BESPOKE COUNSELS

ROWAN LEGAL

AKTUÁLNE OTÁZKY KYBERNETICKEJ BEZPEČNOSTI

JUDr. Martin MAISNER, PhD. , ROWAN LEGAL s.r.o.

MEMBER OF MULTILAW

KYBERNETICKÁ BEZPEČNOST

- **Čím sa líši kybernetická bezpečnosť od bezpečnosti všeobecnej ?**
- **Ilúzia v súvislosti s KB**
- **Vymedzenie hraníc KB**
  - **Teritoriálne (kyberpriestor?)**
  - **Vecné**
  - **Chránenými cieľmi**

KYBERPRIESTOR JE KEĎ....

- *„Konsenzuálna halucinácia každý deň prežívaná miliardami oprávnených operátorov všetkých národov, deťmi, ktoré sa učia základy matematiky… Grafická reprezentácia dát abstrahovaných z bánk všetkých počítačov ľudského systému. Nemysliteľná komplexnosť. Línie svetla zoradené v nepriestore mysli, zhluky a súhvezdia dát. Ako svetlá mesta …“*

William Gibson ***Neuromancer*** (1984)

ĎALŠIE DEFINÍCIE .....

- = vesmír digitálnych sietí,
- = oblasť akýchkoľvek digitálnych informácií simulovaná ako trojrozmerný priestor, ktorého pohyblivú geografiu je možné poznávať ľudskými zmyslami,
- = označenie všetkých telekomunikačných a počítačových sietí, a to predovšetkým internetu.

A EŠTE ĎALŠIE....

- = počítačový trojrozmerný svet analogický s internetom, v ktorom sa užívatelia pohybujú pomocou virtuálnej reality.

- Kyberpriestor v žiadnom prípade nie je statický. Rozrastá sa tak v počte serverov, ako aj stránok, ktorých počet sa dnes odhadom blíži k desiatim miliardám. Spontánny a neregulovateľný rast celosvetovej počítačovej siete a jej neustála premenlivosť prakticky vylučujú presné zmapovanie.

CHRÁNENÉ CIELE

- Čo má byť chránené?
- Dáta? Subjekty údajov? Majetok? Život ? Zdravie? Sloboda?
- = nerušené fungovanie systému tak, aby k informáciám, ktoré systém obsahuje, mali nerušený prístup oprávnené osoby, zatiaľ čo osoby neoprávnené nebudú mať prístup žiadny

PRINCÍPY KKB

- **Žiadny systém nie je bezpečný, pokiaľ nie sú riešené všetky hroziace riziká vo vzájomných súvislostiach**

- Teda:
  - Všetky druhy rizík
  - Všetky riešiť aktívne
  - Riešiť vo vzájomných súvislostiach

OBLASTI OCHRANY

– Personálna (kádrová) bezpečnosť
– Administratívna bezpečnosť (systematická)
– Administratívna bezpečnosť (aplikačná)
– Technologická bezpečnosť (hardware)
– Technologická bezpečnosť (software)
– Technická (živelná) bezpečnosť
– Ekonomická (finančná) bezpečnosť
– Vymáhateľnosť práva a záväzkov (zmluvná)
– Vymáhateľnosť práva (riešenie sporov)
– Evolučná (plánovacia) bezpečnosť

PERSONÁLNA BEZPEČNOSŤ

- Rozpracované systémové vedenie a subordinácia vrátane príslušnej dokumentácie a systému jeho dodržovania
- Slušný no efektívny monitoring činnosti na sieti a činnosti zamestnancov
- Profilovanie škodcu a preventívne sledovanie problémových aktivít
- Sústavná a aktívna práca s ľuďmi a ich výchova

ADMINISTRATÍVNA BEZPEČNOSŤ

- Súlad s právnymi predpismi
- Vyriešená procesná štruktúra
- Trvalá verifikácia a zlepšovanie štruktúry

TECHNOLOGICKÁ BEZPEČNOSŤ

- Akékoľvek riešenie je iba dočasné a musí počítať s vývojom
- Technológia nie je cieľom, ale prostriedkom
- Technologické aspekty sú účinné iba v súvislosti s ostatnými aspektmi bezpečnosti

VYMAHATEĽNOSŤ PRÁVA

ROWAN LEGAL

- **Kontraktačná kultúra**
  - Zmluvná stratégia a politika
  - Taktika rokovania o zmluvách a obchodnej stratégii
  - Obvyklé chyby a ich dôsledky
- **Zmluvné zabezpečenie vzťahov so zamestnancami a dodávateľmi**
  - Všetky aspekty zmluvného vzťahu musia byť vyvážené
  - Kvalitné zmluvné zabezpečenie je zárukou bezpečnosti
  - Zaistenie záväzkov v praxi
- **Riešenie sporov**
  - Princípy efektívneho riešenia sporov
  - Súdne spory
  - Alternatívne spôsoby riešenia sporu

PRINCÍP KKB

- KKB = komplexná kybernetická bezpečnosť
- Žiadny systém nie je bezpečný, pokiaľ nie sú riešené všetky hroziace riziká vo vzájomných súvislostiach
- Cieľom je zabezpečiť chod systému tak, aby plnil úlohy pre vlastníka, aby boli v ňom obsiahnuté dáta neprerušene dostupné oprávneným osobám

POČÍTAČOVÁ KRIMINALITA

- **Čo je počítačová kriminalita**
  - Neexistuje jednotná definícia
  - V podstate sa jedná o všeobecnú kriminálnu činnosť, kde podstatnú rolu zohráva IT
- **Stíhanie počítačovej kriminality**
  - Veľmi komplikované
  - Súčasný prístup veľmi problematický
  - Možné riešenia
- **Obrana a prevencia**
  - Systematický prístup
  - Každé podcenenie sa nevyplatí

POČÍTAČOVÁ KRIMINALITA

- trestné činy proti počítačom
- trestné činy páchané pomocou počítača
- zahŕňa zneužitie údajov získaných prostredníctvom výpočtovej techniky alebo ich zmenu

DRUHY POČÍTAČOVEJ KRIMINALITY

- útok na počítač, program, údaje
- neoprávnené užívanie počítača
- neoprávnený prístup k údajom
- krádež počítača, programu údajov
- zmena v programoch a údajoch
- zneužívanie počítačových prostriedkov k páchaniu inej trestnej činnosti
- podvody páchané v súvislosti s výpočtovou technikou
- šírenie poplašných správ (Hoax)

WAREZ

- = používanie, šírenie a vytváranie prostriedkov na odstránenie ochranných prvkov slúžiacich na chránenie autorských diel alebo používanie a šírenie takto upravených autorských diel, s ktorými je nakladané v rozpore s autorským právom

DRUHY WAREZU

- Aplikácie
- Cracky
- Key generators
- Games
- Movies
- Music/mp3
- E-books

PRIENIK DO SYSTÉMU (hacking)

- druhou najrozšírenejšou trestnou činnosťou
- = neoprávnené vniknutie do systému za akýmkoľvek účelom

NAJČASTEJŠIE METÓDY PRIENIKU DO SYSTÉMU

- Útok hrubou silou
- Slovníkový útok
- Odpočúvanie sieťovej komunikácie
- Využitie neukončeného spojenia
- Zadné vrátka
- Odchytenie hesla

ÚTOK HRUBOU SILOU

- metóda, ktorá spočíva vo vyskúšaní všetkých možných kombinácií znakov. Útočník zostrojí program, ktorý sa pokúša postupným vyskúšaním všetkých možností uhádnuť Vaše heslo.

- Rozlúšteniu takéhoto hesla zabránite použitím dostatočne dlhého hesla).

SLOVNÍKOVÝ ÚTOK

- Tento útok spočíva v skúšaní všetkých slov daného jazyka.
- Takémuto útoku sa dá predísť tak, že použijete heslo, ktoré nie je slovom žiadneho jazyka

ODPOČÚVANIE SIEŤOVEJ KOMUNIKÁCIE

- Odpočúvanie nezabezpečených komunikácií ako prostriedok k získaniu hesla
- Nikdy nezadávajte svoje údaje do stránky, ktorá nie je zabezpečená šifrovanou komunikáciou

VYUŽITIE NEUKONČENÉHO SPOJENIA

- Útočník môže využiť, že sa zabudnete odhlásiť zo systému. Využije otvorené spojenie, ktoré zneužije vo svoj prospech.

- Niektoré stránky sa proti takýmto útokom chránia automatickým ukončením spojenia pri nečinnosti

ZADNÉ VRÁTKA (BACKDOOR)

- Útočník zostrojí program nazývaný Backdoor (zadné vrátka), ktorý mu umožní pripojiť sa do systému bez nutnosti poznať správne používateľské meno a heslo.

- Tento program rozšíri pomocou tzv. počítačového červa alebo tzv. trójskeho koňa.

ODCHYTENIE HESLA

- Útočník zostrojí program nazývaný Key-logger, ktorý zaznamenáva stlačené klávesy a takto získané údaje mu odosiela prostredníctvom Internetu.

- Tento program rozšíri pomocou tzv. počítačového červa alebo tzv. trójskeho koňa.

POČÍTAČOVÉ BANKOVÉ KRÁDEŽE

- Phishing
- Pharming
- Spoofing
- MITM

PHISHING

- Správy, ktoré Vás pod určitou zámienkou nabádajú ku zmene osobných údajov sa odborne nazývajú Phishing (v preklade „rhybárčenie“).
- V takomto emaile je umiestnený odkaz, na ktorom si heslo máte zmeniť. Odkaz však nesmeruje na stránku banky, ale na jej dokonalú napodobeninu.

PHARMING

- Táto metóda spočíva v presmerovaní názvu www stránky na inú adresu.
- Pomerne jednoduchým spôsobom sa dá toto nastavenie zmeniť. Ak zadáte mennú adresu do Vášho prehliadača, miesto stránky banky sa zobrazí jej dokonalá napodobenina

SPOOFING

- Do tejto kategórie patria všetky metódy, ktoré používajú hackeri na zmenu totožnosti odosielaných správ.
- Jednou z týchto metód je i náhrada emailovej adresy pri phishingu, ktorá zabezpečí, aby správa vyzerala tak, že ju odoslala banka.
- Ďalšou metódou je podvrh IP adresy na stránky, ktoré takýmto spôsobom overujú totožnosť prihlasujúceho.

MITM

- (man-in-the-middle v preklade „muž v strede“).
- Táto metóda spočíva v narušení komunikácie medzi klientom a bankou, pri ktorej útočník naruší šifrovací systém verejného a súkromného kľúča, ktorý sa používa pri komunikácii

TRESTNOPRÁVNE ASPEKTY IT

- Trestné činy spáchané na škodu IT
- Trestné činy spáchané za pomoci IT
- Trestné činy vyskytujúce sa pri prevádzke IT

ĎAKUJEM ZA POZORNOSŤ

JUDr. Martin MAISNER, PhD.

ROWAN LEGAL
maisner@rowanlegal.com
+420 603 532 252