Eliminácia rizík zo sociálnych sietí

Ľubomír Kopáček

vedúci divízie bezpečnosti | GAMO, a.s.

eFOCUS

GAMO

INFORMAČNÉ TECHNOLÓGIE

Riziká, hrozby, zraniteľnosti

- Riziká sociálnych médií pre biznis sú výsledkom kombinácie faktorov
  - **Hrozieb** (Insider Threat – ľudia z prostredia organizácie, cielené útoky „z vonku“)
  - **Zraniteľností** (chýbajúce pravidlá a technické opatrenia)
  - a používaním **útočných techník** (samotné sociálne médiá sú **exploitom** a **útočným vektorom** zároveň)

Každá organizácia je **mimoriadne toxické prostredie**, zamorené hrozbami ;)

Hurikán vs. človek

- **Hrozba** hurikánu je mimo akejkoľvek kontroly, ale vieme že môže potenciálne udrieť
- **Zraniteľnosť** je fakt, že nemáme plán pre prípad, že hurikán fyzicky poškodí naše stavby, infraštruktúru, informačné prostriedky atď. (ku škodám príde aj napriek plánu...)
  - alebo nemáme **prostriedky**, ktorými sa chrániť pred vznikom rizík
- **Rizikom** je to, že kvôli existujúcim zraniteľnostiam a výskytu hrozby prišlo ku škodám, ktoré videli k poškodeniu nášho biznisu (ak máme plán, vieme aspoň reagovať)

Definícia sociálnych sietí / médií

- Webové služby umožňujúce jednoduché **vytváranie** osobných aj obchodných **interakcií** bez geografického obmedzenia

- Vytváranie obsahu samotnými užívateľmi formou **zdieľania** správ, dokumentov alebo multimediálneho obsahu

Facebook, Instagram, Youtube, Twitter, Pinterest, Tumblr, LinkedIn a tisíce ďalších

Vzťah sociálnych médií a podnikového sveta

- Organizácia **cielene využíva** sociálne médiá ako marketingový a komunikačný nástroj, prípadne ako inú súčasť svojej činnosti

- Používanie / zneužívanie sociálnych médií predstavuje **útočnú techniku** (exploit) a zároveň aj **vektor útoku** („cestu“ ktorou je útok vedený)
  - Z insidera sa tak stane buď „**human attack surface**“ (ten na koho je útok smerovaný) alebo útočník (ten kto útok vykonáva)

„Zábavné“ fakty

- Podvodné správy (scams) na Facebooku sú prvou voľbou pokusu o prienik do sietí a systémov (zdoj: CISCO)
- Obsah správ u % užívateľov sociálnych médií: 92% spam, 54% phishingové linky, 23% malware. 1 z 5 užívateľov bol hacknutý (zdroj: Barracuda)
- 29.000.000 tweetov denne je „závadných“ (zdroj: Trend Micro)
- Náklady na phishing cez sociálne médiá v USA dosahujú 1,2 miliardy USD (zdroj: Kaspersky Lab)

Riziká vo firemnom prostredí

- Reputačné riziká
- Finančné riziká
- Riziká informačnej bezpečnosti
- Riziká ochrany súkromia
- Právne riziká
- Prevádzkové riziká

Reputačné riziká

- Publikovanie negatívnych informácií o organizácii
- Oficiálne publikované, ale marketingovo nesprávne komunikované informácie
- Zdrojom reputačných rizík môže byť tak insider, ako aj externá hrozba
- Technické riešenie nie je možné

Finančné riziká

- Publikovanie finančných dát na sociálne médiá skôr ako mali byť oficiálne zverejnené
- Finančné straty ako dôsledok všetkých ostatných rizík
- Zdrojom finančných rizík môže byť tak insider, ako aj externá hrozba
- Technické riešenie nie je možné

Riziká informačnej bezpečnosti

- Infiltrácia škodlivým kódom
- Únik dát
- „Overshare“ – zdieľanie príliš veľkého množstvá informácií a detailov zjednodušuje útočníkom prvú fázu útoku
- Krádež prihlasovacích údajov ako dôsledok phishingu cez sociálne médiá
- Insider môže poslúžiť ako spoľahlivý human attack surface
- Technické riešenie je čiastočne možné

Riziká ochrany súkromia

- „Overshare“ – zdieľanie príliš veľkého množstvá informácií
- Dôsledok právnych rizík v súvislosti s ochranou osobných údajov
- Technické riešenie nie je možné

Právne riziká

- Možný dôsledok reputačných rizík a rizík informačnej bezpečnosti
- Ochrana osobných údajov
- Kybernetická bezpečnosť
- Regulačná legislatíva
- Nové problémy - napr. lustrácia zamestnancov cez sociálne médiá s negatívnymi dôsledkami na základe „kompromitujúcich“ informácií
- Technické riešenie nie je možné

Prevádzkové riziká

- Znížená produktivita práce v dôsledku aktívneho používania sociálnych médií zamestnancami
- Zneužívanie pracovných prostriedkov
- Neprimerané vyťažovanie sietí
- Technické riešenie je čiastočne možné

Všeobecné riziká

- Zneužitie identít jednotlivcov, značiek, organizácií
- Krádeže účtov
- Distribúcia škodlivého kódu
- Phishing
- Fake news
  - Manipulácia verejnej mienky
  - Šírenie hoaxu
  - Propaganda

Kyberšikana = smrteľné riziká

- Stalking (prenasledovanie)
- Ostrakizácia (vylúčenie jednotlivca zo skupiny)
- Grooming (manipulácia obete za účelom zneužitia)
- Sexting (vylákanie multimediálneho obsahu obete so sexuálnou tematikou s následným zverejnením)
- Happy Slapping (agresor si vytvorí videozáznam s napadnutím obete a následne ho zverejní)

Evolúcia paralelnej reality

1993
WWW pre verejné používanie

1994
Vzniká **Yahoo!**

1996
Vzniká **Hotmail**, Nokia prináša prvý telefón s pripojením na internet **Nokia 9000**

1997
Registrácia domény **google.com** a vznik služby

2004
Mark Zuckerberg spúšťa službu **thefacebook.com** a **Google** vstupuje na burzu

2005
Vzniká **Youtube**

.com bublina

Evolúcia paralelnej reality

2006
Google kupuje **Youtube**, vzniká **Twitter**

2007
Apple spúšťa predaj prvej verzie **iPhone**

2009
Hodnota **Twitteru** na burze dosahuje **$1.000.000.000**

2010
Vzniká **Instagram**

2011
Google spúšťa vlastnú sociálnu sieť **Google+**

2012
Facebook prekonal hranicu **1.000.000.000** aktívnych užívateľov

Evolúcia paralelnej reality

2012

Facebook kupuje **Instagram** za **$1.000.000.000**

2014

Facebook kupuje **WhatsApp** za **$19.000.000.000**

2016

Facebook nepriamo dopomohol k víťazstvu **Donalda Trumpa** v prezidentských voľbách

2017

Facebook prekonal hranicu **2.000.000.000** aktívnych užívateľov

Od roku 2012 "éra" Facebooku

- Celkovo 66 akvizícií
- Hodnota akvizícií vyše **$23.000.000.000**
- 3x viac užívateľov ako všetky ostatné siete spolu

Globálna štatistika za január 2017

- **2,789** miliardy aktívnych užívateľov
  - **37%** celkovej svetovej populácie

- **2,549** miliardy užívateľov cez mobilné telefóny
  - **34%** celkovej svetovej popuplácie cez mobilné telefóny

Celý kontinent - Európa

839 mil. obyvateľov	Za 1 rok
▪ 637 mil. (76%) online	⬆ 3% (21 mil.)
▪ 412 mil. (49%) na soc. sieťach	⬆ 5% (20 mil.)
▪ 1,101 mld. (131%) mobilných telefónov	⬇ 0,1% (1 mil.)
▪ 340 mil. (40%) soc. siete cez mobil	⬆ 11% (35 mil.)

Celý kontinent - Amerika

1,006 mld. obyvateľov	Za 1 rok
▪ 718 mil. (71%) online	⬆ 8% (53 mil.)
▪ 599 mil. (60%) na soc. sieťach	⬆ 17% (88 mil.)
▪ 1,069 mld. (106%) mobilných telefónov	⬇ 0,3% (3 mil.)
▪ 535 mil. (53%) soc. siete cez mobil	⬆ 22% (98 mil.)

Aktívni užívatelia za mesiac

- **1,871** mld. Facebook
- **1,000** mld. Youtube
- **600** mil. Instagram
- **550** mil. Tumblr
- **317** mil. Twitter
- **150** mil. Pinterest
- **106** mil. LinkedIn

Sila sociálnych médií – kampaň 1/10

- Virálna kampaň v Českej republike – **www.1z10.cz**
- „Obeťou“ kampane český moderátor Leoš Mareš – najvplyvnejší „influencer“ na Instagrame s dosahom na Českú a Slovenskú republiku
- Kampaň využila silu sociálnych médií a efekt „influencera“
- V priebehu niekoľkých hodín kampaň zasiahla prakticky všetky mainstreamové médiá v Českej republike – náklady na virálnu časť kampane boli presne **0,- Kč**

Sila sociálnych médií – kampaň 1/10

- Kampaň 1 z 10 nebola prvou úspešnou virálnou kampaňou, ale na rozdiel od väčšiny ostatných sa nespoliehala na humor ale stavila na
  - **Hate / nenávisť**
  - **Spoločného nepriateľa**
- Fanúšikovia Leoša Mareša a médiá informácie šírili s negatívnou emóciou – zlosť na tvorcov celej kampane
- Bližšie info **www.stream.cz** – One Man Show

Riešenie na záver ;)

„Já bych všechny ty internety a počítače zakázala“

17.9.1999 Věra Pohlová, 72 rokov, dôchodkyňa

Ďakujeme za pozornosť

GAMO
INFORMAČNÉ TECHNOLÓGIE

eFOCUS