Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Bezpečnost firem na sociálních sítích

Bakalářská práce

2021 Lucie Doležalová

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Lucie Doležalová**
Osobní číslo:	**E18783**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Téma práce:	**Bezpečnost firem na sociálních sítích**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je zmapovat sociální sítě využívané ve firemní praxi a popsat možnosti zabezpečení firemních dat. Součástí práce je stanovení základních opatření a pravidel pro firemní prezentace na sociálních sítích.
Osnova:
- Princip sociálních sítí
- Zabezpečení firemních dat
- Sociální sítě využívané ve firemní praxi
- Opatření a pravidla pro firemní prezentace na sociálních sítích

Rozsah pracovní zprávy: **35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1.
KOVACICH, Gerald L. *Průvodce bezpečnostního pracovníka informačních systémů: zavádění a prosazování bezpečnostní politiky informačních systémů*. Brno: Unis, 2000. ISBN 80-86097-42-0.
LOSEKOOT, Michelle a Eliška VYHNÁNKOVÁ. *Jak na sítě: ovládněte čtyři principy úspěchu na sociálních sítích*. V Brně: Jan Melvil Publishing, 2019. Žádná velká věda. ISBN 978-80-7555-084-2.
SHIH, Clara Chung-wai. *Vyděláváte na Facebooku: jak využít sociální sítě k oslovení nových zákazníků, vytvoření lepších produktů a zvýšení prodejů*. Přeložil Patrik MÍŠA. Brno: Computer Press, 2010. ISBN 978-80-251-2833-6.

Vedoucí bakalářské práce: **Ing. Renáta Bílková, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2020**
Termín odevzdání bakalářské práce: **30. dubna 2021**

L.S.

prof. Ing. Jan Stejskal, Ph.D.
děkan

RNDr. Ing. Oldřich Horák, Ph.D.
vedoucí ústavu

V Pardubicích dne 1. září 2020

PROHLÁŠENÍ AUTORA

Prohlašuji:

Práci s názvem Bezpečnost firem na sociálních sítích 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 29.11.2021

Lucie Doležalová v. r.

Poděkování

Tímto bych ráda poděkovala vedoucí mé bakalářské práce Ing. Renátě Bílkové, Ph.D. za poskytnutí kvalitních a odborných rad a doporučení, které mi při zpracování této práce velice pomohly. Také bych chtěla poděkovat mému zaměstnavateli, který se mnou spolupracoval a v neposlední řadě děkuji své rodině a všem, kteří mě po celou dobu studia podporovali.

ANOTACE

Bakalářská práce se zabývá sociálními sítěmi využívané ve firemní praxi a popisuje možnosti zabezpečení firemních dat. Obsah práce představuje základ sociálních sítí, možná rizika, která se na internetu vyskytují a uvádí základní opatření a pravidla pro prezentaci na sociálních sítích.

KLÍČOVÁ SLOVA

Sociální síť, rizika, ochrana dat, zabezpečení

TITLE

Company's security on social media

ANNOTATION

The bachelor thesis deals with social media used by companies and describes the possibilities of securing company data. It also includes the basics and possible risk that can appear on social media and proposes basic measures and rules for their presentation.

KEYWORDS

Social media, risk, data protection, and security

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK

EUR	Oficiální měna, symbol €
iOS	Mobilní operační systém firmy Apple pro telefony iPhone
ID	Jedinečný identifikátor (z angl. Identification)
IP	Protokol internetu (z angl. Internet Protocol)
iPadOS	Mobilní operační systém firmy Apple pro tablety iPad
IT	Informační technologie (z angl. Information Technologie)
macOS	Operační systém firmy Apple pro počítače (z angl. Macintosh Operation Systém)
MB	Násobná jednotka bytu a jednotka binárních dat (Megabyte)
MDM	Nástroj pro hromadnou správu firemních mobilních zařízení (z angl. Mobile Device Management)
MFA	Vícenásobná autentikace (z angl. Multi-Factor Authetication)
PIN	Osobní identifikační číslo (z angl. Personal Identification Number)
tvOS	Operační systém firmy Apple pro TV
URL	Definuje doménovou adresu serveru (z angl. Uniform Resource Locator)
USB	Rozhraní pro připojení přídavného hardware (z angl. Universal Serial Bus)
USD	Oficiální americká měna, symbol $
VPN	Virtuální privátní síť (z angl. Virtual Private Network)

Úvod

Bezpečnost na sociálních sítích je jednou z nejdůležitějších věcí, které by každý uživatel měl věnovat velkou pozornost. V dnešní době jsou podniky dennodenně vystaveny nebezpečí v podobě kybernetických zločinců, kteří míří na soukromé údaje. Podniky většinou podceňují svoji ochranu, dokud se nestane menší či větší malér.

V současné době, kdy sociální sítě určují nové trendy a popularitu, přicházejí i útočníci s novými a zdokonalenými útoky na zařízení. Tato práce se zabývá možnostmi, jak se před těmito útoky chránit a eliminovat tak škody a ztráty u podniků. Nejprve práce charakterizuje sociální sítě a detailní popis sociálních sítí Facebook a Instagram, které používá vybraná firma pro praktickou část. Dále představuje nejpoužívanější techniky podvodů a způsoby, které pomohou firmám zabezpečit soukromé údaje a ochránit tak své jméno, zaměstnance i zákazníky.

Cílem práce je zmapovat sociální sítě využívané ve firemní praxi a popsat zabezpečení firemních dat. Součástí práce je stanovení základních opatření a pravidel pro firemní prezentace na sociálních sítích.

1 SOCIÁLNÍ SÍTĚ

Doba se mění a my s ní. Už nemusíme čekat, až nám přijde dopis od někoho blízkého, nemusíme chodit ven do telefonních budek, abychom slyšeli jejich hlas. V dnešní době je vše mnohem jednodušší. Můžeme kohokoliv vidět, slyšet a zjistit co dělá, kdykoliv se nám jen zachce. K tomu všemu nám v neposlední řadě pomáhá fenomén zvaný sociální sítě. A toho využívají i firmy, které tak vystavují svoje služby a produkty a dostávají se skrze sociální sítě k milionům potencionálních uživatelů.

1.1 Definice sociální sítě

Jedná se o internetovou službu, která zaregistrovaným uživatelům umožňuje si vytvářet osobní nebo firemní profily, za účelem zviditelnění se a udržováním komunikace různými prostředky.

Sociální sítě se pro nás staly zdrojem zábavy, seberealizace, nástrojem komunikace i navazování či udržování vztahů nebo dokonce velkým pomocníkem při studiu i budování kariéry. Jednoduše řečeno, sociální síť nám umožní sdílet cokoliv v podstatně okamžitě a mezi větším počtem uživatelů než jiné prostředky. [12]

1.2 Rozdělení sociálních sítí

Existuje mnoho sociálních sítí. Některé vznikly na základě udržení rodinných vazeb nebo kamarádů, jiné na seznámení s novými lidmi, novými službami nebo produkty.

Lze je rozdělit do několika kategorií [21]:

- Profilově založené sociální sítě: Facebook, Baidu Tieba, VKontakte, LinkedIn
- Obsahově založené sociální sítě: YouTube.com, Instagram, Snapchat, Pinterest
- Virtuální sociální sítě: Second Life, World of Warcraft, World of Tanks
- Micro-blogovací sociální sítě: Twitter, Jaiku
- Komunikační služby: Facebook Messenger, WhatsApp, Viber

V České republice se řadí mezi nejpoužívanější sociální sítě Facebook, Instagram, Youtube, Linkedin, Snapchat a Twitter.

Jaké sociální sítě se řadí mezi TOP 10 ve světě, čím se zabývají a počty jejich aktivních uživatelů ukazuje *Tabulka 1: Nejpoužívanější sociální sítě*. Služby sociálních sítí představují sdílení fotek, sledování videí, poslouchání písniček, psaní blogů, vedení deníku. Komunikace reprezentuje sdílení zpráv mezi uživateli. Hodnoty jsou brány k říjnu 2021. [14]

Tabulka 1: Nejpoužívanější sociální sítě

Pořadí	Název	Stručný popis	Počet uživatelů/měsíc
1.	Facebook	Služby sociální sítě	2 ,895 miliardy
2.	YouTube	Sdílení videí	2 ,291 miliardy
3.	WhatsApp	Komunikace	2,000 miliardy
4.	Instagram	Služby sociálních sítí	1,386 miliardy
5.	Facebook Messenger	Komunikace	1,300 miliardy
6.	WeChat	Komunikace	1,251 miliardy
7.	TikTok	Služby sociálních sítí	1,000 milionu
8.	QQ	Služby sociálních sítí	591 milionu
9.	Snapchat	Komunikace	538 milionu
10.	Twitter	Diskuzní fórum	463 milionu

Zdroj: [14]

Na sociálních sítích je dnes 45 % světové populace. Z téměř 4,4 miliard lidí, kteří mají na světě přístup k internetu je skoro 3,5 miliard lidí na sociálních sítích. Odhaduje se, že v roce 2022 dosáhnou stránky sociálních sítí 3,96 miliardy uživatelů a očekává se, že tato čísla porostou, jak se používání mobilních zařízení a mobilních sociálních sítí stále více prosazují. [14]

To je za tak krátkou dobu jejich existence naprosto fascinující posun v dějinách mezilidské komunikace.

1.3 Jak sociální sítě fungují

Sociální sítě zahrnují rozvoj a udržování osobních a obchodních vztahů pomocí technologie. Děje se tak pomocí sociálních sítí, jako je Facebook, Instagram a Twitter. Tyto stránky umožňují lidem a společnostem vzájemně se spojovat, aby mohli rozvíjet vztahy a sdílet informace, nápady a zprávy.

Členové rodiny, kteří jsou daleko od sebe, mohou zůstat ve spojení prostřednictvím osobních sociálních sítí. Mohou sdílet fotografie a novinky o věcech, které se dějí v jejich životech. Lidé

se také mohou spojit s ostatními (zejména s cizími lidmi), kteří mají stejné zájmy. Jednotlivci se mohou navzájem najít prostřednictvím skupin, seznamů a používání hashtagů. [21]

Obchodníci běžně používají sociální sítě, aby mohli zvýšit podvědomí o značce a podpořit její loajalitu. Díky tomu, že se společnost zpřístupňuje novým zákazníkům a je lépe rozpoznatelná pro stávající zákazníky, pomáhá marketing v sociálních médiích propagovat hlas a obsah značky. [19]

Například častý uživatel Facebooku může poprvé slyšet o společnosti prostřednictvím kanálu zpráv a rozhodnout se koupit produkt nebo službu. Čím více jsou lidé vystaveni značce společnosti, tím větší jsou šance společnosti na nalezení a udržení nových zákazníků.

Obchodníci používají sociální sítě jako způsob, jak zlepšit konverzní poměry. Vytváření následujících položek poskytuje přístup a interakci s novými, nedávnými i starými zákazníky. Sdílení příspěvků, obrázků, videí nebo komentářů na sociálních médiích umožňuje sledovatelům reagovat, navštívit web společnosti a stát se zákazníky.

1.4 Funkce na sociálních sítích

Na sociálních sítích se můžeme setkat s řadou funkcí, které nám ulehčují procházení. Jedny z nejdůležitějších a často opakovaných funkcí na sociálních sítích představím v následujících odstavcích.

Profil

Na všech sociálních sítích má uživatel nebo společnost svoji jakousi vizitku s údaji, podle kterých se na sociálních sítích prezentují a jsou podle nich lépe dohledatelní. Kromě jména uživatele to může být bydliště, datum narození, záliby, informace o vzdělání nebo rodinném vztahu. U společnosti to může být název, sídlo, vznik, služby a produkty. Je pouze na každém z nás, co odkryjeme za citlivé údaje, ale je potřeba si uvědomit, že ne všechna data by měla být volně přístupná. Můžeme si rozmyslet, která data budou dostupná široké veřejnosti, jen vybraným uživatelům nebo která raději neuvedeme vůbec. [8]

Stránky

Dnes téměř každá společnost používá ke své propagaci různé sociální sítě. Stránky slouží především pro představení společnosti a možnosti spojení se zákazníky a fanoušky. Stránky mohou zákazníci sledovat, dávat „To se mi líbí“ a tím se jim na svých profilech začnou zobrazovat nejnovější příspěvky od dané stránky, na které mohou reagovat. Pro vytvoření

stránky je potřeba mít založený profil. Stránky jsou převážně veřejné, takže si je může vyhledat každý. [13]

Komunita

Sociální sítě nabízejí členům příležitost k zakládání komunity neboli skupiny lidí online. Je spoustu faktorů, které mohou způsobit, že se lidé budou chtít připojit do skupin. Například společné pozadí (rodinné skupiny, bývalí spolužáci), kvalifikace (pracovní funkce, status absolventa), zájmy nebo koníčky (sport, domácí zvířata, politická příslušnost, druh nemoci, náboženství atd.). Členství ve skupinách je dobrovolné a může podléhat schválení správce skupiny. Skupiny mohou být veřejné, soukromé nebo tajné. [13]

Veřejná skupina je viditelná. Dá se nalézt přes vyhledávání, jsou vidět její správci, členové i veškerý obsah. Ideální pro předvedení určitého produktu a získání největšího počtu členů. [13]

Soukromá neboli uzavřená skupina, je také viditelná ve vyhledávání, ale veškerý obsah, členové a správci viditelné nejsou. Přístup k těmto údajům mají pouze schválení členové skupiny. V této skupině si lze nastavit prověřovací otázky a na základě toho přijímat nové členy, aby se zamezilo tomu, že dotyčný pouze omylem nezabloudil. [13]

Tajná skupina je naprosto soukromá a skrytá ve vyhledávání. Kromě členů skupiny je pro všechny neviditelná a je možné se do ní přidat pouze na základě pozvánky. Ideální varianta pro žákovské nebo rodičovské skupiny v rámci škol, produktové testování nebo VIP zákazníky. [13]

Interakce mezi uživateli

Na sociálních sítích nejde pouze o to, že si vytvoříte profil (stránku) a připojíte se do nějaké skupiny. Můžete se také sami projevovat a to prostřednictvím statusů, jinak řečeno příspěvků v podobě textu nebo multimediálních obsahů, které si budou moci zobrazit ostatní uživatelé. Ti pak na takový příspěvek mohou zareagovat, ať už třeba přidáním komentáře pod příspěvkem, označením „To se mi líbí“ či jiných reakcí nebo že mohou váš status sdílet na svém profilu či na dalších sociálních sítích. Reakce „To se mi líbí“, označuje, že se danému uživateli líbí konkrétní příspěvek. Může být také značeno palcem nahoru nebo srdíčkem.

Sdílení je další způsob interakce. Týká se jak vlastních příspěvků a příspěvků propojených uživatelů, tak i obsahu jako jsou videa, obrázky, články. Především u sdílení, by si měli uživatelé dát pozor, komu co budou sdílet. Většina sociálních sítí nabízí dobré možnosti pro sdílení obsahu. Můžete si nastavit zda bude veřejný, kde si obsah mohou zobrazit všichni

uživatelé nebo soukromý, kde si zobrazí pouze propojení uživatelé případně jen pár z nich. Máte na výběr, komu budete chtít daný příspěvek ukázat. [8]

Počet označení, komentářů nebo sdílení u jednotlivých příspěvků udává jejich viditelnost a tak i viditelnost autorů. Tomuto se na sociálních sítích říká sociální filtr, kde se zobrazují informace, které jsou doporučeny od lidí s nimiž jste v nějakém způsobu propojeni a z toho se předpokládá, že i vás by například takový příspěvek mohl zajímat. [8]

1.5 Výhody a nevýhody sociálních sítí

Sociální sítě mají schopnost ovlivňovat jednotlivce i společnosti - pozitivně i negativně. Proto je důležité zvážit výhody i nevýhody používání těchto stránek sociálních médií.

Výhody

Jak již bylo zmíněno výše, sociální sítě umožňují jednotlivcům udržovat kontakt s rodinou a přáteli, s nimiž by se jinak nemohli spojit kvůli vzdálenosti nebo proto, že jednoduše ztratili kontakt. Lidé se také mohou spojit s dalšími jednotlivci, kteří mají stejné zájmy a rozvíjet nové vztahy.

Sociální sítě umožňují společnosti spojit se s novými i stávajícími klienty. Mohou využívat sociální média k vytváření, propagaci a zvyšování povědomí o značce. Spoléhají také na recenze a komentáře jejich klientely. Čím více zákazníků zveřejní informace o společnosti, tím cennější je autorita značky. To vede k vyšším prodejům a vyššímu hodnocení ve vyhledávačích. Sociální sítě proto mohou pomoci vytvořit značku jako legitimní a důvěryhodnou. [18]

Společnost může pomocí sociálních sítí prokázat svoji úroveň služeb zákazníkům a obohatit své vztahy se spotřebiteli. Pokud si například zákazník stěžuje na produkt nebo službu na Facebooku, může společnost problém vyřešit okamžitě, omluvit se a podniknout kroky k nápravě. [13][18]

Nevýhody

Sociální sítě mohou mít velký dopad na šíření dezinformací, které se mohou během několika okamžiků nekontrolovatelně rozšířit. Tyto informace začínají jako fámy, které se šíří rychleji než fakta. Ačkoli je sociální síť sama o sobě zdarma, budování a udržování profilu společnosti trvá každý týden hodiny. Podniky navíc potřebují mnoho uživatelů, než začne marketingová kampaň na sociálních médiích generovat pozitivní návratnost investic. Určitě se shodneme na tom, že odeslání příspěvku 15 sledovatelům nemá stejný účinek jako odeslání příspěvku 15 000

sledovatelům. Mezi nevýhody určitě patří veškerá rizika sociálních sítí, které představím v následujících kapitolách. [18][19]

2 FACEBOOK

Tuto sociální síť jsem si vybrala z důvodu, že firma o které budu psát níže, tak se zaměřuje pouze na dvě sociální sítě a tím je právě Facebook a Instagram. Proto představím tyto sociální sítě, které jsou zároveň jedny z nejpoužívanějších na světě.

Facebook je sociální internetová stránka, která po zaregistrování a přihlášení umožní vytvořit si vlastní profil nebo stránku a navazovat kontakty s dalšími lidmi. Na Facebooku se tyto kontakty nazývají přáteli nebo fanoušky. Je pouze na Vás, zda si mezi své přátelé přidáte pouze lidi, které znáte osobně a jsou vašimi přáteli i v reálném životě, nebo budete udržovat kontakt s lidmi, které znáte jen přes internet. [16]

Největší síla a zdroj popularity této sociální sítě je, že umožní být v kontaktu s reálnými lidmi, ať už to jsou přátelé, členové rodiny a nikoli s virtuálními alter egy, nicky a podobně znějícími pojmy, které jsou z virtuálních světů. I přesto, že se s nimi nemůžete fyzicky setkávat a sdílet životy, můžete je sdílet aspoň přes Facebook. Přesně o tom je český překlad sloganu „Facebook vám pomáhá spojit se a sdílet s lidmi ve vašem životě.“ [13][18]

2.1 Vznik a rozvoj

V listopadu v roce 2003 Harvardský druhák Mark Zuckerberg vytváří ve své koleji web s názvem Facemash a sdílí odkaz kolem kampusu. Zuckerberg napadl harvardskou studentskou databázi, aby naplnil web obrázky a vytvořil hru „hot or not“, ve které uživatelé porovnávají fotografie studentů. Tato hra byla nakonec ukončena, protože se nezamlouvala představenstvu univerzity. [26]

Facebook se spustil 4. února 2004. Zuckerberg a spoluzakladatelé Dustin Moskovitz, Chris Hughes a Eduardo Saverin zahájili Facebook pro studenty Harvardu. O měsíc později se otevírá studentům Yale, Columbia a Stanford. Facebook by se brzy stal fenoménem v univerzitních kampusech v Americe. Téhož roku v prosinci představuje „The Wall“, oblast profilu uživatele, kde mohou přátelé a fanoušci zveřejňovat veřejné zprávy. Tato funkce se ukazuje jako populární a lepkavá a láká uživatele zpět, aby často kontrolovali zprávy. O 3 měsíce později společnost oznamuje, že překročila 1 milion aktivních uživatelů. [26]

Na začátku roku 2005 se Facebook poprvé rozšiřuje mimo univerzitní kampusy a otevírá se studentům středních škol. V září 2005 se snižuje věk registrace na 13 let. [26]

Microsoft v roce 2007 kupuje 1,6 % podílu Facebooku za 240 milionů USD. Investice oceňuje společnost na 15 miliard dolarů. V únoru 2008 Facebook urovnal dlouhodobý soud

s ConnectU, společností, kterou z Harvardu založili bratři Winklevossové. Dvojčata obvinila Marka Zuckerberga z krádeže jejich nápadu a jeho přeměny na Facebook. [26]

V roce 2009 Facebook zapíná ikonické tlačítko „To se mi líbí“.

Roku 2012 klesly akcie na Facebooku pod 18 dolarů a po měsících obav o schopnost společnosti vydělávat peníze na mobilních uživatelích dosáhnou svého historického minima. O měsíc později Facebook překračuje 1 miliardu aktivních uživatelů měsíčně. Společnost, která se nyní dotýká přibližně každého sedmého jedince na Zemi, nadchla investory a inzerenty, jež pokračuje v pochodech k internetové dominanci. [26]

2.2 Podmínky pro používání facebookových stránek

Před tím, než si rozhodnete vytvořit facebookový profil nebo tzv. Facebook Pages, je nutné se seznámit s podmínkami pro jejich užívání. Stejně jako osobní profilové stránky, tak i ty firemní musí dodržovat obecné zásady týkající se sběru dat a nakládání s nimi, prohlášení o právech a povinnostech a zásady facebookové komunity. Já se v této práci zaměřím pouze na Podmínky používání facebookových stránek. [18]

1. Stránku značky, místa, organizace nebo veřejně známé osobnosti může spravovat pouze oprávněný zástupce.
2. Kterýkoli uživatel smí vytvořit stránku za účelem vyjádření podpory nebo zájmu o značku, entitu nebo veřejně známou osobnost za předpokladu, že si ostatní nebudou moci takovou stránku splést s oficiální stránkou nebo taková stránka nebude porušovat ničí práva.

   Pokud chcete založit stránku značky, entity nebo veřejně známé osobnosti, musíte dodržovat tyto pravidla:

   - nezveřejňovat příspěvky, které budí dojem, že pocházejí od oprávněného zástupce obsahu stránky,
   - jasně uvést, že stránka není oficiální stránkou značky, entity nebo veřejně známé osobnosti.
3. Názvy stránek na Facebooku musí přesně reflektovat zaměření vaší společnosti, organizace, komunity či zájmové skupiny. U stránek, které tento požadavek nesplňují, Facebook může požadovat změnu zvoleného názvu či vám odebrat práva ke správě stránky.

4. Pokud shromažďujete obsah a informace přímo od uživatelů, musíte jasně uvést, že tak činíte vy, uživatele na to upozornit a získat od nich souhlas s použitím shromažďovaného obsahu a informací.
5. Informace získané z interakce uživatele s vaší výzvou k akci (například registrace k odběru newsletteru) nepoužívejte k jinému účelu než k poskytování služby spojené s danou výzvou k akci. Chcete-li tyto informace použít k jinému účelu, musíte nejprve získat výslovný souhlas příslušného člověka.
6. Jste povinni dodržovat všechny platné zákony i nařízení a osobám používajícím Facebook poskytnout veškeré nezbytné informace. Může jít například o informace, které jsou potřebné k označení komerční povahy obsahu příspěvku. K placeným příspěvkům Facebook automaticky přidává označení „sponzorováno“, aby uživateli bylo jasné, že se jedná o komerční sdělení.
7. Všechny úvodní obrázky jsou veřejné. Znamená to, že váš úvodní obrázek uvidí každý, kdo navštíví vaši stránku. Úvodní obrázky nesmějí být klamavé nebo zavádějící a nesmějí porušovat ničí autorská práva. Nesmíte pobízet jiné uživatele, aby si váš úvodní obrázek nahráli na svojí osobní stránku.
8. Pokud Facebook používáte ke komunikaci nebo správě propagačních akcí (např. soutěží či loterií), nesete odpovědnost za jejich legální průběh, zejména za: oficiální pravidla, podmínky nabídky a požadavky pro splnění podmínek (například omezení: týkající se věku a trvalého bydliště) a dodržování příslušných pravidel a nařízení vztahujících se na propagační akce a všechny udělované výhry (např. registrace a získání nezbytných regulačních povolení).
9. Pro přístup ke stránkám propagujícím soukromý prodej regulovaného zboží nebo služeb (včetně střelných zbraní, alkoholu, tabákových výrobků nebo produktů pro dospělé) musí být nastavena minimální věková hranice 18 let. Stránky propagující nebo podporující online hazardní hry, znalostní hry nebo loterie, například online kasina, sportovní sázky, bingo nebo poker, jsou povoleny jen v určitých zemích na základě schválení Facebookem.
10. Stránky nesmějí propagovat prodej léků na předpis. Bez předchozího schválení ze strany Facebooku jsou stránky propagující online lékárny zakázány. Stránky nesmějí obsahovat nesprávná, zavádějící, podvodná nebo klamná tvrzení. Do úvodní fotky nebo profilového obrázku stránky nesmíte přidávat produkty, značky třetích stran ani sponzory.

2.3 Typ stránky

Řada podnikatelů, kteří začínají s propagací na Facebooku, dělají jednu zásadní chybu hned v úvodu. Při zakládání firemního profilu si volí mezi osobním profilem a skupinou. Nejsou si vědomi existence Facebook Pages - stránek. Osobní profil, dle oficiálních pravidel, který slouží pro jednotlivce a jejich soukromý život, nesmí podnikatelé pro svoje podnikání používat.

Osobním profilem se v této práci zabývat nebudeme a zaměříme se na rozdíl mezi stránkou a skupinou. Firemní stránky uživatelé sledují (stávají se fanouškem) nejčastěji proto, že daná společnost, značka či produkt je zajímá, mají ji rádi a chtějí sledovat jejich novinky. Zatímco do skupiny se připojují proto, že je zajímá dané téma a chtějí o něm komunikovat s ostatními, nejen v komentářích pod příspěvkem. Každá firma by si měla ujasnit, jakým způsobem se chce prezentovat a jaké má plány se svým obsahem a zákazníky. Přehled rozdílů mezi stránkou a skupinou uvádí *Tabulka 2: Rozdíl mezi stránkou a skupinou*. [13]

Tabulka 2: Rozdíl mezi stránkou a skupinou

Stránka (firemní profil)	Skupina
Má fanoušky/sledující	Má členy
Je veřejná	Může být veřejná, soukromá či tajná
Umožňuje placené kampaně	Nelze propagovat
Nabízí pokročilou analytiku	Pouze základní přehledy o aktivitě
Umí fotky, GIFy a videa	Umí přidat i soubory do 100 MB
Příspěvky přidávají správci	Příspěvky mohou přidávat i členové
Fanouškem se může stát každý	Členy lze schvalovat

Zdroj: [13]

Optimální pro mou bakalářskou práci tedy je tzv. Facebook Pages neboli Facebooková firemní stránka, protože společnost, o které se v této práci píši, má tuto stránku také. Ta má na této stránce absolutní kontrolu a slouží jako komunikační prostor, ve kterém si buduje své dobré jméno.

Facebook nabízí celkem 4 varianty stránek. Jedná se o varianty Firma nebo značka a Komunita nebo veřejně známá osobnost. Každá z nich je něčím specifická a má různé způsoby zadávání informací. Pro firmu a značku můžete přidat adresu, kontakt, či otevírací dobu. Pokud děláte aktivitu u které chcete, aby byla spojována s vaším jménem, tak je pro vás nejlepší kategorie

veřejně známa osobnost. Pod touto aktivitou se schovává pokud fotíte, vyrábíte umělecké předměty na zakázku nebo navrhujete například šaty. Stránky věnované například neziskovým či studentským organizacím nebo zaměřující se na volnočasovou aktivitu (sport, knihy, festivaly atd.) spadají pod účel komunity. [18]

V rámci všech variant je možnost větší specifikace vašeho podnikání pomocí specifických klíčových slov, které nejlépe vystihují zaměření zakládané stránky. Je důležité, aby bylo zvolení těchto vlastností správné a pravdivé, aby uživatelům usnadnilo vyhledávání společnosti. Je to vlastně prvotní navázání kontaktu uživatelů s vaší stránkou, kteří mají podobné zájmy. [18]

Obrázek 1: Kategorie stránek

Zdroj: [27]

2.4 Vytvoření firemní stránky

Pokud s Facebookem začínáte, tak najedete na webovou stránku facebook.com a vpravo je možnost se přihlásit či nově registrovat, o trošku níže zvolíte Vytvořit stránku pro celebritu, skupinu nebo společnost. Zobrazí se výběr pro vytvoření stránky. Je na výběr podle typu stránek, které jsou uvedeny v odstavci 2.3. Po kliknutí na tlačítko Začínáme se otevře okno pro přihlášení, kde si vytvoříte nový účet. Pokud již účet máte, tak se stačí přihlásit. Ovšem je zakázané, abyste svůj soukromý profil používali k prezentaci firmy a nepřevedli ho na stránku. Facebook by profil mohl zablokovat. [27]

Pokud nemáte žádný profil, klikněte na Vytvořit nový účet. U registrace se vyplní základní údaje, které jsou potřeba pro vytvoření účtu. Kliknutím na Zaregistrovat se vyjádříte svůj souhlas se smluvními podmínkami.

Pro ověření emailové adresy přijde kód na danou emailovou adresu, který je potřeba zadat v dalším kroku, aby se otevřela hlavní stránka Facebooku a tím se stanete novým uživatelem.

Po otevření hlavní stránky si přes ikonku + vpravo nahoře vyberete variantu stránka a hned můžete vytvořit novou firemní stránku. Zadáte povinné údaje, jako je název stránky, kategorie a popis.

V názvu stránky by měl být použit název firmy, značky nebo organizace, popřípadě název, který stránku bude vystihovat. Název by neměl obsahovat velké množství velkých písmen, symbolů nebo interpunkčních znamének. Pokud již máte jiná sociální média, měl by být název totožný s názvem na Facebooku.

V možnosti kategorie vyberte až 3 kategorie, které popisují typ firmy, organizace nebo tématu, kterému stránka odpovídá. Kategorie se vám zobrazí, když začnete psát počáteční písmena pro popis vaší firmy např. prodej. Do pole popis popište, co firma dělá, služby, které poskytujete, nebo účel stránky.

Po zvolení Vytvořit se zobrazí možnost doplnění profilového obrázku, kde můžete použít logo firmy nebo obrázek, který lidem pomáhá identifikovat vaši stránku ve výsledcích hledání. Přidání úvodní fotky, představíte sledujícím to, o čem nová stránka je. Obrázky můžete nahrát z počítače nebo importovat fotku z webové stránky. Profilový obrázek se zobrazí v záhlaví vašeho profilu a současně bude jako miniatura u každé zprávy, kterou napíšete. Jelikož je miniatura poměrně malá, tak je vhodné, aby neobsahovala příliš detailů.

Také je tam okno Přidat tlačítko, kterým vyzvete uživatelem, aby na stránce podnikli nějaké akce, třeba vás začali sledovat nebo si něco koupili.

Tuto a další stránky je možné spravovat pomocí Business Manageru. V jeho rozhraní lze nastavovat přístupy, zakládat nové položky a používat další užitečné nástroje. Je vhodný zejména v případě, kdy máte ve správě více účtů, protože všechny informace uvidíte na jednom místě. Do Business Manageru se přidáte po kliknutí na Nastavení firmy a pod záložkou Účty vyberete Stránky. Kliknete na tlačítko přidat a vyberete variantu stránky, která vám bude vyhovovat. [13][25]

A nyní už můžete začít publikovat první statusy a pozvat fanoušky. Nejprve pozvěte zaměstnance, přátele, rodinu. Klienty či nové zákazníky začněte zvát až bude stránka zaběhnutá, bude mít nějakou historii a také fanoušky.

2.5 Zabezpečení na Facebooku

Facebook využívají miliardy lidí na světě, ale většina z nich vůbec nemá ponětí, jak a kde správně nastavit zabezpečení svého účtu.

Mezi nejdůležitější faktor patří silné heslo, je to alfa omega celého zabezpečení. Zbylé kroky pro správné nastavení lze nastavit na profilu, kde se přes ozubené kolečko dostanete do Nastavení a soukromí a poté do Zabezpečení. Facebook má tuto část velmi hezky zpracovanou a dokáže každého provést několika kroky, které pomohou ochránit účet. [18]

V zabezpečení si lze zkontrolovat, na jakých zařízeních jsme přihlášeni a v jakých prohlížečích a zařízeních máme uložené přihlašovací údaje. Je doporučováno tyto nastavení pravidelně kontrolovat, abychom měli přehled, že jsme opravdu přihlášeni pouze na těch zařízeních, na kterých jsme se sami přihlásili. Dále si zde můžeme nastavit dvoufázové ověření, výstrahu při nerozpoznaném přihlášení, vybrat 3 -5 přátel, kteří nám v případě ztráty přístupu k účtu pomůžou dostat se k němu zpět a nastavení soukromí, co vše chcete sdílet buď veřejně nebo pouze mezi přáteli.

Mezi pokročilé nastavení patří taktéž Šifrování e-mailových upozornění. Zvyšuje bezpečnost e-mailových upozornění z Facebooku, tyto šifry dokážeme dešifrovat pouze my samotní. Dále Obnovení externích účtů, kde přes účet na Facebooku můžeme obnovit svůj přístup na různé weby.

Facebook také nabízí ověření osobních profilů a facebookových stránek. Ověřovací značka zvyšuje důvěryhodnost firmy. Když uživatelé uvidí na stránce nebo profilu ověřovací značku, zaručuje to, že komunikují se skutečnou organizací nebo osobou. Ověřené stránky a profily také lépe fungují při vyhledávání. [7]

Pro Facebook a Instagram jsou pravidla pro ověření stejná.

Při ověřování stránek a profilů na Facebooku vyhodnocujeme řadu faktorů, podle kterých určujeme, zda splňují zájmy veřejnosti i naše ověřovací kritéria. [7]

Kromě smluvních podmínek a zásad komunity na Facebooku musí být stránky a profily [7]:

- autentické - musí reprezentovat skutečného člověka, registrovanou firmu nebo organizaci,
- jedinečné - musí být jedinou identitou daného člověka nebo firmy. Pro jednoho člověka nebo firmu je možné ověřit pouze jednu stránku nebo profil, s výjimkou stránek a profilů s různými jazykovými mutacemi. Ověření neposkytují stránkám a profilům reprezentujícím obecné zájmy (například: fotky štěňátek),
- dokončené - musí mít oddíl informace, fotku stránky nebo profilovou fotku a nedávnou aktivitu včetně alespoň jednoho příspěvku,
- zajímavé - musí reprezentovat známou, často vyhledávanou osobu, značku nebo organizaci. Kontrolují stránky a profily zmiňované na více zpravodajských webech, a placený nebo propagační obsah nepovažují za věrohodné hodnocení.

V rámci ověření je zakázané převádět vlastnictví a upravovat účel. Facebook veškeré úpravy jména, kategorie a informace v biu před zveřejněním kontroluje. [7]

Pokud si každý projede průvodce nastavení, tak má jistotu, že pro svoji ochranu na Facebooku udělal maximum a může být klidný, že svůj účet má zabezpečený.

3 INSTAGRAM

Další velice populární sociální síť. I tuto síť používá moje firma XY, kterou jsem vybrala pro tuto práci, proto ji v pár bodech představím.

Instagram je převážně mobilní aplikace, ale i web, který je pro své uživatele zaměřen na sdílení fotek, videí či sdílení živých přenosů. Má estetický aspekt, snadné používání a každým dnem se stává oblíbenějším.

Je známý především používání hashtagů. Hashtag je klíčové slovo, které umožní uživatelům třídit a kategorizovat obsah a zároveň představuje účinný analytický a optimalizační nástroj pro firmy. Instagram umožní až 30 hashtagů u jednoho příspěvku, avšak staticky se udává, že nejlépe fungují příspěvky do deseti klíčových slov. Firemní nebo branded hashtagy jsou specifické pro danou společnost či kampaň. Může se jednat například o jméno firmy nebo její motto. [13]

Lidé chodí na Instagram proto, aby zde vyhledali inspiraci a objevili to, co je zajímá. Je dokázané, že lidé stráví více času na Instagramu, kde poznávají nové lidi, firmy, výrobky.

Když si zde vytvoříte firemní účet, získáte tím přehled o sledujících, efektivitě účtu, nových kontaktních možnostech a spoustě dalších funkcí. Můžete se podívat na metriky o úspěšnosti vašich příběhů a propagovaných příspěvků v reálném čase. Získáte přehled, jak sledující reagují na váš celkový obsah. Vytvoříte si propagaci, která vám pomůže oslovit víc lidí a vybudovat větší komunitu. Funkce, která usnadňuje zviditelnění a zvyšuje prodeje je dostupná pouze pro firmy. [18]

3.1 Vznik a rozvoj

Zakladatel Kevin Systrom dříve pracoval ve společnosti Google jako spolupracovník pro korporátní vývoj a stážoval ve společnosti Odeo (společnost, která se později vyvinula do Twitteru).[9]

Zatímco Systrom neměl žádné formální vzdělání v počítačové vědě, naučil se kódovat v noci a o víkendech. Nakonec postavil prototyp webové aplikace s názvem Burbn, což byla aplikace umožňující svým uživatelům zveřejnit své plány a fotografie. Systrem přehodnotil Burbn a spolu se svým novým společníkem Mikem Kriegeren, který byl rovněž absolventem Stanfordu, se rozhodli zaměřit především na fotografie pořízené na mobilních zařízeních. [9]

Aplikace Instagram byla spuštěna 6. října 2010 pro iOS a za jeden den získala 25 000 uživatelů. Na konci prvního týdne byl Instagram stažen 100 000krát a do poloviny prosince počet

uživatelů dosáhl jednoho milionu. Po rychlém nárůstu uživatelské základny Instagramu se o společnost začalo zajímat více investorů. [9]

V únoru 2011 společnost Instagram získala 7 milionů dolarů. Jedním z jejich investorů byla společnost Benchmark Capital, která ocenila společnost na zhruba 25 milionů dolarů. Kromě institucionálních investorů přitahovala společnost pozornost dalších předních společností v oboru technologií sociálních médií, včetně Twitteru a Facebooku. Ačkoli toto nové kolo financování poskytlo Systromu a Kriegerovi příležitost najmout více lidí, zakladatelé se rozhodli udržet společnost opravdu malou, sotva 12 zaměstnanců. Do března 2012 se uživatelská základna aplikace rozrostla na přibližně 27 milionů uživatelů. V dubnu 2012 byl vydán Instagram pro telefony Android a byl stažen více než milionkrát za méně než jeden den. Systrom a zakladatel Facebooku Mark Zuckerberg se seznámili prostřednictvím akcí konaných ve Stanfordu a oba byli v komunikaci na začátku rychlého nárůstu popularity Instagramu. V dubnu 2012 Facebook nabídl nákup Instagramu za hotovost a akcie v hodnotě přibližně 1 miliardy USD. Klíčovým ustanovením bylo, že společnost zůstane nezávisle řízena. Krátce nato a těsně před svou počáteční veřejnou nabídkou se Facebook posunul vpřed a získal společnost za hotovost a akcie v hodnotě 1 miliardy USD. [9]

Instagram zpřístupnil webové rozhraní s omezenými funkcemi v listopadu 2012. V roce 2016 vytvořila aplikaci, díky které je kompatibilní s tablety a počítači Microsoft Windows. [9]

3.2 Podmínky pro užívání instagramových stránek

Ikdyž je Instagram jeden z Facebook produktů, tak má svoje vlastní podmínky používání, které musí každý uživatel dodržovat. Smluvní podmínky tedy představují smlouvu mezi vámi a Facebookem Ireland Limited. Podmínky Facebooku se však na Instagram nevztahují.

Rozhodla jsem se, že představím jedny z nejdůležitějších pravidel jak se Instragram nesmí používat, abychom se na sociálních sítích cítili bezpečně. Ve smluvních podmínkách jsou také další zásady, závazky, služby a práva.

Výběr těch nejzákladnějších zní[17]:

1. Nesmíte se vydávat za někoho jiného nebo uvádět nepřesné informace.
2. Na Instagramu nemusíte sdělovat svoji identitu, ale musíte nám poskytnout přesné a aktuální informace (včetně registračních údajů), které mohou zahrnovat i osobní údaje. Nesmíte se vydávat za někoho jiného či něco jiného a nesmíte vytvořit účet pro někoho jiného, pokud nemáte jeho výslovné svolení.

3. Nesmíte dělat nic, co je nezákonné, klamavé nebo podvodné nebo slouží nelegálnímu nebo neschválenému účelu.
4. Nesmíte porušovat (nebo pomáhat jiným porušovat či vybízet někoho k porušování) tyto Smluvní podmínky či naše zásady, mezi které patří zejména Pravidla komunity na Instagramu, Smluvní podmínky platformy Facebooku a Zásady pro vývojáře a Pravidla pro hudbu.
5. Pokud zveřejňujete značkový obsah, musíte dodržovat naše Zásady pro značkový obsah, které od vás požadují využití našeho nástroje pro značkový obsah. Přečtěte si, jak nahlašovat chování nebo obsah v našem centru nápovědy.
6. Nesmíte dělat cokoli co by mohlo narušit nebo zhoršit správné fungování Služby.
7. To zahrnuje zneužívání našich kanálů pro hlášení, zasílání námitek a odvolávání se, a to například vytvářením podvodných a bezdůvodných hlášení a námitek.
8. Nemůžete prodávat, licencovat či kupovat žádné účty či údaje shromážděné námi či naší Službou.
9. To zahrnuje pokusy o koupení, prodání či převod jakékoli části vašeho účtu a to i včetně vašeho uživatelského jména, stejně tak jako nabízení, shromažďování či používání přihlašovacích údajů či štítky jiných uživatelů, ani o žádné žádosti či shromažďování uživatelských jmen a hesel na Instagramu či přisvojení si přístupových tokenů.
10. Nesmíte zveřejňovat soukromé či důvěrné informace někoho jiného bez jeho svolení či dělat cokoliv, co porušuje práva jiných osob, včetně práv k duševnímu vlastnictví (např. porušení autorských práv, porušení práv k ochranné známce, padělaného nebo pirátského zboží).
11. Můžete použít dílo někoho jiného v souladu s výjimkami a omezeními autorských práv a práv souvisejících dle příslušných právních předpisů. Prohlašujete, že vlastníte nebo jste získali veškerá potřebná práva k obsahu, který zveřejňujete či sdílíte. Další informace, mimo jiné o nahlašování obsahu, který podle vás porušuje vaše práva k duševnímu vlastnictví, si můžete přečíst tady.
12. Nesmíte modifikovat, překládat nebo vytvářet odvozená díla či zpětné analýzy našich produktů nebo jejich komponentů.
13. Bez našeho předchozího písemného souhlasu nesmíte v uživatelském jménu použít název domény nebo URL.

3.3 Vytvoření instagramové stránky

Pro vytvoření účtu na Instagramu je potřeba mezikrok v podobě osobního účtu. Jsou dvě možnosti vytvoření účtu, buď na oficiálních webových stránkách nebo je možnost si stáhnout mobilní aplikaci, která je uživatelsky mnohem více přívětivá. Záleží jaký operační systém využíváte na svém mobilním zařízení, pokud je to iOS, tak v aplikaci najdete ve vašem App Storu, pro Android najdete v Google Play a Windows v Phone Store. Jakmile se aplikace stáhne, začnete kliknutím na ní, čímž ji spustíte.

V případě, že plánujete vytvořit firemní účet, tak doporučuji se zaregistrovat pod vaším firemním e-mailem nebo firemním telefonním číslem. Variantu registrovat se přes Facebook nedoporučuji. Může se stát, že v případě ztráty facebookového profilu, se nebudete moci přihlásit ani na Instagram. Později si ho však můžete propojit v nastavení.

Vytvoříte si uživatelské jméno a heslo. Uživatelské jméno by mělo být jméno vaší společnosti, jelikož pod ním budete na Instragramu vystupovat. Po vyplnění požadovaných vstupních informací máte vytvořený nový účet. Tento účet bude mít pouze omezené možnosti osobního profilu. Pro získání přístupu k pokročilým analytickým nástrojům si převeďte tento profil na firemní. To uděláte tak, že v aplikaci na profilu najedete do nastavení (symbol tří teček), vyberete možnost Účet a posunete se dolů k možnosti Přepnout na profesionální účet. Tento účet je brán jako firemní. Instagram představí nejzákladnější výhody, které získáte tímto převodem. Vyberete kategorii, která nejlépe vystihuje, co děláte. Můžete vybrat, zda chcete, aby tato kategorie se objevila na vašem profilu. Poté vás aplikace upozorní, že přepnutím na profesionální účet, se stane ten váš veřejným a kdokoli si bude moct prohlídnout vaše fotografie a videa. Nebudete schvalovat žádné sledující a automaticky se schválí všechny žádosti o sledování. Pokud s tímto krokem budete souhlasit, kliknete na tlačítko OK a tím se vytvoří firemní účet.

Teď můžete doplnit informace o firmě, jako je provozní doba, adresa sídla, telefonní číslo nebo odkaz na váš web. Je to výhodnější pro lepší spojení s vámi a potencionálními zákazníky.

I tento účet lze přidat do Business Manageru. Po kliknutí na nastavení firmy a instagramové účty v Business Manageru, kliknete na Zaregistrovat nový instagramový účet, vyplníte přihlašovací údaje a dáte uložit. [25]

3.4 Zabezpečení na Instagramu

Stejně jako na Facebooku, je důležité se věnovat zabezpečení účtu na Instagramu. Důležité to je jak pro osobní účty, tak pro ochranu dat firemních účtů, ke kterým máte přístup. Zabezpečení na Instagramu je velice podobné zabezpečení na Faceboooku.

Pro kontrolu nastavení zabezpečení najedete na váš účet, přes tři čárky do Nastavení a poté do Zabezpečení.

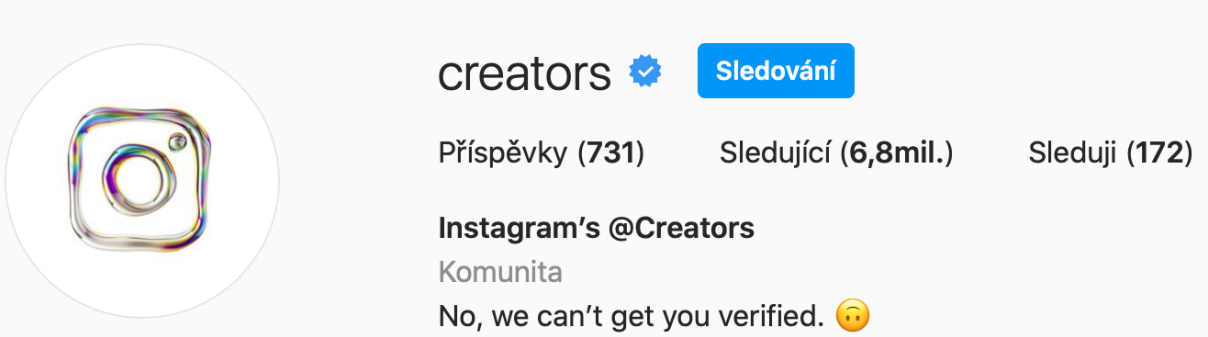
Skrze tuto funkcionalitu si lze změnit heslo, zobrazit přihlašovací aktivitu a uložené přihlašovací údaje, nastavit dvoufázové ověření a zjistit, který e-mail přišel opravdu od Instagramu a který je falešný. [13]

- Přihlašovací aktivita slouží ke zjištění všech zařízení, kde je daný uživatel přihlášen. Zkontroluje si zde lokalitu přihlášení, datum a zařízení. Pokud by jedna z aktivit nebyla uživateli povědomá, lze se přes tři tečky odhlásit. Následně Instagram vyzve, že relace byla odhlášena a jestli si nechcete z důvodu bezpečnosti změnit heslo. Uložené přihlašovací údaje si Instagram zapamatuje, abyste je nemuseli znovu zadávat. Tuto službu si můžete vypnout, ale budete muset při každém přihlášení znovu zadávat uživatelské heslo a jméno.
- Dvoufázové ověření je na Instagramu stejně důležité jako na Facebooku. Při každém novém, případně podezřelém přihlášení na nerozpoznaném zařízení, bude vyžadováno i další potvrzení. Na Instagramu lze nastavit, jakou variantu si z dvoufázových ověření vyberete. Je na výběr z Autentifikační aplikace, která po zadání přihlašovacích údajů vygeneruje nový kód, který je potřeba zadat do aplikace. Instagram přímo doporučuje aplikace jako Duo Mobile nebo Google Authenticator. Další způsob je SMS, která dorazí na telefon s novým kódem pro zadání.
- Doporučení je i pro funkci Záložní kódy. Je to funkce, ve které zjistíte sérii pěti kódů, které vám pomohou získat váš účet, pokud ztratíte telefon nebo nelze přijímat kódy přes aplikaci či SMS. Každý z kódu lze využít pouze jednou, pokud se obáváte, že již kódy byly ukradeny, tak Instagram pošle nové.

Další sekvence ochrany dat je Přístup k datům, Stáhnout data a Historie vyhledávání. [22]

- Přístup k datům umožní k nahlédnutí základních informacích o účtu, jako je datum založení, dřívější telefonní čísla, e-maily, základní údaje o spojení, profilových údajích, informace o interakcích se Stories a zájmy týkající se reklam.
- Stáhnout data umožňuje stáhnout kopii veškerého sdíleného obsahu a zaslat si ho na vybraný e-mail.
- V historii vyhledávání si můžete smazat záznamy vyhledávacích aktivit.

Ověření účtu lze i na Instagramu a je to jedna z nejdůležitějších složek zabezpečení. I zde se značí jako modrý odznak s fajfkou. Tento znak naznačuje, že platforma potvrdila, že daný účet je důvěryhodný, nebo alespoň jsou tím, za koho se vydávají. [20]



Obrázek 2: Ověřovací znak na Instagramu

Zdroj: [6]

O ověřený odznak na Instagramu může požádat kdokoli, ten je však velmi vybíravý (a v mnoha ohledech záhadný), komu tento odznak vystaví. To, že někdo má modré zaškrtnutí například na Facebooku, nezaručuje, že ho dostane i na Instagramu. [20]

Poté, co jejich tým zkontroluje aplikaci a účet, zobrazí se odpověď na kartě oznámení. Vzhledem k historickým a přetrvávajícím problémům s podvodníky je u Instagramu zcela zřejmé, že vám nikdy nepošlou e-mail, nepožádají o peníze, ani jinak neosloví.

Během několika dní nebo týdne se zobrazí přímé ano nebo ne. Žádná zpětná vazba ani vysvětlení.[20]

Mimo tyto základní nastavení je důležité respektovat všechny zásady používání dat, které naleznete v Nastavení - Informace. Zásady jsou stejné jak pro Instagram, tak pro Facebook.

4 RIZIKA SOCIÁLNÍCH SÍTÍ

Sociální sítě mají spoustu svých výhod, které nám ulehčují komunikaci s ostatními lidmi, ale také mají velice rizik, které ohrožují naše soukromí a bezpečnost.

4.1 Krádeže osobních dat a identit

Ke krádeži identity dochází, když jsou osobní nebo firemní údaje odcizeny a použity kybernetickými zločinci nebo podvodníky k vydávání se za jinou osobu nebo podnik. Přihlašovací údaje uživatele lze v zásadě použít k získání přístupu v různých oblastech digitálního života, včetně bankovních účtů, sociálních médií a údajů o kreditní kartě. V rámci získávání přístupu mohou získávat další citlivá data z účtů i z těch, které patří rodině, přátelům, kolegům a zaměstnancům. V některých případech mohou počítačoví zločinci použít přihlašovací údaje k poškození pověsti nebo k veřejnému online ponížení. Celkově mohou způsobit nenapravitelné škody. [3][4]

Krádež identity se obvykle provádí pro finanční zisk. Zloděj identity, kterému se podaří získat kreditní kartu nebo číslo sociálního zabezpečení oběti, by je mohl použít k nákupům nebo otevření účtů pomocí ukradené identity. Lze to také provést pomocí e-mailového účtu, který většina lidí nemá problém sdílet. Také mohou útočníci vyžadovat za vrácení identity finanční částku. Mnoho uživatelů se bojí, že by útočník zveřejnil jejich soukromé údaje, proto raději zaplatí, ale mnohdy se jim účet nevrátí a ještě přijdou o peníze. [4]

4.2 Riziko poškození profesní image

Každý podnikatel si vytváří svojí profesní image s přímým dopadem na jejich podnikání. Pro společnosti je důležité sladit kvalitu svých stránek na sociálních sítích s reputací, kterou pro svoji značku vybudovali. Image může být upevněna společenskou přítomností, která je postavena na prezentování na sociálních sítí a webových stránek. Sociální sítě dokáží mít pozitivní vliv na image značky, služby nebo produktu a být tak přínosem pro celou organizaci, ale má i své úskalí a mohou poškodit veškerou reputaci. Spoustu zákazníku dá na recenze na internetu o daném výrobku nebo firmě a také si je dlouho pamatují. [13][19]

Nejpoužívanějším místem recenzí je Facebook. Vyplývá to z jeho charakteru veřejného sdílení a velkého množství lidí. Debaty na nástěnkách sociálních sítích jsou místem vyostřených debat a nejrůznějších spekulací. Aby nedošlo k poškození značky, musí firma respektovat své publikum a přemýšlet, než bude něco sdílet. Pokud firma nevěnuje pozornost své online přítomnosti nebo neřeší negativní zpětnou vazbu, potenciální dopad negativní publicity na

sociálních sítích může být velmi vážný. Sociální média disponují takovou silou, že jedna negativní událost může během chvilky zničit roky budování značky a veškerou dobrou vůli. [13][19]

4.3 Zveřejňování příspěvků

Na velmi důležitý bod hrozeb bych ráda upozornila, aby si obchodníci dávali pozor na to, co a komu zveřejňují. Je potřeba, aby vždy měli na paměti, že co zveřejní na internetu, už obvykle bohužel nejde vzít zpět. Čím nezvyklejší příspěvek, tím je větší pravděpodobnost, že příspěvek více zaujme a bude se rychleji šířit. To stejné platí o zveřejňování informací o druhých lidech, výrobcích či společností. Vám něco možná bude připadat jako neškodná informace, ale tomu dotyčnému to může velice uškodit. [13]

Rizikem je, že mohou určité informace přilákat zloděje nebo vyděrače. Zloděj může zjistit, kdy například nebudete doma, protože se pochlubíte fotografií, jak celá rodina odlétá na dovolenou. V případě firmy, kdy nebudete na svém centrálním místě, protože všichni zaměstnanci mají firemní večírek.

Průzkum sociálních sítí pomáhá zločincům zjistit, kdo je ve společnosti zranitelný vůči psychologickým manipulacím a taktikám zastrašování. Tyto informace využívají k vytváření zpráv, které vytvářejí pocit naléhavosti a brání oběti racionálně uvažovat. Pokud například útočník zjistí, že jste se připojili k nové organizaci a že je to vaše nová práce, může vám poslat e-mail nebo zprávu a předstírat, že je vysoce postavený manažer a že máte poslat peníze na účet útočníka. S vědomím, že jste v této společnosti nový, si útočník myslí, že ještě neznáte všechny a procesy a zastrašila by vás naléhavá zpráva od vysoce postaveného manažera.[13]

Rada na závěr k tomuto tématu. Je potřeba dávat si pozor, při používání sociálních sítí a přemýšlet o tom, komu a jaké informace dáváme k dispozici.

4.4 Předstírání identity značky

V dnešní době je jednou z častých diskutovaných otázek je zakládání falešných profilů na internetu. Nikdo nevíme, kdo se opravdu skrývá na druhé straně za obrazovkou. Zda osoba se kterou máme nějaký kontakt je opravdu osobou za kterou se vydává. Spousty lidí se dnes schovává za falešný profil za účelem pomluvy či pomsty. Bohužel, je velice snadné založit si nový profil a vydávat se za někoho jiného, případně někoho urážet nebo založit nové diskuzní fórum či skupinu, kde se budou šířit falešné informace o oběti za účelem jejího zesměšnění či zastrašení. [13][8]

Kyberzločinci často vytvářejí falešné stránky a účty, které se vydávají za známé značky. Ty se pak používají k propagaci falešných nabídek, slev nebo dárků, aby oklamali uživatele a vyzradili své přihlašovací údaje nebo jiné citlivé informace. To může ovlivnit podnikání dvěma způsoby – buď může být účet na sociálních sítích předstírán, nebo zaměstnanci mohou být obětí takových podvodů, které vystavují interní síť a obchodní účet bezpečnostním rizikům. Proto musíme být velice opatrní komu budeme na internetu důvěřovat. [3][4]

4.5 Aplikace třetích stran

Za zmínku stojí aplikace třetích stran, které jsou k dispozici. Tyto aplikace mohou chtít povolit přístup k důvěrným firemním informacím, například k IP adrese nebo číslu účtu. Vždy si pozorně přečtěte, jaké údaje si aplikace přeje povolit a zda to souvisí s funkcemi, které nabízí. [13]

Neznámé aplikace mohou značně poškodit firemní zařízení. Především na platformě Android mohou firemní citlivé údaje vynést ven neznámému útočníkovi.

Celkově při registraci do jakékoli služby, je vždy potřeba si důkladně přečíst smluvní podmínky používání, abyste měli přehled, co daná služba o vás bude vědět a jak s těmito informacemi bude dále nakládat. Nemělo by to být o pouhém kliknutí na tlačítko „Souhlasím“, jen aby to co nejrychleji zmizelo.

5 NEJPOUŽÍVANĚJŠÍ TECHNIKY PODVODŮ

Na internetu se šíří kromě legitimních informací také nebezpečné programy, které mají za úkol infiltrovat počítač. Některé programy umí zjistit soukromé informace (přístupová hesla, čísla kreditních karet, důležité dokumenty atp.) a odeslat je neautorizované osobě. Jiné jen obtěžují ubíráním místa na disku a zasíláním nevyžádaných e-mailů. Jsou i takové programy, které dokáží vzdáleně ovládat počítač. [3]

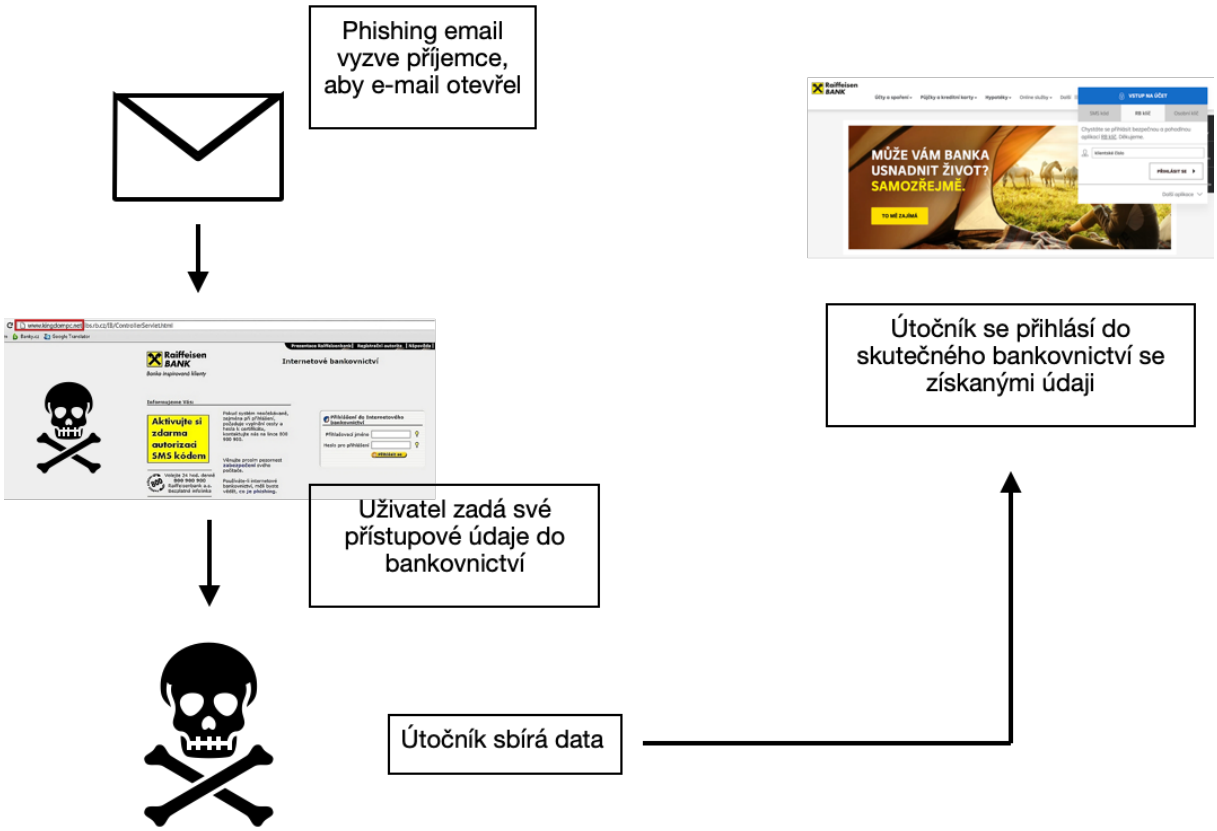
Programy je možné najít na mnoha místech na internetu. Nejvíce se jedná o erotické stránky, které neslouží ke stažení právě těchto programů, ale můžete na ně nevědomky narazit. Tyto programy lze najít i na nelegálních stránkách typu „warez“, které jsou založené na podezřelé a jiné „pirátské“ činnosti. Je také možné, že náš známý nám zašle nějaký infikovaný program nebo dokument. Nemusí o tom mít ani zdání, protože tuto činnost za něj provedl právě nějaký program v jeho počítači. [3]

Vzhledem k tomu, že se takto „nakaženým“ stránkám ve většině případů nevyhneme, tak je potřeba znát nejznámější techniky, které nás mohou ohrozit a na základě toho dodržovat bezpečnostní zásady a naučit se bránit proti nebezpečí, které na nás číhá. V dalších podkapitolách představím, jaké jsou nejzákladnější škodlivé kódy, na které lze narazit.

5.1 Phishing

Phishing je podvodné používání elektronické komunikace k oklamání a využití výhod uživatelů. Phishingové útoky se pokoušejí získat citlivé a důvěrné informace, jako jsou uživatelská jména, hesla, informace o kreditních kartách, pověření v síti a další. Kybernetičtí útočníci, kteří se prostřednictvím telefonu nebo e-mailu vydávají za legitimní osobu nebo instituci, manipulují obětí s prováděním konkrétních akcí například kliknutím na nebezpečný odkaz nebo přílohu. Když kliknete na odkaz, budete přesměrování na webovou stránku, která požaduje soukromé údaje. Další možnost je úmyslné prozrazení důvěrných informací. [12]

Jsou ohroženi jednotlivci i organizace; cenné mohou být téměř jakékoli osobní nebo organizační údaje, ať už jde o spáchání podvodu nebo přístupu k síti organizace. Některé phishingové podvody mohou navíc cílit na organizační data za účelem podpory špionážních snah nebo špionáže opozičních skupin podporovaných státem. [12]



Obrázek 3: Postup phishingu a příklad podvržené banky Raiffeisen BANK

Zdroj: upraveno podle [16]

5.1.1 Typy phishingových útoků

Některé konkrétní typy phishingových podvodů používají cílenější metody k útoku na určité jednotlivce nebo organizace.

E-mailový phishing

Základní phishingový e-mail odesílají podvodníci vydávající se za legitimní společnosti, často banky nebo poskytovatele kreditních karet. Tyto e-maily jsou navrženy tak, aby vás přiměly k poskytnutí přihlašovacích údajů nebo finančních informací, jako jsou čísla kreditních karet nebo čísla sociálního pojištění. [16]

Jiné falešné e-maily se vás mohou pokusit oklamat, abyste klikli na odkaz, který vede na falešný web navržený tak, aby vypadal jako Amazon, eBay nebo vaše banka. Tyto falešné webové stránky pak mohou nainstalovat malware nebo jiné viry přímo do počítače, což hackerům umožní ukrást osobní údaje nebo převzít kontrolu nad vaším počítačem, tabletem nebo chytrým telefonem.

Tyto e-maily často obsahují pravopisné chyby, zvláštní gramatiku a obecné pozdravy jako „Vážený uživateli“ nebo „Vážený kliente“. Odkazy, na které byste měli kliknout, často vedou

na webové stránky s podivnými adresami URL nebo s těmi, které jsou napsány trochu jinak než legitimní webové stránky instituce. [16]

Jsou také podvodné e-maily, ve kterých se útočník snaží přesvědčit oběti, že je natočil přes jejich webové kamery. Cílem je vyděsit a získat peníze pomocí bitcoinového účtu. Takový typ e-mailu z vlastní zkušenosti znám. Útočník mi poslal e-mail, že mám 48 hodin na převedení částky ve výši 1200 EUR na jeho bitcoinovou adresu. Vyhrožuje mi, že pokud tuto zprávu komukoli ukážu, tak uvedené video okamžitě zveřejní. Naopak pokud převedu částku, tak po potvrzení platby video hned smaže a už o něm neuslyším.

A chceš vědět, co všechno s ním můžu udělat? Jediným kliknutím myši ho můžu rozeslat na všechny tvé stránky sociálních sítí a všem tvým emailovým kontaktům.

Zároveň můžu i zveřejnit přístupové údaje k veškeré tvé emailové korespondenci a messengerům, které v současnosti používáš.

Pokud tomu chceš zabránit, stačí na moji bitcoinovou adresu převést částku 1200 EURO (pokud nemáš ponětí, jak to udělat, zadej do svého prohlížeče snadný dotaz: "Koupit bitcoiny").

Ihned po potvrzení platby video smažu a je hotovo. Nikdy víc už o mně neuslyšíš.

Na dokončení transakce máš 2 dny (48 hodin).

Po otevření tohoto emailu, mi dojde oznámení a časový odpočet začne tikat.

Jakýkoliv pokus o podání stížnosti je zbytečný, protože tento email, stejně jako moji bitcoinovou adresu, nelze zpětně vysledovat.

Na svém systému pracuju, jak nejdéle to jen jde, a chybám nedávám sebemenší prostor.

Pokud jakýmkoliv způsobem zjistím, že jsi tuhle zprávu komukoliv ukázal, výše uvedené video okamžitě zveřejním.

Obrázek 4: Ukázka části e-mailu, který jsem obdržela

Zdroj: [vlastní]

Spear phising

E-mailové zprávy spear phising nebudou vypadat tak náhodně jako obecnější pokusy o phishing. A na rozdíl od obecnějších phishingových e-mailů tráví podvodníci, kteří je posílají, čas zkoumáním svých cílů. Tito zločinci budou posílat e-maily, které vypadají, jako by pocházely z legitimních zdrojů. Někteří útočníci dokonce unesou obchodní e-mailovou komunikaci a vytvářejí vysoce přizpůsobené zprávy.

V dalším příkladu spear phishingu mohou e-maily cílit na zaměstnance společnosti. Může se zdát, že e-mail pochází od šéfa a zpráva vyžaduje přístup k citlivým informacím společnosti. Pokud je cíl oklamán, mohlo by to vést k narušení dat, kdy by byly zpřístupněny a odcizeny informace společnosti nebo zaměstnance. [16]

Klonovaný phishing

Další typ phishingu je klonovaný phishing, může být jedním z nejobtížněji zjistitelných. Při tomto typu phishingového útoku podvodníci vytvoří téměř identickou verzi e-mailu, který již oběti obdržely.

Klonovaný e-mail je odeslán z adresy, která je téměř, ale ne úplně stejná, jako e-mailová adresa, kterou používá původní odesílatel zprávy. Tělo e-mailu vypadá také stejně. Co je tedy jiné? Příloha nebo odkaz ve zprávě byly změněny. Pokud na ně oběť nyní klikne, přesměruje je na falešnou webovou stránku nebo otevře infikovanou přílohu. [16]

Lov velryb

Lov velryb se konkrétně zaměřuje na vysoce postavené nebo jiné vysoce postavené manažery ve společnosti. Cílem je přimět tyto mocné lidi, aby se vzdali nejcitlivějších firemních dat. Obsah pokusu o lov velryb se bude často projevovat jako právní komunikace nebo jiný důvěryhodný zdroj v rámci společnosti. [16]

5.2 Malware

Malware znamená škodlivý software. Jednou z nejčastějších kybernetických hrozeb je malware vytvořený počítačovým zločincem nebo hackerem za účelem narušení nebo poškození počítače legitimního uživatele. Malware, který se šíří prostřednictvím nevyžádaných e-mailových příloh nebo legitimně vypadajících souborů ke stažení, mohou zločinci použít k vydělávání peněz nebo k politicky motivovaným kybernetickým útokům. [12]

5.2.1 Typy Malware

Existuje hodně typů malwaru, ale pochopením těchto pár typů je jedním ze způsobů, jak pomoci ochránit naše data a zařízení. [1]

Počítačový virus

Je škodlivý počítačový program, který se připojí k čistému souboru a rozšíří se po celém počítačovém systému a infikuje soubory škodlivým kódem. Na rozdíl od červů, viry ke svému fungování potřebují již infikovaný aktivní operační systém nebo program.

Virus, který se obvykle šíří prostřednictvím infikovaných webových stránek, sdílení souborů nebo stahování příloh e-mailů, zůstane nečinný, dokud nebude infikovaný hostitelský soubor nebo program aktivován. Jakmile k tomu dojde, virus je schopen replikovat se a šířit v systémech. [5][12]

Počítačový červ

Neboli worm je program, který šíří své kopie z počítače do počítače. Červ se může replikovat bez jakékoli lidské interakce a nemusí se připojovat k softwarovému programu, aby způsobil poškození. Červi mohou být přenášeni prostřednictvím softwarových zranitelností. Nebo by počítačoví červi mohli přijít jako přílohy spamových e-mailů nebo okamžitých zpráv. Po otevření by tyto soubory mohly poskytnout odkaz na škodlivý web nebo automaticky stáhnout počítačového červa. Jakmile je červ nainstalován, tiše jde do práce a infikuje stroj bez vědomí uživatele.

Červi mohou upravovat a mazat soubory a dokonce mohou do počítače aplikovat další škodlivý software. Účelem počítačového červa je někdy jen znovu a znovu vytvářet jeho kopie - vyčerpáním systémových prostředků, jako je místo na pevném disku nebo šířka pásma, přetížením sdílené sítě. Kromě toho, že červi způsobí zmatek na zdrojích počítače, mohou také ukrást data, nainstalovat zadní vrátka a umožnit hackerovi získat kontrolu nad počítačem a jeho nastavením systému. [5][12]

Trojský kůň

Trojský kůň je typ malwaru, který je maskovaný jako legitimní software. Kyberzločinci přinutí uživatele nahrát trojské koně do jejich počítače, kde způsobí poškození nebo shromáždí data. Uživatelé jsou obvykle podvedeni k načítání a spouštění trojských koní v jejich systémech. Může být i samostatný program, který si tváří užitečně - například hra, spořič obrazovky nebo jednoduchý nástroj, ale skrytě provádí činnost, která je pro uživatele nežádoucí. [5]

Po aktivaci mohou trojské koně umožnit počítačovým zločincům, aby vás špehovali, ukradli vaše citlivá data a získali přístup do vašeho systému.

Mezi tyto akce patří:

- mazání dat,
- blokování dat,
- úpravy údajů,
- kopírování dat,
- narušení výkonu počítačů nebo počítačových sítí.

Na rozdíl od počítačových virů a červů se trojské koně nedokáží samy replikovat. [12]

Spyware

Program, který tajně sleduje a zaznamenává online aktivitu, získává data, shromažďuje a odesílá data, jako jsou uživatelská jména a hesla, aby mohli počítačoví zločinci tyto informace použít. [12]

Spyware je běžná hrozba, která má na přední straně přitažlivou funkci a na pozadí běží skrytá mise, které si možná nikdy nevšimnete. Často se používá ke krádeži identity a podvodům s kreditními kartami.

Jakmile je spyware v počítači, předává vaše data inzerentům nebo počítačovým zločincům. Některý spyware instaluje další malware, který mění nastavení. [5]

Ransomware

Škodlivý software, který infikuje počítač a zobrazuje zprávy vyžadující zaplacení výkupného, aby systém mohl znovu fungovat. Tato třída malwaru je zločinné vydělávání peněz, které lze nainstalovat pomocí klamných odkazů v e-mailové zprávě, okamžité zprávě nebo na webových stránkách. Má schopnost zamknout obrazovku počítače nebo blokovat důležité, předem určené soubory pomocí hesla. Útočníci také mohou několik hodin sledovat, kolik výkupného si může oběť dovolit, než spustí šifrování dat.

Ubránit se mu z pozice běžného uživatele lze prakticky pouze na pozornosti v e-mailové komunikaci a neotevírat přílohy od neznámých odesílatelů. [12]

Obrázek 5: Příklad ransomware

Zdroj: [12]

Adware

Také známý jako software podporovaný reklamou. Tvůrci adwaru zahrnují reklamy nebo pomáhají distribuovat další software, aby vydělali peníze. [1]

V mnoha případech mohou být reklamy v samotném softwaru. Běžný adwarový program může přesměrovat vyhledávání v prohlížeči uživatele na podobné webové stránky, které obsahují propagace jiných produktů.

Programy adware existují na všech počítačích a mobilních zařízeních. Většina z nich je naprosto bezpečná a legitimní, ale některé mohou sloužit k šíření malwaru. [5][12]

Keylogger

Program, který představuje vážnou hrozbu pro uživatele a data uživatelů, protože snímá stisknutí kláves a zachycují hesla a další citlivé informace zadávané pomocí klávesnice. To dává hackerům výhodu přístupu k PIN kódům a číslům účtů, heslům webových stránek k online nakupování, e-mailovým ID, přihlašovacím e-mailům a dalším důvěrným informacím. [12]

Když hackeři získají přístup k soukromým a citlivým informacím uživatelů, mohou využít extrahovaná data k provedení online peněžní transakce s účtem uživatele. Keylogger neohrožuje přímo počítač, ale ohrožuje data uživatelů. [5]

Browser Hijacker

Únosce prohlížeče neboli hijacker mění chování webového prohlížeče přesměrováním uživatele na novou stránku, změnou jeho domovské stránky, instalací nežádoucích panelů nástrojů, zobrazováním nežádoucích reklam nebo přesměrováním uživatelů na jinou webovou stránku, bez vědomí uživatele. [5]

5.3 Spam

Je jakýkoli druh nechtěné, nevyžádané digitální komunikace, často e-mail, který se rozesílá hromadně. Spam je obrovská ztráta času a zdrojů. Problémy způsobené spamem jsou způsobeny kombinací nevyžádaných a hromadných aspektů: množství nechtěných zpráv zaplavuje systémy zasílání zpráv a přehlušuje zprávy, které příjemci chtějí. [12]

Spam najdete také na internetových fórech, v textových zprávách, komentářích k blogům a na sociálních médiích. E-mailový spam je však zdaleka nejrozšířenější a pro spotřebitele často nejnebezpečnější. [5]

5.4 Hoaxy

Nepravdivé informace neboli hoaxy, které se na sociálních sítích šíří, většinou z důvodů poplašné zprávy, obvykle vymyšlené tak, aby působily dojmem, že se něco takového mohlo stát. Hoax může obsahovat i výzvu o rozeslání mezi co nejvíce dalších adres, proto se může označovat i jako řetězová zpráva nebo e-mail. [5]

Je důležité nevěřit hned každé informaci, kterou si přečtete na internetu. Měli byste si přečtené informace ověřit i z jiného zdroje, než tomu začnete věřit.

6 ZABEZPEČENÍ

Hlavním problémem bezpečnosti nejsou dané služby a jejich technologické možnosti, ale jsme to my, lidé. Místo toho, abychom četli veškeré podmínky, které daná služba má, dodržovali jejich pravidla a znali práva, které nám ukládají, tak je všechny jen přeskočíme a tím s nimi souhlasíme, bez vědomostí, které se v nich skrývají.

Někdy se ovšem stává, že hackeři prolomí bezpečnost určité služby nebo společnosti, která udělá sama přešlap a všechny ohrozí, ale je mnohem pravděpodobnější, že si za to můžeme sami. Pastí je všude kolem nás celá řada, proto je důležité dodržovat pravidla daných služeb a co nejlépe zabezpečit svoje soukromí. Nastavení bezpečnosti na každé sociální síti se často mění a proto je důležité je pravidelně kontrolovat a případně aktualizovat dané možnosti.

6.1 Kybernetická bezpečnost

Kybernetická bezpečnost je praxe obrany počítačů, serverů, mobilních zařízení, elektronických systémů, sítí a dat před škodlivými útoky. Je také známá jako zabezpečení informačních technologií nebo zabezpečení elektronických informací. [24]

S rostoucím počtem uživatelů, zařízení a programů v moderním podniku v kombinaci se zvýšeným přílivem dat, z nichž většina je citlivá nebo důvěrná, význam kybernetické bezpečnosti stále roste. Rostoucí objem a propracovanost kybernetických útočníků a útočných technik tento problém ještě zhoršují. [24]

Kybernetická bezpečnost může být ohromující a velice komplikovaná. Ne každý manažer nebo majitel malého podniku má technické znalosti. Proto představím pár rad, které jsou určené právě pro tento typ lidí.

6.2 Zabezpečení zařízení a sítí

Je důležité zabezpečit veškeré zařízení a síť. V následujících odstavcích jsou nejdůležitější kroky pro správné zabezpečení.

6.2.1 Aktuální software

Zajistěte, aby byl váš operační systém a bezpečnostní software naprogramován na automatickou aktualizaci. Staré aplikace mohou mít mezery, které mohou hackeři zneužít, aby vstoupili do firemních sítí a ukradli citlivá data, zahájili kybernetický útok a způsobili obrovské škody vašemu podnikání a jeho reputaci. Aktualizace mohou obsahovat důležité upgrady

zabezpečení pro nedávné viry a útoky. Většina aktualizací umožňuje naplánovat tyto aktualizace po pracovní době nebo v jiném vhodnějším čase. Aktualizace opravují závažné bezpečnostní chyby, takže je důležité nikdy neignorovat výzvy k aktualizaci. [15][12]

6.2.2 Bezpečnostní software

Nainstalujte si do svých firemních počítačů a zařízení bezpečnostní software, abyste zabránili infekci. Ujistěte se, že software obsahuje antivirové, anti-spywarové a antispamové filtry. Je důležité investovat do softwaru proti malwaru, který byl speciálně navržen pro řešení nejnovějších hrozeb malwaru. Zatímco software proti malwaru dokáže zachytit a izolovat malware a viry, když udeří, je zásadní v první řadě zabránit tomu, aby tyto hrozby útočily na vaše systémy - a to je místo, kde se do hry dostává brána firewall. [12]

6.2.3 Antivirová ochrana a VPN služby

K identifikaci a následnému odstranění počítačových virů slouží antivirové programy. Je to základní ochrana pro počítač, ale chrání jen soubory ve vašem počítači. Nezabývá se další ochranou vašeho soukromí, pokud si tedy nezaplatíte balíček, ve kterém jsou i VPN služby.

Nejdříve se zaměřím, že za samozřejmou ochranu proti počítačovým virům považuji nainstalování antivirového systému, jeho správnou konfiguraci (pravidelné testování, odesílání reportů správci atd.) a pravidelnou aktualizaci (nejlépe automaticky, aby se při každém objevení nových aktualizačních souborů sama spustila). S antivirovou ochranou můžete využít i dalších pravidel, kterými můžete šíření virů značně omezit. Jedním z nich je například automatické odstraňování příloh elektronické pošty, které mají podezřelou přílohu. [4]

Nejznámější antivirové programy jsou Avast, McAfeeAntivirus, ESET NOD Antivirus atd. [12]

Význam antivirových programů tedy je, že se starají primárně o bezpečí vašich dat, zatímco VPN služby (Virtual Private Network) chrání pro změnu vaše soukromí a tím pádem i vaše data. Dokáží zašifrovat spojení počítače nebo jiného zařízení s internetem. Bohužel VPN služby nejsou široké veřejnosti tak známé, jako antivirové programy. Ale jsou velice důležité. Pro hackery není příliš komplikované sledovat vaši aktivitu na internetu, například pokud jste připojeni na veřejné Wi-Fi, natož zjistit si veškerá vaše soukromá data. Stejně tak mohou do vašeho soukromí nahlížet i poskytovatelé internetových služeb. VPN služby tomu dokáží zabránit. Data se nejdříve zašifrují, pak se teprve vypustí na internet, kde projdou serverem

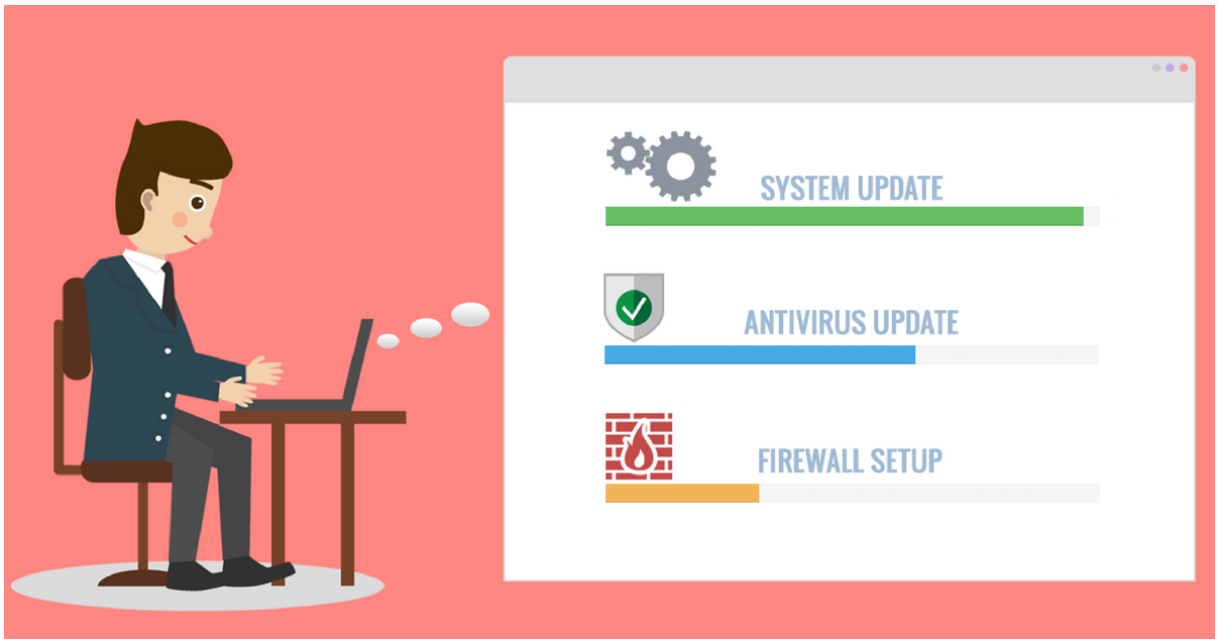
dané VPN služby, rozšifrují se a v původní podobě dorazí tam, kam mají. Dá se to přirovnat k situaci, jako bychom se z domu a zpátky dostávali bez povšimnutí tajným tunelem.

Mezi nejpopulárnější VPN služby jsou například ExpressVPN, CyberGhost, Surfshark nebo NordVPN. [1]

6.2.4 Nastavení brány firewall

Brána firewall je část softwaru nebo hardwaru, která je umístěna mezi počítačem a internetem. Funguje jako strážce brány pro veškerý příchozí a odchozí provoz. Mohou být zabudovány do hardwaru, softwaru nebo kombinace obou. Primárním případem použití brány je zabezpečení. Firewally mohou zachytit příchozí škodlivou komunikaci, než se dostane do sítě, a také zabránit tomu, aby citlivé informace opustily síť. Měl by být naistalován, spuštěn a správně nakonfigurován na každém zařízení, které se bude připojovat mimo chráněnou firemní síť. Můžete ji také nastavit na zařízení, které je na chráněné síti a tím budou chráněny před útoky kolegů z vnitřní sítě. [3][4]

Nezapomeňte nainstalovat bránu firewall na všechna přenosná obchodní zařízení.



Obrázek 6: Kroky pro zabezpečení zařízení

Zdroj: [1]

6.2.5 Ochrana proti spamu

Spam nebo nevyžádaná pošta je v dnešní době velice populární a dá se před ní chránit dvěma způsoby - aktivním a pasivním. Aktivní boj je pomalý a je tam riziko, že se počet nevyžádaných zpráv ještě zvýší. Principem aktivního boje je odhlašování z rozesílacích seznamů, což nabízí každý „slušný“ spamer. Většinou je tento způsob úspěšný, spameři nemají zájem na rozesílání zpráv někomu, kdo o ně nestojí. Jelikož je ale odesílatelů mnoho, prakticky nikdy se nemůže úplně vyhrát. [4]

Pasivní způsob je účinnější. Jeho princip je ve filtrování příchozí pošty. Prakticky všechny poštovní programy nebo i většina webových rozhraní umožňují filtrování pošty do složek podle celé řady parametrů. Pro ochranu je potřeba nastavit filtry, které budou rovnou emaily s nějakou přílohou nebo slovem („porn“, „free“, atd.) rovnou házet do nevyžádaných složek, případně rovnou odstraňovat. Při důkladném rozřazení pravidel se získá za několik dní databáze, která zachytí absolutní většinu spamových zpráv. Pasivní boj má také svojí nevýhodu a tou je, že filtr může zachytit i legální dopis, například obchodní nabídku, která nabízí k zakoupenému zboží něco „free“. Navíc spameři již vytvářejí dopisy, ve kterých nejčastější slova, proti kterým můžete nastavit filtry, nahradí písmenka za jiný znak, který má podobnou optickou podobu. Například místo písmene O napíší číslici 0, je to velmi podobné a filtr ho nezachytí. [4]

Zajímavou možností tedy je vytvořit filtry na e-maily přicházející z jiné domény než je .cz. Jednou za čas zkontrolujte a prověřte vytvořené složky, abyste nepřišli o důležité zprávy. Pro takové případy samozřejmě stanovte výjimky. [4]

6.2.6 Šifrování důležitých dat

Ujistěte se, že jste zapnuli šifrování sítě a šifrujete data, když jsou uložena nebo odeslána online. Šifrování dat zůstává jednou z nejúčinnějších forem bezpečnosti proti narušení dat. Šifrování převádí vaše data na tajný kód, než je odešlete přes internet. Tím se snižuje riziko krádeže, zničení nebo neoprávněné manipulace. Protože pokud se již útočník do počítače dostane, má sice přístup k souborům, ale jejich obsah je pro něj nečitelný. Soubory sice může zničit, ale nemůže zneužít obsah. [10]

Síťové šifrování můžete zapnout pomocí nastavení routeru nebo instalací řešení virtuální privátní sítě (VPN) do zařízení při použití veřejné sítě.

6.2.7 Silná hesla

Hesla na webových stránkách unikají často. Je spoustu databází na internetu, kde si kdokoliv může stáhnout ukradená přihlašovací údaje. Na stránce https://haveibeenpwned.com si po zadaní emailové adresy může každý vyzkoušet, z kolika služeb jeho přihlašovací údaje v minulosti unikly. [13]

Mám 4 emailové adresy, každou používám na jiný způsob komunikace. První je pro přihlašování na e-shopy, kde se přihlašuji za účelem být členem clubu, druhá slouží ke komunikaci v rámci univerzity, třetí pro komunikaci v práci a čtvrtá pro soukromou komunikaci a jako přihlašovací údaj na Facebook a Instagram. Pouze na prvním emailu mám velice lehké heslo, všude jinde mám silná hesla a další bezpečnostní prvky. Vyzkoušela jsem výše zmíněnou stránku, která mi odhalila, že pouze z prvního a nejméně chráněného emailu mi už 5krát v minulosti unikly přihlašovací údaje. To znamená, že v rámci nějaké služby byly moje údaje neúmyslně vystaveny veřejnosti a to jde pouze o úniky, o kterých se ví. Musím tedy vytvářet unikátní hesla pro jednotlivé služby a weby, abych tomu mohla předejít.

Za silné heslo se považuje takové, které není používaní nikde jinde. Zároveň se za silné považuje dlouhé heslo. Nejpoužívanější heslo na světě je „1234556“, které je prolomitelné za necelou vteřinu. Jako druhé nejpoužívanější je „password“ (v překladu heslo). Významnější faktor představuje délka hesla, než kombinace různých znaků, čísel a písmen. Pro nejlépe zvolené heslo může být série náhodných slov po sobě jdoucích, které netvoří souvislou větu. Například „jahodaokurkasushiuniverzitaluciemaledivy“, ale u hesel, která mají více jak 15 znaků, lze použít i smysluplnou větu, případně s mezerami. Lze taky vzít jako heslo první dvě až tři písmena z věty, která je pro vás lehce zapamatovatelná. Například pro Lucii, velkého fanouška seriálu Přátelé, by mohlo být „Joye, viděli jsme tě jak vcházíš, předběhl si nás na schodech“, což by v převodu na heslo vypadalo: Jo,ViJsTěJaVC,PřSiNáNaSc. [13]

Pro shrnutí by zabezpečená přístupová hesla měla být:

- dlouhá - délka alespoň 15 znaků nebo dohromady čtyři a více náhodných slov,
- složitá - velká písmena, malá písmena, číslice a speciální znaky,
- nepředvídatelná - zatímco věta může udělat dobré heslo, mít skupinu nesouvisejících slov vytvoří silnější přístupovou frázi,
- jedinečná - pro každý účet jiné heslo.

Pokud se pro všechno použije stejná přístupová fráze a někdo se jí zmocní, mohou být ohroženy všechny firemní účty.

Zvažte použití správce hesel, který pro vás bezpečně ukládá a vytváří přístupová hesla.

6.2.8 Správce hesel

Důležité je vytvářet si silná hesla, nejlépe zcela unikátní heslo pro každou službu. Ale jak si zapamatovat veškeré hesla? Pomáhá tomu správce hesel. Jedná se o zabezpečený program, do kterého si můžete ukládat vaše hesla a pamatovat si pouze jedno, to které budete zadávat do správce hesel. Mezi nejznámější se řadí 1Password a LastPass. Oba tyto programy nabízejí i varianty, kdy v rámci firmy lze spravovat jednotlivé přístupy a oprávnění. To pomáhá pro monitorování držitelů přihlašovacích údajů k jednotlivým účtům. Pokud tedy někomu ze zaměstnanců bude ukončen pracovní poměr, program nám ukáže k jakým účtům měl přístup a díky němu můžeme bývalému zaměstnanci odebrat veškerý přístup. Jedná se o lepší řešení, než měnit pokaždé heslo, které by mohlo zdržovat i obtěžovat ostatní zaměstnance. Programy správce hesel dnes dokáží pracovat i s dvoufázovým ověřením viz. 6.2.9. [13]

6.2.9 Vícefaktorové ověřovaní (MFA)

Vícefaktorové ověřování (MFA) je proces zabezpečení ověření, který vyžaduje, abyste před přístupem ke svému účtu poskytli dva nebo více důkazů své identity. Před povolením přístupu bude například systém vyžadovat heslo a kód zaslaný na mobilní zařízení. Vícefaktorové ověřování přidává další vrstvu zabezpečení, která útočníkům ztěžuje přístup k vašemu zařízení nebo online účtům. [13][15]

Většina sociálních sítích nabízí možnost dvoufázového ověření a my bychom této možnosti měli pokaždé využít. Znamená to, že po přihlášení do uživatelského účtu bude služba požadovat další ověření ve formě kódu, který přijde na mobilní zařízení. Kód většinou přichází ve formě SMS, případně se zobrazí na obrazovce telefonu. [13]

Lze také mít další aplikaci, ve které nám vyjede kód, který budete zadávat do původní služby, případně budete v aplikaci povolovat, že se jedná opravdu o nás a chceme se nově přihlásit. Dvoufázové ověření může být také, že musíte vaše přihlášení potvrdit na jiném zařízení, takto to funguje třeba u zařízení Apple. Pokud se budete chtít přihlásit pod vaším Apple ID, tak po zadání emailu a hesla se vám zobrazí okénko, do kterého máte vyplnit kód. Ten vám přijde na jiné zařízení, na kterém jste přihlášeni a na kterém musíte povolit, že se opravdu jedná o vaši osobu a povolujete přístup. Dvoufázové ověření je v dnešní době nezbytnou a extrémně důležitou ochranou účtů.

6.3 Zálohování dat

Zálohování dat a webových stránek firmy pomůže obnovit veškeré informace, které se ztratí, pokud dojde k počítačové události. Je důležité, provádět pravidelnou zálohu nejdůležitější data a informací. Naštěstí zálohování obecně nestojí moc a je snadné jej provést.

K zajištění bezpečnosti důležitých souborů je vhodné použít několik záložních metod.

Dobrý záložní systém obvykle zahrnuje [3]:

- denní přírůstkové zálohy na přenosné zařízení nebo cloudové úložiště,
- zálohy serverů na konci týdne,
- čtvrtletní zálohy serveru,
- roční zálohy serveru.

Je důležité pravidelně kontrolovat a testovat, zda lze ze zálohy obnovit data. Zvyknout si zálohovat data na externí disk nebo přenosné zařízení, jako je USB flash disk. Přenosná zařízení ukládat odděleně mimo pracoviště, což firmě poskytne plán b, pokud dojde ke krádeži nebo poškození kanceláře. Nenechávat zařízení připojená k počítači, protože mohou být infikována kybernetickým útokem. [12]

Alternativně můžete také zálohovat data prostřednictvím řešení cloudového úložiště. Ideální řešení bude při přenosu a ukládání dat používat šifrování a pro přístup používat vícefaktorové ověřování. [12]

6.4 Likvidování dat

Mít zavedená vhodná opatření pro likvidaci dat, která již nejsou potřeba, je kritickým faktorem při snižování rizika narušení bezpečnosti.

Zajištění toho, že vyřazená a znovu používaná zařízení a paměťová média byly řádně odstraněny, zajistí, že důvěrná firemní data nebude možné dále získávat – a nedostanou se do nesprávných rukou.

Pamatovat si, že přeinstalace operačního systému, formátování pevného disku nebo smazání konkrétních souborů a složek nezajistí, že data budou pryč. Ve většině případů jsou data stále zcela přístupná pomocí volně dostupných nástrojů. Ujistěte se, že váš technik pro likvidaci dat používá nástroj, který data několikrát přepíše a zajistí, že jsou neobnovitelná. [3]

Podniky by se měly snažit implementovat řádnou politiku ničení dat, která nastiňuje pravidla pro každý případ použití počítačů, telefonů, externích pevných disků atd. Ať už jsou tato zařízení přeřazena v rámci podniku nebo vyřazena na konci jejich životního cyklu. [4]

6.5 Kontrola vybavení a systému

Dalším velice důležitým krokem pro zabezpečení firemních dat je uchovávat záznamy o veškerém počítačovém vybavení a softwaru, který firma používá a ujistit se, že jsou zabezpečené, aby se zabránilo zakázanému přístupu.

Je potřeba připomínat svým zaměstnancům, aby si dávali pozor na[3]:

- kde a jak uchovávají svá zařízení,
- sítě, ke kterým připojují svá zařízení, například veřejné Wi-Fi,
- připojení pomocí USB flash disků nebo přenosných pevných disků - mohly by se na ně náhodně přenést neznámé viry a jiné hrozby z domova do vaší firmy.

Ve firme se odstraní veškerý software nebo vybavení, které již není potřeba, a zajistí se, aby po vyhození na nich nebyly žádné citlivé informace. Pokud starší a nepoužitý software nebo zařízení zůstanou součástí obchodní sítě, je nepravděpodobné, že budou aktualizovány a může jít o slabinu, na kterou by zločinci zaútočili. [3]

Také neautorizovaný přístup přechozích zaměstnanců k systémům je pro podniky běžným bezpečnostním problémem. Okamžitě se musí odebrat přístup lidem, kteří pro firmu již nepracují nebo pokud změní roli a už přístup nevyžadují. [4]

7 FIREMNÍ ZABEZPEČENÍ FIRMY XY

Pro účel své bakalářské práce jsem vybrala skutečnou firmu. Firma si nepřeje být zveřejněna, proto bude označována jako firma XY.

Cílem mé práce je zhodnotit současný stav zabezpečení firmy na sociálních sítích, zda se řídí všemi bezpečnostními pokyny, odhalit případné nedostatky a navrhnout vhodná opatření.

Při vytváření vhodných opatření pro firemní zabezpečení budeme klást důraz na radu, která říká: Absolutní bezpečnost neexistuje, rizika mohou být pouze omezena na tolerovatelnou úroveň. [3]

7.1 Základní údaje o firmě

Společnost se specializuje na maloobchodní prodej koncovým zákazníkům elektroniky a příslušenství prostřednictvím e-shopů a prodejen. V rámci této společnosti se nachází další dvě firmy, které nesou větší zaměření na dané produkty. Pro svoji práci jsem zvolila právě jednu, kterou představím níže, ta druhá je tzv. Gamecentrum.

Firma XY se řadí mezi experty na jednu z nejznámějších a největších značek elektroniky a výpočetní techniky ve světě. Nabízí prodej této značky a příslušenství. Má, jak webové stránky, na kterých lze objednat vše z jejich nabídky, tak má 10 kamenných prodejen, které můžete navštívit a případně dané zboží koupit. Na prodejnách, které jsou do detailu designově vyladěné nabízejí bohatou nabídku příslušenství a služeb, poskytují odborné poradenství, organizují semináře, provádí rozsáhlou poprodejní péči, výkupy zařízení a v neposlední řadě mají autorizovaný servis.

Ve firmě je zaměstnáno kolem 160 lidí, takže se podnik řadí mezi střední podniky. Za minulý rok tato firma vykázala obrat ve výši 2,3 miliardy Kč. Jako střední podniky označujeme ty, které zaměstnávají méně než 250 osob a jejich roční obrat nepřesahuje 50 milionů EUR. [2]

Sídlo společnosti se nachází v hlavním městě České republiky v Praze. Zde se nachází také další tři prémiové prodejny a centrální sklad. Další prodejny se nachází v dalších šesti větších městech, jako jsou například Pardubice, Karlovy Vary a České Budějovice.

7.2 Používání sociálních sítí

Každá společnost bez pohledu na typ podnikání a cílovou skupinu by měla být viděna na sociálních sítí. V České republice není zdaleka vyčerpán potenciál sociálních sítí.

Firma XY si pro své působení na sociálních sítích vybrala Facebook, Instagram. O tyto profily se stará marketingový tým, který má na starosti správu účtu. Společnost je skupina plná mladých lidí, kde se všichni podílejí na sdílení společnosti na sociálních sítích.

Založit profil na sociálních sítích není těžké, nicméně založit jej správně už je těžší. Většina firemních profilů není správně vytvořených, což může ovlivnit aktivní sledující například na Instagramu, kde jsou uživatelé velmi citliví.

7.3 Zabezpečení na sociálních sítích

Společnost si je vědoma rizik, která přicházejí společně s prezentováním na sociálních sítích a tak se snaží chránit veškeré své informace. V této kapitole se zaměřím na stav bezpečnosti firmy.

7.3.1 Programy a VPN služby

Existuje několik špičkových programů pro kybernetickou bezpečnost, které dokážou chránit firmy jakékoli velikosti před malwarem a dalšími hrozbami. Firma z důvodu bezpečnosti nechce uvádět, které programy využívá, ale v rámci firemního zabezpečení používají jak VPN, tak antivirové programy, které spravuje jejich IT oddělení. Pravidelně instalují všechny aktualizace a kontrolují, zda běží vše jak má. Veškeré programy a služby jsou placené, ale firma si zakládá na hesle, že peníze, které utratí za ochranu, stojí za to, protože narušení bezpečnosti je může stát mnohem více.

7.3.2 Přístupové údaje

Opatření pro zabezpečení dat zahrnuje omezení fyzického i digitálního přístupu. Především zajištění toho, aby byly všechny počítače a zařízení chráněny povinným zadáním přihlášením, a aby do fyzických prostor mohl vstupovat pouze autorizovaný personál.

V této firmě mají zpravidla přístupové údaje na sociálních sítích interní zaměstnanci marketingového týmu. Jedná se zhruba o max. 3 uživatelé. Popřípadě externí marketingová agentura, která firmě spravuje sociální sítě.

Marketing specialistka pravidelně využívá správcovský přístup ve spolupráci s kolegyní, která má na starosti online marketing. Každá z nich má v rámci sociálních sítí svou roli. Za brand marketing (marketing specialistka) sdílí posty, stories, videa, a píše texty. Kolegyně vytváří placené propagace.

Obě zaměstnankyně spravují profil pomocí jedné aplikace, kde si uživatel může měnit profil osobní na firemní a naopak.

7.3.3 Hesla a dvoufázové ověření

Správně vytvořená a pravidelně měněná hesla jsou základem každé ochrany na sociálních sítích. Firma XY pro svoje firemní účty vždy nutně uvádí silná hesla a využívá dvoufázové ověření. Pravidelně kontrolují nastavení a mění přístupová hesla a zabezpečení.

7.3.4 Správa zařízení

Procesy ve firmě mají nastavené. Každý zaměstnanec dostává minimálně jedno firemní zařízení a má možnost benefitu, kdy si v rámci participace může půjčit více zařízení k využívání. Tyto zařízení je potřeba také mít pod správou, aby nedošlo k jejich zneužívání případně krádeži.

Jako správu pro svá zařízení využívají MDM produkt. Je to produkt jiného dodavatele, který umožňuje správcům IT na dálku konfigurovat, spravovat, monitorovat dodržování pravidel organizace a aktualizovat iOS, iPadOS, macOS a tvOS zařízení.

7.4 Nedostatky firmy

Cílem této kapitoly je představit nedostatky firmy v rámci zabezpečení na sociálních sítích.

Prvním nedostatkem jsem zaznamenala, že má firma několik kamenných prodejen, kde ke své práci zaměstnanci využívají stolní počítače, ve kterých mají svoje interní informace v rámci celého podniku například údaje od svých zákaznících, přístupy do interních serverů a webového rozhraní, které má sloužit pouze pro ně. Kdykoli od těchto citlivých dat zaměstnanec odejde, nechává volně přístupné veškeré tyto údaje, které může útočník během pár minut zjistit a později tím ohrozit celou firmu.

Společnost nemá své účty na sociálních sítích ověřené, takže se vystavují riziku, kdy si hackeři mohou vytvořit stejný profil a pod názvem firmy nabízet určité služby nebo poškozovat firmu tím, že začnou obchodovat se zákazníky, kteří si pod myšlenkou obchodování se známou firmou mohou cokoli zakoupit. Firma již podobné situace zažila, kdy bylo založeno několik stejných profilů, kde útočníci pod jejich jménem nabízeli soutěže a kvalitní výhry. Tím byli

poškozeni hlavně zákazníci, kteří ztratili důvěru a své soukromé informace a firma tak začala ztrácet na svém dobrém jméně.

Dalším je, že IT oddělení se zabývá především zabezpečením sítě a webové stránky, ale zaměstnaneckého zařízení nikoli. Zaměstnanci se kolikrát dovolávají, že jim nějaká funkce či přístup nefunguje, případně si nevědí rady, ale IT oddělení nemá čas to s nimi hned řešit. Přitom ve většině případů stačí mít aktuální verzi softwaru nebo chybí určitý druh aplikace, které si zaměstnanec sám nestáhl.

Největším nedostatkem firmy jsem zaznamenala zabezpečení svých zaměstnanců a tím i zabezpečení podniku. Zaměstnanci, kteří nepracují v rámci IT oddělení nebo se přímo nepodílejí na správě sociálních účtů, nemají přehled, jak chránit svá zařízení a data. Přitom je jedním z největších rizik, že právě přes zaměstnance bude napadena celá organizace. Sice jsou firemní účty chráněny silnými a pravidelně kontrolovanými hesly, ale účty zaměstnanců, které používají na pracovních zařízeních nejsou ani zdaleka tak chráněna. Útočnici tak mohou napadnout soukromý účet zaměstnance a dostat se tak přes pracovní zařízení do interních dat firmy. Nemají přehled o rizicích a nejaktuálnějších hrozbách. Většinou se dozvědí, až když je někdo napaden a to je už pozdě.

Firma také nemá na všech svých prodejnách stálé zaměstnance, jsou prodejny, kdy se musejí skoro každý měsíc nabírat nový zaměstnanci, protože původní končí a tím pádem se ohrožuje bezpečnost interních systému a informací.

Firemní účet zatím nikdo nenapadl, ale útoky firma vnímá zejména na firemní síť, což se stává v posledních měsících velmi často. Poslední dobou se setkávají s podvodnými e-maily na všechny zaměstnance, ve kterých útočníci požadují zaplacení výkupného na bitcoinovou adresu. Útočník má svoji virtuální bitcoinovou adresu, kterou lze dohledat, ale nelze identifikovat majitele. Také se řadě zaměstnancům stalo, že jim byl zablokován účet a po zaplacení určité částky jim bude znovu odemknut. Ve firmě XY se nachází množství plachých zaměstnanců, kteří se strachovali nebo nevěděli, jak a komu útoky nahlásit.

7.5 Návrhy na zlepšení

Cílem je návrh řešení odstraňující nedostatky v zabezpečeni budov a areálu firmy. Návrhy na zlepšení se týkají hlavně představení zabezpečení zařízení a dat zaměstnancům firmy, kteří mohou nevědomky velice poškodit celý chod firmy. Také doporučení Apple Business Manager, který spolu s MDM programem zjednodušuje nasazení a správu.

Apple Business Manager

Jelikož firma XY má mezi všemi svými zaměstnanci zařízení Apple, tak doporučuji službu Apple Business Manager. Je to služba, která spolupracuje s MDM programem, který firma velmi dobře zná. Tahle kombinace šetří správcům IT čas a dává jim větší míru kontroly, takže můžou bezpečně škálovat zařízení podle aktuálních potřeb firmy. Zjednodušuje práci i zaměstnancům, kteří můžou zařízení začít používat hned po vybalení.

Díky automatické registraci zařízení může organizace rychle nasazovat zařízení Apple, která jsou v jejich vlastnictví a registrovat je do řešení MDM bez nutnosti fyzicky na zařízení sahat nebo připravovat každé zvlášť.

IT tým může spouštět aktualizace konkrétních aplikací i operačního systému nebo je až na 90 dní pozastavit. Takže když firemní zákazník potřebuje, aby zaměstnanci svá zařízení v určité době neaktualizovali, může aktualizace odložit na později. Tuhle úroveň kontroly samotné řešení MDM neposkytuje.

Je to také jednodušší proces nastavení pro zaměstnance, kteří mají zařízení správně nakonfigurované hned při prvním zapnutí.

Organizace má zařízení pod kontrolou pomocí funkce dohledu. Ta zpřístupňuje další možnosti správy zařízení, které v jiných modelech nasazení nejsou dostupné. Správci IT mají přístup k ovládacím prvkům, které samotné řešení MDM nenabízí - můžou podrobněji konfigurovat zabezpečení, blokovat odebrání řešení MDM, spravovat aktualizace softwaru a další.

A největší výhodu vidím v delegování úloh správy pomocí rolí. Organizace si zvolí osoby, které budou pomocí Apple Business Manageru spravovat zařízení, aplikace a účty. Takže budou pouze důvěryhodné a pověřené osoby, které budou mít vše pod kontrolou.

Ověření účtů na sociálních sítích

Doporučuji nechat si ověřit své účty, aby si uživatelé Facebooku a Instagramu byli jisti, že sledují správnou značku. Díky tomu bude firma snadno rozpoznatelná ve výsledcích ve vyhledávání a potvrdí se, že je důvěryhodná a tím, za koho se vydává.

Jak jsem psala v kapitole 3.4, tak se jedná o modrý odznak s fajfkou. Firma XY se převážně prezentuje na Instagramu, z toho důvodu představím poměrně jednoduchý proces, jak se může na této sociální sítí nechat ověřit:

1. přejděte do svého profilu a klepněte na ikonu hamburgeru v pravém horním rohu,
2. klikněte na Nastavení,
3. klikněte na Účet,
4. klikněte na Požádat o ověření,
5. požádat o ověřovací stránku Instagramu.

Dále vyplňte přihlášku:

- vaše zákonné jméno,
- vaše „známé jako“ nebo pracovní jméno (pokud existuje),
- vyberte svou kategorii nebo odvětví (například: blogger/influencer, sport, zprávy/média, obchod/značka/organizace atd.),
- musíte také odeslat fotografii svého oficiálního průkazu totožnosti. Pro jednotlivce to může být řidičský průkaz nebo cestovní pas. Pro firmy postačí účet za energie, oficiální obchodní dokument nebo daňová přiznání.

Po dokončení těchto kroků klikněte na Odeslat. Poté je potřeba vyčkat na výsledek, zda bude schváleno.

Řádné nabírání nových zaměstnanců

V dnešní době je málo lidí, kteří chtějí pracovat, ale v takové organizaci je potřeba si chránit své informace. Pokud jde o najímání nových zaměstnanců, tak by firma měla být zvlášť ostražitá a vybíravá. Zabezpečení proti vnitřním hrozbám hraje klíčovou roli v efektivní kybernetické bezpečnosti. Firma XY by se měla zaměřit na jejich minulost a udělat si představu o tom, jací jsou lidé.

Kromě toho je důležité mít na paměti změny v charakteru stávajících zaměstnanců, protože to může naznačovat jiné problémy.

Vzdělání svých zaměstnanců

Je důležité zajistit, aby všichni v organizaci rozuměli zásadám zabezpečení společnosti.

Zaměstnanci představují problém tím, že mohou kliknout na věci, které by neměli a uvolnit tak viry a malware do zařízení a ohrozit tak společnost.

Je potřeba vyškolit každého zaměstnance, aby si hlídal, co kde sdílí a rozpoznal na co může kliknout, případně do jaké aplikace se může přihlásit a sdílet tak svá data. Aby zaměstnanci, kteří obdrží nezvyklý a podezřelý e-mail, je ihned nahlašovali svému IT oddělení. Naučit zaměstnance správně vytvářet silná hesla, používat dvoufázové ověření a chránit si soukromý účet a tím i firemní data v zařízení.

Možností je vytvářet pravidelná školení pro své zaměstnance, zvyšuje se tím vědomost potenciálních obětí o možných útocích. Na školení se seznámí o rizicích a hrozbách, které existují. Představí se kroky pro preventivních bezpečnostních opatření. Předvede se, jak se má zaměstnanec zachovat v případě detekce útoku. A uvede se havarijní plán spolu s vývojem metod prevence.

Ať už se firma rozhodne to dělat během nástupu na palubu nebo bude provádět opakovací kurzy dvakrát ročně, vyplatí se to provést. Je potřeba se opakovaně ujišťovat, že opravdu všichni zaměstnanci dodržují nastavené postupy v celé společnosti.

8 OPATŘENÍ PRO PREZENTACI NA SOCIÁLNÍCH SÍTÍCH

V této kapitole představím, jaké jsou základní opatření pro firemní prezentaci na sociálních sítích. Tato opatření mohou pomoci firmám, které si nejsou jisté, jak si správně vytvořit opatření proti rizikům v celé společnosti.

8.1 Vytvoření politiky sociálních médií

Pokud firma používá sociální média nebo se na to chystá, potřebujete zásady sociálních médií. Tyto pokyny popisují, jak by firma a její zaměstnanci měli používat sociální média zodpovědně.

Firemní zásady pro sociální média by měly zahrnovat minimálně:

- pokyny pro značky, které vysvětlují, jak mluvit o společnosti na sociálních sítích,
- pravidla týkající se důvěrnosti a osobního používání sociálních médií,
- aktivity na sociálních sítích, kterým je třeba se vyhnout, jako jsou kvízy na Facebooku, které požadují osobní údaje,
- která oddělení nebo členové týmu jsou zodpovědní za jednotlivé účty na sociálních sítích,
- pokyny týkající se autorských práv a důvěrnosti,
- pokyny, jak vytvořit účinné heslo a jak často hesla měnit,
- očekávání pro aktualizaci softwaru a zařízení,
- jak identifikovat podvody, útoky a další bezpečnostní hrozby a jak se jim vyhnout,
- koho upozornit a jak reagovat, pokud vznikne obava o bezpečnost sociálních médií.

Pomůže to ochránit nejen před bezpečnostními hrozbami, ale také před špatnými vztahy s veřejností nebo právními problémy.

8.2 Určení zranitelných míst

Základním krokem k ochraně před kybernetickými útoky je zjištění zranitelných míst v podniku.

Jsou základní otázky, na které by firma měla ohledně bezpečnosti znát odpovědi:

- co chce ochránit,
- proč to chce ochránit,
- jak to chce chránit,
- jak ověří, že je chráněno,
- co bude dělat, když se něco pokazí.

Jako první krok si zjistíte veškeré důležité údaje, kterými podniky disponuje. Může se jednat prakticky o veškeré informace, od soukromých údajů podniku po finanční informace. Jakmile budete znát všechny procesy a data, se kterými vy a vaši zaměstnanci pracují a budete vědět z jakého důvodu je potřeba tyto údaje chránit, můžete přemýšlet o tom, jakými způsoby vše dokážete ochránit.

8.3 Havarijní plán

Tímto odpovídám na poslední základní otázku ohledně bezpečnosti. Dobře naplánovaný a efektivní plán obnovy po katastrofě připraví půdu pro rychlou reakci, pokud vaše organizace v budoucnu zažije kybernetický útok. Mělo by mít přesně definovanou cestu eskalace a proaktivní komunikace má být upřednostněna v případě, že dojde k takové nešťastné události.

Havarijního plán by měl obsahovat [4]:

- odstranění akutního nebezpečí,
- obnovení systému,
- obnovení dat,
- zavedení protiopatření.

Je důležité mít osobu, která bude za tento plán zodpovědná a v případě potřeby bude přesně stanovovat, jaké kroky je třeba podniknout. Bude rozhodovat o tom, že nastal krizový stav a kdy může být tento stav ukončen.

8.4 Správcovská oprávnění

Jedná se o možnost, kde se udělují různé přístupy zaměstnancům, aby každý měl přístup pouze k tomu, k čemu opravdu má dovoleno. Oficiální účty by měly být ve správě a vlastnictví organizace tak, aby v případě personálních změn nemuselo docházet k zakládání nových účtů, či jejich přejmenování, které je často problematické. Pro každý účet je potřeba vytvořit e-mail, který bude svázán a používán výhradně pro správu sociálních účtů. [15]

Je potřeba jasně definovat, kdo má k účtům přístup a pravidelně kontrolovat, komu jsou přidělena jednotlivá administrativní práva.

Na Facebooku jsou nabízená více úrovně administrace. Správce, je nejvyšší úroveň, kterou by mělo zastávat minimum lidí, nejlépe dva lidé. Pokud by byl pouze jeden, je riziko, že by se s ním nebo jeho účtem mohlo něco stát a nikdo se ke stránce už nedostane, u tří a více lidí je riziko, že by se nepohodli. Správce má práva pro celou stránku a pouze on může přidat či odebrat dalšího administrátora s libovolnou rolí. Další role je například Editor, která má přístup pouze pro vytváření samotného obsahu.

Správcovská oprávnění umožňují někomu provádět vyšší nebo citlivější úkoly než obvykle. Budou se velmi lišit od standardních oprávnění nebo uživatelských oprávnění hosta. Zločinci budou tato privilegia často hledat, aby jim poskytli lepší přístup a kontrolu nad vaším podnikáním.

Chce-li firma toto riziko snížit, je potřeba používat účty s oprávněními správce pouze v případě potřeby. Omezit ty, kteří mají přístup a nikdy nečíst e-maily ani nepoužívat internet, když je používán účet s oprávněními správce.

8.5 Připojení k sociálním sítím

Útočníci běžně zakládají nezabezpečené a neznámé sítě, aby mohli zachytit přihlašovací a jiné údaje, proto je potřeba do těchto účtů přistupovat ze zabezpečené sítě a zařízení. Což se dostáváme k tomu, aby se pro správu oficiálních firemních účtů nepoužívala soukromá zařízení.

Stejně tak je potřeba se vyhnout odkazům v e-mailu či zkračovačům URL, abyste se vyhnuli riziku přesměrování na podvodné stránky. [15]

Pro přístup na mobilních zařízení využívat jedině oficiální zdroje (např. App Store, Google play), které nabízejí důvěryhodné aplikace. Můžete tak zkontrolovat, zda se jedná o známého

výrobce, aplikaci a jaké má recenze či počet stažení. Tyto aplikace a zařízení, ze kterého se přihlašujete je potřeba pravidelně kontrolovat a aktualizovat.

Abyste předešli některým typům útoků a měli jistotu, že odchozí provoz z vašeho zařízení bude šifrovaný, tak je nezbytné se mimo kancelář přihlašovat pomocí VPN služby.

Při předpokladu dočasného opuštění používaného zařízení a pozdějšího pokračování v dané aktivitě, musíte uzamknout obrazovku. Pokud jste si jisti, že s danou aktivitou končíte, tak řádně zkontrolujte bezpečné odhlášení. Těmito kroky minimalizujete rizika cizího vniknutí do zařízení a na účet.

8.6 Bezobslužné účty na sociálních sítích

Je dobré rezervovat si značku firmy na všech kanálech sociálních médií, i když zrovna nejsou v plánu je hned všechny používat. To umožní udržovat přítomnost napříč sítěmi, takže lidé firmu snadno najdou.

Aby se snížilo riziko, že se útočníci pokusí napodobit stránku organizace, nebo se budou vydávat za oficiální účet, je potřeba si na sociálních sítích zaregistrovat i alternativní názvy oficiálních účtu organizace. A poté si veškeré účty nechat ověřit. Zajištění u všech účtů ověření, aby se zvýšila důvěryhodnost pro média i veřejnost.

Také je důležité, aby firma neignorovala účty, které ještě nepoužívá, které přestala používat nebo nepoužívá často. Nesledované účty na sociálních sítích se mohou stát cílem hackerů, kteří by pod firemním jménem mohli začít zveřejňovat podvodné zprávy. Jakmile hackeři získají kontrolu, mohou poslat cokoli. To může znamenat nepravdivé informace, které poškodí firmu. Nebo možná jsou to viry infikované odkazy, které způsobí vážné problémy sledujícím. A ani si toho nevšimnete, dokud za vámi zákazníci nezačnou chodit pro pomoc.

8.7 Personální bezpečnost

Pokud jde o kybernetickou bezpečnost, existuje běžné rčení - „jste stejně zabezpečení jako váš nejméně informovaný zaměstnanec“ - a to platí. Co když nic netušící zaměstnanec ve vaší kanceláři použije slabá hesla nebo se pokusí o phishing - a jeho systém je ohrožen?

Proto je zásadní zajistit, aby zaměstnanci věděli, jak by je zločinci mohli oklamat, aby odhalili citlivé soukromé informace. Měli by být schopni okamžitě identifikovat podezřelý telefonní hovor nebo e -mail. Naučit je, jak chránit organizaci před těmito druhy útoků.

Zásady kybernetické bezpečnosti pomáhají zaměstnancům pochopit jejich odpovědnosti a to, co je přijatelné. Zaměstnanci by měli vědět, kde najdou veškeré zásady a na koho se mají obrátit v případě nejasností. [4]

Vzdělávání zaměstnanců je o:

- udržování dobrých hesel a přístupových frází,
- jak identifikovat a vyhnout se kybernetickým hrozbám,
- co dělat, když narazí na kybernetickou hrozbu,
- jak nahlásit kybernetickou hrozbu,
- jak se chovat a co zveřejňovat na sociálních sítích.

Pravidelné programy zvyšování povědomí a školení mohou zaměstnancům pomoci identifikovat útoky na sociálních sítích a pomoci chránit firmu před útoky na sociálních sítích.

Většina zaměstnanců je aktivních na platformách sociálních médií, jako je Facebook, Instagram atd. Informace, které na těchto platformách zveřejňují, mohou být seškrábnuty aktéry hrozeb, aby vytvořili vysoce cílené e-maily typu spear phishing za účelem ukradení účtů a poškození reputace organizace nebo získali přístup do interních sítí. To, jak zaměstnanci komunikují na sociálních sítích, se navíc může odrazit na značce podniku a online pověsti.

Když zaměstnanci rozumí osvědčeným postupům a cítí se jistě při používání sociálních médií pro svou práci. Jsou pak dobře vybaveni k používání sociálních médií pro osobní i profesní účely.

8.8 Ochrana zákazníků

Je zásadní, aby firma udržovala své zákazníky v bezpečí. Ztratí-li nebo kompromituje jejich informace, poškodí to obchodní pověst a může čelit právním následkům.

Důležité je se ujistit, že firma:

• investuje a poskytuje bezpečné online prostředí pro transakce,

• zajišťuje veškeré osobní informace o zákaznících, které ukládá.

Pokud společnost provádí platby online, zjistí si, co může poskytovatel platební brány udělat, aby zabránil podvodům s online platbami.

Ochrana zákazníků spočívá také v tom, že firma nedopustí, aby se zákazník mohl stát obětí útočníků na podvodném sociálním účtu. Existují zákony o tom, co může společnost dělat s jakýmikoli osobními údaji, které shromažďuje od svých zákazníků.

8.9 Kontrola a aktuální informace

Mezi bezpečnostní zásady také patří pravidelné kontroly a audity. Tyto kroky zaznamenávají informace o činnostech a procesech vykonaný jménem uživatele, takže v případě poškození je daný držitel odpovědný za svou činnost. Audity mohou pomoci předejít všem hrozbám, než bude pozdě. Kontrolují zda se veškeré zásady dodržují správně a je tak zachována určitá prevence. Je ale velmi důležité, aby kontrola byla prováděna pravidelně a byla nezávislá na prosazování činnosti bezpečnosti.

Rovněž je důležité mít přehled o nejnovějších hrozbách a případně se proti nim chránit. Zajištění bezpečnosti společnosti před kybernetickými hrozbami vyžaduje spoustu péče a vývoje spolehlivé strategie kybernetické bezpečnosti. Spojením osvědčených postupů a profesionálního poradenství můžete tyto výzvy efektivně řešit.

ZÁVĚR

Cílem práce bylo popsat rizika a nebezpečí při prezentaci na sociálních sítích a na základě výsledků vytvořit důkladné opatření a zabezpečení, které pomohou firmám založit správnou bezpečnostní politiku v celé organizaci.

Velkým nedostatkem firem je nedostatečné zabezpečení zařízení a dat. Pro návrh jsem vytvořila základní bezpečnostní politiku, ve které jsou popsány zásady a postupy před bezpečnostními hrozbami. Určením co, proč a jak to chce chránit, si firma vytvoří zranitelná místa a lépe si pak připraví a naplánuje efektivní havarijní plán, díky kterému se rychle a účinně zbaví kybernetických útoků. Také je důležité, aby si každá společnost hlídala své oficiální účty, vytvořila z nich ověřené účty a nahlašovala každý podvodný, který se jej snaží napodobit a poškodit reputaci. Za hlavní nedostatek považuji řádné informování a naučení firemních zaměstnanců, kteří se podílejí na sdílení na sociálních sítích a ochraně podniku. Zaměstnanci neznají možná rizika a nevědí, jak se proti nim chránit a tím je ohrožena celá firemní politika. Proto je důležité vytvářet pravidelné školení a programy pro zvyšování povědomí, na kterých se zaměstnanci budou vzdělávat a opakovat, jak chránit svá i firemní data. Firma by také neměla zapomínat na ochranu svých zákazníků. Právě zaměstnanci a zákazníci jsou lidé, kteří budují dobré jméno firmy a ta se díky nim stává populárnější. V neposlední řadě je důležité být v neustálém pozoru, sledovat aktuální a nejnovější hrozby a provádět pravidelné kontroly a audity veškerých nastavení a zásad.

Dle mého názoru by firma XY neměla spoléhat, že je správně zabezpečena a mohla se tak soustředit hlavně na obchodní část. Spoléhá na své IT oddělení, které daný problém v konkrétní chvíli vyřeší, ale možný útok může nastat přes účet zaměstnance v jakoukoli hodinu a den a tím tak poškodit zařízení, data a reputaci společnosti.

POUŽITÁ LITERATURA:

[1] Co je to VPN? *Získejte nejnovější McAfee VPN | McAfee.* [online]. Copyright © 2021 McAfee, LLC [cit. 21.11.2021]. Dostupné z: https://www.mcafee.com/cs-cz/vpn.html.

[2] Definice malého a středního podnikatele - CzechInvest. *Object moved* [online]. © 1994 [cit. 20.11.2021]. Dostupné z: https://www.czechinvest.org/cz/Sluzby-pro-male-a -stredni-podnikatele/Chcete-dotace/OPPI/Radce/Definice-maleho-a -stredniho-podnikatele.

[3] DOBDA, Luboš. *Ochrana dat v informačních systémech*. Praha: Grada, 1998. ISBN 80-7169-479-7.

[4] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[5] HUB, Miloslav. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice: Univerzita Pardubice, 2013. ISBN 978-80-7395-701-8.

[6] Instagram's @Creators. *Instagram* [online]. [cit. 2021-11-20]. Dostupné z: https://www.instagram.com/creators/?hl=cs.

[7] Jak můžu na Facebooku požádat o štítek ověření? *Facebook* [online]. 2021 [cit. 2021-11-20]. Dostupné z: https://www.facebook.com/help/1288173394636262/?helpref=uf_share.

[8] Jak na Internet - Sociální sítě. *Jak na Internet - Jak na Internet* [online]. © 2021 CZ.NIC, z. s. p. o. [cit. 20.11.2021]. Dostupné z: https://www.jaknainternet.cz/page/1751/socialni-site/.

[9] Jak vznikl a následně uspěl Instagram, jehož hodnota se dnes odhaduje na 35 miliard dolarů? - *CzechCrunch. CzechCrunch - byznys, technologie, startupy, lifestyle, vzdělávání* [online]. © 2014 [cit. 18.11.2021]. Dostupné z: https://cc.cz/jak-vznikl-a -nasledne-uspel-instagram-jehoz-hodnota-se-dnes-odhaduje-na-35-miliard-dolaru/.

[10] JAŠEK, Roman. *Informační a datová bezpečnost*. Ve Zlíně: Univerzita Tomáše Bati, 2006. ISBN 80-7318-456-7.

[11] KOVACICH, Gerald L. *Průvodce bezpečnostního pracovníka informačních systémů: zavádění a prosazování bezpečnostní politiky informačních systémů*. Brno: Unis, 2000. ISBN 80-86097-42-0.

[12] KOHOUT, Roman a Radek KARCHŇÁK. *Bezpečnost v online prostředí*. Karlovy Vary: Biblio Karlovy Vary, 2016. ISBN 978-80-260-9543-9.

[13] LOSEKOOT, Michelle a Eliška VYHNÁNKOVÁ. *Jak na sítě: ovládněte čtyři principy úspěchu na sociálních sítích*. V Brně: Jan Melvil Publishing, 2019. Žádná velká věda. ISBN 978-80-7555-084-2.

[14] Most used social media 2021 | Statista. • *Statista - The Statistics Portal for Market Data, Market Research and Market Studies* [online]. © Statista 2021 [cit. 20.11.2021]. Dostupné z: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.

[15] Národní úřad pro kybernetickou a informační bezpečnost - Doporučení pro správu sociálních sítí, verze 1.0. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka [online].* Dostupné z:https://www.nukib.cz/cs/infoservis/doporuceni/1518-doporuceni-pro-spravu-socialnich-siti-verze-1-0/.

[16] Národní úřad pro kybernetickou a informační bezpečnost - Phishing - stále aktuální hrozba. *Národní úřad pro kybernetickou a informační bezpečnost - Úvodní stránka* [online]. Dostupné z: https://nukib.cz/cs/infoservis/doporuceni/1494-phishing-stale-aktualni-hrozba/.

[17] Podmínky použití. *Facebook* [online]. 2020 [cit. 2021-11-20]. Dostupné z: https://www.facebook.com/help/instagram/581066165581870/?helpref=hc_fnav&bc[0]=Nápověda%20pro%20Instagram&bc[1]=Centrum%20soukrom%C3%AD%20a%C2%A0bezpečnosti.

[18] SEMERÁDOVÁ, Tereza a Petr WEINLICH. *Marketing na Facebooku a Instagramu: využijte naplno organický dosah i sponzorované příspěvky*. Brno: Computer Press, 2019. ISBN 978-80-251-4959-1.

[19] SHIH, Clara Chung-wai. Vydělávejte na Facebooku: jak využít sociální sítě k oslovení nových zákazníků, vytvoření lepších produktů a zvýšení prodejů. Přeložil Patrik MÍŠA. Brno: Computer Press, 2010. ISBN 978- 80-251-2833-6.

[20] SOCHŮRKOVÁ, Martina Frascona'. Jak získat ověřený instagramový účet. *Newsfeed*[online]. 2019 [cit. 2021-11-20]. Dostupné z https://newsfeed.cz/jak-ziskat-overeny-instagramovy-ucet/.

[21] Sociální sítě - INTERNETEM BEZPEČNĚ. *INTERNETEM BEZPEČNĚ - Užívejme internet bezpečnějším způsobem* [online]. © 2018 INTERNETEM BEZPEČNĚ. Všechna práva vyhrazena. [cit. 20.11.2021]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/socialni-media/socialni-site/.

[22] SOCHŮRKOVÁ, Martina Frascona'. Jak si zabezpečit instagramový účet. *Newsfeed*[online]. 2019 [cit. 2021-11-20]. Dostupné z: https://newsfeed.cz/jak-si-zabezpecit-instagramovy-ucet/.

[23] SPENCER, Jamie. 101 Social Networking Sites You Need To Know About In 2021. *Makeawebsitehub* [online]. 2021 [cit. 2021-11-20]. Dostupné z: https://makeawebsitehub.com/social-media-sites/.

[24] ŠILHÁNEK, Martin. *REŠERŠE INFORMAČNÍCH ZDROJŮ SVĚTA K INFORMAČNÍ A KYBERNETICKÉ BEZPEČNOSTI*. Praha, 2020. Bakalářská práce. AMBIS vysoká škola a.s. Vedoucí práce Ing. Vladimír Šulc, Ph.D.

[25] Vše, co potřebujete vědět o Facebook Business Manager | Socials. 302 Found [online]. Copyright © 2021 [cit. 28.11.2021]. Dostupné z: https://www.socials.cz/cs/blog/vse-co-potrebujete-vedet-o-facebook-business-manager-24/.

[26] Vznik a historie Facebooku | Zdeněk Blažek. Zdeněk Blažek | Expert strategického (360) marketingu [online]. © 2016 [cit. 22.11.2021]. Dostupné z: https://www.zdenekblazek.cz/vznik-a -historie-facebooku/.

[27] Zásady používání dat. *Facebook* [online]. 2020 [cit. 2021-11-20]. Dostupné z: https://www.facebook.com/about/privacy/update.