14. 10. 2020
Základní bezpečnost pro uživatele

Populace 7,4 miliard lidí, **3,6 miliard lidí jsou aktivními uživateli Internetu** a více než 2,1 miliard lidí jsou aktivní uživatelé sociálních sítí. Mobilní telefony vlastní více než 3,6 miliardy uživatelů.

Útoky na benešovskou nemocnici a doly OKD únor 2020

- botnet Emotet + malware TrickBot + ransomware Ryuk

- Emotet je schopen navázat na předchozí legitimní e-mailové konverzace oběti (legitimizace), příloha obsahuje makro, které stáhne TrickBot (sbírá citlivá data), útok je dokončen spuštěním ransomware (šifrování dat na všech dostupných discích uživatele). Výkupné většinou nefunguje

Co můžu udělat pro snížení hrozeb kybernetických útočníků

a) Pravidelná aktualizace operačního systému, pouze podporované operační systémy
b) Antivirová ochrana + ochrana proti ransomware
c) Firewall - ochrana mezi PC a internet, operační systém WinXP - 10
d) 2FA - dvoufaktorová autentizace (uživatel + heslo a další faktor)
e) Microsoft Office - zakažte makra (docx, xlsx, pptx, accdb)
f) Zálohujte svá data na externí média (usb - disky se šifrováním)
g) Oddělujte hesla pro různé služby
h) Nevolte jednoduchá hesla (8, 12 – 14)[1]
i) Ukládání hesel - například aplikace KeePass, https://keepass.info(šifruje soubor)
j) Nenechávejte si hesla a přístupové kódy v e-mailu
k) Zabezpečit domácí WIFI (admin, password), aktualizace firmware
l) Anonymní WIFI jsou nebezpečné, používejte raději mobilní data
m) Kde zadávám citlivé údaje, vyžaduji HTTPS a platný certifikát
n) Neposkytujte osobní údaje sociálním sítím
o) E-mail, který není podepsán elektronickým podpisem, není důvěryhodný
p) Šifrujte data - VeraCrypt
q) Pozor na ztracené USB disky
r) Pozor na nalezené USB disky a jiná média
s) Pozor na podvodná volání ze zahraničí a SMS
t) Ztráta notebooku pod heslem neznamená, že se útočník nedostane k datům
u) Při likvidaci PC, notebooku, telefonu, tabletu důkladně zničte disk – seriál Most Čočkin
v) Aktualizace aplikací

https://www.jaknainternet.cz/page/1249/elektronicky-podpis/
https://www.jaknainternet.cz/page/1251/sifrovani/

[1] Časová náročnost prolomení hesel - https://www.internetembezpecne.cz/internetem-bezpecne/navody/heslo/

Digitální stopa v kyberprostoru

Pokud kdykoliv cokoliv nahrajete, přenesete, zprostředkujete, vložíte do kyberprostoru, zůstane to tam „navždy“.

Můžeme rozdělit na stopy ovlivnitelné a neovlivnitelné.

Neovlivnitelná digitální stopa (Informace z počítačového systému, připojení k počítačovým sítím; využívání poskytovaných služeb atd.)

IP adresa, MAC adresa – předáváme při připojení svému ISP
ICANN – Internet Corporation for Assigned Names and Numbers
„Euro-asijská“ oblast - RIPE NCC: https://www.ripe.net/
https://www.nic.cz/whois
Jak zjistit IP adresu počítače, e-shopu? **svkul.cz**
Ověření domény v registru whois.
https://whois.smartweb.cz/

E-mail
E-mail není anonymní služba. Zpráva, která je odeslána od zdroje k adresátovi, v sobě typicky nese celou řadu informací, které mohou identifikovat jednak poskytovatele služby e-mail, poskytovatelé připojení, software ze kterého byl odeslán e-mail.

Web prohlížeče
- Navštívený server získává od klienta používaný webový prohlížeče, operační systém, IP adresu, historie, cookies
- Aplikace Lightbeam
- Anonymní režim, pročištění prohlížeče

Určení počítačového systému na základě informací z jeho komponent

Ovlivnitelná digitální stopa
(blogy, fóra, sociální sítě, e-mail, datová úložiště, cloudové služby atd.)

Google
uživatel sám poskytne (jméno, e-mail, telefon, platební kartu)
informace, které si sám Google zjistí používáním služeb – informace o hardware, využití služeb Google, informace z telefonování, informace o poloze zařízení, informace o souborech

Sociální sítě
Sociální sítě vytváří prostředí, které umožňuje potenciálnímu útočníkovi velmi rychlý přístup k oběti a informacím, které o sobě oběť sama dobrovolně zveřejní.
Doporučení pro uživatele sociálních sítí.
Kyberšikana
Právo na zapomenutí
Ares, Justice, Insolvenční rejstřík, Certifikační autority (elektronický podpis)

Kyberkriminalita

Proč nám kyberkriminalita narůstá?

a) Bez rizika fyzické újmy
b) Obrovské zisky (globální business)
c) Pravděpodobnost dopadení je menší než u jiné druhy kriminality
d) Závislost společnosti na Internetu
e) Nízká ICT gramotnost uživatelů

Sociální inženýrství (Sociotechnika)

- není tím pravým kybernetickým útokem, příprava na kybernetický útok,
- ovlivňování, přesvědčování, manipulace s cílem donutit lidi provést určitou akci s cílem získat informaci, kterou bychom jinak ne-poskytli,
- nechce získat heslo silou, ale dobrovolně, oběť je uvedena v omyl a sama prozradí citlivé údaje nebo heslo.

Botnet

- síť softwarově propojení botů (robotů), které provádí činnost na základě správce, legální síť slouží k výpočtů, nelegální ke kriminálním skutkům,
- pokud se zneužije jeden mail server, který bude odesílat desítky milionů e-mailových zpráv denně, bude tento server za velmi krátkou dobu odhalen a zablokován ISP,
- jestliže útočník využije sítě botnet bude mít k dispozice tisíce počítačů a každý z nich odešle např. (1000 až 2000 zpráv denně) nebude to vůbec nápadné a takový to provoz nebude považován za problematický a nebude zastaven,
- napadený (infikovaný) počítač se nazývá „zombie“ či „bot“ a stane se zotročeným počítačovým systémem, který bude připojen k centrálnímu řídícímu serveru „comman-and-control server“, útočník má kontrolu nad zombie a C&C
- do sítě botnet je možné zapojit i ledničku (IoT zařízení), 2014 odesláno 750 000 e-mailů, které měly povahu spamu.

Malware (https://viry.cz/)

- malicious software – škodlivý software využitý k narušení standardní činnosti počítačového systému, zisku informace, přístup k počítačovému systému
- šíření – e-mail, počítačové sítě, web, média a další
    - Adware
    - Spyware
    - Viry
    - Červi
    - Trojské koně
    - Backdoor
    - Rootkity
    - Keylogger
    - Ransomware (vyděračský malware)
- nejohroženější operační systém v rámci mobilních zařízení je OS Android, většina zařízení s OS Android neumožňuje aktualizovat operační systém. Je odhadováno, že 77 % hrozeb útočících na OS Android by bylo možné eliminovat právě používáním nejnovější verze tohoto operačního systému

Spam

- hromadné šíření veškerých nevyžádaných sdělení, hromadné šíření nevyžádaného obchodního sdělení,
- Scam (podvod švindl), spam, sociální inženýrství – získat důvěru uživatele a donutit ho vykonat požadované úkony (otevření přílohy e-mailu, navštívení zobrazeného URL)
- mezi scam patří:
    - podvodné nabídky
    - podvodná volání
    - podvodné SMS
    - Phishing (získání informace o uživateli)
        - Phishing není zaměřen pouze na e-maily. Je možné nalézt phishing v rámci instant messages (Skype, ICQ, Jabber aj.), sociálních sítí, SMS a MMS zpráv, chatovacích místností, scamu (podvodné nabídky práce, zboží aj.), falešných aplikací do prohlížeče
        - Dluh/Banka/Exekuce, Česká pošta3,Vánoce a dárky, Seznam.cz – One Time Password
        - Vishing telefonický phishing, získání citl. Údajů, VOIP
        - Smishing – SMS zprávy
            - Upozorneni – toto je automaticky vygenerovana zprava z (název lokální banky), Vase kreditni karta byla zablokovana. K reaktivaci volejte 866### ###“
    - Podvodné webové stránky (firmy)
    - Hoax (smyšlenka, žert, novinářská kachna), www.hoax.cz

Seznam prolomených účtů https://haveibeenpwned.com/

Další počteníčko:
www.viry.cz,
https://kafemlejnek.tv/dil-25-historie-malware/
https://www.nukib.cz
https://nic.cz
https://www.internetembezpecne.cz/