INTERNETOVÁ BEZPEČNOSŤ NA SLOVENSKU

PhDr. Emanuel Orban, PhD.

emoorbo@gmail.com
emanuel.orban@statistics.sk

Štatistický úrad SR

The aim of the article is to raise awareness of questions about internet security currently being discussed by experts in the field of social sciences. It defines the methodological apparatus applied in relation to internet security and the resulting problems for the use of certain online media. Based on the results of this analysis, the article then sets out the measures necessary to ensure the protection of personal/confidential data in the online space. As a Member State of the European Union, the Slovak Republic is obliged to improve the security of information systems by emphasising the importance of digital literacy in the pedagogical and work environment.

Keywords: internet security, protection of personal data, information and communication technologies

Obr. 1 Internetová bezpečnosť. Zdroj: © 2022 Investree

ÚVOD

Internet je najrozšírenejší mediálny prostriedok v globálnom význame, čo sa týka vyhľadávania, sprostredkovania a distribúcie informácií. Patrí do kategórie nových médií spolu s videom a káblovou televíziou (Charvát-Šefčák 1998).

Internet má v súčasnosti nezastupiteľnú úlohu takmer v každej domácnosti, pretože predstavuje pre užívateľa kľúčový zdroj informácií o významných spoločenských, kultúrnych udalostiach, okrem toho nachádzame na ňom aj zaujímavé rady z bežného života a prostredníctvom neho realizujeme aj viaceré systémové operácie (napr. platobné prevody, úhrada faktúry, objednávanie tovaru, rezervácia podujatí a pod.). K spomínanému účelu sú prispôsobené rezervačné portály, prípadne online systémy v oblasti bankovníctva, cestovného ruchu, informatizácie a pod. Internet poskytuje nespočetné množstvo výhod, ktoré sa väčšinou vzťahujú k praktickému využitiu. Hlavnou výhodou internetu je úspora času, vďaka rýchlemu internetovému pripojeniu prostredníctvom bezdrôtového charakteru tzv. sieť WiFi, optického kábla (router napr. Huawei HG 8245H) s neobmedzenou kapacitou prenosu množstva dát, zákazník si vybaví v pohodlí domova danú požiadavku v priebehu niekoľkých minút, čiže nemusí chodiť osobne na vybrané klientske centrum.

Významné telekomunikačné spoločnosti (Slovak Telekom, Orange, UPC Slovensko a pod.) poskytujú výhodné balíčky služieb pre domácnosti s týmito novinkami – internet, televízia a telefón v jednom. Uvedené pripojenie je dostupné bežnému užívateľovi prostredníctvom prenosnej skrinky tzv. modemu, sieťového produktu, ktorý garantuje prechod od analógového signálu na digitálny. Na sieťovom produkte je vyobrazené internetové pripojenie s názvom WiFi siete a kľúčovým heslom (kombinácia číslic, písmen, malých a veľkých znakov). Znakom funkčnosti operačného procesu je displej so zeleným vyobrazením, ak je červenej farby, pripojenie nie je dostupné v dôsledku opotrebovania modemu alebo nedostatočného pokrytia signálu v odbernom mieste (domáce spotrebiče sú väčšinou inštalované v obývacej izbe, plniacej status odbytiska dostupných informácií, kde užívateľ trávi väčšinu času dňa). V prípade spomínaných technických problémov zákazník má možnosť obrátiť sa prostredníctvom telefonického kontaktu na kompetentného pracovníka vybraného klientskeho

centra. Technický pracovník telekomunikačnej spoločnosti ako prevádzkovateľ multifunkčnej siete spoločnosti zákazníka naviguje, častokrát sa tu využíva služba hlasového videohovoru. Služba hlasového videohovoru cez mobilný internet predstavuje typický unikát, pretože je výhodná nielen pre užívateľa, ale aj pre firemného pracovníka, ktorému taktiež ušetrí čas a s ním spojené náklady.

Internet predstavuje významné interaktívne médium, ktorého význam spočíva v efektívnom využití viacerých služieb užívateľom prostredníctvom rôznorodých aktivovaných technických vymožeností (analógový, digitálny signál, káblová sieť a pod.). Význam digitalizácie v online prostredí je orientovaný na zoskupení veľkého množstva dát do malého súboru tzv. komprimovaného priečinku (ZIP formát), externých pamäťových zariadení (USB kľúč, pamäťové karty) a pod. S využitím princípov tzv. virtuálnej reality sa stretávame v rámci online komunikačného kanála YouTube VR ponúkajúceho široké spektrum herných programov (napr. preteky so žralokmi, preteky Formule 1) s technológiou 3 D (virtuálna realita – bezpečnostné okuliare), ktorej sú dokonca prispôsobené jednotlivé mobilné aplikácie.

Príspevok poukazuje na kľúčovú úlohu internetu ako vysokorýchlostného multimédiá v súvislosti s jednotlivými operačnými systémami, vo všeobecnosti zdôrazňuje princípy interaktivity a digitalizácie ako dôležité špecifiká publikovania v online priestore, definuje pojem internetová bezpečnosť a jej celkový vplyv na spoločnosť. Cieľom nášho úsilia je na základe analýzy sprístupniť verejnosti obraz o stave internetovej bezpečnosti v domácnostiach na Slovensku.

POJEM INTERNETOVÁ BEZPEČNOSŤ

Internetová bezpečnosť podľa stanov Eurostatu zahŕňa viacero systémovo prijímaných opatrení, kontrolných mechanizmov a metodických postupov s cieľom zabezpečiť integritu, autenticitu, dostupnosť, dôvernosť údajov a systémov IKT.

Bezpečnostná politika IKT definuje kľúčových aktérov a ich zodpovednosť pri riešení kolízií, dokonca sa zmieňuje aj o pohotovostných plánoch, ktoré vyplývajú zo vzniknutej problémovej situácie (*Are you looking for statistics on internet security?* 2018). Dátové súbory sa zaoberajú bezpečnosťou IKT, konkrétne identifikujú problémy užívateľov internetu vzťahujúce sa najmä k prístupu k osobným informáciám pomocou softvérových aplikácií. Internetová bezpečnosť je legislatívne podchytená príslušnými orgánmi Európskej únie. V decembri 2015 bol ratifikovaný Európskym parlamentom a členskými štátmi EÚ historicky prvý dokument – *Nariadenie o informačnej a sieťovej bezpečnosti kritickej infraštruktúry* (angl. *Concerning the European Union Agency for Network and Information Security*, pozn. autora). Uvedené nariadenie prispieva k zlepšeniu zabezpečenia a odolnosti digitálnej infraštruktúry voči kybernetickým útokom, či dokonca k prehĺbeniu spolupráce členských štátov. Obsah jednotlivých nariadení sa vzťahuje ku konkrétnym osobám, konkrétne k veľkým internetovým predajcom, vyhľadávačom a cloudom podávajúcich správy o závažných incidentoch a prijímaní opatrení na riadení rizík (Bacigál, Hajdúková a Hlavička 2017). Legislatívne nariadenie je zárukou správneho fungovania bezpečnosti v systéme riadenia digitálnych médií.

Internetová bezpečnosť je nevyhnutná pri manipulácii s informáciami predstavujúcimi konkrétne súbory dát, ktoré sú uložené na príslušnom počítačovom serveri. Hlavný význam internetovej bezpečnosti je objasnený v tejto definícii: „Informačná bezpečnosť má multilaterálny charakter, t. j. musí zohľadňovať záujmy vlastníkov IKT systémov, potreby ich používateľov, ako aj práva fyzických a právnických osôb, ktorých údaje sa v systémoch spracovávajú. Z hľadiska používateľov sú pri spracovaní informácie najdôležitejšie tieto faktory: účel a obsah informácií, presnosť, aktuálnosť, prístupnosť, autenticita, usporiadanie a kvalita informácií. Z hľadiska vlastníkov a prevádzkovateľov je najdôležitejší spoľahlivý prístup k informačným zdrojom s prístupom on-line a ich zabezpečenie pred únikom informácií, neoprávneným použitím a narušením integrity údajov, ako aj autorita a dobré meno vlastníka systému“ (*Národná stratégia* 2008, s. 4). Internetová bezpečnosť a jej pozitívna odozva závisí najmä od rešpektovania základných technických a etických zásad. Od uvedených faktorov závisí fungovanie celého informačného systému. Technickí pracovníci zohrávajú významnú úlohu pri zabezpečení pripojenia na internet, čiže musia bezpodmienečne dodržiavať vhodnú postupnosť jednotlivých krokov podľa rámcového návodu (používateľskej príručky s technickým nákresom obvodov) príslušnej firemnej organizácie. Etické hľadisko v oblasti internetovej bezpečnosti je taktiež potrebné akceptovať, pretože súvisí s predpísanými pravidlami štábnej kultúry, väčšinou

je dané spoľahlivosťou pracovníka (precíznosť inštalácie pripojovacích káblov, konektorov a pod.) a jeho správnym rešpektom ku klientovi (zdvorilý prístup, ochota). V rámci rozvoja informačných technológií je potrebné venovať špecifickú pozornosť otázke spravovania a zverejňovania informácií, za čo plne zodpovedá správca programu, pretože ide aj o dôležitú etickú záležitosť: „Správca programu má morálnu povinnosť pristupovať zodpovedne k zvereným informačným aktívam… Závažnosť etického problému sa vzťahuje predovšetkým k bezpečnosti systému a ochrane šírených údajov, a to napr. pri počítačovom útoku na program, či už zo strany užívateľov alebo aj nečlenov organizácie. Z praxe sú známe početné prípady neoprávnených prístupov k počítačovým systémom, resp. prípady zlyhania zabezpečenia ich ochrany. Poskytovatelia IT služieb alebo odborní technickí pracovníci spravidla najlepšie rozumejú možným hrozbám tohto druhu. Od zodpovedného správcu programu sa očakáva ešte v prípravnej fáze projektu prijať opatrenia, ktoré by eliminovali výskyt podobných hrozieb“ (Ukropová 2012, s. 152-153). Správca programu má konať v súlade so stanovami stratégie internetovej bezpečnosti, pretože zodpovedá za bezpečnú realizáciu informačných služieb. Internetová bezpečnosť je vo všeobecnosti inštitucionálne podchytená čo sa týka medzinárodných dní a sviatkov v globálnom význame. Každoročne si pripomíname Svetový deň bezpečného internetu, ktorý slávime vo februári. Väčšinou sa k nemu neodmysliteľne vzťahuje propagácia bezpečného a zodpovedného používania online technológií a mobilov (deti, mladí ľudia).

Stratégia internetovej bezpečnosti obsahuje konkrétne plány a riešenia vyznačujúce sa precíznosťou a ambicióznosťou. Jednotlivé strategické materiály schvaľuje vláda. Strategické plánovanie, ktoré rešpektuje uvedené kritériá predstavuje vynikajúcu cestu k úspechu pri budovaní príslušného bezpečnostného povedomia. V praxi stratégia definuje konkrétne úlohy na dosiahnutie úrovne bezpečnostného povedomia:

A „zvyšovanie úrovne poznania občanov, komerčných a nekomerčných organizácií, verejných inštitúcií o rizikách spojených s používaním IKT

Obr. 2 Svetový deň bezpečného internetu. Zdroj: Národný bezpečnostný úrad

a možnostiach ochrany pred hrozbami pomocou internetu, masovokomunikačných prostriedkov a metodických materiálov,

B rozšírenie vzdelávania (začlenenie základov informačnej bezpečnosti do výučby informatiky na školách),

C zavedenie programov zvyšovania bezpečnostného povedomia a kompetentnosti používateľov IKT so zvláštnymi nárokmi na informačnú bezpečnosť" (*Národná stratégia* 2008, s. 10).

Hlavným zámerom stratégie informačnej bezpečnosti je prispieť ku skvalitneniu online služieb v oblasti informatiky a pedagogiky. V tejto súvislosti dôležitú úlohu zohráva online vzdelávanie so zameraním na problematiku informačnej bezpečnosti v školských a firemných inštitúciách. Informácie môžu byť veľmi užitočné aj pre jednotlivcov v domácnostiach.

V súvislosti s domácnosťami je potrebné vo všeobecnosti neustále apelovať na zvýšenie pozornosti užívateľov pri počítačových operáciách a technických úkonoch v rámci inštalácie programových balíkov a optických káblov. Dôležitú úlohu tu zohráva manažment rizík zahŕňajúci aj oblasť informačných a komunikačných technológií: „Samotná výpočtová technika je z hardwarového i softwarového pohľadu zdrojom rizík úplného zničenia požadovaných informácií. Na druhej strane môže byť zdrojom informačných rizík aj prenos informácií. Výroba a služby a ich bezproblémové fungovanie sú priamo závislé od včasnosti a úplnosti informácií" (Šimák 2006, s. 36). Z tohto hľadiska je potrebné konať v predstihu a opatrne pri technologických postupoch, obzvlášť pri manipulácii s výpočtovou technikou, aby sme predišli problémovým situáciám. Správne nasadenie bezpečnostnej stratégie je mimoriadne dôležité, pretože zásadne ovplyvňuje celkový proces využitia informačných technológií.

OPATRENIA NA ZABEZPEČENIE INTERNETOVEJ BEZPEČNOSTI

K internetovej bezpečnosti sa vzťahuje viacero preventívnych opatrení, ktoré garantujú ochranu osobných údajov v emailovej komunikácii, pri bezhotovostnom platobnom styku, na sociálnych sieťach, na internetových prehliadačoch a pod. Preventívne opatrenia predstavujú kľúčové východisko eliminácie vzniknutých problémov v online prostredí pomocou bezpečnostných riešení. Na realizáciu priebehu daných riešení dohliadajú kompetentní pracovníci technických služieb, čiže im sa pripisuje aj patričná etická zodpovednosť.

Technickí pracovníci firemnej organizácie zodpovedajú za inštaláciu programového softvéru a správne technické pripojenie počítačového zariadenia v domácnostiach. Prispievajú k vytváraniu pozitívneho imidžu firmy, ktorého kľúčovým ukazovateľom je spokojnosť zákazníkov, a preto by mali disponovať patričnou kvalitou po odbornej stránke. Firemní technickí pracovníci sú skúsení IT manažéri, pohybujúci sa vo verejnom sektore, väčšinou ide o špecialistov na vnútropodnikovú komunikáciu (intranet prístupný pre užívateľa z miesta výkonu práce, vo výnimočných prípadoch aj z domova) a databázových marketingových pracovníkov pracujúcich s bázou veľkého množstva dát (úsek geografického informačného systému, vizualizácia údajov – konkrétne ide o výsledky práce počítačových grafikov, napr. diagramy a pod.).

Obr. 3 Antivírusová ochrana proti počítačovému vírusu. Zdroj: Agentúra@virusovo.sk

Súčasťou databázového marketingu je i ochrana osobných údajov na internete pred vírusovým zneužitím (napr. phishing, pharming, malware, trójsky kôň a pod.) Deštrukčné účinky počítačových vírusov spočívajú nielen v tom, že poškodzujú hardvér a softvér počítačového zariadenia, ale aj môžu napáchať obrovské škody pre samotných klientov.

Phishing (lovenie hesiel) môžeme definovať ako určitú formu vydierania zákazníka prostredníctvom neoprávneného získavania osobných údajov (mena a hesla) s cieľom ich bezbrehej diskreditácie najmä fyzickej povahy (napr. krádež informácií, finančného konta). Ide tu o vopred premyslenú a cielenú formu útoku. Podobný účel významu má i služba pharming, ktorá najčastejšie prostredníctvom internetového bankovníctva dokáže v priebehu niekoľkých minút pripraviť zákazníka o úspory. V jej centre pozornosti stoja vynaliezaví hackeri, ktorí sa dokážu bez problémov napojiť na server a vykradnúť jeho celkovú databázu obsahu. Zákazník vo víre každodenných povinností si mnohokrát ani neuvedomí, že sa pri platobných operáciách prihlásil na falošnú repliku online portálu vytvoreného hackerom, ktorá je vo viacerých prípadoch podobná stránke portálu banky, keď to zistí, je už neskoro. Kľúčovou podstatou malwaru je odcudzenie uložených informácií na počítačovom zariadení, no v súčasnosti riziku napadnutia týmto typom vírusu sú väčšinou vystavené smartfóny. Mimoriadne záškodnou formou malwaru je Botnet. Ide o automatický program riadený príslušným operátorom na diaľku. Hlavným zdrojom infekcie je legálne a nelegálne sťahovanie (Petrowski 2014). Ak chce užívateľ smartfónu predísť uvedeným komplikáciám, musí si nainštalovať správny bezpečnostný softvér a jeho štandardné produkty – antivírus, antispam a firewall. Trójsky kôň je počítačový vírus spôsobujúci deštrukciu takmer celého online systému, najčastejšie prostredníctvom nevyžiadaných príloh k emailovým správam a spustenia nežiaducich súborov užívateľom, čím sa naruší dôveryhodnosť softvéru. Deštruktívne trójske kone častokrát nahrádzajú spustiteľné súbory za bežné príkazy. V praxi trójsky kôň nahrádza kópie súborov (príkazov), v rámci ktorých užívateľ skopíruje súbor príkazným výberom a následne spôsobí vírus (Cameron 1996). Vírusové programy je možné eliminovať prostredníctvom inštalácie antivírusových programov napr. NOD, AVG a ESET. Antivírusové programy predstavujú vhodnú ochranu voči možným kybernetickým útokom na uložené dáta a hardvér. Ich inštalácia je veľmi dôležitá, až priam nevyhnutná, čo sa týka zachovania bezpečnostného softvéru v rámci rozvoja informačných technológií.

Ochrana osobných údajov sa prevažne vzťahuje k zberu terénnych dát podľa legislatívy členských krajín Európskej únie, pretože ide aj o ich celkovú sumarizáciu – archiváciu údajov v internetovom prostredí na príslušnom nosiči, napr. USB kľúč, priečinky Total Commander, prístup je výlučne určený pre oprávnené osoby, kde vstup je podmienený špecifickým heslom. Prihlasovacie heslo je potrebné meniť a pravidelne aktualizovať, pretože častokrát sú súbory napadnuté nežiaducimi škodcami tzv. hackermi a potom ľahko dochádza k úniku a následnej strate informácií. Hackeri sú počítačoví zločinci, predstavujúci dokonca skupinu registrovaných užívateľov na diskusnom fóre príslušného online portálu, ktorí šíria svoje skúsenosti vedúce k nezákonnému prístupu do siete a následnej destabilizácii počítačového systému prostredníctvom nápomocných bulletinov systémov elektronických vývesiek tzv. BBS – Bulletin Board Systems (Cameron 1996).

S podobnou situáciou sa stretávame aj v emailovej komunikácii, typickým príkladom je portál centrum.sk, ktorej obeť útoku býva psychicky vydieraná pod hrozbou finančnej pokuty, zverejnenia citlivých informácií, zastrašovania a pod. Ide o tzv. emailové červy, medzi ktoré patria vírusy typu Mellisa a ILOVEYOU. Iniciátormi uvedených akcií sú hackeri. Je potrebné preto prijať špecifické bezpečnostné opatrenia chrániace záujmy skupín registrovaných užívateľov, zväčša treba uplatniť sprísnený overovací prístup užívateľov do informačnej siete, ktorých identita by mala byť v dostatočnej miere preverená, čo je aj predmetná záležitosť administrátorov webovej stránky či portálu sociálnych sietí a pod. Administrátor ako kľúčová osoba, plniaca mimochodom status spravovateľa informácií, má vykonávať dostatočný dozor nad uverejnením príspevkov rôznych užívateľov, ak je nežiaduci (útok na ľudskú dôstojnosť, rasová, náboženská neznášanlivosť a pod.) je povinný ho zmazať a prípadne navždy zablokovať prístup kompromitovanému autorovi.

Uvedené záležitosti chrániace záujmy ostatných online užívateľov vo svojej platforme rieši aj *Etický kódex elektronických médií* (2010), ktorý vydáva Asociácia internetových médií na Slovensku, jeden z jeho článkov zahŕňa aj túto formuláciu: „Okrem rešpektovania užívateľových preferencií vyjadrených buď priamo v odpovedi odosielateľovi, alebo prostredníctvom účasti v programe preferovanej služby je potrebné zabezpečiť opatrenia, aby ani marketingová komunikácia a ani iné aplikácie umožňujúce užívateľom otvorenie iných marketingových a reklamných správ, nenarušovali užívateľovi bežné používanie elektronických médií.“ *Etický kódex elektronických médií* deklaruje významné etické zásady, ktorými sú transparentnosť a nerušenie bežného užívania daného online médiá.

Internetová bezpečnosť je mimoriadne dôležitá pri vzájomnej komunikácii medzi zákazníkom a užívateľom, pretože svojím spôsobom garantuje ochranu osobných údajov pred zneužitím, konkrétne vzťahuje sa k nej inštalácia bezpečnostného softvéru počítača, antivírusového programu a antispamového filtra (firewall). Brána firewall predstavuje zásadnú bariéru medzi jednotlivými sieťami, na základe vopred naprogramovaného súboru pravidiel sa dá pristúpiť k analýze príslušnej sieťovej prevádzky (Vaculík 2018).

S pravidlami internetovej bezpečnosti sa stretávame aj pri významných elektronických identifikačných postupoch, napr. v bankovníctve zariadenie token slúžiace na autorizáciu informačných systémov prostredníctvom PIN kódu, kryptografického kľúča s digitálnym podpisom alebo biometrických dát s odtlačkom prsta. V súvislosti s prenosom citlivých údajov v online bankovníctve je potrebné zmieniť sa o bezpečnostnom protokole Secure Sockets Layer (ďalej SSL), neskôr i Transport Layer Security (ďalej TLS) chrániaci prenos IP paketov prostredníctvom využitia šifrovacieho kódu (Petrowski 2014).

V súvislosti s internetovým bankovníctvom sa využíva vo veľkej miere aj karta s čítačkou, prostredníctvom ktorej sa užívateľ bezpečne prihlási do systému, následne potvrdí realizované platobné operácie a telefonicky kontaktuje vybrané call centrum. Čítačka kariet zabezpečuje bezpečnú úschovu financií užívateľa, manipulácia s ňou je veľmi jednoduchá, navyše je možnosť stiahnuť ju do vybraného mobilného zariadenia vo forme aplikácie. V občianskom preukaze so špeciálnym zabudovaným systémovým aktivovaným čipom sú uložené informácie o osobných údajoch, ale aj o zdravotnom stave užívateľa, pretože je tam prepojenie na európsky preukaz zdravotného poistenia. Ak sú obidva osobné doklady aktivované pri kontakte (dotyku) s elektronickým snímačom údajov, na počítačovej obrazovke sa automaticky objavia uvedené dáta.

V emailoch, prípadne sociálnych sieťach sa uplatňuje systém jednoduchého prihlasovania príslušným užívateľom prostredníctvom mena a hesla. Nie je žiaduce, ak prihlasovacie údaje (heslo) na portál emailu a na príslušnú sociálnu sieť sú totožné. V tomto prípade riskujeme väčší útok hackerov na naše konto. Podobne sa treba taktiež vyhnúť aj funkcii automatického prihlásenia do informačného systému bez príslušnej opakovanej registrácie. Funkcia zapamätania dát sa mnohokrát nevyplatí, pretože sa sociálna sieť môže stať terčom útokov hackerských skupín. V rámci hackerských skupín väčšinou ide o tzv. jedincov trpiacich psychickými poruchami osobnosti s neustálou potrebou vyhrážania sa, zastrašovania a vydierania aj bez relevantnej príčiny: „V súčasnosti nie je ťažké dostať sa do e-mailu iného používateľa alebo na konto sociálnej siete, a to najmä v prípade detí a dospievajúcich, ktorí používajú rovnaké heslá na viacerých doménach. Veľmi často sa stáva, že sa z jednotlivých kont neodhlasujú, ani v prípade, keď nie sú aktívni na internete, prípadne prítomní v miestnosti, kde si nechali zapnutý počítač alebo mobil s pripojením na internet. V takejto situácii nie je ťažké zneužiť neprítomnosť osoby, ‚skryť' sa pod cudziu identitu a rozposielať nevhodné komentáre, fotografie, videá a i. Takéto správanie následne môže vyvolať nielen emocionálnu ujmu u osoby, ktorá sa stala obeťou zneužitia svojho konta, ale aj osoby, ktorá sa stála príjemcom negatívnych, urážlivých a inak dehonestujúcich kyberútokov" (Hollá 2017, s. 69). Sociálne siete (Facebook, Pokec, Instagram a pod.) sú ohniskom zverejnenia inkriminovaných informácií (fotografií detí a mladistvých, väčšinou ide o dospievajúce vekové kategórie, pozn. autora) dokonca hraničiacich s pornografiou, ktoré predstavujú ľahkú korisť pre jedincov trpiacich pedofíliou: „Obete prežívajú strach z vystupňovania šikanovania a kyberšikanovania, pretože anonymita kyberpriestoru ‚chráni' kyberagresorov. To vysvetľuje, prečo sa žiaci najmenej zdôverujú pedagogickým a nepedagogickým pracovníkom" (Hollá 2017, s. 104). Nutná je preto osveta v podobe pedagogických školení s citlivým prístupom pre žiakov/študentov so zameraním na informačnú, digitálnu a mediálnu gramotnosť. Užívateľ dospievajúcej vekovej kategórie si musí presne ujasniť, ktoré informácie a fotografie zverejnení na danom sociálnom médiu, čiže mal by postupovať opatrne a prezieravo. Morálnou povinnosťou rodičov alebo poverených osôb je neustále kontrolovať užívateľský profil sociálnej siete dieťaťa a mladistvého, pretože plne zodpovedajú za ochranu súkromia daných osôb. V kolíznom prípade je potrebné znemožniť prístup na internetové stránky s nevhodným obsahom prostredníctvom inštalácie blokovacieho softvéru.

Blokovací typ softvéru zamedzuje prístup vekovej kategórie detí a mladistvých k pornografii, k videám s násilným obsahom, s propagáciou drog, netolerancie a iných subkultúr. Uvedenú službu využívajú aj viacerí mobilní operátori (*Ako chrániť svoje dieťa* 2020). Prevencia formou diskusie na pálčivé témy (rozhovory rodičia a deti) je nevyhnutná, pretože prispieva k zabezpečeniu bezpečnosti v online prostredí, no nie vždy dokáže naplniť patričný účel.

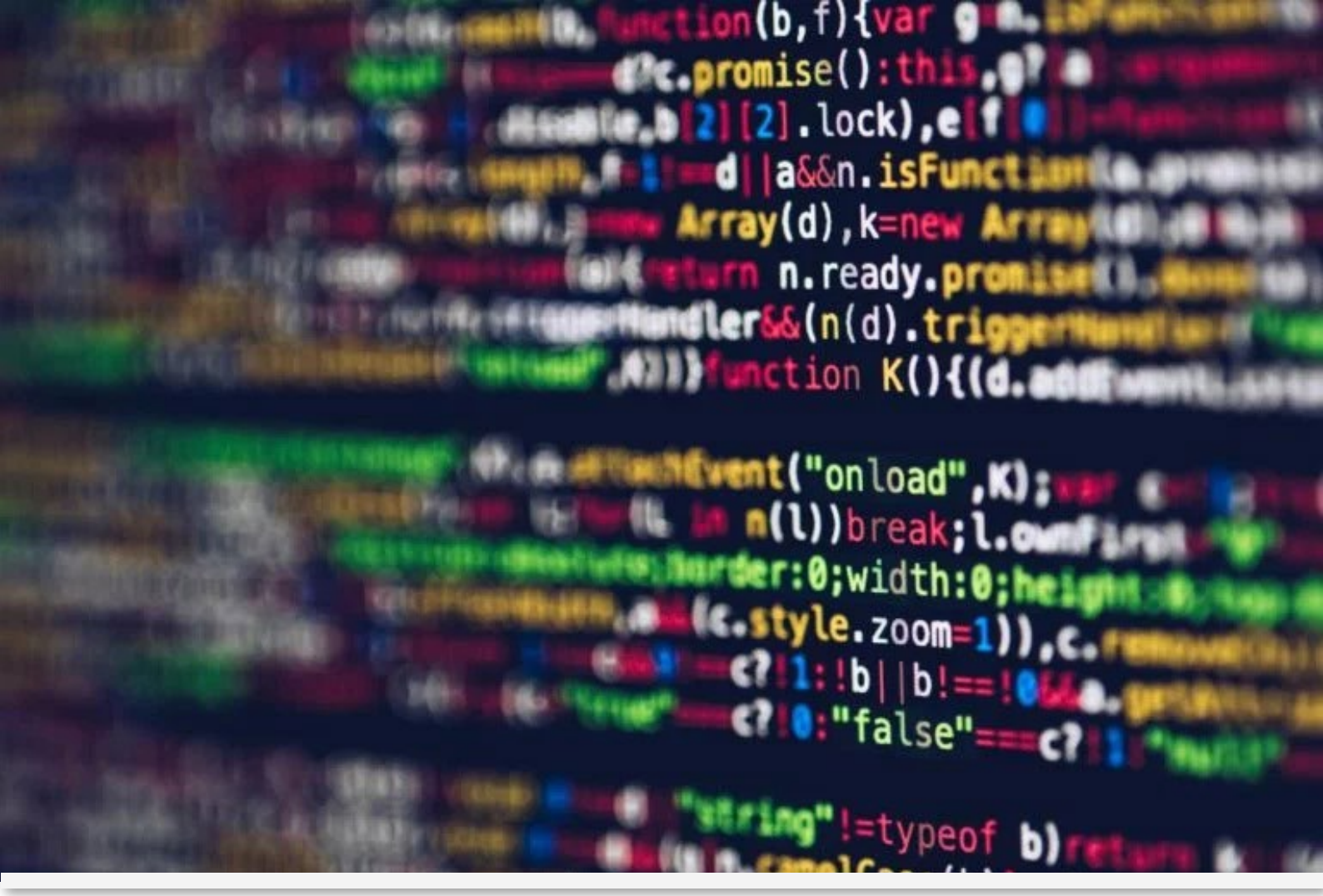
Preventívny a osvetový aspekt obsahujú dva významné projekty s inovatívnym potenciálom Zodpovedne.sk a Stopline.sk. Ich prínos vystihuje poradenská psychologička Jarmila Tomková: „Občianske združenie eSlovensko hrá v mediácii bezpečného používania internetu významnú rolu. Realizuje projekt Zodpovedne.sk, podporovaný Európskou komisiou v rámci komunitárneho programu Safer Internet. V rámci neho prevádzkuje Centrum bezpečného internetu Zodpovedne.sk, ktorého cieľom je zvyšovanie povedomia, šírenie osvety o zodpovednom používaní internetu, nových technológií a prevencia pred trestnými činmi" (Tomková 2012, s. 2). Žiaci základných a študenti stredných škôl majú možnosť oboznámiť sa s projektom, ktorý podporuje mediáciu Zodpovedne.sk v rámci hodín výučby mediálnej výchovy. Podobné aktivity vyvíja i Národné centrum pre nahlasovanie nezákonného obsahu na internete: „Národné centrum pre nahlasovanie nezákonného obsahu alebo činností na internete Stopline.sk bojuje proti zneužívaniu detí (detská pornografia, sexuálne vykorisťovanie, detská prostitúcia, obchod s deťmi, grooming atď.), proti rasizmu a xenofóbii a inému obsahu alebo činnostiam, ktoré vykazujú znaky trestného činu. Prostredníctvom neho sa Slovensko zapojilo do medzinárodnej siete INHOPE – siete národných centier a organizácií pre bezpečnosť informačných technológií" (Tomková 2012, s. 13). Projekt má v súčasnosti mimoriadne opodstatnenie, pretože spomínané problémy vykazujúce znaky trestného činu (nárast kriminality, extrémizmu, zneužívania detí a mládeže) sú zo spoločenského hľadiska aktuálne.

V súčasnom rozvoji informačných technológií je potrebné napĺňať myšlienky osvety prostredníctvom výchovno-vzdelávacích programov, ktoré budú ponúkať konkrétne riešenia slúžiace na elimináciu daného problému. V školskom prostredí by sa mala internetovej bezpečnosti venovať náležitá pozornosť už od prvého stupňa základných škôl, v rámci ktorého sa žiaci oboznámia so základnou terminológiou v oblasti internetu (čo je hardvér, softvér, prečo vzniká počítačový vírus a pod.) a úkonmi bežného používateľa (ako zapnúť/vypnúť počítač, ako si otvoriť jednotlivé programy WORD, EXCEL a pod.). V súčasnosti jedinec už v období mladšieho školského veku dokáže ovládať tablet, prípadne smartfón a robiť základné operácie (surfovanie po internete, chatovanie na sociálnych sieťach a pod.).

Aj v oblasti štátnej správy sa stretávame s kurzami internetovej a kybernetickej bezpečnosti. „ŠÚ SR informačnú bezpečnosť chápe ako súhrn a uplatnenie bezpečnostných opatrení a postupov slúžiacich v rámci informačných a komunikačných systémov pred narušením dôvernosti, integrity, práv občanov na ochranu osobných údajov, autentickosti a dostupnosti údajov, a schopnosti s nimi pracovať v rozsahu pridelených oprávnení. Kybernetickú bezpečnosť ŠÚ SR vníma ako schopnosť informačných a komunikačných systémov odolávať na určitom stupni spoľahlivosti náhodným udalostiam alebo škodlivým aktivitám v kybernetickom priestore" (*Politika kybernetickej* 2020). Štatistický úrad predmetný kurz formou cyklického školenia každoročne realizuje od decembra 2020. Predmetným cieľom kurzu je celková ochrana údajov pred narušením ich dôvernosti, integrity, k čomu sú prispôsobené aj jednotlivé bezpečnostné opatrenia. „Permanentné vzdelávanie v oblasti informačnej bezpečnosti je veľmi dôležité, pretože hrozieb a rizík je stále viac. Používateľov IT je preto potrebné systematicky informovať a zvyšovať ich povedomie v oblasti informačnej bezpečnosti. Ide najmä o informovanie zamestnancov o typoch možných bezpečnostných incidentov, existencii bezpečnostných smerníc v podniku, postupoch pri nahlasovaní vzniknutých bezpečnostných incidentov a pod. Modernou formou vzdelávania sú kurzy vypracované formou e-learningu, ktoré môže každý zamestnanec absolvovať sám, vlastným tempom a pri svojom počítači" (Hennyeyová 2013, s. 38). V rámci kurzov informačnej bezpečnosti sa účastník oboznámi so základnými pracovnými postupmi pri riešení bezpečnostných udalostí-incidentov, distribúcii súborov s citlivými údajmi v oblasti personalistiky a celkovými pravidlami fungovania informačných systémov. Informačné systémy súvisia väčšinou so správnou heslovou politikou (pravidelná aktualizácia, obmieňanie tri razy do roka, zablokovanie za pomoci správcu informačných technológií).

V súvislosti s ochrannými opatreniami dôležitú úlohu zohrávajú aj príslušné internetové prehliadače. Užívateľ si prostredníctvom internetového prehliadača zobrazí obľúbenú webovú stránku, ide o programové softvéry (obr. 4) typu Internet Explorer (IE), Mozilla Firefox (MF), Opera (O), Google Chrome (GCH).

Do špecifickej kategórie patrí aj internetový prehliadač malého dátového (textového) súboru tzv. cookies, ktorý je inštalovaný v smartfóne a tablete. Spustenie súboru prehliadača cookies sa realizuje prostredníctvom funkcie v spomínaných programových softvéroch. Stránky súborov cookies sú uložené v prehliadačoch IE, MF, O a GCH (*Informácie o používaní cookies* 2022). Kom-



Obr. 4 Programový softvér. Zdroj: Paneurópska vysoká škola

plexne prispievajú ku skvalitneniu štruktúry a obsahu internetových služieb, konkrétne k zvýšeniu informačnej bezpečnosti. Návštevnosť jednotlivých webových stránok sa meria pomocou nástroja Google Analytics, ktorý sumarizuje vybranú skupinu užívateľov.

Softvér anti-tracking slúži na zabránenie akéhokoľvek sledovania užívateľa a jeho činnosti na internete. Má špecifický názov AVG AntiTrack. Bez inštalácie daného typu softvéru hackerské skupiny nemajú problém zistiť o užívateľovi takmer všetky citlivé informácie vzťahujúce sa k jeho bankovým údajom, zdravotným informáciám, histórii navštívenia webových stránok, rodinným informáciám, nastaveniu prehliadača a pod. (*AVG AntiTrack* 2020). Antitrackingový nástroj je spojený s nastavením obrannej funkcie v prehliadači Internet Explorer, jednou z jeho typických alternatív je služba Do Not Track Me (ďalej DNTM), ktorej význam spočíva v integrácii dát do prenosového mechanizmu. Inštalácia danej služby okamžite zastaví proces nežiaduceho prenosu dát z prehliadača smerom k iným webovým stránkam (Petrowski 2014). Ide o užitočný nástroj, čo sa týka zabezpečenia ochrany údajov na internete, ktorý je veľmi vyhľadávaný užívateľmi.

K skvalitneniu bezpečnostných služieb v online prostredí prispieva aj služba siete VPN, ide o komplexný balík produktu AVG Secure. Produkt AVG Secure predstavuje bezpečnú Wi-Fi sieť bezpodmienečne chrániacu činnosť užívateľa v online prostredí v rámci týchto činností – surfovanie, bankovníctvo, online nákupy, emaily, chaty a pod. Pri inštalácii siete AVG Secure sa automaticky zablokuje činnosť reklám a zamaskuje sa stopa prehliadača pomocou tzv. šifrovania údajov, ide o 256-bitový štandard AES. Uvedený typ bezpečného prehliadača prispieva k väčšej ochrane súkromia užívateľa.

Význam bezpečnostných opatrení spočíva v zabránení narušenia normálneho fungovania IKT v organizáciách najmä na národnom záujme. Koncepcia informačnej bezpečnosti spočíva v 3 dôležitých krokoch:

a prevencia – ochrana pred hrozbami,
b detekcia – odhalenie neoprávnenej činnosti a zraniteľné miesta v systéme,
c náprava – odstránenie zraniteľného miesta v systéme (Bacigál, Hajdúková a Hlavička 2017).

Zachovanie jednotlivých správnych krokov prispieva k navýšeniu efektívnej kapacity daného online médiá.

Štatistiky prístupu domácností na internet vykazujú za Slovenskú republiku tieto výsledky, konkrétne počty boli zverejnené Eurostatom v rokoch 2016 – 81 % a 2021 – 90 % (Digital economy and society statistics – households and individuals, Eurostat).

Počet pripojení domácností na internet každoročne narastá, čo potvrdzujú aj viaceré štatistiky informačnej gramotnosti Slovenskej republiky. Enormný nárast využitia informačných a komunikačných technológií evidujeme v členských krajinách Európskej únie: „Význam informačných a komunikačných technológií sa zdôrazňuje aj v Európskej únii, kde sa dokonca považujú za hlavnú hnaciu silu európskeho hospodárstva. Informačným a komunikačným technológiám sa v EÚ vďaka technologickému pokroku a investíciám v tomto odvetví pripisuje od roku 1995 polovica rastu produktivity práce…" (Fabová 2014, s. 68). V informačnej spoločnosti je preto nevyhnutné vytvoriť podmienky na podporu moderného a konkurencieschopného hospodárstva. Pretože narastá význam digitálnych technológií v kontexte spoločenského rozvoja Európskej únie: „Občania a podniky v EÚ sa čoraz častejšie pripájajú na internet, viac nakupujú on-line a sebavedomejšie a zručnejšie sa pohybujú v oblasti IKT. Zvýšenie digitálnych zručností je kľúčové pri budovaní európskej digitálnej spoločnosti" (Želonková 2015, s. 78). Znalosť informačných technológií je v dnešnej dobe nevyhnutná, pretože svojím vplyvom prispievajú k odstráneniu bariér sociálnej komunikácie.

ZÁVER

Internetová bezpečnosť je cieľavedomý proces stanovenia kvalít jednotlivých informačných systémov. Je súčasťou legislatívy členských štátov Európskej únie, preto sa na pôde parlamentu vedú častokrát diskusie o úskaliach obsahu zverejneného na internete a prijímajú sa jednotlivé preventívne opatrenia. S informačnou bezpečnosťou súvisí riešenie bežných problémov pri využívaní internetu. Najčastejšie ide o stratu údajov na počítačovom zariadení v dôsledku vírusového útoku, zneužitia osobných údajov cez internet (fotografií, videí), ďalej finančnú stratu v dôsledku presmerovania užívateľa na falošné webové lokality, infiltráciu podvodných správ, realizáciu podvodov s platobnou kartou a pod. Bezpečnostná politika IKT závisí od kvality informácií (webových stránok) prezentovaných v online priestore za čo v plnej miere zodpovedá správca príslušného počítačového programu, ktorý svojím úsilím prispieva k bezpečnostnej stratégii. Pracovníci technických služieb preberajú kompetenciu nad inštaláciou programového softvéru anti-tracking vzťahujúceho sa k zabráneniu činnosti sledovania pohybu osôb v online priestore. V tejto súvislosti je potrebné apelovať na posilnenie významu pedagogických školení zameraných na preventívnu ochranu programov pred vírusovým zneužitím a jednotlivými úskaliami vyplývajúcimi z morálno-etických rizík.

ZOZNAM POUŽITÝCH ZDROJOV

Ako ochrániť svoje dieťa pred nevhodným obsahom na internete [online]. 2020. Projekt je spolufinancovaný EÚ programom Connecting Europe Facility. Partnermi projektu sú Ministerstvo školstva, vedy, výskumu a športu SR, Úrad podpredsedu vlády SR pre investície a informatizáciu a Linka detskej istoty. Bratislava: eSlovensko Bratislava o. z. [cit. 2022-09-09]. Dostupné na: https://www.zodpovedne.sk/index.php/sk/ohrozenia/nevhodny-obsah-na-internete

AVG AntiTrack. Vždy, keď ste na internete, spoločnosti využívajú vašu „digitálnu stopu" na sledovanie vašich činností. Zabránime tomuto sledovaniu a poskytneme vám skutočné súkromie [online]. AVG 1988 – 2020. Bratislava: Solitea Slovensko, a. s. [cit. 2022-09-09]. Dostupné na: https://www.avg.com/sk-sk/antitrack#pc

European Commission – Eurostat – Products Eurostat News – Are you looking for statistics on internet security?: Eurostat Your Key to European Statistics [online]. 2018. Luxemburg: Eurostat [cit. 2022-09-09]. Dostupné na: https://ec.europa.eu/eurostat/en/web/products-eurostat-news/-/WDN-20180206-1

BACIGÁL, Ivan, HAJDÚKOVÁ, Tatiana a Lukáš HLAVIČKA, 2017. *Bezpečnosť online komunikácie a ochrana dát*. Bratislava: Akadémia Policajného zboru. 175 s. ISBN 978-80-8054-690-8.

CAMERON, Debra, 1996. *Security Issues for the Internet and the World Wide Web*. Charleston: Computer Technology Research Corp. 218 s. ISBN 1-56607-973-X.

Digital economy and society statistics – households and individuals. Eurostat Statistics Explained. Internet access of households [online]. 2016 and 2021. Luxemburg: Eurostat. [cit. 2022-09-09]. Dostupné na: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals

Etický kódex elektronických médií [online]. 2010. Bratislava: IAB Slovakia – Združenie pre internetovú reklamu. [cit. 2022-09-19]. Dostupné na: https://www.iabslovakia.sk/wp-content/uploads/2014/10/IABsk-Eticky-kodex-elektronickych-medii.pdf

FABOVÁ, Ľudmila, 2014. IKT – hybná sila ekonomického rozvoja. *Journal of knowledge society (časopis znalostní společnosti)*. Brno: Knowler – Evropský institut pro výzkum, inovace a vzdělávání, z. s. [online]. **2**(2), 64-74 [cit. 2022-10-12]. ISSN 2336-2561. Dostupné na: jks_2014_02_064-074_Fabova.pdf (euin.org)

HENNYEYOVÁ, KLÁRA, 2013. Bezpečnostné aspekty využívania IKT v podnikoch. In: *Informačné a komunikačné technológie v riadení a vzdelávaní*. Zborník príspevkov z medzinárodného vedeckého seminára 1. marec 2013 [online]. Nitra: Katedra informatiky FEM SPU v Nitre 2013. s. 35-39 [cit. 2022-10-12]. ISBN 978-80-552-0983-8. Dostupné na: 978-80-552-0983-8.pdf (slpk.sk)

HOLLÁ, Katarína, 2017. *Detekcia kyberagresie – kyberšikanovania a sextingu*. Nitra: Pedagogická fakulta UKF. 113 s. ISBN 978-80-558-1205-2.

CHARVÁT, Juraj a Ľuboš, ŠEFČÁK, 1998. *Médiá a politika*. Bratislava: TATRAPRESS, spol. s. r. o. 63 s. ISBN 80-967754-3-X.

Informácie o používaní cookies. Odpadová aplikácia ELO. Firmy, obce, spracovatelia odpadov [online]. [cit. 2022-09-09]. Dostupné na: https://elo.sk/informacie-o-pouzivani-cookies/

Národná stratégia pre informačnú bezpečnosť v Slovenskej republike [online]. 2008. Bratislava: Ministerstvo financií Slovenskej republiky. 20 s. [cit. 2022-09-09]. Dostupné na: SK_NCSS_2009_sk (2).pdf

PETROWSKI, Thorsten, 2014. *Bezpečí na internetu. Pro všechny*. (Preložil Tomáš Kurka). Liberec: Dialóg: knižní velkoobchod a nakladatelství. 243 s. ISBN 978-80-7424-066-9.

Politika kybernetickej a informačnej bezpečnosti. Interná smernica: Oddelenie krízového riadenia, bezpečnosti IS a utajovaných skutočností. 2020. Bratislava: Štatistický úrad SR.

ŠIMÁK, Ladislav, 2006. *Manažment rizík* [online]. Žilina: Fakulta špeciálneho inžinierstva. Žilinská univerzita. 116 s. [cit. 2022-09-09]. Dostupné na: Manazment_rizik (uniza.sk)

TOMKOVÁ, Jarmila, 2012. *Mediácia bezpečného používania internetu* [online]. Bratislava: Výskumný ústav detskej psychológie a patopsychológie. 16 s. [cit. 2022-09-09]. Dostupné na: prieskum eslovensko.pdf (iuventa.sk)

UKROPOVÁ, Silvia, 2012. Aplikácia ISO 26000 v etickom vzdelávaní využitím informačných technológií. In: FOBEL, Pavel, PALOVIČOVÁ, Zuzana, ORAVCOVÁ, Jitka a Helena ČIERNA, 2012. *Etika & poradenstvo & prax*. Banská Bystrica: Fakulta humanitných vied Univerzity Mateja Bela. s. 146-157. ISBN 978-80-557-0385-5.

VACULÍK, Juraj, 2018. *Od telemetrie k internetu vecí II. Dátová analytika, umelá inteligencia, bezpečnosť a digitálna ekonomika*. Žilina: EDIS-vydavateľské centrum Žilinskej univerzity. 205 s. ISBN 978-80-554-1522-2.

ŽELONKOVÁ, Vladimíra, 2015. Elektronické zručnosti a využívanie IKT domácnosťami na Slovensku. *Slovenská štatistika a demografia* [online]. Bratislava: Štatistický úrad Slovenskej republiky, **25**(4), 68-85 [cit. 2022-10-12]. ISSN 1339-6854. Dostupné na: https://ssad.statistics.sk/SSaD/