Univerzita Pardubice

Fakulta ekonomicko-správní

Analýza rizik internetového bankovnictví

Bakalářská práce

2019 Vojtíšková Pavlína

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2018/2019**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Pavlína Vojtíšková**
Osobní číslo:	**E16243**
Studijní program:	**B6208 Ekonomika a management**
Studijní obor:	**Ekonomika a provoz podniku**
Název tématu:	**Analýza rizik internetového bankovnictví**
Zadávající katedra:	**Ústav podnikové ekonomiky a managementu**

Zásady pro vypracování:

Cílem práce je analyzovat možná rizika online elektronického bankovnictví z hlediska uživatelského přístupu prostřednictvím internetu a návrh možných opatření.

Osnova:

- Možnosti přímého bankovnictví.
- Internetového bankovnictví a jeho rizika.
- Návrh možných opatření pro eliminaci rizik.
- Vyhodnocení a závěr.

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 60 stran**

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

Kim, Peter. HACKING - praktický průvodce penetračním testováním. Brno: Zoner Press, 2015. ISBN 978-80-7413-313-8.
Kožíšek, Martin a Písecký, Václav. Bezpečně na internetu. Praha: Grada Publishing, a.s., 2016. ISBN 978-80-247-5595-3.
Král, Mojmír. Bezpečný internet - Chraňte sebe i svůj počítač. Praha: Grada Publishing, a.s., 2015. ISBN 978-80-247-5453-6.
Mejstřík, Michal, Pečená, Magda a Teplý, Petr. Bankovnictví v teorii a praxi. Praha: Nakladatelství Karolinum, 2014. ISBN 978-80-246-2870-7.
Petrowski, Thorsten. Bezpečí na internetu. Liberec: Dialog, 2014. ISBN 978-80-7424-066-9.

Vedoucí bakalářské práce: **doc. Ing. Pavel Petr, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **3. září 2018**

Termín odevzdání bakalářské práce: **30. dubna 2019**

L.S.

doc. Ing. Romana Provazníková, Ph.D.
děkanka

doc. Ing. Marcela Kožená, Ph.D.
vedoucí ústavu

V Pardubicích dne 3. září 2018

Prohlašuji:

Tuto práci jsem vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury. Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 30. 11. 2019

Pavlína Vojtíšková

PODĚKOVÁNÍ

Tímto bych ráda poděkovala doc. Ing. Pavlu Petrovi, Ph.D. za odborné vedení, připomínky a rady při konzultacích k této bakalářské práci.

ANOTACE

Tato bakalářská práce je zaměřena na rizika internetového bankovnictví a jejich analýzu. V úvodních dvou částech jsou popsány současné možnosti využívání internetového bankovnictví v souvislosti s nejčastějšími hrozbami, kterým uživatelé internetového bankovnictví mohou čelit. V následujících dvou částech práce je zpracována analýza možných rizik internetového bankovnictví a předložen návrh opatření vedoucích k jeho bezpečnějšímu užívání. Práce dochází k závěru, že největší riziko v oblasti využívání internetového bankovnictví stále představuje uživatel sám.

Pro tuto práci byly čerpány informace jednak z knih, které se zabývaly problematikou bankovnictví, internetu a rizik internetu, jednak z internetových článků zabývajících se internetovým bankovnictvím a z webových stránek bank.

KLÍČOVÁ SLOVA

Analýza rizik, internetové bankovnictví, hrozby internetu, zabezpečení internetového bankovnictví

TITLE

Internet banking risk analysis

ANNOTATION

The present bachelor thesis focuses on internet banking risks and their analysis. The first two parts describe the current possibilities of internet banking in relation to the most frequent threats internet banking users may face. The following two parts present an analysis of possible internet banking risks as well as proposed measures aiming at safer use internet banking. The thesis draws the conclusion that it is still the user who represents the most serious risk in the area of internet banking.

The information used in this bachelor thesis was gathered from literature dealing with the issues of banking, internet and internet risks. Internet articles focused on internet banking and bank websites represent an additional source of information.

KEY WORDS

Risk analysis, internet banking, internet threats, internet banking security

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM ZKRATEK A ZNAČEK

BBS – Bulletin board system

ČS – Česká spořitelna

ČSOB – Československá obchodní banka

GSM – Groupe spécial mobile

HTTPS – Hypertext transfer protocol secure

KB – Komerční banka

PDA – Personal digital assistant

PIN – Personal identification number

RIPRAN – Risk project analysis

SIPO – Sdružené inkaso plateb obyvatelstva

SSL – Secure sockets layer

WAP – Wireless application protocol

WLAN – Wireless local area network

ÚVOD

Tématem této bakalářské práce je „Analýza rizik internetového bankovnictví“. Internetové bankovnictví je dnes velmi populární a jistě i v budoucnosti bude nepostradatelnou součástí našeho běžného života. A je velmi pravděpodobné, že ještě ve větší míře než nyní. Všichni, kdo v současnosti používají IB, tak konají s vidinou úspory, především tím spoří čas a peníze. Časová úspora pro klienta banky znamená, že při využívání bankovních služeb není nijak časově limitován docházením do kamenné pobočky banky v pevně vymezenou pracovní dobu, protože mu je banka k dispozici 24 hodin denně 7 dní v týdnu. K přístupu postačuje jen vhodné elektronické zařízení a připojení k internetu.

Výsledkem časové úspory zpravidla bývá i úspora finanční, jak přesně vystihuje obecně známé rčení „čas jsou peníze“. Kromě toho úsporu peněz přináší i finančně výhodnější samoobslužné využívání možností bankovního účtu, kdy klient za zpoplatněné internetové bankovní transakce zaplatí méně než za zpoplatněné transakce uskutečněné v rámci klientských služeb na kamenných pobočkách bank.

Spolu s rostoucí oblibou internetového bankovnictví však zároveň přibývá útoků na jeho uživatele, potažmo útoků přímo na banky. Tato bakalářská práce se zaměřuje na zranitelná místa zejména na straně uživatelů internetového bankovnictví. Ze zcela pochopitelných důvodů je zabezpečení bank značně složité a informace o bezpečnostních protokolech nedosažitelné. Banky velmi dbají na svou pověst, a bezpečnost kladou na první místo, protože jakékoli pochybení při zajištění ochrany vkladů klientů a následná ztráta důvěry by pro ně mohly mít fatální důsledky. Z těchto důvodů není cílem této práce zabývat se dodržováním bezpečnosti ze strany bankovních institucí.

Je ovšem velmi zajímavé prozkoumat zvyklosti běžných uživatelů internetového bankovnictví, respektive uživatelů internetu jako celku, neboť oboje spolu úzce

souvisí. V každodenním životě naprostá většina z nás považuje za samozřejmé dodržovat běžná bezpečnostní opatření, jakými jsou například zavření oken a uzamčení vchodových dveří k bytu, popř. nastavení alarmu a vypuštění psa při odchodu z bydliště. Nezabezpečený byt by jistě vzbudil nejen všeobecný údiv, ale i nežádoucí zájem zlodějů. Otázky zabezpečení by při následné likvidaci pojistné události zcela určitě pečlivě zkoumala i příslušná pojišťovna.

Proto je pozoruhodné, jak rozdílně k otázce zabezpečení přistupují uživatelé internetu: stále není běžné používání dostatečně silných hesel a stále existuje většinová tendence používat jedno heslo pro mnoho aplikací. Aktualizace softwaru, které nabízejí výrobci zdarma, mnoho lidí obtěžují, a proto jsou spouštěny nepravidelně nebo vůbec. I na tento problém upozorňuje tato práce.

První kapitola je zaměřena na pojmy související s problematikou internetového bankovnictví. Vysvětluje způsoby možného využití internetového bankovnictví. Zabývá se základními pojmy, počátky přímého bankovnictví a způsoby, jakými lze realizovat přímé bankovnictví.

Druhá kapitola popisuje rizika, která mohou ohrožovat nejen uživatele internetového bankovnictví, ale internetu jako celku.

Třetí kapitola obsahuje analýzu rizika, a to nejprve z pohledu teoretického, kde jsou popsány základy nutné k rozboru rizika v jakémkoliv rozsahu, ať už se jedná o riziko podnikatelské nebo i zcela subjektivní. Jsou zde tedy uvedeny jednoduché rozbory pro každé riziko. Následuje část zaměřená přímo na analýzu rizik internetového bankovnictví. Inspirací se stala metoda RIPRAN, která je zde uzpůsobena zejména subjektivnímu užití analýzy rizik z pohledu uživatele internetového bankovnictví.

Ve čtvrté kapitole jsou vyjmenovány zásady bezpečného používání internetového bankovnictví. Tyto zásady vyvěšují na své stránky samotné banky a jsou v zásadě podobné u všech bankovních ústavů. Tato kapitola navíc obsahuje legislativní

opatření a popisuje i bezpečnostní postupy, které prozatím nejsou standardní, ale v oblasti zabezpečení představují budoucnost.

V kapitole číslo pět jsou shrnuty a zhodnoceny zásadní zjištění předcházejících kapitol.

CÍL PRÁCE

Cílem této bakalářské práce je odhalit, identifikovat a analyzovat možná rizika internetového bankovnictví z pohledu uživatele. Dále je cílem práce navrhnout opatření zvyšující bezpečnost online elektronického bankovnictví.

1 MOŽNOSTI PŘÍMÉHO BANKOVNICTVÍ

Historie přímého bankovnictví spadá do poloviny osmdesátých let, kdy se v USA objevily první systémy umožňující vzdálené připojení k bankovním účtům. Pod názvem „Home Banking“ bylo možné se telefonicky připojit k počítači banky a realizovat základní úkony. Tento způsob bankovnictví vznikl jako odpověď na restrikce, pro které bankovní domy neměly možnost provozovat filiálky v některých státech. V roce 1997 byla v USA uvedena do provozu první virtuální banka světa s názvem Security First Network Bank. Vymoženosti, jako jsou možnost návštěvy osobního účtu na internetu, kontrola a schopnost jednoduché operace, si od roku 2001 mohli vyzkoušet vkladatelé opět v Americe. [1]

V obecné rovině lze za platební produkty elektronického bankovnictví pokládat všechny bankovní produkty, při nichž je spojení mezi klientem a bankou realizováno elektronicky. Zákon o platebním styku určuje tyto dva způsoby elektronických platebních prostředků [2]:

- prostředek vzdáleného přístupu k peněžní hodnotě, kdy je požadována identifikace přiděleným osobním číslem, popřípadě jiným způsobem,
- elektronický peněžní prostředek, ve kterém je peněžní hodnota uložena elektronicky a který je posléze označován pojmem elektronické peníze.

Rozdíl mezi těmito označeními je zásadní. První znamená klasické použití platebních prostředků, avšak jiným způsobem nežli platbou v hotovosti, zatímco druhým způsobem se peníze transformovaly do elektronických peněz. [2]

Internetové bankovnictví a bankovnictví jako celek obsahuje velké množství pojmů, které je zapotřebí vysvětlit a tím vymezit prostor, ve kterém se tato práce bude pohybovat.

Platební styk a jeho zajištění je jedna z nejdůležitějších funkcí banky. Kvalitní platební styk udržuje stávající klienty banky a přivádí nové, má vliv i z pohledu profitability

(generuje přímé a nepřímé výnosy banky). Platební styk lze klasifikovat na základě mnoha kritérií, přičemž v této práci rozlišujeme zejména mezi hotovostním platebním stykem, kde dochází k předání fyzických peněz mezi plátcem a příjemcem (výběr z bankomatu, nákup za hotové atd.) a bezhotovostním platebním stykem, který je zásadně ovlivňován nárůstem digitálních technologií. Bezhotovostní platební styk se vyznačuje jako převod peněz zápisem na účtech plátce a příjemce. [3]

Bankovní platební styk lze realizovat bankovním převodem, inkasní formou placení, šekem, platební kartou, směnkou a elektronickými penězi. [3]

Elektronické bankovnictví – jsou to veškeré způsoby, kdy je kontakt mezi klientem a bankou prováděn elektronicky. Podle Zákona o platebním styku, zákon č. 370/2017 Sb. § 15, se za elektronický platební prostředek považuje komunikace s bankou podmíněná identifikací uživatele, k níž jsou použity následující komunikační nástroje: [3]:

- telefon (call-banking, phone-banking, GSM-banking, internet-banking);
- počítač (home-banking, internet-banking);
- adaptér Personal Digital Assistant (PDA-banking).

V následujícím výčtu jsou vyjmenovány možné způsoby používání přímého bankovnictví [2]:

a) BBS stanice,
b) komunikační programy,
c) vyspělé komunikační programy,
d) nejvyspělejší komunikační programy,
e) internet.

a) BBS stanice – poskytují možnosti použití elektronického bankovnictví totožné s kompatibilními médii, připojení probíhalo pomocí vytáčené telefonní linky a modemu [2].

b) Komunikační programy – využití k příkazům k úhradě i k inkasu v tuzemském platebním styku, poskytují výpisy z účtu a zůstatky na účtech [2].

c) **Vyspělé komunikační programy –** umožňují oproti předchozí možnosti navíc příkazy k úhradě v zahraničním platebním styku, avíza k tuzemským platbám, kurzovní lístek banky a poskytují textové informace klientům banky [2].
d) **Nejvyspělejší komunikační programy –** oproti svým předchůdcům nabízejí navíc i možnost zadání trvalých příkazů k úhradě a inkasu, ovládání termínovaných vkladů a ovládání vkladových účtů s výpovědní lhůtou [2].
e) **Internet –** nabízí možnosti všech předchozích, navíc poskytuje historii pohybu na účtech za zvolené období, avíza k tuzemským i zahraničním platbám, ovládání SIPO [2].

Přímé bankovnictví: nabízí nové produkty, souvisí s vývojem nových technologií. Mezi tyto produkty lze zařadit internet banking, telebanking, home banking a také smartphone banking (smartbanking); dále rovněž GSM banking a WAP banking, tyto produkty jsou klientům dostupné sedm dní v týdnu, 24 hodin denně. [4]

V online bankovnictví je výpočetní technika prakticky využitá k ovládání bankovního účtu, používají se počítače nebo chytré telefony. Výhodou online bankovnictví je přístup k účtu 24 hodin denně 365 dní v roce kdekoli, kde máme připojení k internetu, ovládání je intuitivní a jednoduché. Největší nevýhodou je možné zneužití přístupových dat k účtu a následná ztráta financí. [5]

Mezi lety 2007 až 2017 byl u bankovních klientů zaznamenán nárůst zájmu o internetové bankovnictví z 12 % na 57 %. Podle Davida Navrátila, analytika České spořitelny, je v ČR osm milionů klientů bank a z toho používá internet banking polovina. Čeští uživatelé dokonce v procentním srovnání předčili i uživatele z Německa (56 %). Na prvních místech se s 90 % umístili Dánové. Všeobecně jsou největšími uživateli internetového bankovnictví severské země. [6]

Tabulka 1 Realizace vzdálené komunikace klient – banka

zdroj: [2]

Způsob ovládání účtu	**Konkrétní realizace**
Elektronické (přímé) bankovnictví	Home banking (pomocí komunikačních programů)
	Internet banking (přes internet)
Telefonní bankovnictví	Call centrum (živí operátoři)
	IVR (komunikace s hlasovým automatem)
	SMS zprávy
	GSM-SIM toolkit
	WAP

Tabulka 1 vyjmenovává možné způsoby ovládání účtu včetně konkrétních realizací, podrobněji je popsáno níže:

Home banking

Tento způsob obsluhy bankovního účtu je založen na obsluze s pomocí počítače, internetového připojení a softwaru dodávaném bankou. Po instalaci softwaru a s pomocí internetového připojení může klient obsluhovat svůj účet. Použití je ovšem možné pouze přes jeden konkrétní počítač s instalovaným programem. Home banking používají především firmy, bývá kompatibilní s účetním a ekonomickým softwarem, což je pro podnikatele důležité. [4]

Internet banking

K realizaci potřebných úkonů na účtu je možno použít jakýkoliv počítač, který bude komunikovat s bankou pomocí internetu. K identifikaci postačuje zadat uživatelské jméno a certifikační kód na www adrese konkrétní banky. Ochranu před zneužitím zvyšuje autorizační klíč. [4]

Mobilní bankovnictví

S rostoucí oblibou chytrých telefonů roste i obliba používání bankovních aplikací vytvořených právě pro tato zařízení. Banky umožňují stahování aplikací pro ovládání bankovnictví v mobilu i tabletu. [4]

Telebanking

Telefon – má stejné využití jako fax, navíc lze získat informace o zůstatcích na účtech, pohybech, neprovedených platbách, převodech mezi účty klienta a dále poskytuje možnosti hotline k platebním kartám a komunikačním programům. [2]

Phonebanking je také alternativním názvem telefonního bankovnictví. Tato služba je prováděna dvěma možnými způsoby, kdy klient volá na linku telefonického bankovnictví a prokazuje se identifikačním číslem a heslem [4]:

- v prvním případě komunikuje s automatickým hlasovým systémem,
- v druhém případě je komunikace vedena s telefonním bankéřem [4].

GSM banking

Podobný telefonu, navíc zasílá SMS zprávy, pokud nastane pohyb na účtu, a nabízí možnost použití kurzovního lístku. [2]

Fax – tímto způsobem lze ovládat termínované a spořicí účty, trvalé a inkasní příkazy, také je vhodný pro tvorbu příkazů k úhradě a inkasu v tuzemském i zahraničním platebním styku. [2]

WAP banking

Kompatibilní média – diskety s textovými soubory – používány k příkazům k úhradě nebo inkasu v tuzemském platebním styku, účtují se na nich položky na klientových účtech z banky, dále poskytují výpisy z účtu. [2]

Nové technologie

V poslední době se rozmáhá používání mobilních telefonů jako kreditních karet. Jedná se o poměrně novou technologii a jistě stojí za zmínění [7, 8]:

- Apple pay,
- Google pay.

Apple pay

Platby jsou realizovány se zařízeními iPhon, Apple Watch, iPad a Mac. Používají se identickým způsobem jako klasická kreditní karta. Kartu si uživatel nakopíruje do zařízení a může používat. Při platbách na internetu je to dokonce bezpečnější způsob než klasická platební karta, protože se nikde neukládá její číslo, nepředává se obchodníkům a na každou platbu se aplikuje specifické číslo a unikátní transakční kód. [7]

Google pay

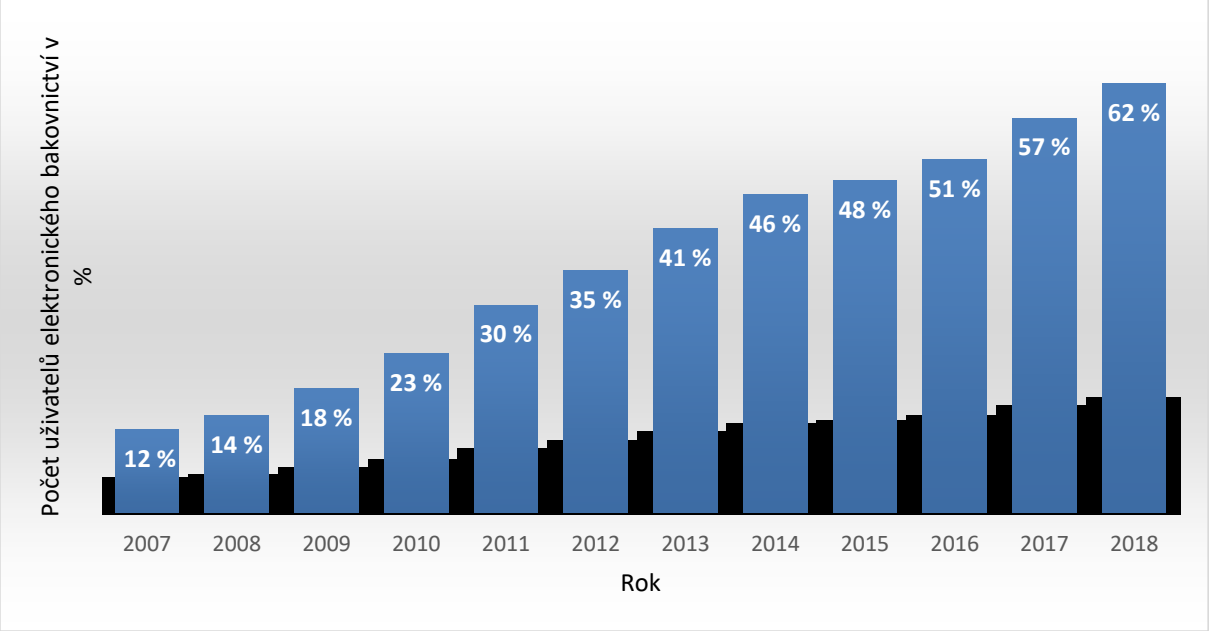
Tento způsob použití je pro uživatele v zásadě shodný s předchozím Apple pay. Jen platby jsou prováděny pomocí zařízení, která používají operační systém Android 5.0 a vyšší a nutností je také podpora NFC[1]. Placení mobilem je jednoduché a zároveň

bezpečné a stejně jako v případě bezkontaktních úhrad do Kč 500 postačí pouhé

[1] Technologie NFC funguje na základě radiové komunikace mezi elektronickými zařízeními do vzdálenosti 4 cm. Je to způsob, jakým váš telefon může oboustranně komunikovat s jiným zařízením ve své bezprostřední blízkosti. Velkou výhodou této technologie je, že nepotřebuje ke svému fungování Wi-Fi, LTE nebo mobilní data.

přiložení. Při vyšších úhradách je nutné zadání PIN a odemknutí přístroje, kterým je prováděna platba. [8]

Obrázek 1, čerpal data z Eurostatu a ukazuje rostoucí zájem o užívání elektronického bankovnictví mezi uživateli bankovních služeb v letech 2007–2018. Jak je zřejmé z údajů, v roce 2007 používalo IB pouze 12 % a v roce 2018 již 62 %, nárůst je 50%. [9]



Obrázek 1 Nárůst uživatelů elektronického bankovnictví v letech 2007–2018

zdroj: vlastní zpracování

Shrnutí

Tato kapitola se zaobírá internetovým bankovnictvím od jeho počátků, dále popisuje, jakými způsoby a prostředky lze praktikovat komunikaci s bankou. Přínosem této kapitoly je seznámení s pojmy souvisejících s přímým bankovnictvím.

2 INTERNETOVÉ BANKOVNICTVÍ A JEHO RIZIKA

Největším rizikem internetového bankovnictví, dále bude v textu používaná zkratka IB, je nedodržování bezpečnostních zásad ze strany uživatelů. Pokud nejsou dodržena zásadní pravidla, hrozí právě uživateli finanční ztráta. Při práci se zařízením prováděné online je nutné [1]:

- ověřit spojení se správným serverem;
- používat licencované antivirové ochrany;
- zařízení neponechávat bez dozoru;
- odhlásit se, zavřít okna s rozhraním banky po ukončení činnosti;
- chránit heslo;
- měnit hesla pro přístup k internetovému bankovnictví;
- pracovat s bankou online pouze na bezpečných přístupových bodech k síti;
- pravidelně kontrolovat výpisy z účtu.

I přes veškerá rizika má IB budoucnost [1].

Dnes je pro mnoho lidí IB zcela běžné, a i když jsou základní zásady bezpečnosti všeobecně známé, přesto jsou podle průzkumů zanedbávány. Tím se ovšem otevírá cesta pro zneužití údajů a popřípadě i pro příležitost ukrást peníze z účtu, kterou hackeři hledají a rádi využijí. Běžně lze uživatele zmást falešnou internetovou stránkou. Překvapivé je zjištění, že téměř každý se nechá splést. Pro bezpečné přihlášení k internetovému bankovnictví je vhodné používat webové stránky banky. Mnoho lidí si „zjednodušuje“ přístup do přímého bankovnictví pomocí vyhledávače. Tento fakt již odhalili hackeři a jsou schopní vyrobit stránky, které jsou téměř k nerozeznání od pravých stránek banky. Banka ČSOB zkusila prověřit pozornost a opatrnost svých klientů a nechala vyrobit falešnou stránku na vyhledávačích Seznam a Google. Na tento podvod se nachytalo 61 434 klientů během jednoho měsíce. A nešlo pouze o kliknutí na falešnou stránku. Ti, kteří se nechali zmást, se dokonce pokoušeli přihlásit k účtu svými přístupovými údaji. V okamžiku přihlášení se zobrazila

informace, že jde o experiment. V případě podvodné stránky hackerů by pravděpodobně oklamaní klienti přišli až o 20 milionů korun. [10]

Pro komunikaci s webovými stránkami používá počítač internetové prohlížeče a protokol http. V rámci bezpečnosti je důležité použití bezpečnějšího protokolu, který obsahuje navíc literu „s“ (https), která znamená „secure“ a označuje zabezpečenou komunikaci. [10].

Zjednodušeně lze protokol https (Hypertext Transfer Protocol Secure) definovat jako “jazyk” používaný při komunikaci prohlížeče se serverem, kdy server do prohlížeče posílá webovou stránku. Uživatel pozná zabezpečený web podle zámečku v adresním řádku a písmena „S“ znamenajícího „secure“, tedy zabezpečený. To je podstatné. Velká část webů ovšem „S“ nemá, je tedy nezabezpečená. Data od prohlížeče k severu cestují v podobě textu, který si může kdokoli přečíst nebo i pozměnit. Zde je možné daný proces připodobnit k obyčejné pohlednici, kterou si na cestě od odesílatele k adresátovi může přečíst každý, komu se dostane do ruky. [11]

Jedním z velkých nebezpečí pro IB jsou bezesporu hackeři. To jsou lidé, kteří s nekalými úmysly umějí proniknout do systémů běžných uživatelů. Dnes už jsou běžnou součástí internetového světa a nelze jejich organizovanost a rafinovanost podceňovat. Pokud se jim podaří proniknout do systému, který používá velká skupina uživatelů, poskytnou své zkušenosti dalším. Peter Kim ve své knize HACKING průvodce penetračním testováním upozorňuje na průnik do systémů společnosti Adobe, při kterém bylo zcizeno mnoho dat (například e-mailové adresy, zašifrovaná hesla a rady, jak hesla odhalit). Tento obsáhlý soubor byl dán k dispozici nejprve malé skupince zasvěcených, ovšem v současné době je možno jej nalézt zcela veřejně, stačí zadat do internetového vyhledávače Adobe a users.tar.gz. [12]

Nejběžnější rizika internetového bankovnictví [12, 13]:

- Sociální inženýrství,
    - Phishing,
    - Pharming,
    - Hoax,
- Spyware,
- Bluetooth,
- Skimming,
- Trojský kůň.

Sociální inženýrství

Jedná se o manipulování s lidmi s cílem získat informace vedoucí k odhalení přístupu k internetovým účtům. Nejde o přímý kontakt útočníka s obětí, ale o manipulaci a přesvědčování napadené osoby. Sociální inženýři jsou schopni se přizpůsobit a poučit se ze svých chyb. [13]

Sociální inženýrství se dělí na několik metod, které lze zařadit do následující skupiny ohrožení jako například [12]:

- záměna domény: zde je využívána nepozornost uživatelů, kteří zapomenou třeba jen napsat tečku mezi doménou a subdoménou; pokud je založena dvojnická doména k doméně oficiální společnosti, může být toto opomenutí velmi bolestné, zvláště u internetového bankovnictví. Při takové chybě poskytne uživatel účtu veškeré přihlašovací údaje a může přijít i o ovládání tohoto účtu,
- sociální inženýrství s Microsoft Excelem: útočník využije důvěry vytipované oběti a podsune ji kalkulační tabulku Excelu obsahující virus; vztah důvěry v tomto pojetí znamená vyhledat osobu, s níž si vyhlédnutá oběť vyměňuje data, a použít, resp. zfalšovat e-mailovou adresu dotyčného uživatele. Proto je také, pokud je používán Excel, upozorňováno na přítomnost makra, které

právě může být škodlivé, a tudíž i na nutnost velké opatrnosti při instalaci takového souboru,

- fyzické sociální inženýrství: jedná se o velice jednoduchou metodu: stačí někde „zapomenout“ USB nebo CD, a pokud se najde nějaká osoba, která si toto medium spustí na svém přístroji, má útočník vyhráno. Jedná se o velmi jednoduchý a velmi účinný způsob, kdy lze získat přístupové údaje k účtům.

Phishing

Český ekvivalent tohoto pojmu je „rybaření“. Jedná se o velmi častou podvodnou techniku, která slouží k vylákání přístupových údajů k účtům. Útočník se vydává například za exekutora, bankéře či IT specialistu a pomocí falešných stránek se snaží získat informace o tom, kde se nejčastěji vyplňují hesla, jména a čísla kreditních karet, data potřebná ke kontrole účtů s cílem zcizit „ulovenému“ člověku peníze. Při tomto manipulativním jednání mezi podvodníkem a manévrovaným nedochází k fyzickému kontaktu. V oblasti sociálního inženýrství jde o velmi používanou metodu. Jestliže se oběť nezachytne do sítí, lovec se poučí a příště svou metodu lovu zdokonalí. [13]

Cílený phishing: v počátcích používání tohoto podvodu byly nigerijské dopisy, které slibovaly velké zisky v budoucnosti, pokud se okamžitě odešle určitá „zanedbatelná“ částka kamsi do neznáma. Tyto dopisy se vyznačovaly zásadními gramatickými chybami a bylo jednoduché je identifikovat. V dnešní době jsou již tyto nástroje mnohem kultivovanější a k odhalení je nutná pozornost uživatele. Útočníci mohou používat nástroje, které naleznou k dispozici na internetu zdarma (Social Engineering Toolkit), avšak existují i komerční, mnohem kvalitnější a efektivnější nástroje. Nelze například opomenout Metasploit Pro vyznačující se přehledným rozhraním a snadným nakonfigurováním a monitorováním útoku na rybu (viz český překlad „rybaření“). Modul může sbírat pouze data v budoucnosti využitelná k útoku na účet, nebo vytvoří webovou stránku, která zaútočí na oběti. [12]

Útoky provádí útočník nejčastěji způsobem dávkových e-mailů [12].

Pharming

Tomuto problému jsou vystaveny veškeré instituce poskytující bankovní služby na území České republiky. Podvod spočívá v přesměrování uživatele na jinou webovou stránku, která je vzhledově téměř identická se stránkou původně požadovanou. Správná kombinace přihlašovacích údajů útočníkovi poskytne potřebné přístupové informace k originálním webovým stránkám instituce. [13]

Hoax

Hoax je nevyžádaná zpráva obsahující klamavou zprávu, většinou poplašného charakteru. Součástí této zprávy je často žádost o další přeposlání přátelům, proto je někdy označován názvem řetězový e-mail. Jeho škodlivost spočívá v prozrazení důvěrných informací, e-maily jsou hromadně rozesílány a často zůstávají v adresním řádku adresy všech příjemců součástí zprávy. Dále mohou poškodit pověst a narušit důvěru určité společnosti. [14]

Spyware

Tyto programy prohlížejí a kontrolují data počítače. Tento software se umí napojit přes WLAN na vašeho souseda, samozřejmě bez jeho vědomí. Umí sledovat jeho přihlašovací jména, hesla i čísla kreditních karet. [15]

SSL – jedná se o bezpečnostní protokol, který chrání IP přenos paketů. Veškerá data po internetové síti putují jako malé balíčky (IP pakety). Pokud někdo zachytí tato přenášená data, potom existuje možnost, že je složí zase zpět do souborů, údajů. Proti tomuto zneužití dat právě napomáhá bezpečnostní protokol SSL – Secure Sockets Layer (vrstva bezpečných sonetů). [15]

Bluetooth

Bezdrátová technologie umožňující propojení elektronických přístrojů, například dvou telefonů či počítače a telefonu. V poslední době jsou hojně využívána bezdrátová sluchátka propojená s přístrojem právě pomocí bluetooth. Na první pohled je to velmi užitečná technologie, ovšem má svá značná úskalí: jedná se například o bluejacking, stáhnutí škodlivého programu. Existují i bluetoothové viry, které využívají nedostatky v operačních systémech, u moderních smartphonů se již naštěstí tento jev nevyskytuje. [15]

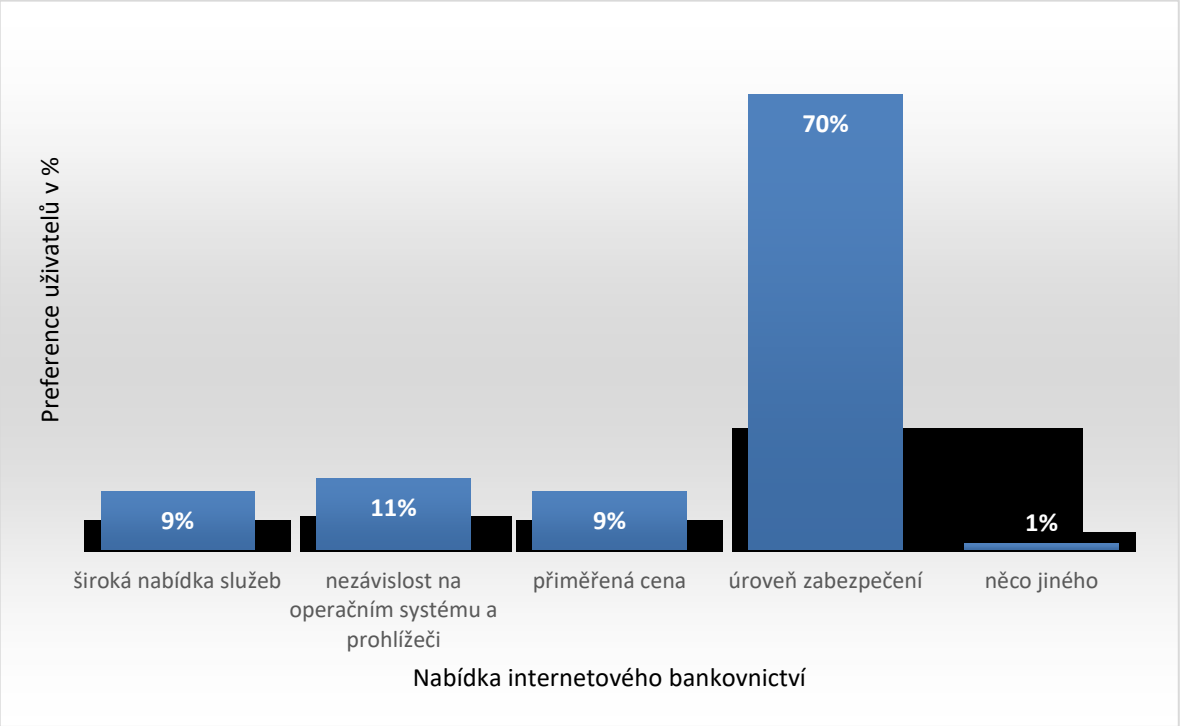
Skimming

S touto metodou podvodu je možné se setkat především při výběru z bankomatu, na němž je nainstalována čtečka informací z magnetického proužku [13].

Trojský kůň

Data potřebná k přístupu na účet napadeného posílá infikovaný program agresora, který se tváří jako užitečný, často dochází k vydírání oběti [13].

Web Info, měšec.cz na svých stránkách připravil v roce 2005 anketu zaměřenou na to, co považují uživatelé na IB za důležité. V okamžiku, kdy byly výsledky vytěženy do této práce, hlasovalo 148 lidí. Jak vyplývá z obrázku 2, pro 70 % uživatelů byla už v roce 2005 nejdůležitější bezpečnost. [16]



Obrázek 2 Preference uživatelů internetového bankovnictví

zdroj: vlastní zpracování

Shrnutí

Druhá kapitola shrnuje pojmy související s riziky při užívání internetového bankovnictví, zabývá se stručně zásadami pro bezpečné používání internetu. Ústředním tématem této kapitoly jsou rizika, se kterými se běžný uživatel může setkat při používání internetového připojení a všeobecně při používání počítačů.

3 ANALÝZA RIZIK

Transparentní, jasná, opakovatelná – taková je charakteristika analýzy rizik. Musí umožňovat identifikaci dalších rizik při použití stejných postupů. Výsledek analýzy rizik je ve své podstatě pravděpodobnost, s jakou nastane určitá událost. Dalším postupem lze riziko podrobněji prozkoumat, omezit nežádoucí jevy a přijmout opatření. [17]

3.1 Analýza rizik – teorie

Pojem riziko je známý již od 17. století, kdy byl využíván v souvislosti s námořní plavbou. Označoval „úskalí“, kterému je nutno se vyhnout. Později se tímto pojmem označovalo „vystavení nepříznivým okolnostem“. V dnešní době je v teorii rizika tento pojem spojován především s hrozbou, nebezpečím vzniku škody. Rizikem může být [18]:

- pravděpodobnost či možnost vzniku ztráty,
- variabilita možných výsledků nebo nejistota jejich dosažení,
- odchýlení od očekávaných výsledků,
- příznivá šance,
- vyšší zisk,
- nebezpečí chybného rozhodnutí,
- spekulativní riziko,
- ohrožení systému specifickou hrozbou.

Pro riziko je nutné spojení, že určitá událost se stane s určitou pravděpodobností, kdy výsledný efekt se liší od původního předpokladu. Riziko souvisí s různým vývojem, kdy se odlišuje prognóza od skutečnosti. [18]

Klasifikace rizika

Každá lidská aktivita je spojena s určitým způsobem investice. Ať už se jedná o finanční prostředky, informace, popřípadě o jiné chráněné aktivum, pokaždé je očekávána návratnost v podobě peněz, času, pohodlí, rychlosti apod. I riziko má dvě stránky, a to pozitivní stránku, která skýtá naději na vyšší zisk a vyšší úspěch, nebo negativní stránku, kdy existuje nebezpečí ztrát. [18]

Rizika lze rozdělit [19]:

a) dle charakteristiky,
b) dle věcné klasifikace rizik,
c) dle věcné podstaty.

a) Rozdělení dle charakteristiky [19]**:**

- interní a externí,
- ovlivnitelné a neovlivnitelné,
- předvídatelné a nepředvídatelné,
- hmotné a nehmotné,
- skutečné a spekulativní,
- systematické a nesystematické,
- pojistitelné a nepojistitelné.

b) Rozdělení dle věcné klasifikace rizik [19]**:**

- výrobní,
- ekonomická,
- obchodní,
- informativní,
- sociální,
- technická,
- logistická.

c) **Rozdělení dle věcné podstaty** [19]**:**

- základní rizika (živelní katastrofy, přerušení provozu),
- operační rizika (rizika z každodenní činnosti),
- strategická rizika (ovlivňují obchodní politiku),
- finanční rizika (nedostatečná likvidita).

Přístupy k riziku [18]**:**

- **averze** – uživatel se vyhýbá rizikovým projektům a jeho volba vždy padne na bezpečné projekty,
- **sklon k riziku** – opak předchozího typu, tento uživatel si vybírá rizikovější činnosti, které slibují vyšší zisk,
- **neutrální postoj** – rovnovážný postoj, vybírá dle situace a zvažuje vhodnou strategii.

3.2 Postup a hodnocení

Každé zkoumání rizik má svůj specifický postup, který lze shrnout do čtyř kroků [18]:

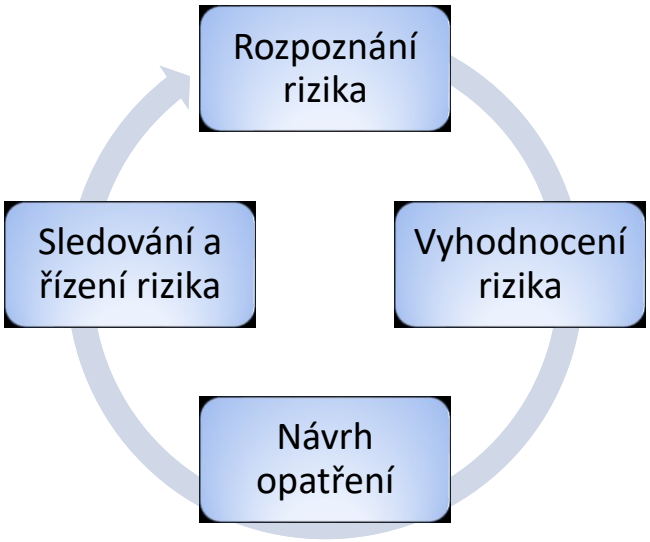
- Nejprve se musí identifikovat chráněná aktiva – aktivum je vše, co má pro konkrétní subjekt hodnotu a přináší prospěch.
- Stanoví se hodnota aktiv – objektivně (hodnota, kterou lze vyčíslit), subjektivně (individuální hodnota).
- Identifikuje se zranitelnost a hrozba – hrozba může způsobit subjektu škodu nebo ztrátu, zranitelnost je vlastnost, která umožňuje uplatnění hrozby.
- Určí se pravděpodobnost výskytu hrozby a míra zranitelnosti aktiva.

Postup při hodnocení a řízení rizika [18]:

- Rozpoznání rizika,
- Vyhodnocení rizika,
- Vytvoření rizikových plánů,
- Sledování a řízení rizika.

Na současném trhu existují společnosti, které se zabývají studiem a rozborem rizika ze všech možných úhlů a jsou schopny poskytnout zadavatelům potřebné výstupy.

Tyto výstupy je pak možno použít ke snížení rizika. Ve velké většině případů jde o podnikatelská rizika. Analýza rizik pak může probíhat v cyklu, který je znázorněn na obrázku 3. [17]



Obrázek 3 Mechanismus hodnocení a řízení rizika

zdroj: vlastní zpracování

Vzhledem k širokému spektru možného ohrožení je nutné veškerá rizika roztřídit, ohodnotit a zaměřit se na klíčové možnosti ohrožení subjektu. Jelikož v rámci celého procesu neexistuje pouze jediné riziko, je nutné zkoumat více hrozeb. Mechanismus uplatnění rizika je znázorněn na obrázku 2. [19]

Obrázek 4 Mechanismus uplatnění rizika

zdroj: vlastní zpracování

Pro stanovení velikosti rizik existují dva základní přístupy [20]:

- **kvantitativní** – číselné vyjádření hodnoty.
- **kvalitativní** – riziko je vyjádřeno subjektivně.

Kvantitativní – číselné vyjádření hodnoty. [20]

Kvalitativní – riziko je vyjádřeno určitým rozsahem (například <1 až 10> popřípadě je možnost i slovního hodnocení <malé; střední; velké>). Výhoda tohoto hodnocení spočívá především v jednoduchosti a rychlosti, je ovšem subjektivní, hůře se určuje přijatelná výše finančních nákladů potřebných k eliminaci hrozby. [20]

3.3 Výskyt a dopad rizika

Metodika sjednocuje pohled při vyhodnocování prováděné analýzy. Jejím základem je určení stupnice hodnocení dle hlediska úrovně pravděpodobnosti výskytu rizika a míry dopadu. Doporučeno je 5 stupňů a údaje se řadí do tabulky, jak je uvedeno v tabulce 2. Následuje tabulka 3, která známkuje dopady rizika podle dopadu rizika na chráněné aktivum a intervalu pravděpodobnosti. [18]

Tabulka 2 Hodnocení výskytu rizika

zdroj: **[17]**

Pravděpodobnost výskytu rizika			
Úroveň	Označení	Číselné vyjádření	Interval pravděpodobnosti
5	téměř jisté	4,1–5,0	výskyt téměř vždy
4	pravděpodobné	3,1–4,0	výskyt je pravděpodobný
3	možné	2,1–3,0	výskyt může nastat
2	nepravděpodobné	1,1–2,0	možný výskyt, ale nemusí nastat
1	téměř vyloučené	0,1–1,0	výskyt pouze výjimečně

Tabulka 3 Dopad rizika – hodnocení

zdroj: [17]

Dopad rizika			
Úroveň	Označení dopadu	Číselné vyjádření	Interval pravděpodobnosti
5	katastrofický	4,1–5,0	totální ztráta
4	velmi významný	3,1–4,0	výrazné poškození
3	významný	2,1–3,0	nutnost okamžitého řešení
2	drobný	1,1–2,0	ovlivnění pouze dílčích aktivit
1	téměř neznatelný	0,1–1,0	neovlivňuje znatelně fungování

Krajní poloha rizik – před samotným hodnocením rizik je vhodné si nejdříve stanovit krajní polohy rizika [17].

Hodnocení rizik – v tomto kroku se každému zjištěnému riziku přidělí hodnocení pravděpodobnosti výskytu P a podle míry významnosti z úhlu dopadu D lze vypočítat významnost rizika, která se rovná D x P [17].

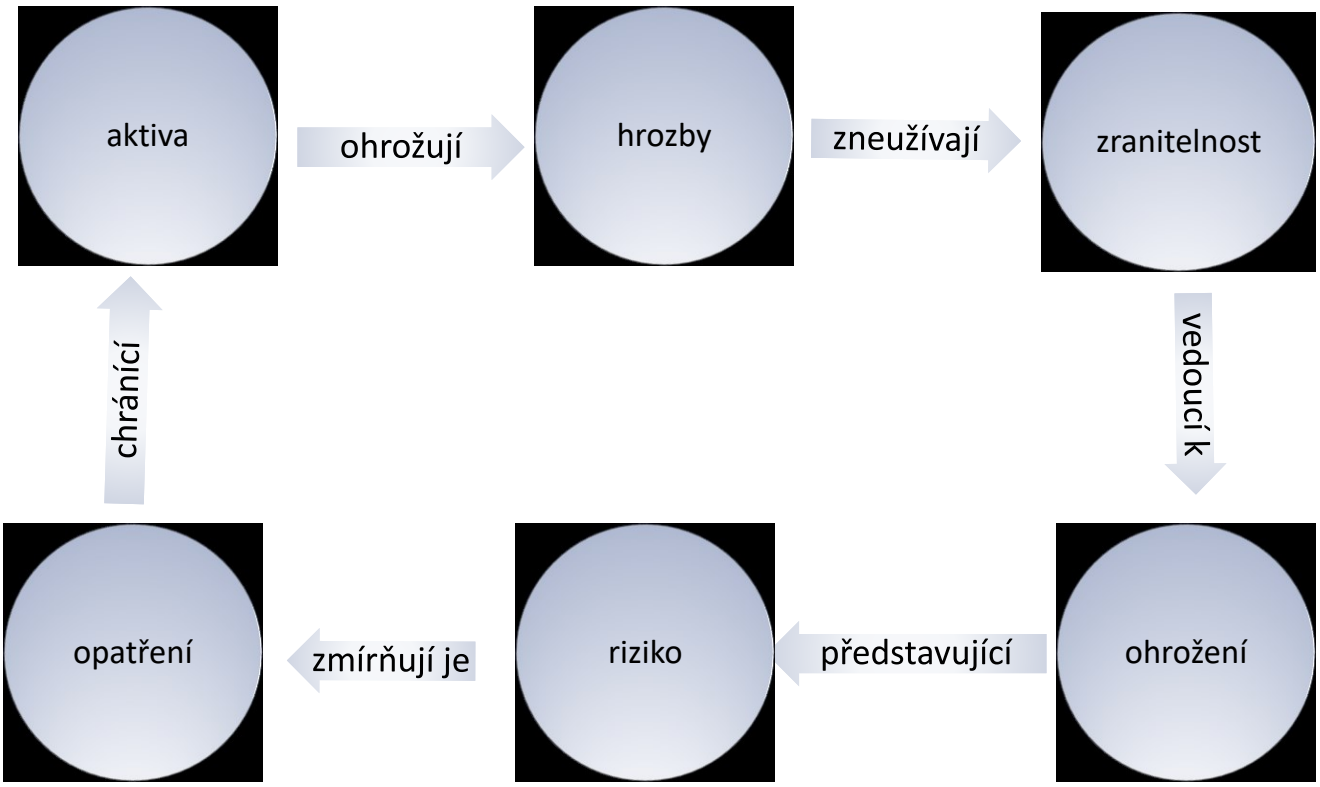
Nezávislý pohled – hodnocení rizika je vhodné přenechat nezávislé osobě, která objektivně a bez zaujetí ohodnotí míru ohrožení [17].

Výstup analýzy rizik – finálním výstupem musí být relevantní a kompletní údaje [17].

Po zhodnocení všech identifikovaných rizik by mělo následovat rozdělení dle metody semaforu [17]:

běžná rizika **závažná rizika** **kritická rizika**

Obrázek 5 ilustruje koloběh rizika: existence aktiv vede k ohrožení, to následně k přijetí opatření, za nimiž se dále cyklicky opakují další kroky. [17]



Obrázek 5 Analýza rizik

zdroj: vlastní zpracování

3.1 Analýza rizik internetového bankovnictví

Při každé analýze rizik je nutné si nejdříve uvědomit, co chceme chránit, jaké ohrožení a jaké následky mohou nastat a jak se lze chránit. Pro tuto analýzu bude inspirací metoda RIPRAN, upravená pro potřeby analýzy rizik IB.

Při práci s internetovým bankovnictvím je nutné si uvědomit, co je chráněným aktivem:

- finanční prostředky: finance uložené na účtu uživatele;
- osobní údaje: údaje, které by bylo možné zneužít a způsobit tak uživateli účtu majetkovou škodu. Pokud se útočník naboural do bankovního účtu uživatele, může účet ovládat a uzavírat smluvní vztah s bankou.

Hrozby je možné rozdělit na dvě základní skupiny:

- vnitřní,
- vnější.

Vnitřní hrozby, kde hrozbou je uživatel sám:

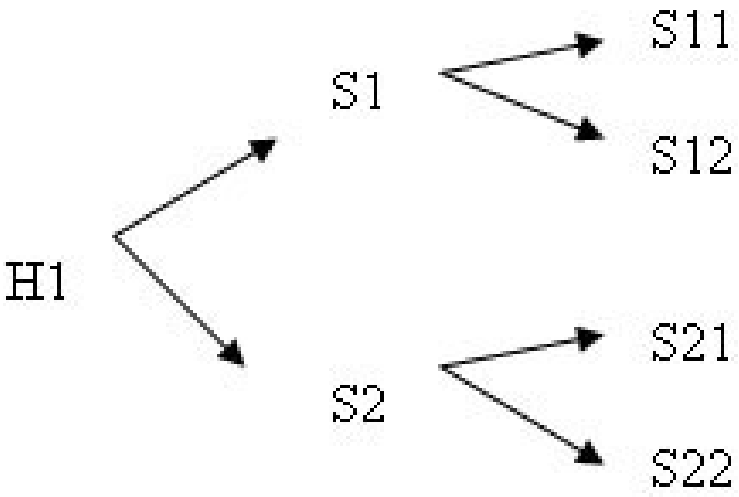
- nepozornost,
- nezodpovědnost,
- lehkomyslnost,
- naivita,
- důvěřivost.

Vnější hrozby, ohrožení přichází z okolí:

- náhoda, zde pachatel pouze využívá nastalé situace bez předchozí přípravy, například zapomenutá karta s poznačeným PIN kódem, zapomenuté zařízení s otevřeným přístupem k účtu;
- úmysl, zde je již nutná příprava a aktivní účast útočníka, vylákání přístupových kódů, výroba podvodných stránek, podstrčení viru atd.

3.2 RIPRAN

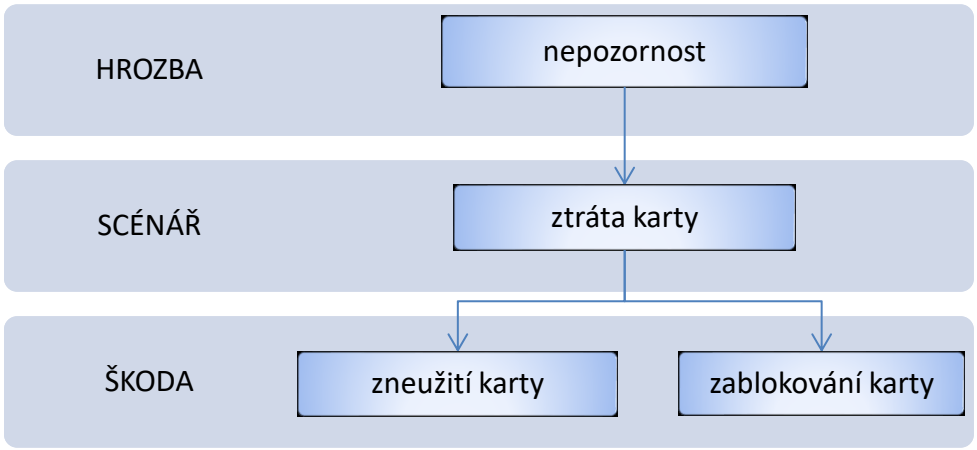
RIPRAN (RIsk PRoject Analysis) je metoda, kterou lze kontrolovat a řídit projektová rizika. Její princip se zakládá na tvorbě tandemů ohrožení – scénář, obrázek 6. V analýze se stanovuje pravděpodobnost vzniku negativních jevů a velikost následků, tabulka 4. Vymezuje se stupnice dopadu a stanoví postup zmírňující nebo odstraňující riziko. Dalším krokem je nové stanovení hodnoty rizika, které je pravděpodobné i přes využití opatření. [21]



Obrázek 6 Dvojice hrozba – scénář

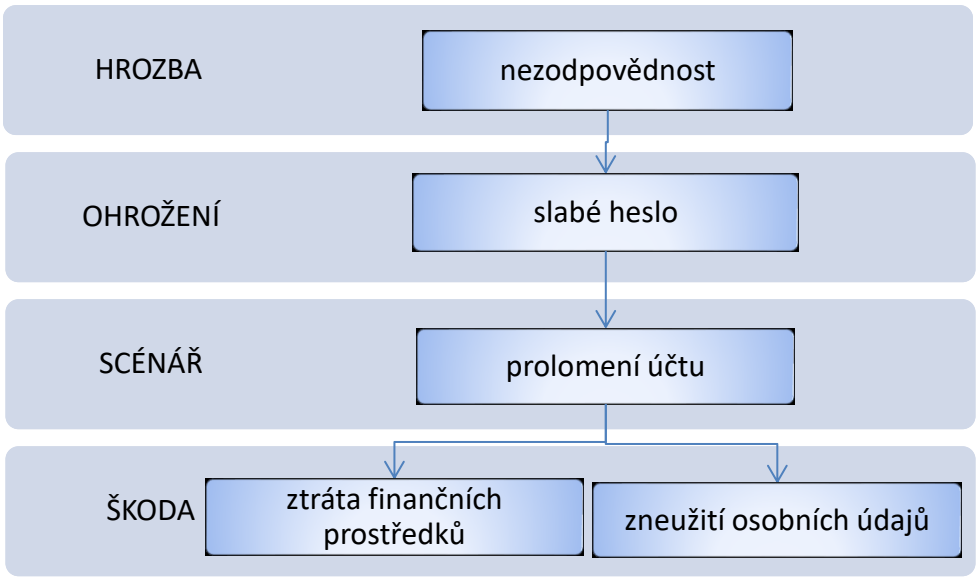
zdroj: [22]

Metodou RIPRAN je inspirováno šest následných znázornění, obrázek 7–12, možných hrozeb a scénářů IB. Jsou zde uvedeny i škody a ohrožení, tak jak se vztahují k uvedeným hrozbám IB.



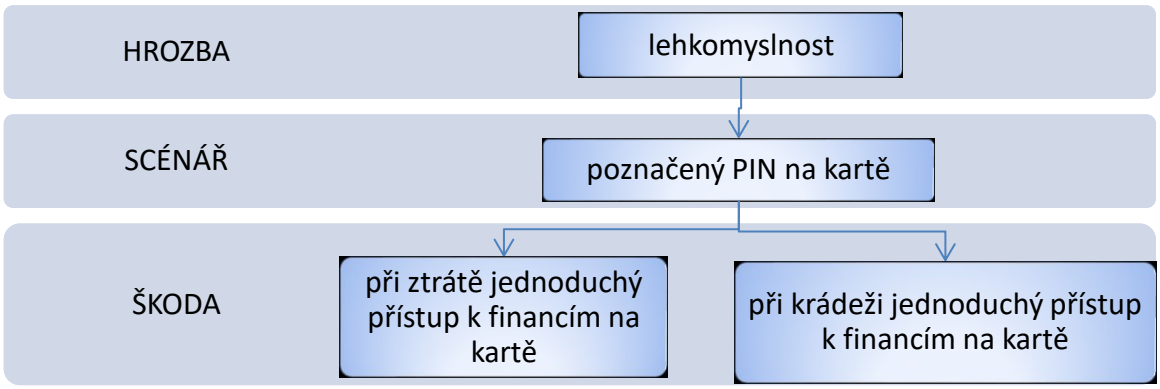
Obrázek 7 Vnitřní hrozba – nepozornost

zdroj: vlastní zpracování



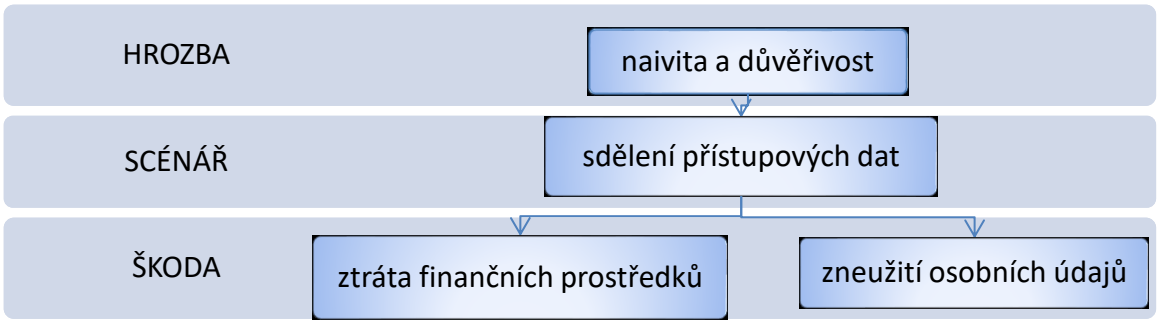
Obrázek 8 Vnitřní hrozba – nezodpovědnost

zdroj: vlastní zpracování



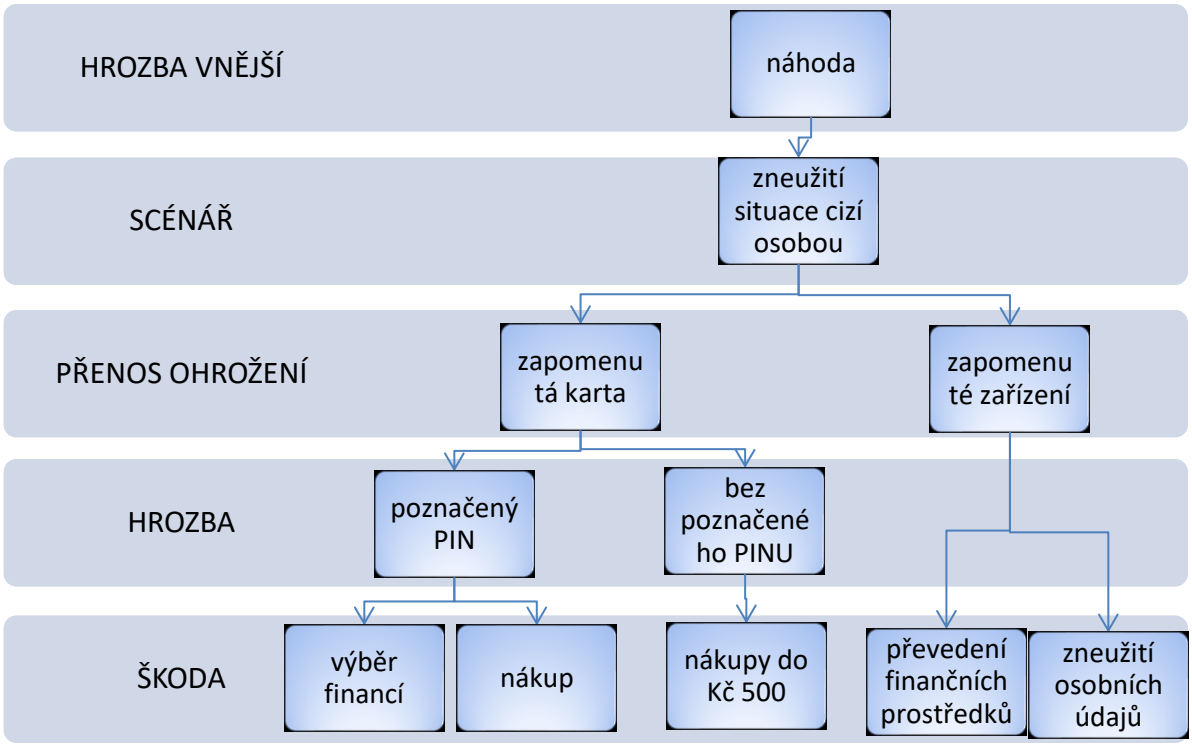
Obrázek 9 Vnitřní hrozba – lehkomyslnost

zdroj: vlastní zpracování



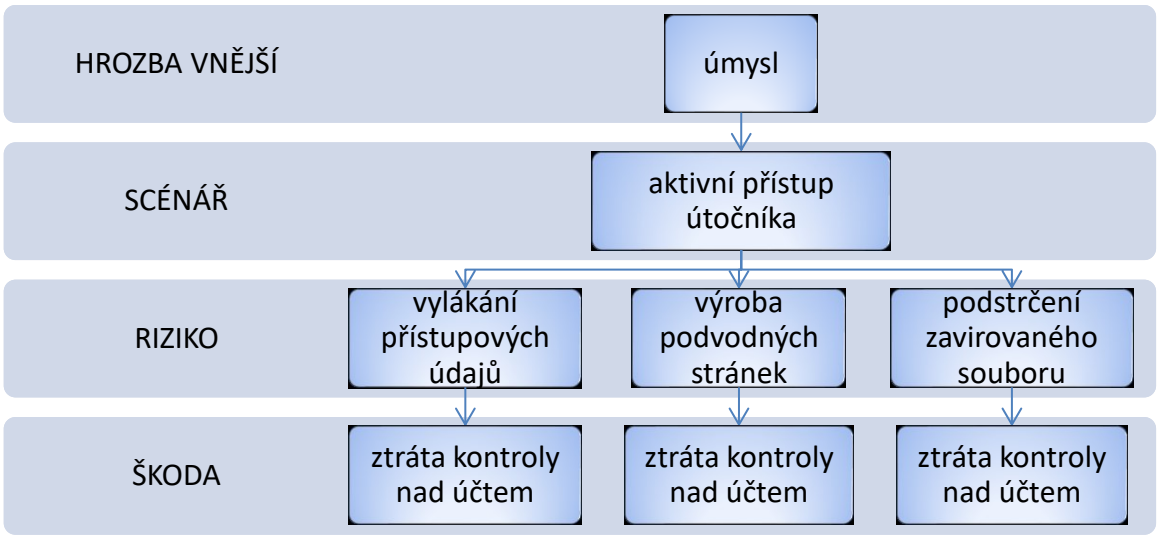
Obrázek 10 Vnitřní hrozba – důvěřivost

zdroj: vlastní zpracování



Obrázek 11 Vnější hrozba – náhoda

zdroj: vlastní zpracování



Obrázek 12 Vnější hrozba – úmysl

zdroj: vlastní zpracování

Třídy pravděpodobnosti používané v analýze rizik RIPRAN [22]**:**

- Zanedbatelná pravděpodobnost = menší nebo rovno 50 %
- Významná pravděpodobnost = větší než 50 %.

Třídy ztrát [22]**:**

- Zanedbatelná ztráta vyžadující operativní zásahy a škoda nižší než 10 %.
- Významná ztráta ohrožující projekt a škoda je větší nebo rovna 10 %.

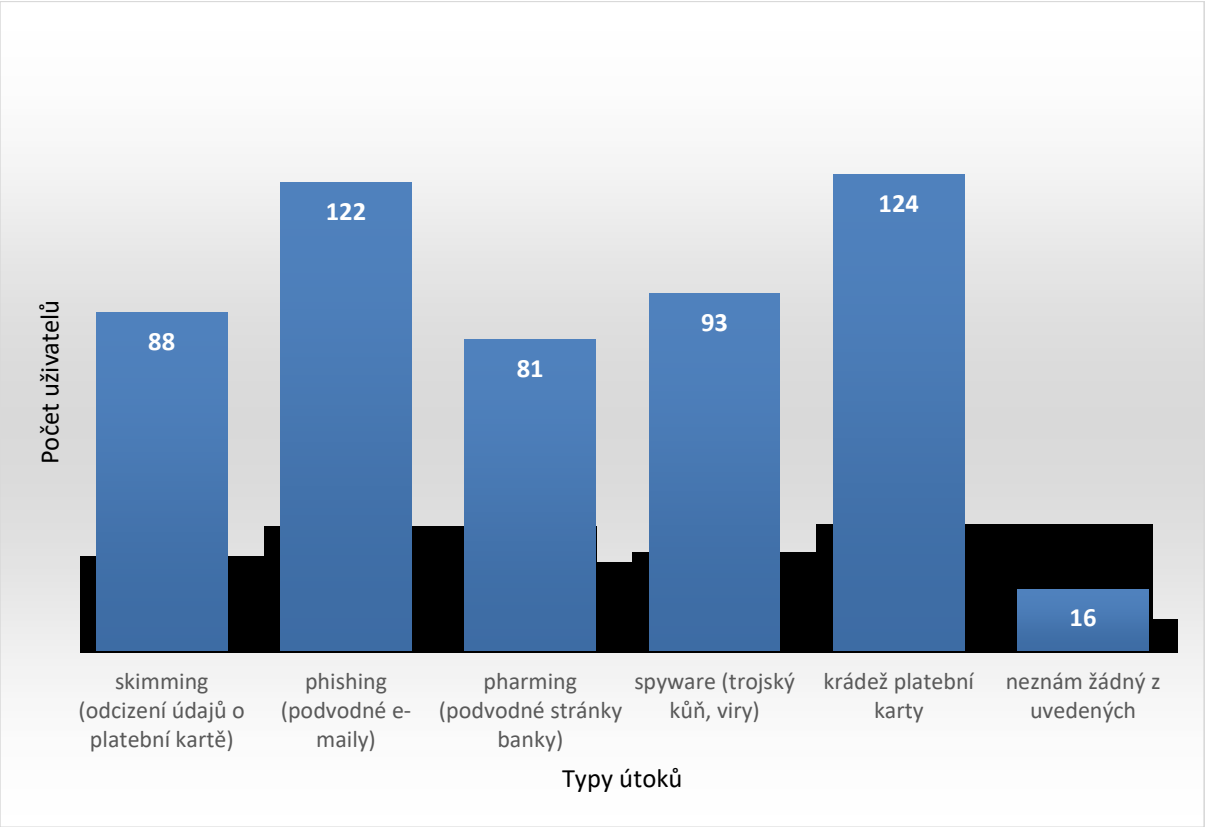
V tabulce 4 jsou zhodnoceny rizika související s IB.

Tabulka 4 RIPRAN hodnocení rizika

zdroj: vlastní zpracování

	Zanedbatelná pravděpodobnost	Významná pravděpodobnost
Zanedbatelná ztráta	ztráta komfortnosti užívání internetového bankovnictví	zablokování účtu ztráta důvěry v internetové bankovnictví
Významná ztráta	ztráty finanční hotovosti zneužití osobních údajů	nenalezena

Na obrázku 13 byly zpracovány informace od 165 respondentů, které v roce 2017 shromáždil Lukáš Kyttler. Je zde sledováno, s jakými typy útoků na elektronické bankovnictví se uživatelé setkali osobně, popřípadě zda znají někoho, kdo byl takto poškozen. [23]



Obrázek 13 Typy útoků

zdroj: vlastní zpracování

Rizika

V každé analýze je rizikem pravděpodobnost ztráty chráněného aktiva. Pokud se týká internetového bankovnictví, jedná se o pravděpodobnost:

- ztráty finanční hotovosti,
- zneužití osobních údajů,
- zablokování účtu,
- ztráta důvěry v IB,
- ztráta komfortnosti užívání internetového bankovnictví.

Opatření

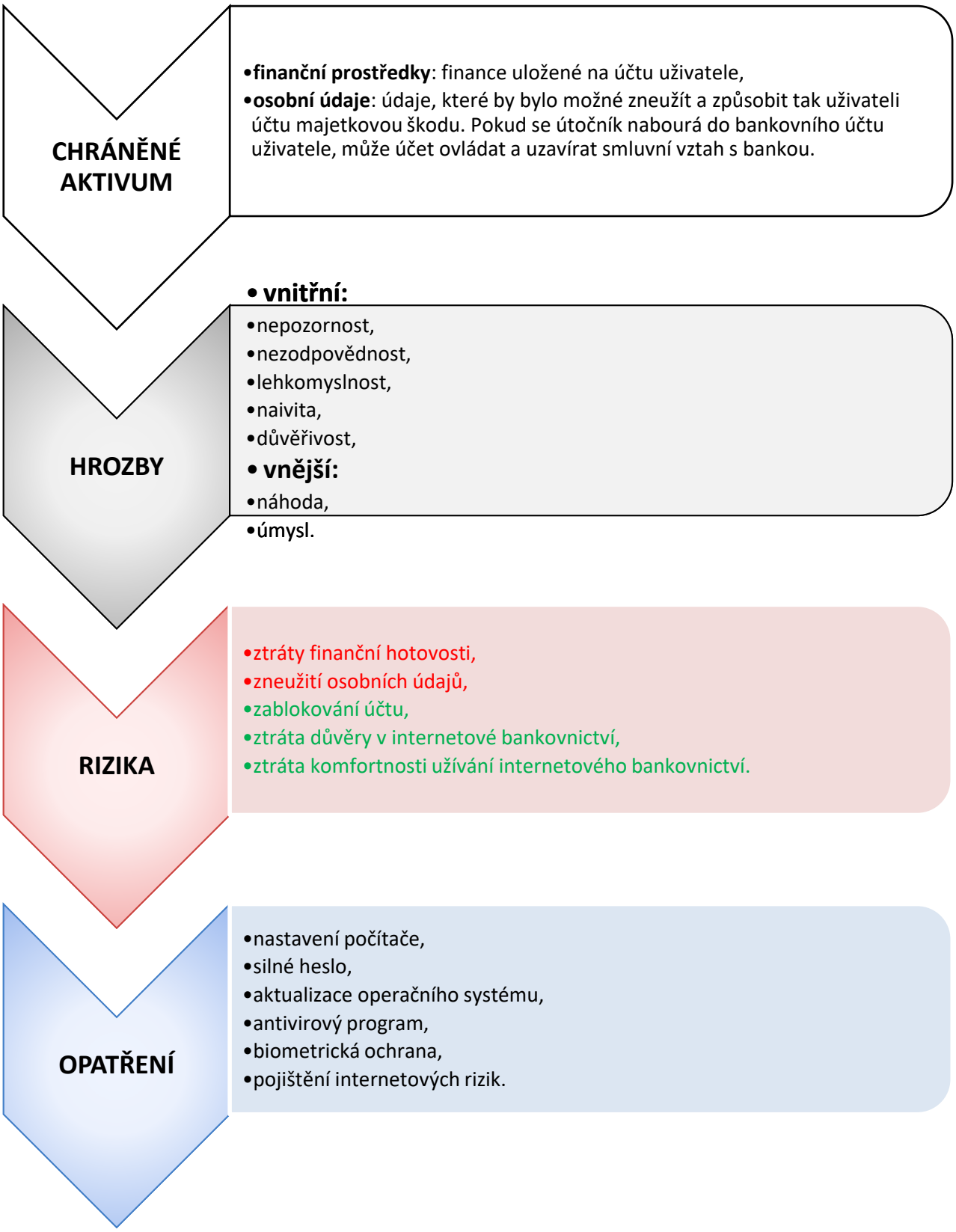
Po zjištění a ujasnění aktiv, která je nutno ochraňovat, a po odhalení pravděpodobných rizik je dalším nezbytným krokem vyhodnocení rizik a návrh opatření.

Každé riziko má určitou pravděpodobnost vzniku, jeho následky určitou hodnotu, kterou lze vypočítat. Způsob výpočtu velikosti ztráty ukazuje obrázek 14. [18]

Obrázek 14 Předpokládaná (možná) velikost ztráty

Zdroj: [18]

Rizika IB je možné analyzovat i způsobem realizovaným v obrázku 15. Zde je jasně vyjádřeno chráněné aktivum, možné hrozby, rizika dle závažnosti zbarvená dle metody semaforu, červeně závažná a zeleně méně vážná. V části opatření se nacházejí heslovitě vyjmenovaná vhodná doporučení pro bezpečnější užívání IB.



Obrázek 15 Analýza rizik IB

zdroj: vlastní zpracování

U IB je velmi těžké odhadnout pravděpodobnost vzniku nežádoucí události, protože je závislá na chování uživatele IB. Při zpracování tabulky 5 je předpokladem zodpovědné chování obou uživatelů, a proto byla odolnost chráněného aktiva stanovena na 80 %. Zbytkové riziko, které stále zůstává i přes správné chování obou uživatelů, je vypočítáno součinem pravděpodobnosti, že nastane negativní událost, a možné škody, zranitelnosti aktiva. Pravděpodobnost vzniku negativního jevu je složité zjistit, okolnosti jsou subjektivní, pro následující studii byla tedy ohodnocena 10 %.

Tabulka 5 Výpočet vhodnosti opatření

zdroj: vlastní zpracování

Data rozhodující ke zjištění vhodnosti opatření	**Uživatel IB „A“**	**Uživatel IB „B“**
Měsíční příjem	23 000 Kč	48 000 Kč
Měsíční náklady	22 100 Kč	22 100 Kč
Zůstatek na bankovním účtu měsíčně	900 Kč	25 900 Kč
Vzorec hodnocení rizika (pravděpodobnost x škoda)	HR = P x Š	HR = P x Š
Odolnost chráněného aktiva	80 %	80 %
Zranitelnost chráněného aktiva	20 %	20 %
Výše pravděpodobné škody před zavedením opatření, vypočítána:	180 Kč (900 x 20 %)	5180 Kč (25 900 x 20 %)
Hodnota rizika (pravděpodobnost 10 %)	18 Kč	518 Kč
Náklady opatření – pojištění internetových rizik (nabídka ČSOB)	67 Kč	67 Kč
Je vhodné zavádět opatření	NE	ANO

Analýza rizik je nepřetržitý proces, který se stále opakuje v cyklech. Jakmile se po každém z těchto cyklů prověří hrozby, přijmou opatření a provede následná

kontrola, pokaždé se navíc odhalí zbytkové riziko, popřípadě se objeví riziko nové. V předcházejícím případě, který měl znázornit subjektivitu výše rizika u jednotlivých uživatelů IB, bylo možno riziko přenést na pojišťovnu. U uživatele „A“ se ovšem toto řešení jeví jako nevýhodné, v důsledku čehož by daný uživatel mohl zaujmout postoj retence k riziku s tím, že by žádné opatření přijato nebylo. Oproti tomu uživatel „B“ by zřejmě transfer rizika uvítal a riziko případné škody na pojišťovnu přenesl.

Shrnutí

Kapitola analýza rizik se zabývá podrobně teorií týkající se odhalování možných pravděpodobností ohrožení, popisuje metodiku známých a užívaných analýz. Zjišťování rizik se promítá do veškerých činností. Vždy záleží na daném oboru a na vhodné volbě metody pro analýzu rizik.

Pro účely této práce zaměřené na rozbor možných rizik internetového bankovnictví z pohledu uživatele byla pro analýzu vybrána metoda RIPRAN přizpůsobená zadanému tématu a tzv. postup rozhodovacích stromů. Nejdříve byly identifikovány možná rizika, navazovaly scénáře, které mohou zapříčinit nežádoucí situace. Nakonec byly v bodech vyjmenovány návrhy opatření.

Uživatele internetového bankovnictví je nutno považovat za jednotlivce, proto i způsob analýzy je individuální, zaměřený na subjektivní hodnocení rizik a škod, se snahou o zevšeobecnění. Dále jsou všechna rizika týkající se ztráty dat či peněz v souvislosti s elektronickým bankovnictvím považována za fatální. Za méně závažná rizika lze považovat zablokování účtu, popřípadě ztrátu důvěry k internetovému bankovnictví. To, co uživatel jistě vnímá jako kritickou situaci, je jak ztráta dat, tak i ztráta finanční. Náročnost opatření je nutno uvážit podle velikosti rizika a výše možné škody. Vzorec je součin pravděpodobnosti a výše škody (HR = P x Š).

Dopad ztráty na jednotlivé uživatele je individuální. Pouhé zablokování účtu však uživatele nezasáhne tak intenzivně a takovou silou, jako ztráta financí či zneužití

osobních dat. Z tohoto důvodu jsou rizika ztráty financí a osobních údajů značena červeně a ostatní pravděpodobná rizika zeleně, což lze připodobnit k barvám na semaforu rovněž signalizujícím míru rizika.

Podrobnější popis opatření následuje v další kapitole.

4 NÁVRH MOŽNÝCH OPATŘENÍ A ELIMINACE RIZIK

Řízení rizik je identifikace, vyhodnocování, sledování a přijímání opatření, která vedou k omezování podstupování rizik. Jedná se o [3]:

- nastavení počítače,
- silné heslo,
- aktualizace operačního systému,
- antivirový program.

Nastavení počítače

Zabezpečení internetového bankovnictví začíná u zabezpečeného počítače. Nutnou obranou při používání každého PC je zajistit správné uživatelské nastavení a nenechat na počítači pracovat nikoho cizího. Pokud i přesto chceme umožnit používat počítač jiné osobě, lze tak učinit s využitím speciálního účtu Host. V tomto režimu nelze měnit nastavení počítače. [5]

Silné heslo

Základní prvkem bezpečného používání internetu je silné heslo, které musí být dostatečně dlouhé, tj. obsahovat minimálně osm znaků. Není vhodné použít jednoduché kombinace čísel ani jednoduše uhodnutelná slova, jako jsou například jména blízkých osob, název oblíbeného sportu či jména domácích mazlíčků. Za dostatečně bezpečná hesla se považují kombinace velkých a malých písmen, znaků a čísel. [5]

Příklad správné tvorby hesla: lze použít i lidovou písničku, například:

Kočka **l**eze **d**írou, **p**es **o**knem = Kldpo, doplníme zapamatovatelnou kombinací čísel, která pro nás něco znamená (např. 198), a navíc pro jistotu proložíme znaky K1*ld9%p8o. Takové heslo dlouhé deset znaků již bude dostatečně silné.

Současnost nás však nutí používat mnoho hesel a není reálné si všechna zapamatovat. Proto je vhodné používat generátory hesel. Použití těchto programů je jednoduché a bezpečné, navíc úschova hesel je odpovědí na způsob, jak si vygenerovaná hesla pamatovat. Uživateli zbývá jen jedno heslo, které si musí uchovávat v paměti, a to je heslo k databázi. [5]

Aktualizace operačního systému

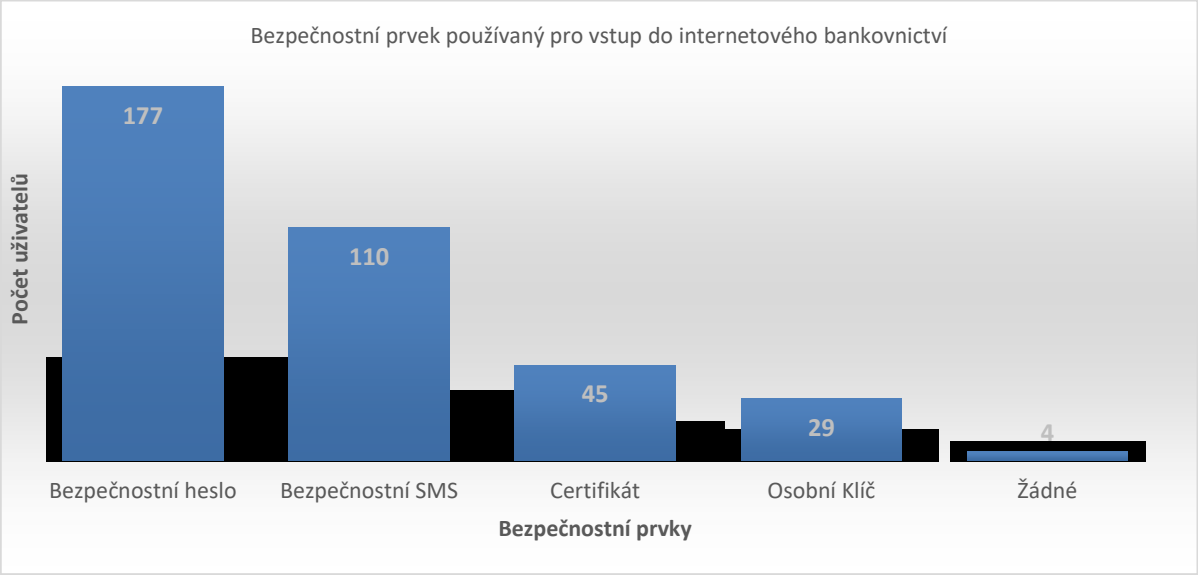
Operační systémy mají své nedostatky, které můžou útočníci využívat, aby se dostali dovnitř systému. Tyto nedostatky výrobci pravidelně opravují. Znamená to, že buď jednotlivé chyby zacelují (hotfixy), nebo opravují více chyb najednou (service packy). Tato vylepšení jsou známá pod pojmem aktualizace, které jsou na internetu k dispozici zdarma a stahují se automaticky. Lze je však nastavit i tak, aby se před každou aktualizací program uživatele zeptal, jestli s aktualizací souhlasí. Pro bezpečnost systému je ovšem nezbytné opravy stahovat a instalovat, jinak by systém byl náchylný k infekci viry. [5]

Antivirový program

Stejně důležité jako aktualizace operačního systému jsou i aktualizace antivirového programu. Každý den na světě vznikají nové počítačové viry a z tohoto důvodu musejí společnosti, které antivirové programy vyvíjení, s vývojem virů držet krok a proti každému nově vzniklému nebezpečí co nejrychleji vyvinout obranu a poskytnout ji svým zákazníkům. [5]

S antivirovým programem úzce souvisí i další činnost, která by měla probíhat pravidelně, ideálně automaticky, a to je antivirová kontrola [5].

Pro obrázek 16 byly použity údaje od 250 respondentů. Jsou zde vyjmenovány nejběžnější prvky používané pro přihlášení do internetového bankovnictví. Dotazník byl zpracován v roce 2018 Kateřinou Mullerovou. [24]



Obrázek 16 Bezpečnostní prvky IB

zdroj: vlastní zpracování

Doporučení ČSOB

Každá banka má na svých internetových stránkách svá doporučení, jak IB bezpečně užívat. Pro názornost jsou zde uvedena doporučení banky ČSOB, obrázek 17:

Obrázek 17 Doporučení ČSOB

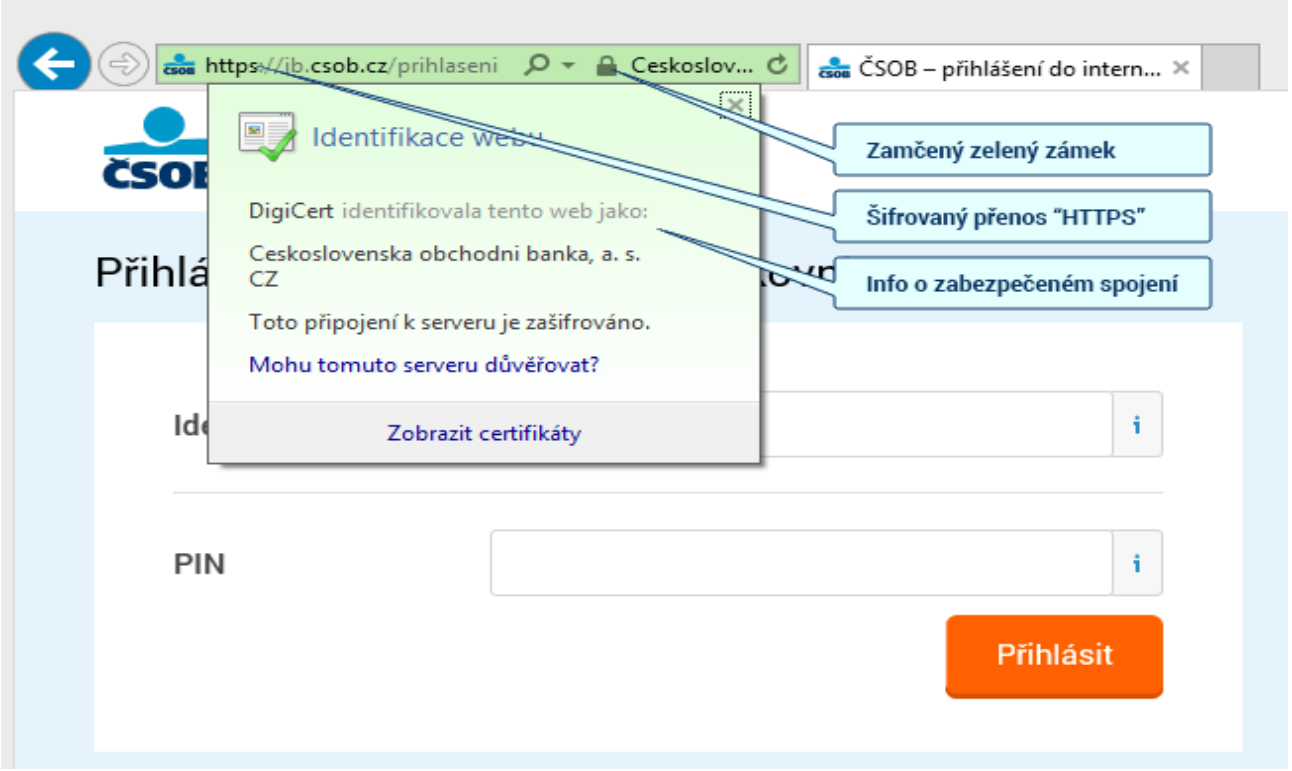
zdroj: vlastní zpracování

Jednotlivé body doporučené bankou ČSOB [25]:

1. **Používejte bezpečný počítač** – pro užívání internetového bankovnictví je zásadní použití bezpečného počítače, kde je v moci uživatele ohlídat jeho nastavení.
2. **Chraňte své přihlašovací údaje** – PIN, identifikační číslo, uživatelské jméno, vstupní heslo; tyto údaje je nutné si zapamatovat, nesdělovat dalším osobám, zvláště ne přes sociální sítě.
3. **Svá hesla a PIN volte pečlivě** – není vhodné používat jednoduchá hesla a PIN, je nutné je měnit a k různým službám používat různá hesla.

4. **Chraňte svůj mobilní telefon** – není bezpečné půjčovat mobilní telefon cizím osobám nebo jej nechávat bez dozoru.
5. **Přihlašujte se pomocí SMS klíče nebo Smart klíče** – jedná se další bezpečnostní ochranu při přihlašování k účtu.
6. **Přihlašujte se pouze na stránkách internetového bankovnictví** – v adresním řádku musí být adresa banky, např.: https://ib.csob.cz, vedle ní ikona zámku.

Jak má vypadat bezpečné přihlášení, je názorně ukázáno na obrázku 18.

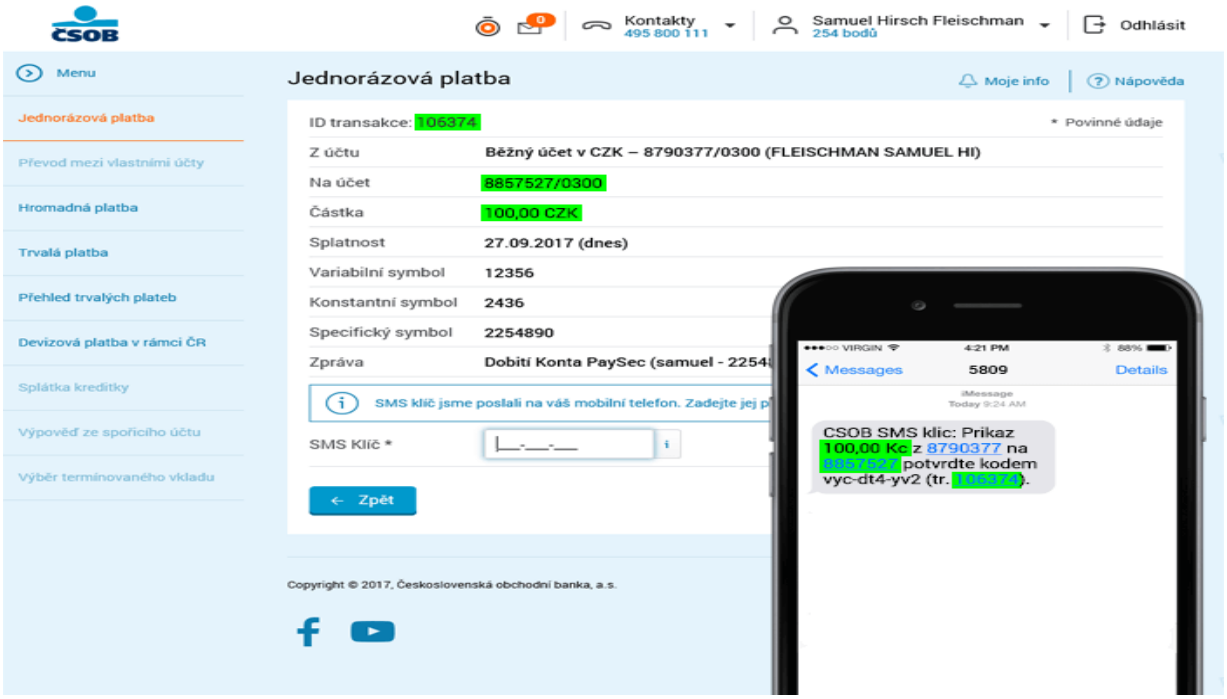


Obrázek 18 Vzor správného přihlášení do IB

zdroj: ČSOB

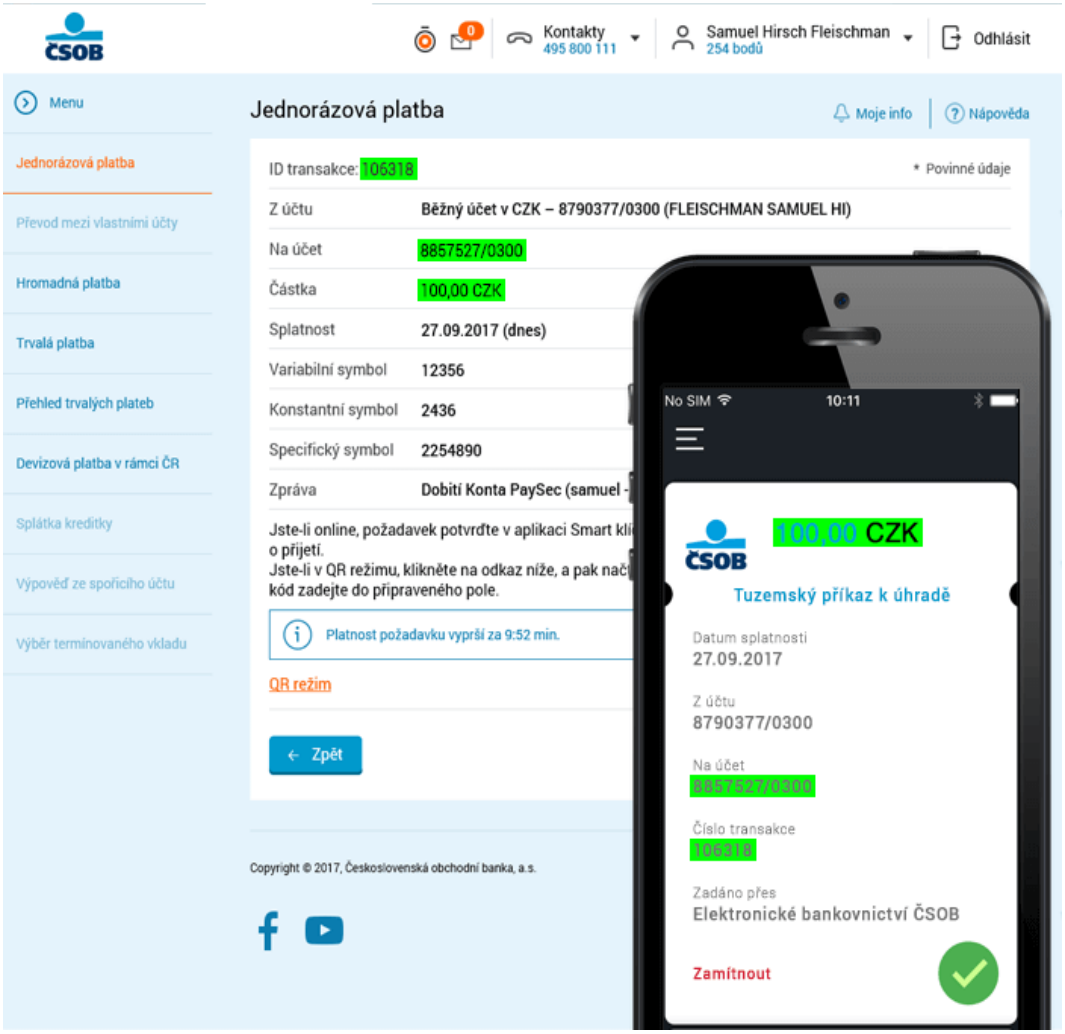
7. **Neotevírejte nedůvěryhodné e-maily a neznámé soubory z internetu** – podezřelé e-maily je vhodné okamžitě mazat. V případě neznámých odesilatelů je bezpečnější v elektronické poště neotevírat přílohy nebo odkazy. Nikdy nereagujte na e-mail, který vyžaduje sdělení osobních údajů. Za bezpečnostní riziko se rovněž považuje, pokud jsou navštěvovány nedůvěryhodné stránky a pokud dochází ke stahování neznámých souborů, zvláště souborů s příponu EXE.

8. **Zvyšte bezpečnost svého účtu pomocí informačních SMS nebo e-mailů** – v internetovém bankovnictví lze nastavit zasílání zpráv o veškerých operacích na účtu. Na každý pohyb je pak klient včas upozorněn.
9. **Čtěte komunikaci s bankou** – v případě potvrzování transakcí pomocí SMS klíče nebo Smart klíče je nanejvýše vhodné překontrolovat zaslanou zprávu od banky, zda souhlasí veškeré údaje ve zprávě s údaji zadanými v elektronickém bankovnictví. Příklady komunikace s bankou jsou znázorněny na obrázcích 19 a 20.



Obrázek 19 Příklad ověřovací SMS zprávy

zdroj: ČSOB



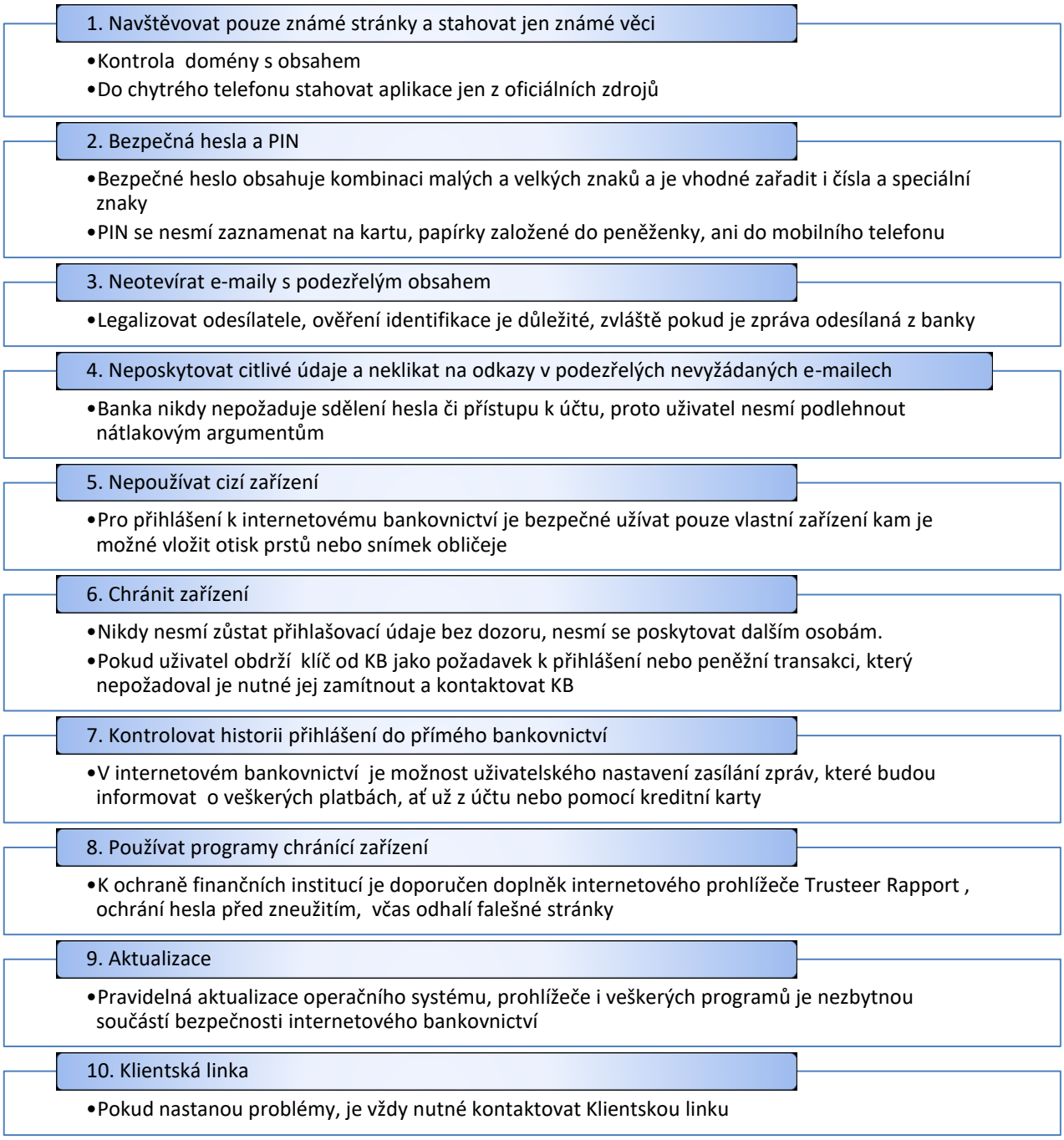
Obrázek 20 Jednorázová platba

zdroj: ČSOB

10. **Chraňte svůj privátní klíč na čipové kartě** – podpis v elektronické podobě na čipové kartě je jako vlastní podpis, musí proto být ochráněn před zneužitím a uložen na bezpečném místě.

Doporučení Komerční banky

I na stránkách Komerční banky, a.s., lze nalézt doporučení pro bezpečné užívání internetového bankovnictví. Obrázek 21 zobrazuje informace čerpané z oficiálních stránek KB. [26]



Obrázek 21 Doporučení Komerční banky

zdroj: vlastní zpracování

V poslední době se v médiích často objevují upozornění na útoky, kde oběťmi jsou uživatelé přímého bankovnictví. Je pravděpodobné, že právě díky zveřejňování tohoto rizika je v současnosti 80 % klientů bank obezřetnější při užívání internet bankingu. Z dotazovaných respondentů společností Moneymag má 95 % uživatelů nainstalovaný antivirový program a 90 % z nich používá při přihlášení

do elektronického bankovnictví pouze své vlastní zařízení, 83 % uživatelů neotevírá přílohy a odkazy od neznámých odesílatelů e-mailů. Největším rizikem, které ohrožuje uživatele, je nesledování historie a nezabezpečený přístup dětí k počítači. [27]

Jak uvedl Mojmír Prokop, manažer Distribučních kanálů a Customer Intelligence Komerční banky, Česká republika je zemí, která je určena pro testování stále vynalézavějších metod, jakými lze zcizit peníze na napadeném účtu uživatele elektronického bankovnictví. Dále uvedl, že ačkoliv se přístup Čechů k bezpečnosti počítačů v poslední době napravil, stále je zapotřebí se zaměřit na tři oblasti [27]:

- velmi rizikové stahování nelegálního softwaru, toto riziko podstupuje přibližně 20 % dotazovaných;
- nesledování historie přihlašování do internetového bankovnictví, pouze 47 % respondentů ji kontroluje;
- počítač určený k přihlašování do elektronického bankovnictví používají bez dozoru i děti uživatelů elektronického bankovnictví, běžně asi 36 %.

4.1 Všeobecné zásady bezpečnosti internetového bankovnictví

Od ledna 2019 platí v České republice zákon č. 370/2017 Sb. o platebním styku, který v § 223 nařizuje používání silného ověření uživatele. V praxi to znamená, že pokud je používán platební účet uživatelem prostřednictvím internetového bankovnictví, je bankou požadováno silné ověření. [28]

Ve výše uvedeném zákoně se říká [28]:

„Silným ověřením uživatele se pro účely tohoto zákona rozumí ověření, které je založeno na použití alespoň 2 z těchto prvků:

a) údaje, který je znám pouze uživateli,

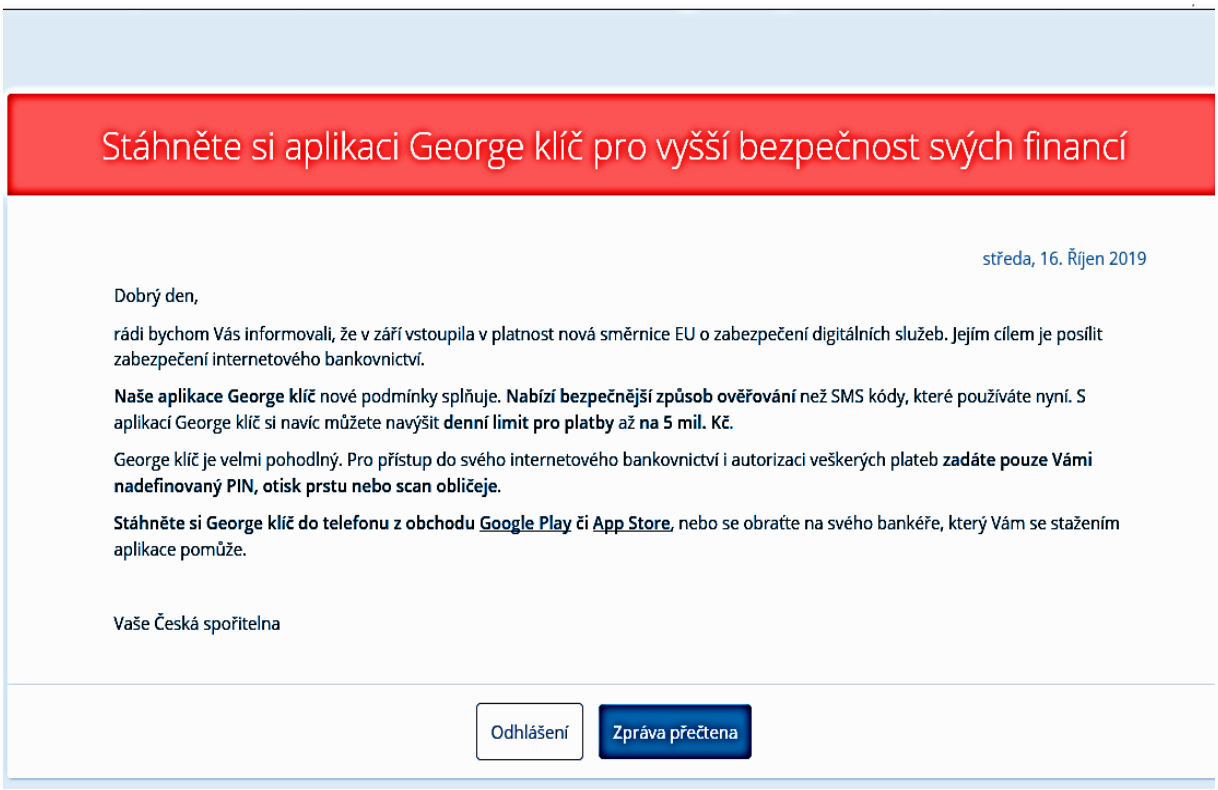
b) věci, kterou má uživatel ve své moci,

c) biometrických údajů uživatele.

Prvky ověření musí být vzájemně nezávislé a prolomení jednoho prvku nesmí ovlivnit spolehlivost prvků ostatních. Postup ověření musí zabránit zneužití prvků, které jsou k ověření používány.“

Dalším důležitým dokumentem je směrnice PSD 2. Stěžejní úlohou směrnice Evropské unie PSD 2 (Payment Services Directive, druhá směrnice EU o platebních službách) je pojistit bezpečnost plateb elektronického bankovnictví a snížit pravděpodobnost podvodného jednání. V rámci zákona č. 370/2017 Sb., o platebním styku přinesla tato směrnice povinnost silného ověření klienta. Dvoufaktorové ověření podle směrnice PSD 2 museli banky a ostatní poskytovatelé bankovních služeb uvést do praxe do 14. září 2019. [29]

Česká spořitelna upozorňuje své klienty přihlašující se do bankovní aplikace George na možnosti většího zabezpečení financí, aplikací George klíč nabízí bezpečnější způsob přihlášení do IB, obrázek 22.



Obrázek 22 Upozornění ČS

zdroj: [30]

Silné ověření klienta – jedná se o dvoufaktorovou autentizaci, tj. spojení dvou ze tří elementů. Tyto prvky ověření musí být navzájem nezávislé. Pokud je překonán jeden, je nepřípustné, aby ohrozil spolehlivost elementů dalších. [29]

Prvky silného ověření klienta [29]**:**

- data, která zná pouze uživatel – znalostní prvek,
- movitá věc v rukou uživatele – majetkový prvek,
- biometrické údaje uživatele.

Data, která zná pouze uživatel – znalostní prvek [29]**:**

- heslo, PIN, používaný pohyb při zabezpečení smartphonu,
- soukromé údaje známé uživateli.

Za prvek znalosti nelze uznat údaje o platební kartě, uživatelské jméno ani emailovou adresu.

Movitá věc v rukou uživatele – majetkový prvek

Jedná se o zařízení a aplikace, jež lze považovat za stvrzení, že jsou opravdu v užívání klienta, například: mobilní telefony, chytré hodinky, aplikace spojené s ověřeným zařízením apod. [29]:

- zařízení, na které je zaslán autentizační kód, SMS;
- elektronický podpis uložený na určitém zařízení zákazníka;
- hardwarový nebo softwarový token;
- karta přečtená čtečkou karet.

Biometrické údaje uživatele [29]**:**

- skenování sítnice a duhovky a otisků prstů,
- rozpoznávání obličeje, hlasu, geometrie ruky
- dynamismus srdečního pulsu.

Silné ověření klienta je požadováno v následujících případech [29]**:**

- klient se přihlašuje do elektronického bankovnictví,
- při platbě platební kartou,
- při zadání příkazu k úhradě z internetového bankovnictví.

Není důležité, u jaké banky má uživatel založený účet, zásady pro bezpečné užívání internetového bankovnictví je možné zevšeobecnit.

Internetový prohlížeč

Internetový prohlížeč představuje otevřené dveře do internetového světa, a tak je důležité věnovat pozornost nejen jeho bezpečnosti, ale i jeho výběru. Server Odstranitvirus.cz uvádí 5 nejbezpečnějších prohlížečů roku 2019 [31]:

- Google Chrome,
- Tor,
- Microsoft Edge,
- Epic Privacy Browser,
- Opera. [32]

Aktualizace softwaru

Základem bezpečnosti operačního systému a internetového prohlížeče je používání aktuální verze. Výrobci softwaru pracují neustále na odhalování chyb a následných bezpečnostních záplatách. Chyby, které jsou možným bezpečnostním rizikem, by mohli útočníci použít k přístupu do neaktualizovaného počítače. Aktualizovat je proto nutné bez odkladu. [31]

Doplňky prohlížeče

Instalace doplňků do počítače vyžaduje ve většině případů souhlas s přístupem k přehledu aktivit, které jsou na počítači prováděny, tj. co je stahováno, vkládáno, navštívené stránky a kam se uživatel přihlašuje. Ačkoliv se to zdá být nevinné, tyto informace mohou být zneužity. Hrozí riziko podvrhu škodlivého softwaru, přestože byl doplněk stahován z oficiálního zdroje. Aplikace a doplňky z podezřelých zdrojů je velmi rozumné odmítnout. U oficiálních distributorů je vhodné zkontrolovat recenze ostatních uživatelů. [31]

Možnosti zabezpečení

Pokud antivirový nebo další bezpečnostní program umožňuje pracovat ve virtuálním prohlížeči, znamená to, že internetový prohlížeč nedisponuje přístupem k systému. Nemůže tak umožnit internetovým stránkám, které jsou hrozbou, atakovat počítač, vložit do něj malware nebo virus. [31]

Antivirus a další zabezpečení

Antivirový program je dnes brán jako samozřejmost, ale připomenout jeho důležitost je jistě významné nejen při zabezpečování počítače, ale i ostatních přístrojů, kterými se lze připojit k internetové síti. Je vhodné i použití firewallu, který v počítačové síti dokáže povolit nebo zakázat komunikaci podle nějakých předdefinovaných pravidel. Má schopnost bránit útokům, u kterých hrozí riziko převzetí kontroly nad připojeným zařízením. Lze jej jednoduše připodobnit ke stráži, která rozhodne, komu povolí vstup

do svého hlídaného objektu. [33] Není proto vhodné tuto funkci antivirovému programu zakazovat. Pokud již existuje podezření na proniknutí škodlivého softwaru, lze provést bezprostřední revizi pomocí jednorázového prověření pomocí Online Scanneru. [31]

Cizí zařízení

Své vlastní zařízení uživatel dokonale zná, disponuje veškerými potřebnými informacemi o jeho zabezpečení. U cizích zařízení však tyto informace zůstávají skryty. Obzvláště u počítačů v internetových kavárnách je bez záruky, jakým způsobem bylo se zařízením pracováno či co tam bylo nainstalováno. Pro přihlášení k internetovému bankovnictví jsou proto takováto zařízení naprosto nevhodná. [31]

Neobvyklé chování prohlížeče a počítače

I přes nejvyšší možnou obezřetnost je možné, že bude útok na zařízení uživatele úspěšný. Stává se to v rámci interní sítě domácnosti či firmy. Útok lze rozpoznat podle samovolného spouštění programů, aplikací, chybových hlášení. V tom okamžiku je nutné neprodleně spustit antivirovou kontrolu a nainstalovat aktualizace. V případě přetrvávajících potíží je nutné vyhledat odborníka. [31]

Získání informací

Neuvěřitelně rychlý vývoj v oblasti IT může způsobit, že se uživatel v množství nových funkcí může ztrácet a nepochopí je. Pak je vhodné zkusit hledat informace v uživatelském manuálu či na internetu. Pokud však potíže i nadále přetrvávají, lze se obrátit na odborníky či na zákaznickou linku výrobce či prodejce. Pokud se novinky týkají produktu bankovnictví, tak je správné volat pobočku banky, kde školení pracovníci rádi vyřeší každý problém. [31]

Signály [31]:

- Bankovnictví obsahuje chyby – mohou chybět části grafiky, text obsahuje pravopisné a gramatické chyby, bez jakékoliv informace od banky má systém

jiné vlastnosti; v takovém případě existuje možnost, že se jedná o podvržené stránky.

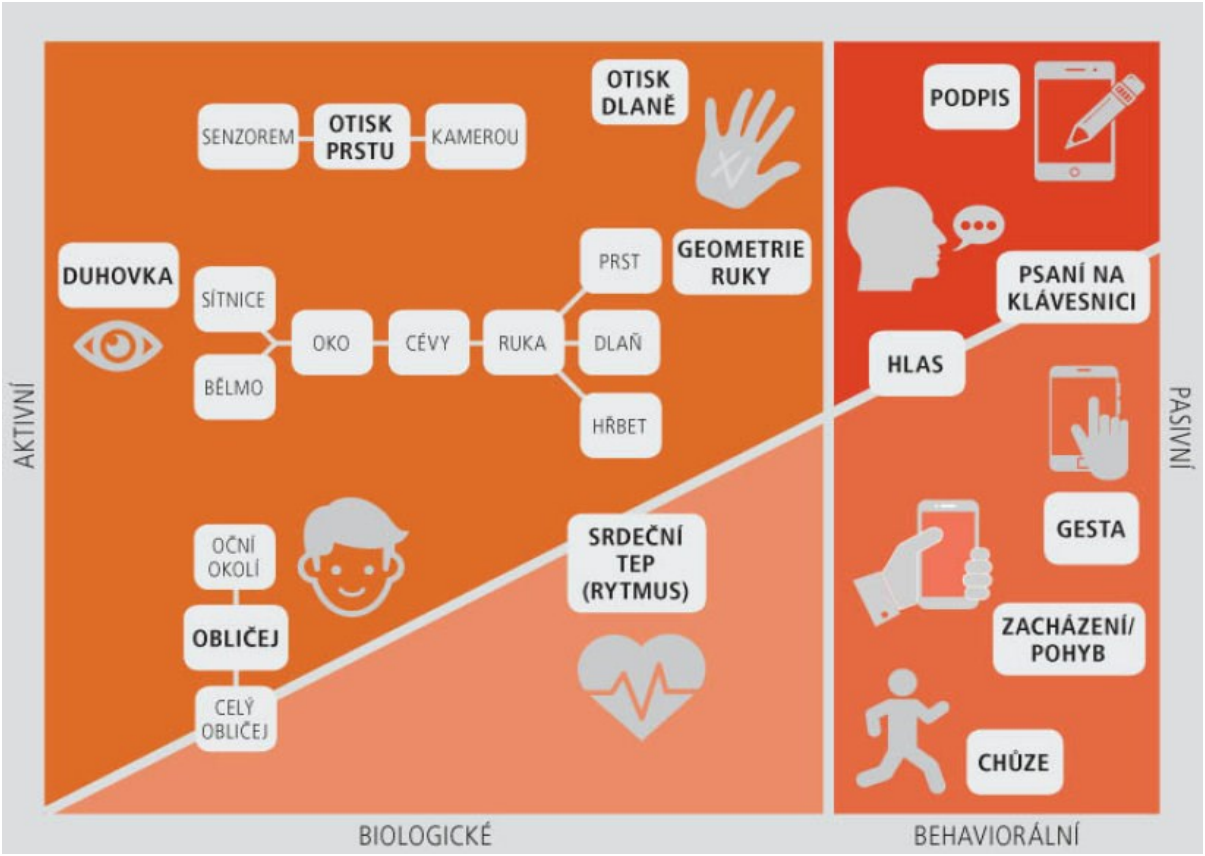
- Jiná adresa webu nebo chybí zabezpečení – odlišná doména od původní, generická doména není „cz“, chybí bezpečnostní „s“. Zde je riziko, že uživatel byl přesměrován na jiný server.
- Nahlášená chyba certifikátu – certifikát hlásí chybu po zadání adresy nebo při zvolení záložky, problémem může být odvolaný certifikát, neodpovídající adresa certifikátu. V tomto případě existuje riziko podvrženého certifikátu.
- Přišla autorizační SMS, ovšem žádnou platbu uživatel nezadal – je celkem jisté, že v tomto případě jde o podvod. Útočník zneužil přihlašovací údaje, ale bez zadané autorizační SMS nemůže dokončit převod peněz.

Co dělat, pokud uživatel zaznamená něco podezřelého [31]**:**

- neprovádět v internetovém bankovnictví další činnost,
- ukončit připojení k bankovnictví,
- při dalším přihlášení do internetového bankovnictví užít jiný internetový prohlížeč,
- při opakovaném problému ukončit připojení k bankovnictví a informovat banku.

4.2 Biometrická ochrana

Biometrie bude v budoucnosti používána pro ověřování identity v mnohem větší míře, než ve které je používána v současné době. Obrázek 23 zobrazuje široké možnosti biometrie.



Obrázek 23 Biometrické znaky a postupy

zdroj: Infografika **[34]**

Stále větší nabídka na trhu služeb, aplikací či sdílených dat nutí běžného uživatele užívat mnoho hesel. To je velmi nekomfortní, navíc je nutno zabraňovat ustavičně se množícím atakům, ať už ručních, automatizovaných, hromadných či cílených. Biometrická ochrana je možným a pohodlným řešením ochrany uživatele. Čtečky otisků prstů jsou dnes již celkem běžnou ochranou mobilních zařízení. Obliba biometrie jistě v budoucnu poroste spolu s vývojem techniky. [34]

Biometrický znak vhodný pro použití k potvrzení identity musí být jedinečný, trvalý a měřitelný. Pro bezpečnou identifikaci osoby je dále nutné, aby byl vzorek (snímek,

záznam) spolu s identifikačními daty zachovatelný. Při tomto uložení nesmí být narušena jeho jedinečnost. Při výběru příhodných biometrických znaků se jejich vlastnosti známkují, hodnotí se jejich univerzálnost, míra jedinečnosti, stability, měřitelnosti a další kritéria. [34]

Stabilní biologické znaky jsou charakteristické svou pomalou proměnou a svou jedinečností. Jedná se například o obličej, otisk, duhovku, cévy. [34]

Za méně stabilní jsou považovány behaviorální znaky. Ty se mohou během času měnit i působením nemoci, stresu či věkem a kontrolní vzorek je tak nutno aktualizovat. Jedná se například o gesta, hlas, tempo psaní na klávesnici. [34]

Kombinace dvou nebo více znaků se nazývají multimodální postupy, kde lze volit mezi pohodlím (uživatel si zvolí ověřovaný znak) a spolehlivostí (spojení ověření více znaků). Zásady více faktorového ověření ovšem běžně nepovolují kombinování více biometrických metod potvrzení. [34]

Při používání biometrie jako prvku ověření je nutné počítat s rozdíly oproti klasickému ověření heslem či tokenem. Biometrie je variabilní, sejmutí prvků podléhá mírným odlišnostem. Naopak hesla a klíče mají vždy přesnou shodu. Pro ověření není tedy poskytnuta přesná shoda, ale hledá se správná míra podobnosti. Tento způsob poskytuje pohodlí pro uživatele i postačující rozsah ochrany. Biometrie používá znaky, které nelze utajit, ale její podstata bezpečné ochrany spočívá v obtížnosti napodobení (musí být získány a předloženy snímacímu zařízení). Jednou z velmi důležitých schopností takovýchto snímacích zařízení je proto ověření, zda předložené znaky prezentuje žijící osoba. [34]

Předpovědi analytiků společnosti Gartner, které se týkají oblasti biometrického ověřování [35]:

- Organizace používající biometrické způsoby ověření budou do konce roku 2020 kombinovat ze 70 % ověření obličeje, hlasu a pasivních behaviorálních znaků místo otisku prstu, v současnosti tyto kombinace využívá jen z 5 %.

- Společnosti používající již dnes biometrické ověřování na mobilních zařízeních budou do konce roku 2020 ze 30 % užívat metody nestandardních funkcí zařízení nebo OS, dnes je využívá jen 5 %.
- Je předpoklad používání kombinací biometrických metod a analytiky s mobilními push postupy u 70 % podniků do konce roku 2022. V současnosti toto spojení není prakticky používáno.

4.3 Pojištění internetových rizik

V současné době vnímá 29 % lidí ztrátu dat i on-line bezpečnost za riziko, se kterým se pravděpodobně osobně během následujících pěti let osobně střetne. Mezi tato rizika spadá i zneužití přímého bankovnictví. Z těchto důvodů v poslední době vzrůstá poptávka po možnosti pojištění rizik takovýchto oblastí, což prokázala i studie společnosti BNP Paribas Cardif uskutečněná v šesti zemích v Evropě. [36]

Velkým ohrožením pro uživatele internetového bankovnictví je převážně nekázeň samotných uživatelů. Společnost Europ Assistance společně s agenturou Lexis provedla průzkum pravidelné změny hesla, kdy z výsledků plyne, že pouze 11 % dotazovaných provádí pravidelnou změnu hesel a naopak 38 % českých uživatelů internetu nikdy nemění dobrovolně svoje heslo. [36]

Pokud dojde ke zneužití údajů z platebních karet na internetu, popřípadě internetového bankovnictví, může pomoci pojištění internetových rizik. Pojištění umožňuje díl rizika souvisejícího s používáním internetu přesunout na pojištění. Jakmile nastane pojistná událost, pojištění poskytne jednak pomoc odbornou, jednak plnění finanční. [36]

Co vše je schopno pokrýt pojištění internetových rizik, je graficky znázorněno na následujícím obrázku 24.

Obrázek 24 Co kryje pojištění internetových rizik

zdroj: Security magazín

Shrnutí

Tato kapitola se zabývá popisem vhodných opatření, která, pokud jsou dodržována, vedou k větší bezpečnosti při používání internetového bankovnictví. Jistě je možné podotknout, že ani tato opatření nejsou schopna zajistit dokonalou bezpečnost. Tu opravdu nelze zaručit nikdy, přestože se vývojáři snaží vyvíjet stále bezpečnější programy a zákony nařizují ověření více stupni přístupových údajů. Na druhé straně pomyslné barikády totiž vždy stojí útočníci, kteří vymýšlejí stále rafinovanější způsoby, jak odcizit uživatelům elektronického bankovnictví jejich přístupové údaje nebo rovnou finance z účtu.

Tuto kapitolu lze považovat za návod k dostatečnému zvýšení úrovně zabezpečení internetového bankovnictví a dále za zdroj informací o možnostech nejen současných technologií, ale i technologií blízké budoucnosti.

5 ZHODNOCENÍ A DOPORUČENÍ

Analýza rizik je proces, který začíná zjištěním, co je opravdu nutné chránit. Při používání internetového bankovnictví jsou za chráněné aktivum považovány finanční prostředky na účtu, avšak osobní údaje je též nutné chránit. Jakmile je známo, co je nutné ochraňovat, následuje další krok, a to odhalení pravděpodobných rizik. Na problematiku rizika je možné nahlížet z mnoha úhlů, jelikož riziko má mnoho podob. Někdy je možné riziko vyčíslit, v jiném případě je možné jej ohodnotit pouze subjektivně. Některé riziko lze ovlivnit a v tomto případě je možné se mu i zcela vyhnout, v jiném případě je však riziko neovlivnitelné a potom lze pravděpodobné škody pouze redukovat, například pojištěním, nebo přistoupit k retenci rizika, což znamená nečinit žádná opatření.

Tato práce upozorňuje především na rizika ovlivnitelná. V takovémto případě je na uživateli internetového bankovnictví, jaký zaujme postoj a jakou část zodpovědnosti za zabezpečení svého bankovnictví přijme.

V této fázi analýzy rizik začíná zkoumání účinných opatření, které lze implementovat do běžného používání internetu, nejenom při práci s přímým bankovnictvím. Čtvrtá kapitola podrobně popisuje správné chování klientů elektronického bankovnictví a využití bezpečnostních prvků. Je opravdu velmi alarmující, jak nezodpovědně se mnozí klienti chovají, aniž si uvědomují ohrožení, a to nejenom finančních prostředků, ale i osobních údajů, které útočník může zneužít a velmi zkomplikovat své oběti existenci.

Při výběru metody a volby opatření je velmi důležité znát poměr ceny chráněného aktiva a pravděpodobnost, s jakou může nastat nežádoucí jev. Volba vhodného opatření závisí nejen na míře jeho účinnosti, ale také na míře jeho přiměřenosti k případné škodě. V případě, že na účtu máme minimální zůstatek postačující na bankovní poplatky, je celkem zbytečné uzavírat pojištění internetových rizik.

Ze zjištění v předchozích kapitolách vyplývá, že za většinu problémů spojených s bezpečností internetového bankovnictví si mohou sami jeho uživatelé. Nedodržují základní zásady související s používáním internetového připojení. Po vyhodnocení materiálů použitých v této bakalářské práci bylo zjištěno, že největším rizikem pro klienta přímého bankovnictví je klient sám. Nedodržování základních pravidel poskytuje prostor útočníkům, kterým tak k jejich nemalé radosti uživatel značně usnadňuje nelegální činnost.

Přitom řešení je velmi jednoduché: stačí pravidelně měnit hesla, aktualizovat software a dbát na fyzické zabezpečení přístroje, který je používán k přihlášení do elektronického bankovnictví.

ZÁVĚR

V dnešní době, která je charakteristická svou uspěchaností a neustálým nedostatkem volného času, je zvykem i nutností, zjednodušovat běžné lidské činnosti. Mezi ně patří i obyčejné placení účtů. Jen velmi málo lidí v produktivním věku je ochotných zajít s nastřádanými poštovními poukázkami na pobočku pošty. Je to považováno nejen za ztrátu času, ale ani poplatky spojené s úhradou poukázek nejsou zrovna zanedbatelné. Mnohem jednoduší je pohodlně zapnout počítač, připojit se k internetu na webovou stránku příslušné banky, zaplatit nejen veškeré účty, ale i zkontrolovat výši konta, popřípadě zaktivovat další služby, které banka nabízí.

Za posledních deset let se možnosti internetového bankovnictví v oblasti poskytovaných služeb značně rozšířily. Nejenže lze nahlížet do účtu a zadávat platby v Kč či cizí měně, lze také uzavírat půjčky a pojištění. V současnosti dokonce není nutností být doma u počítače, protože účty je možno platit na jakémkoli místě s připojením k internetu, což v dnešní době až na pár výjimek znamená všude. Tento vývojový skok v přístupu k účtům umožňují nové technologie, které jsou širokým vrstvám obyvatelstva k dispozici skrze stále rozšířenější chytré telefony, tablety a v blízké budoucnosti pravděpodobně i chytré hodinky.

S neustále rozmanitějším spektrem možností zároveň stoupá i míra rizika plynoucího z používání těchto přístrojů. I v počátku elektronického bankovnictví existovala rizika, a i tehdy se útočníci snažili vymámit z uživatelů přístupové údaje. Oproti dnešním podvodům však byly tehdejší ataky mnohem naivnější a snáze odhalitelné: obvykle je prozradil chybný pravopis a neodpovídající grafika. Spolu s pokrokem v oblasti ochrany uživatelů však současně roste i míra sofistikovanosti útočníků.

Každý, kdo používá elektronické bankovnictví, si proto musí uvědomit, že největší část zodpovědnosti za bezpečné užívání leží právě na nás, na uživatelích. I když se banky snaží být vždy o krok před útočníky, nedokážou ochránit účty klientů, pokud klienti sami nedodržují zásadní bezpečnostní doporučení. Ve čtvrté části byly způsoby

ochrany elektronického bankovnictví podrobně popsány.

V zásadě jde o ochranu zařízení, které je pro účel připojení k účtu používáno, počínaje ochranou před zneužitím, přes aktualizaci programů a antivirů, po ochranu přihlašovacích údajů. Na ochranu uživatelů myslí i legislativa, která zákonem nařizuje zvýšenou ochranu uživatelů. Od roku 2019 musela většina bank zpřísnit způsob přihlášení k účtu, kdy nepostačí pouze znát přihlašovací jméno a heslo, ale je povinný další údaj, například SMS kód. Hlavním účelem směrnice Evropské unie PSD 2 je zvýšit úroveň zabezpečení plateb a snížit riziko podvodného jednání. V rámci zákona č. 370/2017 Sb. byla zavedena povinnost silného ověření.

I když má elektronické bankovnictví svá rizika, pro uživatele je tento způsob přístupu k účtu natolik komfortní, že zcela zaručuje další nárůst uživatelů. Cesta zpátky dnes už prakticky není možná, jelikož návrat uživatelů zpět k papírovým složenkám a ochotě trávit svůj volný čas ve frontě na poště či v bance je velmi nepravděpodobný.

Na závěr je důležité zmínit, že cíl práce, tj. najít, identifikovat a analyzovat rizika z pohledu uživatele internetového bankovnictví, byl naplněn. Dalším cílem bylo formulovat doporučení týkající se správného a bezpečného chování při užívání IB. I v tomto ohledu bylo cíle dosaženo.

POUŽITÁ LITERATURA

1. **Finrada.** Internetové bankovnictví převahy a slabiny. *Finrada.cz.* [Online] Finrada.cz, 07. září 2018. [Citace: 26. květen 2019.] https://finrada.cz/noviny/internetove-bankovnictvi-prevahy-a-slabiny.

2. **MÁČE, Miroslav.** *Platební styk - klasický a elektronický.* Praha : Grada Publishing, a.s., 2006. ISBN 80-247-1725-5.

3. **MEJSTŘÍK, Michal, Magda PEČENÁ a Petr TEPLÝ.** *Bankovnictví v teorii a praxi.* Praha : Nakladatelství Karolinum, 2014. ISBN 978-80-246-2870-7.

4. **Finance.cz.** Přímé bankovnictví. *Finance cz.* [Online] 2012. [Citace: 02. únor 2019.] https://www.finance.cz/ucty-a-sporeni/bezne-ucty/abeceda-beznych-uctu/prime-bankovnictvi/.

5. **KRÁL, Mojmír.** *Bezpečný internet Chraňte sebe i svůj počítač.* Praha : Grada Publishing, a.s., 2015. ISBN 978-80-247-5453-6.

6. **Bankovnípoplatky.** Podíl klientů internetového bankovnictví v ČR roste nejvíce v EU. *ČTK.* [Online] ČTK, 11. červen 2018. [Citace: 2. únor 2019.] https://www.bankovnipoplatky.com/podil-klientu-internetoveho-bankovnictvi-v-cr-roste-nejvice-v-eu-36816.

7. **Komerční banka.** Apple Pay je tady! *Komerční banka.* [Online] 2019. [Citace: 4. červen 2019.] https://www.kb.cz/cs/ostatni/nase-aplikace/mobilni-platby/apple-pay?utm_id=43864&utm_medium=cpc&utm_source=seznam&utm_campaign=apple_pay~apple_pay&utm_content=search&utm_term=apple_pay_banky.

8. **Moneta.** Co je Google Pay? *Moneta Money Bank, a.s.* [Online] MONETA Money Bank, a. s., 2019. [Citace: 4. červen 2019.] https://www.moneta.cz/caste-dotazy/odpoved/co-je-google-pay.

9. **Eurostat.** ZÁVĚREČNÁ ZPRÁVA Z HODNOCENÍ DOPADŮ REGULACE. *Eurostat.* [Online] 03. 12 2018. [Citace: 15. 08 2019.]

www.ictu.cz/fileadmin/user_upload/documents/.

10. **JEŽEK, Martin.** Jak se nenechat nachytat na internetu. *Finance.cz.* [Online] Mladá fronta a. s., 16. říjen 2017. [Citace: 03. únor 2019.] https://www.email.cz/web-office/GVANzd4dxoQz8MYAS3a6c11Ey-_4hhcz7Wc93Yv_GaKcFjFSnuluJ849EEfayRzT11Uoc-M/bezpečnostní%20prvky.docx.

11. **KRAUS, Tomáš.** Proč a jak přejít na https. *tk tomaskrause.* [Online] 11. leden 2017. [Citace: 19. květen 2019.] https://tomaskrause.cz/proc-a-jak-prejit-na-https/.

12. **KIM, Peter.** *HACKING - praktický průvodce penetračním testováním.* Brno : Zoner Press, 2015. ISBN 978-80-7413-313-8.

13. **KOŽÍŠEK, Martin a Václav PÍSECKÝ.** *Bezpečně n@ internetu.* Praha : Grada Publishing, a.s., 2016. ISBN 978-80-247-5595-3.

14. **KOPECKÝ, Karel.** Co je hoax. *E-bezpečí.* [Online] Pedagogická fakulta Univerzity Palackého v Olomouci, 5. 18 2008. [Citace: 11. 10 2019.] https://www.e-bezpeci.cz/index.php/temata/hoax-spam/91-25. ISSN: 2571-1679.

15. **PETROWSKI, Thorsten.** *Bezpečí na internetu pro všechny.* Liberec : Dialog, 2014. ISBN 978-80-7424-066-9.

16. **měšec.cz.** Internetové bankovnictví: Co je nejdůležitější? *Měšec.cz.* [Online] internet.info.Měšec.cz, 2005. [Citace: 11. 10 2019.] https://www.mesec.cz/clanky/internetove-bankovnictvi-co-je-nejdulezitejsi/. ISSN 1213-4414.

17. **Braintools.** Analýza rizik. *BrainTools.* [Online] Brain Tools Group, s.r.o., 2019. [Citace: 2. únor 2019.] https://www.braintools.cz/toolbox/zvladani-rizik/jak-analyzovat-rizika.htm.

18. **SMEJKAL, Vladimír a Karel RAIS.** *Řízení rizik ve firmách a jiných organizacích.* Praha : Grada Publishing, a.s., 2011. ISBN 978-80-247-7005-5.

19. **STAROBA, Jan.** Analýza podnikatelských rizik v podniku. *Bakalářská práce.* Zlín :

Univerzita Tomáše Bati ve Zlíně, 2013. [vedoucí práce] KONEČNÝ, Jiří.

20. **FOTR, Jiří a Jiří HNILICA.** *Aplikovaná analýza rizika ve finančním managementu a investičním rozhodování.* Praha : Grada Publishing, a.s., 2014. ISBN 978-80-247-5104-7.

21. **PMConsulting.** Slovník. *PM Consulting.* [Online] 2019. [Citace: 23. 10 2019.] https://www.pmconsulting.cz/slovnikovy-pojem/ripran/.

22. **RIPRAN.** RIPRAN. *RIPRAN.* [Online] RIPRAN, 2019. [Citace: 23. 10 2019.] https://ripran.cz/popis2.html.

23. **KYTLER, Lukáš.** Bezpečnost a rizika platebních karet (výsledky průzkumu). [Online] 2017. https://bezpecnost-a-rizika-platebni.vyplnto.cz..

24. **MULLEROVÁ, Kateřina.** Internetové bankovnictví (výsledky průzkumu). [Online] 2018. https://64419.vyplnto.cz.

25. **ČSOB.** Zásady bezpečného užívání elektronického bankovnictví. *ČSOB.* [Online] ČSOB, 2019. [Citace: 03. únor 2019.] https://www.csob.cz/portal/bezpecnost/jak-se-branit/zasady-bezpecneho-uzivani-elektronickeho-bankovnictvi.

26. **KB.** Desatero bezpečnosti. *KB.* [Online] Komerční banka, 2019. [Citace: 03. únor 2019.] https://www.kb.cz/cs/bezpecnost/desatero.

27. **Moneymag.** Buďte opatrní při přihlašování do internetového bankovnictví. *MoneyMAG.cz.* [Online] 20. červenec 2015. [Citace: 2. únor 2019.] https://moneymag.cz/bankovnictvi/4748-budte-opatrni-pri-prihlasovani-do-internetoveho-bankovnictvi. ISSN 2336-2588.

28. **Česko.** Zákon č. 370/2017 Sb. ze dne 1.4.2019, o platebním styku, částka 129. *Sbírka zákonů.* Praha : Poslanecká sněmovna, 2019.

29. **SOUKAL, Marek.** Silné ověření klienta při poskytování platebních služeb. *epravo.cz.* [Online] EPRAVO.CZ, a.s., 18. 09 2019. [Citace: 16. 10 2019.] https://www.epravo.cz/top/clanky/silne-overeni-klienta-pri-poskytovani-platebnich-sluzeb-109952.html. ISSN 1213-189X.

30. **ČS.** George. *Česká spořitelna.* [Online] Česká spořitelna, 16. 10 2019. [Citace: 21. 10 2019.] https://george.csas.cz/loggedout.html?logout=automatic&state=overview&institute=1&lang=cs&country=CZ.

31. **c-journal.cz.** Bezpečné internetové bankovnictví: Je váš internetový prohlížeč opravdu bezpečný? *c-journal.cz.* [Online] 28. březen 2018. [Citace: 2. únor 2019.] https://www.c-journal.cz/clanky/bezpecne-internetove-bankovnictvi-je-vas-internetovy-prohlizec-opravdu-bezpecny/.

32. **WOODS, Alice.** Mít bezpečný prohlížeč nebylo nikdy důležitější. *Nejbezpečnější prohlížeč roku 2019.* [Online] OdstranitVirus.cz, 16. leden 2019. [Citace: 23. květen 2019.] https://odstranitvirus.cz/nejbezpecnejsi-prohlizec/.

33. **ESET.** Slovník pojmů. *Eset.* [Online] 2019. [Citace: 25. květen 2019.] https://www.eset.com/cz/firewall/.

34. **ERBEN, Lukáš.** Biometrie je více než otisk prstu. *Hospodářské noviny.* [Online] Economia, a.s., 7. listopad 2017. [Citace: 26. květen 2019.] https://ictrevue.ihned.cz/c3-65967870-0ICT00_d-65967870-biometrie-je-vice-nez-otisk-prstu. ISSN 1213-7693.

35. **Gartner.** Technology Insight for Biometric Authentication. *studie společnosti Gartner.* místo neznámé : Security World, 2017.

36. **Bankovnictví.** Pojištění internetových rizik pomůže při zneužití karetních údajů na nebo internetového bankovnictví. *Bankovnictví.* [Online] 4H production s.r.o., 12. duben 2019. [Citace: 26. květen 2019.] https://bankovnictvionline.cz/aktuality/pojisteni-internetovych-rizik-pomuze-pri-zneuziti-karetnich-udaju-na-nebo-internetoveho.

37. **RENOMIA.** Risk management. [Online] 2018. [Citace: 24. březen 2019.] https://www.renomia.cz/risk-management.