa vo všeobecnosti oba pojmy týkajú bezpečnosti informácií, ich obsah a „rozsah“ je odlišný. Ich vzájomnú súvislosť a prepojenie znázorňuje Obrázok 3.



Obrázok 2 Informačná a kybernetická bezpečnosť
Zdroj: ISO/IEC 27032:2012

Informačná bezpečnosť

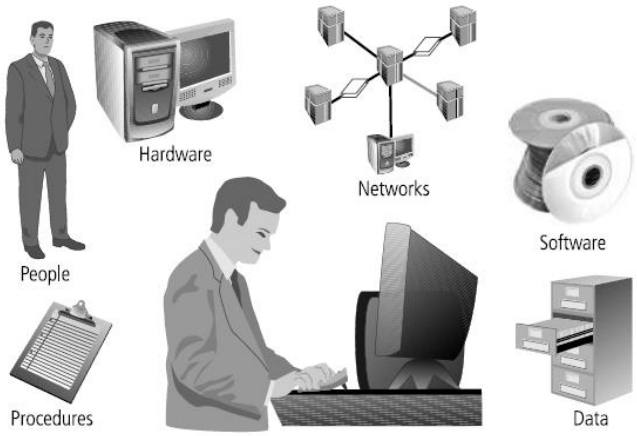
- Informačná bezpečnosť ***je širšou kategóriou***.
- Informačná bezpečnosť je súbor pravidiel, postupov na ochranu informácií ***v tlačenej a digitálnej forme*** pred neoprávneným prístupom, použitím, zverejnením, úpravou, kontrolou, zaznamenaním alebo zničením s cieľom zabezpečiť dôvernosť, integritu a dostupnosť informácií. Informačné aktíva nemusia byť nevyhnutne v kybernetickom priestore.
- Týka sa procesov a nástrojov na ochranu citlivých informácií a informačných systémov.
- Je kľúčovou súčasťou kybernetickej bezpečnosti.
  (IT Governance. n.d.)

Kybernetická bezpečnosť

- Kybernetická bezpečnosť ***je podmnožinou*** informačnej bezpečnosti.
- Kybernetická bezpečnosť je súbor pravidiel, postupov na ochranu informácií ***v elektronickej a digitálnej forme***, ktoré sa nachádzajú v počítačoch, úložných zariadeniach a sieťach (tj. v kyberpriestore).
- Cieľom je ochrana kybernetického priestoru – tj. sietí, intranetov, serverov, informačných, a počítačových systémov a infraštruktúry pred útokmi, neoprávneným prístupom alebo poškodením.
  (ISO/IEC, 2012)

2. Informačná bezpečnosť organizácie

Pre organizácie sú informácie dôležité pre ich chod, bez správnych informácií môžu vznikať chyby v kľúčových procesoch. V súčasnosti v organizáciách prevláda elektronická forma spracovania informácií prostredníctvom počítačových systémov, kde samotné spracovanie zabezpečuje komplexné softvérové riešenia - informačný systém a podporné aplikačné programy. Z pohľadu informačnej bezpečnosti je ***informačný systém*** organizácie ucelený súbor ľudí, procedúr a postupov, technických prostriedkov (hardvér, softvér, siete) a dát, ktoré zabezpečujú požadovanú funkčnosť a poskytujú informácie pre definovaný účel (Obrázok 3). Tieto komponenty umožňujú automatický zber, prenos, uchovanie, transformáciu, aktualizáciu a prezentáciu informácií pre potreby organizácie. Podľa Whitmann a Mattord (2012) má každý z uvedených komponentov silné a slabé stránky, vlastné charakteristiky a použitie. ***Každý komponent IS má aj svoje vlastné bezpečnostné požiadavky.***



Obrázok 3 Komponenty IS
Zdroj: Whitmann a Mattord (2012)

2.1. Klasifikácia zložiek informačnej bezpečnosti z pohľadu organizácie

Cieľom informačnej bezpečnosti organizácie je ochrana informačných aktív spracovávaných informačným systémom na všetkých úrovniach spracovania. Z pohľadu organizácie ide o ***mnohostranný systém s viacerými úrovňami zabezpečenia informácií***. Pre klasifikáciu jednotlivých zložiek je rozhodujúca je forma spracovania informácii - v klasickej, papierovej forme alebo v elektronickej forme. V prípade papierovej formy spracovania informácií je bezpečnosť zameraná na fyzickú bezpečnosť a definovanie oprávnení a prístupov pre osoby, ktoré s nimi pracujú (tj. procedurálna a personálna bezpečnosť). V prípade elektronickej formy spracovania prostriedkami IKT sa bezpečnosť rozširuje o ďalšie požiadavky na bezpečnosť: hardvéru, softvéru, sietí a komunikačných kanálov. Podľa uvedeného zložky informačnej bezpečnosti možno vymedziť nasledovne:

- ***Fyzická bezpečnosť*** - ochrana ***hardvéru*** pred poškodením (servery, PC, mobilné telefóny, sieťová infraštruktúra, systémy pre ukladanie údajov: diskové polia, cloud, napájacie zdroje, záložné zdroje), ale vo všeobecnosti aj ochrana objektov, priestorov pred neoprávneným prístupom a zneužitím.
- ***Sieťová a komunikačná bezpečnosť*** - ochrana ***počítačovej siete a komunikačnej infraštruktúry*** (lokálna počítačová sieť a prepojenia s verejnými sieťami, sieť Wifi, kabeláž, pripojenia a obsah). Prepojením lokálnej počítačovej siete organizácie do Internetu sa jej informačné zdroje stavajú potenciálnym zdrojom útoku.
- ***Aplikačná bezpečnosť*** - ochrana ***softvéru*** (operačné systémy, aplikačný softvér systémové a vývojové nástroje) je považovaná za najnáročnejšiu súčasť zabezpečenia informačného systému a aplikácií (využívanie chýb, slabých stránok, dier v programovaní softvéru).
- ***Informačná bezpečnosť*** je zameraná na ochranu i***nformácií a údajov*** (dokumenty, databázy, systémová dokumentácia a manuály, archivované informácie, súbory súvisiace s bezpečnosťou - súbory hesiel, IP adries, mailových adries, výstupy v papierovej forme). Vzhľadom na množstvo a rôznorodosť typov a formátov informácií vyžaduje ich klasifikáciu podľa významu pre organizáciu a k tomu definované postupy zabezpečenia.
- ***Personálna bezpečnosť*** je zameraná na ochranu ***jednotlivca, skupiny oprávnených osôb*** a ich prístupu k informačným zdrojom (manažéri podniku, administratívni pracovníci, správcovia, používatelia). V literatúre sú ľudia považovaní za najslabší článok informačnej

bezpečnosti pre rôzne dôvody (nedostatočná vzdelanosť v IKT technológiách, poškodenie alebo strata informácií, sociálne inžinierstvo a manipulácia).

- ***Procedurálna a prevádzková bezpečnosť*** je zameraná na ***procedúry a postupy*** pre spracovanie a používanie informačných aktív. Nedostatočná znalosť používaných procedúr a postupov zo strany koncových používateľov môže viesť k ohrozeniu IS. Prevádzková bezpečnosť je zameraná na ochrana podrobností o konkrétnej činnosti, resp. sérii aktivít.

Systém riadenia informačnej bezpečnosti na úrovni podniku patrí do celkového podnikového riadenia. Východiskovým písomným dokumentom je **Bezpečnostná politika**, ktorý obsahuje súhrn bezpečnostných požiadaviek a opatrení pre informačnú bezpečnosť na úrovni fyzickej, počítačovej, komunikačnej, personálnej a administratívnej. Z pohľadu podniku bezpečnostná politika by mala odpovedať na základné otázky:

- Čo je potrebné chrániť?
- Prečo je to potrebné chrániť?
- Ako to budeme chrániť?
- Ako postupovať v prípade zlyhania opatrení?

V praxi je bezpečnostná politika organizácie riešenia formou interných predpisov - smerníc pre jednotlivé oblasti informačnej bezpečnosti (napríklad smernica o kybernetickej bezpečnosti, smernica o kamerovom systéme, smernica o ochrane osobných údajov). Podmienkou je, aby s uvedenými dokumentami boli oboznámení všetci zamestnanci, resp. používatelia s prístupom k podnikovým informačným zdrojom. Povinnosťou organizácie je zabezpečenie permanentného vzdelávania zamestnancov v oblasti informačnej bezpečnosti.

3. Informačná bezpečnosť a jednotlivec

Dnešný svet charakterizuje obrovský nárast digitalizácie vo všetkých oblastiach nášho života - čoraz viac služieb a transakcií sa presúva online. Tradičné služby sú transformované do digitálnej podoby a „presunuté“ do online prostredia. Prístup jednotlivca k týmto službám vyžaduje vytvorenie digitálnej identity, ktorá je analogická s jeho fyzickou identitou v reálnom svete. Služby sa stávajú dostupnejšími a poskytujú jednotlivcom časovo a geograficky neobmedzený prístup k informáciám, osobnému rozvoju, vzdelávaniu, komunikácii a sociálnej interakcii, spolupráci. Nevýhodou virtuálnej identity jednotlivca sú negatívne prejavy spojené s jej možným zneužitím, manipuláciou, ale aj prejavmi ako je kyberšikana a strata priamej sociálnej komunikácie ľudí.

3.1. Vymedzenie pojmu digitálna identita a digitálna bezpečnosť

Digitálne identity sú potrebné na zabezpečenie dôvery ľudí voči poskytovateľom online služieb a naopak a ich vzájomným online interakciám. Tieto identity sú úzko spojené so skutočnou identitou jednotlivca/organizácie. Existuje viacero definícií digitálnej identity:

- Digitálna identita je zvyčajne definovaná ako vzťah jedna k jednej medzi človekom a jeho digitálnou prítomnosťou. Digitálna prítomnosť môže pozostávať z viacerých účtov, poverení a oprávnení spojených s jednotlivcom.

- Digitálna identita sú všetky digitálne informácie, ktoré sa používajú na preukázanie identity jednotlivca online a ktoré umožňujú používateľom interakciu a transakcie vo virtuálnom svete. Tieto informácie sú neprenosné a opätovne použiteľné.
- Digitálna identita je online reprezentácia osoby, organizácie alebo subjektu. Pozostáva zo všetkých prepojených digitálnych údajov a informácií, ako je meno, e-mailová adresa, profily sociálnych médií a online správanie.

Digitálna identita jednotlivca obsahuje citlivé/osobné informácie, napríklad:

- Osobné údaje (meno a priezvisko, dátum a miesto narodenia, vodičský preukaz, povolanie, pracovisko, rodné číslo, e-mail, IP adresa, zdravotné záznamy)
- Používateľské poverenia (prihlasovacie údaje, heslá, biometrické údaje)
- Záznamy online správania a interakcií (verejne publikované príspevky, komentáre, fotografie, videá, história prehliadania, vyhľadávacie dotazy)

Tieto informácie môžu byť odcudzené a zneužité na spáchanie podvodu voči ich vlastníkovi alebo na spáchanie podvodu v mene vlastníka. S ochranou jednotlivca v digitálnom priestore sa spája pojem digitálna bezpečnosť.

Digitálna bezpečnosť je ochrana digitálnej identity a obsahuje súbor osvedčených postupov a nástrojov používaných na ochranu osobných údajov a online identity v online priestore. Príkladmi nástrojov: webové služby, antivírusový softvér, biometrické a bezpečné osobné zariadenia, programy pre správu hesiel, rodičovskú kontrola. V digitálnej bezpečnosti je rozhodujúce vzdelávanie koncového používateľa a jeho proaktívny prístup k ochrane svojej identity, osvojenie si osvedčených postupov a praktík zabezpečenia svojich online aktivít.

Príklady zneužitia digitálnej identity:

- Krádež identity: neoprávnený prístup k osobným údajom napríklad na získanie falošných dokladov totožnosti, otvorenie podvodných účtov.
- Porušenie súkromia jednotlivca: poskytnutie osobných údajov poskytovateľa služby tretím stranám bez súhlasu vlastníka identity alebo únik informácií v dôsledku hackerského útoku (napríklad hromadné krádeže identít používateľov populárnych sociálnych sietí, online služieb, aplikácií).
- Phishingové útoky: krádež finančných informácií.
- Kyberšikanovanie, obťažovanie zastrašovanie.
- Monitorovanie pohybu osôb prostredníctvom využitím geolokačných údajov používaných zariadení (PC, mobil, Smart hodinky).
- Sociálne inžinierstvo: podvrhnuté e-maily (v mene zamestnávateľa, banky) s cieľom získať citlivé informácie alebo kliknúť na škodlivé odkazy.

3.2. Digitálna stopa

Mnohé online služby a aktivity zvyčajne vyžadujú overenie digitálnej identity jednotlivca, ale mnohé z nich zhromažďujú informácie automaticky (často bez vedomia jednotlivca). Na internete sa nachádza obrovské množstvo ***verejne dostupných*** osobných, pracovných údajov jednotlivcov/organizácií. Používaním online služieb a svojimi online aktivitami jednotlivec vytvára digitálnu stopu. Digitálna stopa sa zaznamenáva vždy, keď

používateľ používa online službu alebo vykonáva akúkoľvek sledovateľnú online činnosť. Definície digitálnej stopy:

- Digitálna stopa je dátová stopa vytvorená online aktivitami používateľa a stopami, ktoré po sebe úmyselne alebo neúmyselne zanecháva.
- Digitálna stopa (označovaná aj ako digitálny tieň) je sledovateľný údaj a činnosť, ktoré používateľ zanecháva na internete.

Charakteristiky digitálnej stopy:

- Digitálna stopa je trvalou a nezmazateľnou súčasťou online existencie jednotlivca.
- Digitálna stopa rastie permanentne s každou online aktivitou používateľa alebo sledovaním aktivít používateľa webovými stránkami/aplikáciami.
- Digitálna stopa zohráva významnú úlohu pri vytváraní online reputácie používateľa.
- Zabezpečenie a správa obsahu digitálnej stopy poskytuje ochranu pred kriminálnymi činmi a podvodmi.

Typy digitálnej stopy:

- Pozri prezentáciu v LMS Moodle.

Poznámka: texty ku kapitole 4 a 4.1 sú v prezentácii publikovanej v LMS Moodle

4. Právo a Internet

4.1. Legislatíva Slovenskej republiky v oblasti informačnej, kybernetickej a digitálnej bezpečnosti

Použitá literatúra

AIRSLATE. *Paperless Office 2022: How post-pandemic workplace behavior is shifting towards efficiency*. In: *airSlate Blog* [online] 2024. Dostupné na: https://www.airslate.com/blog/paperless-office-workplace-behavior-survey/?source=landing

BEYONDTRUST. n.d. *Definition of digital identity*. In: *BeyondTrust* [online] n.d. Dostupné na: https://www.beyondtrust.com/resources/glossary/digital-identity

DASHLANE. 2024. *What is a digital footprint and why is it important?* In: *Dashlane* [online] 2024. Dostupné na: https://www.dashlane.com/blog/what-is-a-digital-footprint.

DOCK. n.d. *Digital Identity: The ultimate guide 2024*. In: *sDock Labs.* [online] n.d. Dostupné na internete: https://www.dock.io/post/digital-identity#introduction

GERENSER, Mike. 2020. *The security triad*. In: *REDCOM* [online] 2020. Dostupné na: https://www.redcom.com/security-triad/.

Information. *BussinessDictionary.* [Online] Web Finance Inc. Dostupné na: http://www.businessdictionary.com/definition/information.html.

ISO/IEC 27002:2005. *Online Browsing Platform.* [Online]. 2005. Dostupné na: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-1:v1:en.

ISO/IEC 27032:2012. *Information—Security Techniques—Guidelines for Cybersecurity.* [online]. 2012. Dostupné na: https://www.iso.org/standard/44375.html

IT Governance. n.d. What is Cyber Security? In *IT Governance Cyber security solutions* . [online] n.d. Dostupné na: https://www.itgovernance.co.uk/what-is-cybersecurity.

SANS. *SEC401: Security Essentials - Network, endpoint, and cloud*. In: *SANS Institute* [online] Dostupné: https://www.sans.org/information-security/

SEDLÁK, Petr, KONEČNÝ, Martin. *Kybernetická (ne)bezpečnost: Problematika Bezpečnosti V Kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021. s.428. ISBN: 978-80-7623-068-2.

Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii. *EUR-Lex.* [online] Dostupné na: http://data.europa.eu/eli/dir/2016/1148/oj.

VERIZON. n.d. *What is a digital footprint?* In *Verizon* [online] n.d. Dostupné na: https://www.verizon.com/about/blog/digital-footprint-definition-examplens-and-ways-reduce

WHITMAN, Michael E., MATTORD, Herbert J. *Principles of Information Security*. Boston, MA: Course Technology, 2012. s. 658. ISBN-13: 978-1-111-13821-9.