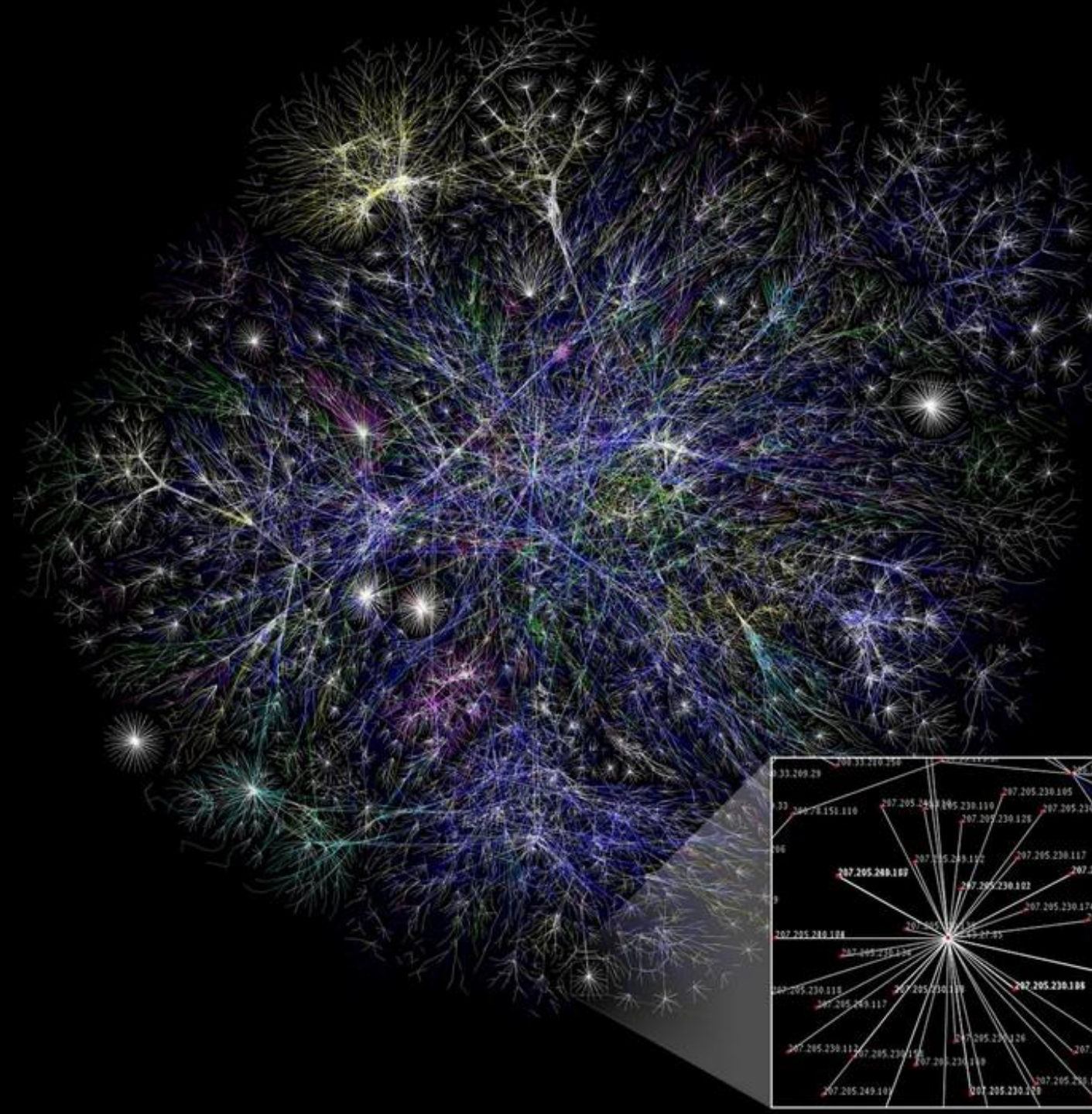
Befolyásolási technikák a digitális térben

„…nem hihetünk annak, amit vaksi szemünkkel látunk, süket fülünkkel hallunk, vagy épp tompa agyunkkal gondolunk…”
(Bacsó Péter; A Tanú)



NEMZETI TEHETSÉG PROGRAM

- **Az előadás a NEMZETI TEHETSÉG PROGRAM -** „A hazai és a határon túli felsőoktatási intézmények tehetséggondozó programjainak támogatása" címmel kiírt nyílt pályázat keretében a **„Digitális technológiák használata a közösség szolgálatában" című „NTP-FKT-20-0002"** azonosító számú pályázat keretében valósult

A pirosat vagy a kéket választod?

- „A kék visszavisz a Mátrixba. Holnap reggel felébredsz az ágyadban, és nem emlékszel semmire. Az életed megy tovább a régi, "normális" kerékvágásban. De ha a pirosat választod, az életed már soha nem lesz az, ami régen volt. Kilépsz a Mátrixból, és megismered a Valóságot!"

- a technológiai fejlődés hatására nemcsak alternatív értelmezéseit találjuk meg a valóságnak, hanem maga a valóság alternatív síkokon játszódik

- a valós tér, a kibertér, a kiterjesztett valóság tere és a virtuális valóság tere olyan hatás-kölcsönhatás mechanizmusokkal működik, amelyet egy átlagos ember nem tud ésszel felfogni

- A 21. század legfontosabb világtérképén már nem tengerek, óceánok és szárazföldek találhatóak, hanem összefüggő nagy hálózatok, amelynek minden egyes pontjában több millió kapcsolódást találhatunk. Ez az internet térképe, a korszakunk legfontosabb térképe.

- Ez a folyamatos és robbanásszerű aktivitás napjainkban 4,5 milliárd embert jelent, és a számuk napról napra növekszik, a Föld lakosságának több mint 50 %-át jelenti.

- Percenként egymillió dollárt költünk on-line, és az Amazon percenként 6659 csomagot küld.

- A Facebookot 2,6 milliárdan használják, a WhatsApp-ot és a Youtube-ot 2 milliárdan, az Instagramot több mint 1 milliárdan, a kínai WeChat alkalmazást több mint 1,2 milliárdan.

2019 This Is What Happens In An Internet Minute

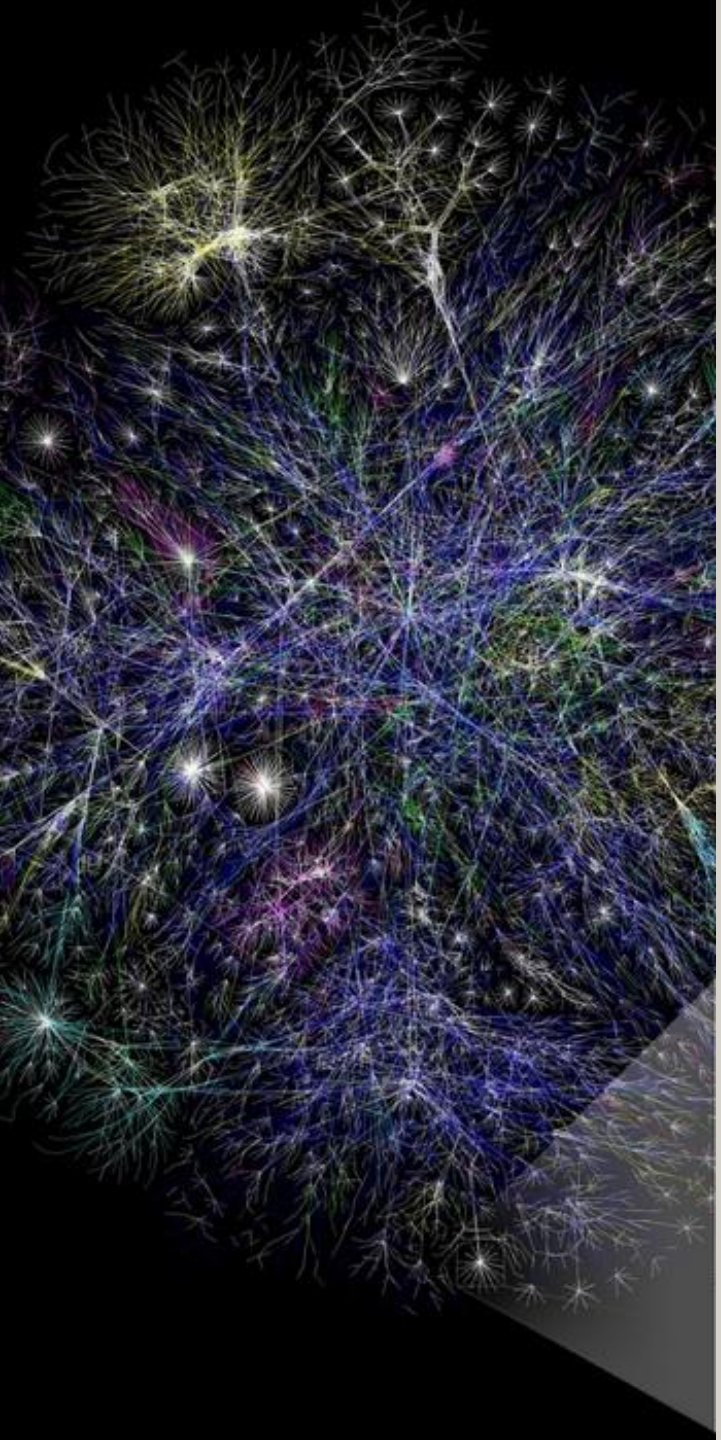
2020 This Is What Happens In An Internet Minute

Mi történik még?

Statisztikailag bizonyított, hogy a leggyakoribb internetes hazugságok a következők:

- elolvastam a “term of use oldalt”
- igen, elmúltam 18 éves

Naponta nagyjából 150 millió ilyen hazugság történik!!!



KIBERTÉR DEFINÍCIÓJA

- nem elsősorban egy technológia megnevezését értjük alatta, hanem egyfajta, négydimenziós világunkban nehezen értelmezhető térfogalmat
- 1982-ben az amerikai, William Gibson sci-fi író használta először „Izzó króm" című novellájában
- szakértők mindegyike megegyezik, hogy a kibertér a hálózatok és benne az internet, valamint a hálózathoz vezetéken vagy vezeték nélkül csatlakozó eszközök működési tartománya
- **Kibertér:** *információtechnológiai infrastruktúrák összefüggő hálózata*
- **„A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információrendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti."**
- a kibertér fel lett a fentiek által osztva
  - folyamatokra,
  - infrastruktúrákra és
  - adatokra-információkra
- Amikor a kibertérről beszélünk, akkor soha ne csak az internetre, ne csak a számítógépünkre gondoljunk. Már egyre inkább megszokott, hogy a kibertér eszközein az okostelefonjainkat is értjük, de minden más okoseszközt is értsünk ide! Az okosórák, szenzorok, okostévék stb. egyaránt a kibertér részei, egyaránt adatokat tárolnak, közvetítenek, és egyaránt figyelnünk kell rájuk!

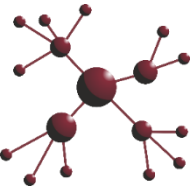
KISVILÁG

- Egy **kisvilág-tulajdonság**ú gráfban vagy hálózatban a csúcsok közötti átlagos távolság a csúcsok számához képest kicsi.

- Az elnevezés Stanley Milgram kisvilág-kísérletéből ('60-as évek) származik, ami azt vizsgálta, legkevesebb hány személyes ismeretségi kapcsolaton keresztül eljutni egy embertől egy másikig, vagyis mekkora az ismeretségi kapcsolatokat leíró szociális hálóban az átlagos távolság.

- A kis-világ tulajdonság számos fontos hálózatra jellemző, például a szociális hálókra, az Internetre vagy a génexpressziós hálózatokra.

- BARABÁSI ALBERT-LÁSZLÓ http://barabasi.com/



INTERNET

Az *internet* kifejezés nemzetközileg elterjedt szó, az angol eredetű *internetwork* szóból ered, mely magyarul leginkább 'hálózatok hálózata'-ként adható vissza, szó szerint *hálózatok közötti*-t jelent; az egész világot körülölelő számítógép-hálózat, hatalmas rendszer, amely kisebb számítógép-hálózatokat fog össze.

Az internet nem fizikai hálózat, hanem annak módja, ahogy az egymástól különböző hálózatokat összekötik, hogy egymással kommunikálni tudjanak (IP)

- Minden hálózat, amely az internethez csatlakozik, önálló életet él. Ezen hálózatok csatlakoztatásának összehangolását, az ezzel kapcsolatos információk szolgáltatását, illetve a felmerülő mérnöki tevékenységeket az 1992 januárjában létrehozott, profitmentes **Internet Society** (ISOC) irányítja, amelynek bárki szabadon tagja lehet. Központja az amerikai Virginia állambeli Restonban van.
- Az internetet felépítő és szabályozó protokollok mindenki számára hozzáférhetőek.

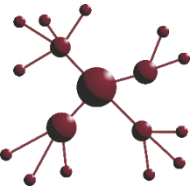
TCP/IP

- A **TCP/IP** betűszó az angol **T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol (átviteli vezérlő protokoll/internet protokoll) rövidítése, mely az internetet felépítő protokollstruktúrát takarja. Nevét két legfontosabb protokolljáról kapta, a TCP-ről és az IP-ről.

- A **TCP/IP felépítése a rétegződési elven alapul, minden egyes réteg egy jól definiált feladatot végez el, és a rétegek egymás között szolgálatelérési pontokon keresztül kommunikálnak**.

- Minden réteg csak a vele szomszédos réteggel képes kommunikálni, mivel ezek egymásra épülnek.

- Alapvetően négy réteg alkotta, melyet ötre bővítettek.

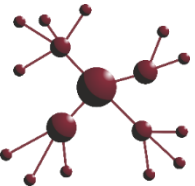


E-MAIL

- Az **e-mail** (ejtsd és „sajnos” már írd is: *ímél*) az angol *electronic mail* kifejezésből származik, a mai e-mail-rendszerek szinte kivétel nélkül az internetet használják közvetítőnek, és ezáltal az e-mail az internet használatának egyik legkedveltebb formája lett.

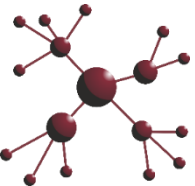
- **Az üzenetek, számítógépek között, az SMTP** (angolul: *Simple Mail Transfer Protocol*) **típusú kapcsolat segítségével kerülnek továbbításra**.

- **A felhasználók üzeneteiket POP, illetve IMAP típusú kapcsolatok segítségével töltik le a kiszolgálókról**. Nagyobb vállalati rendszereknél előfordulnak ettől eltérő típusú megoldások is, mint például **Microsoft Exchange**.



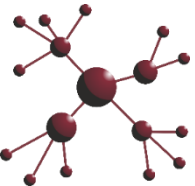
FTP

- A **File Transfer Protocol**, vagy rövid nevén **FTP** TCP/IP hálózatokon – mint amilyen az internet is – történő állományátvitelre szolgáló szabvány.
- Gyakran van szükség arra, hogy valamilyen állományt hálózaton keresztül töltsünk le saját gépünkre, vagy egy állományt mások számára hozzáférhetővé tegyünk. Erre alkalmas **az FTP, ami lehetővé teszi a különböző operációs rendszerű gépek között is az információcserét**. A világon nagy mennyiségű információforrás áll rendelkezésre, melyek letöltése ilyen módon megvalósítható.
- Azt a folyamatot, amikor egy távoli számítógépről fájlt mentünk a saját számítógépünk háttértárára, ***letöltés***nek nevezzük; ***feltöltés***nek nevezzük, ha a folyamat fordított irányban zajlik, és mi töltünk fájlt mások gépére.
- Az **FTP kapcsolat ügyfél/kiszolgáló alapú**, vagyis szükség van egy kiszolgáló- (=szerver) és egy ügyfélprogramra (=kliens). Elterjedt protokoll, a legtöbb modern operációs rendszerhez létezik FTP-szerver és kliens program, sok webböngésző is képes FTP-kliensként működni.



WWW

- A **világháló** (angol eredetiben *World Wide Web, WWW* vagy röviden *Web)* **az interneten működő, egymással úgynevezett hiperlinkekkel összekötött dokumentumok rendszere**.
- A rendszert webböngésző program segítségével lehet elérni. Ez a program képes megjeleníteni az egyes dokumentumokat, „weblapokat”.
- A felhasználó a lapokon található hiperlinkek segítségével további lapokat kérhet le, amelyeken újabb hiperlinkek lehetnek. A rendszer „háló”-jellegét is ez adja; a dokumentumok a háló csomópontjai, míg a hiperlinkek a háló szálai, amelyeken keresztül egy vagy több lépésben tetszőleges csomóponthoz eljuthatunk.
- A Világháló három szabványra épül:
- A ***Uniform Resource Locator*** (URL), leírja, milyen egyedi „címmel” kell rendelkeznie az egyes oldalaknak;
- A ***hipertext átviteli protokoll*** *(Hyper Text Transfer Protocol,* HTTP), megadja, hogyan küld egymásnak információt a böngésző és a kiszolgáló,
- ***hipertext leíró nyelv*** *(Hyper Text Markup Language,* HTML), az információkódolás eljárása, mellyel az oldal sokféle eszközön megjeleníthetővé válik.



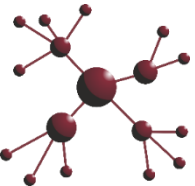
clearweb – deepweb – darkweb

- A **publikusan, bárki számára elérhető szolgáltatások és weboldalak tartoznak a ClearWeb**, vagy más néven a SurfaceWeb kategóriába. Általában az olyan forrásokra használják a megnevezést, amelyeket a különféle keresők képesek indexelni, így kereshetők és általánosságban véve hozzáférhetők. A ClearWeb mérete becsülhető a Google és a Bing (a két legnagyobb keresőrendszer) indexelési statisztikáinak alapján. Jelenleg (2020 márciusi adatok alapján https://www.worldwidewebsize.com) kb. 67 milliárd különböző weboldalt indexel együttesen a két kereső.

- **Deepweb: a keresők által nem indexelt oldalak**; egy tanulmány szerint (Bergman 2001) 550X nagyobb mint a clearweb

- Maga a dark web kifejezés a Time magazin Cybersecurity (kiberbiztonság) különszámával került be a hétköznapi szóhasználatba 2018-ban, de legalább 2009 óta használjuk. A DarkNet méretéről nem állnak rendelkezésre pontos adatok. **A DarkNet egy adatréteg, amely a TOR hálózatra épül, de a TOR hálózat nem maga a DarkNet.** A TOR hálózatot az 1990-es években az amerikai haditengerészet kutatólaboratóriumában kezdték fejleszteni, mára a TOR Project nevű szervezet irányítja és koordinálja a fejlesztést. A TOR hálózat jellemzője, hogy csak speciális kliensprogrammal vehető igénybe, erős titkosítás mellett működik, és anonimitást garantál (amennyire ez lehetséges egyáltalán). A TOR hálózat méretéről közel pontos adatok állnak rendelkezésre. Egy ötéves periódust vizsgálva látható, hogy 2017-ben volt a legtöbb, csak a TOR hálózaton elérhető weboldal vagy szolgáltatás, de a több mint 120 ezer oldal elhanyagolható a ClearWeb méretéhez képest. A Tor böngésző, azon túl, hogy lehetőséget ad az internet sötét oldalán való szörfölésre, még anonimitást is garantál

- A „dead drop" eljárást a kémek és hírszerzők használták (használják) olyan esetekben, amikor valamilyen csomagot kell átadni. A módszer előnye, hogy teljesen aszinkron, azaz az értékesítő (vagy közvetítő) és a vásárló nem tartózkodik egy időben az átadási ponton, nem lehet a csomagokat követni vagy feltartóztatni, a vásárlónak nem kell kontakt vagy más személyes adatot megadnia a kézbesítéshez (pl. cím, postafiók stb.), így a kereskedőnek nem is kell ezeket az adatokat tárolnia és megvédenie, nem tudnak egymásra vagy egymás ellen vallani rejtekhelyként használható helyek száma – a rendvédelem megfigyelési kapacitásával szemben – gyakorlatilag végtelen



- Kis túlzással, *a DarkNeten 2019-ben jellemzően már álcázott FBI-ügynökök adnak el kokaint a beépült DEA-ügynököknek, akik a fedett CIA-ügynököktől vásárolt hamis pénzzel fizetnek érte.*

Decentralizált hálózatok

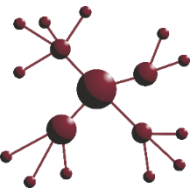
- Bár gyakran a DarkNet/DarkWeb (vagy Sötét Web) kategóriába sorolják őket, például a ZeroNethez vagy FreeNethez hasonló peer-to-peer alapú decentralizációs hálózatok alapvetően nem tartoznak a fent említett kategóriába.

- A ZeroNet hálózat decentralizált működése a tartalommegosztás szempontjából azt jelenti, hogy nincs egyetlen központi szerver, amely tárolná és megosztaná a tartalmakat.

- Amikor valaki meglátogat egy ZeroNet-oldalt, azzal letölti magát a tartalmat és a weboldalt a saját eszközére, más látogatók pedig akár már az ő eszközéről fogják letölteni a tartalmat magukhoz, és onnan kiszolgálni más látogatókat. Mivel a meglátogatott oldal letöltődik a látogató eszközére, a tartalom böngészése is onnan valósul meg, azaz a látogató a saját gépére másolódott tartalmat fogja elérni.

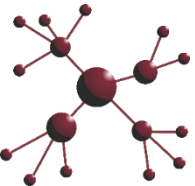
- A decentralizált működés miatt egy tartalom teljes eltávolításához minden eszközről – amely meglátogatta az eredeti oldalt – törölni kellene a tartalmat, erre pedig nincsen lehetőség.

- A ZeroNet és a hasonló *peer-to-peer* hálózatok felhasználói élmény szempontjából hasonlatosságokat mutatnak a DarkNet/TOR használati élményével. Mindkettő eléréséhez külön kliens szükséges, és a hagyományos ClearWebhez képest kényelmetlenebb a használatuk, az általános felhasználói tudáshoz képest jóval több szakismeret szükséges a használatukhoz



A KIBERTÉREN TÖRTÉNŐ VISSZAÉLÉSEK CÉLJAI ÉS MÓDJAI

- Alapvetően érdemes megkülönböztetnünk azt, hogy a visszaélés személy ellen történik, vagy valamilyen szervezet rendszere ellen
- 1. az információs rendszer működésének zavarása,
- 2. adat megszerzésére irányuló támadás,
- 3. adat módosítására irányuló támadás.
- Ezek tehát az adat, információ úgynevezett rendelkezésére állását (1.), bizalmasságát (2.) és sértetlenségét (3.) fenyegetik. Ezek a fogalmak azért is fontosak, mert a hatályos magyar jogszabályozás is nevesíti őket
- Az információs visszaélések számos formáját ismerjük. Ezeket két csoportba tudjuk sorolni attól függően, hogy emberi tényezők által következnek be, vagy valamilyen informatikai rést használnak ki:
- 1. valamilyen rosszindulatú szoftverrel (malware) előidézett információs visszaélés,
- 2. social engineering módszerrel előidézett információs visszaélés (humán és nem humán eredetű visszaélések), korrupció.

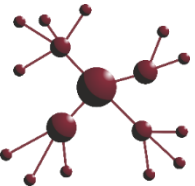


Biztonsági követelmények

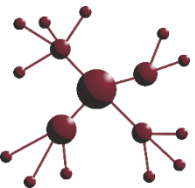
- **bizalmasság** (confidentiality): röviden annyit jelent, hogy valamit csak az arra jogosultak ismerhetnek meg, korlátozott a megismerése jogosultak köre; vagy ahogyan az Infotörvény fogalmazza meg – az elektronikus információs rendszer azon tulajdonsága, hogy a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról.

- **sértetlenség, vagy integritás** (integrity): röviden úgy mondanánk, hogy valami az eredeti állapotának megfelel és teljes. Az Infotörvény értelmezésében az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát (letagadhatatlanságát) is, illetve az elektronikus információs rendszer elemeinek azon tulajdonságát, amely arra vonatkozik, hogy az elektronikus információs rendszer eleme rendeltetésének megfelelően használható;

- **rendelkezésre állás** (availability): lényegében annyit jelent, hogy a szükséges infrastruktúrák valamint adatok ott és akkor állnak a felhasználó rendelkezésére, amikor arra szükség van, vagy ahogyan az Infotörvény fogalmazza meg, annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek.

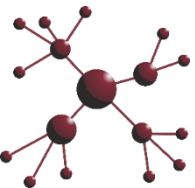


„…a legnagyobb biztonsági kockázat a szék és a billentyűzet között található…”



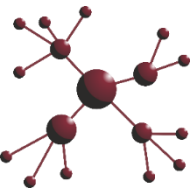
Social engineering

- A social engineering fogalomnak napjainkban nincs igazán jó magyar megfelelője.
- Kevin David Mitnick, a „legendás hacker” az alábbiak szerint fogalmazott: „A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.”
- érdemes elkülöníteni a számítógépes eszközzel és az anélkül lefolytatott social engineering módszereket



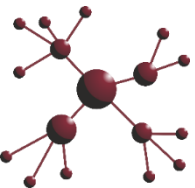
Social engineering

- A social engineering módszerek a kihasználható emberi tulajdonságokra épülnek.
- Ezeket a következőképpen tudjuk kategorizálni:
  - személyes tulajdonságok,
  - munkahelyi tulajdonságok,
  - pillanatnyi tulajdonságok,
  - stresszhelyzet okozta tulajdonságok.
-



Social engineering - Információszerzésre alkalmas social engineering technikák

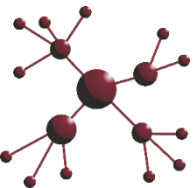
- kártékony programok,
- adathalaszat,
- WiFi sebezhetőségei,
- közösségi platformok általi információ gyűjtés



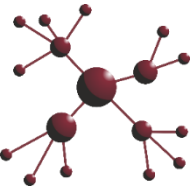
MALWARE

```
:(){ :|:& };:
```

- vírus (virus)
- féreg (worm)
- követő „sütik” (tracking cookies)
- logikai bomba (logic bomb)
- trójai faló, trójai program (trojan horse)
- hátsó ajtó vagy csapóajtó (backdoor/trapdoor)
- billentyűzetfigyelők (keylogger)
- zsaroló programok (ransomware)
- átverés, álhír, kacsa (magyarban is használatos: hoax)
- levélszemét (spam)
- szolgáltatásmegtagadással járó támadások (DoS – Denial of Service és DDoS – Distributed…)
- APT (Advanced persistent threat)

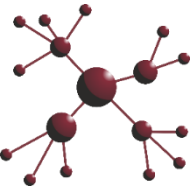


…a támadónak nem „X.Y.” számítógépére van általában szüksége, hanem „millió gépre, köztük „X.Y.” számítógépére is…



Social engineering

- A humán alapú social engineering módszerek, amelyekhez közvetlen, személyes kontaktus szükséges a támadó és áldozata között, a következők:
  - • segítség kérése: a támadó segítséget kér, a célpont pedig szívesen segít;
  - • segítség nyújtása: általában a támadó teremt egy helyzetet, amikor felajánlhatja segítségét a célpontnak, így nyerve el bizalmát, és információkat szerez meg tőle;
  - • kölcsönösség kihasználása: a támadó korábban megtett valami az áldozatnak, most azt kéri vissza;
  - • megszemélyesítés: a támadás során a támadó egy hitelesített személynek (biztonsági cég alkalmazottja, vízszerelő) adja ki magát, így szerez meg bizalmas információkat;
  - • shoulder surfing – képernyő lelesése: a célpont válla fölött a támadó a mobilra, monitorra kukucskál;
  - • tailgating: bejutás a bejáraton más embert követve, annak tudtán kívül;
  - • piggybacking: bejutás a bejáraton más embert követve, annak tudtával;
  - • dumpster diving: információk felkutatása a hulladékban.
- Klasszikusan nem szokás a social engineering módszerek közé sorolni (mivel a célpont ekkor nem marad ártatlan), de tényezőit vizsgálva mégis ideérthetjük a korrupciót



Social engineering

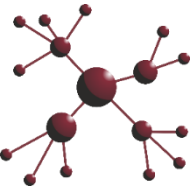
- A támadás felépítése a támadó részéről a következő négy lépcsőből áll:

- 1. Információszerzés: minőségi és mennyiségi információ szükséges ahhoz, hogy a támadó behatárolja a megfelelő embereket mint potenciális célpontokat. Általában a vállalati, szervezeti weboldalakról, közösségi portálokról, netes keresőkről könnyen meg lehet szerezni a szükséges információkat, ha mégsem, telefonon is érdeklődhet („XY vagyok a humánosztályról, szeretném kérni az informatikai vezetőt, mert főnököm ZX megkért...”), de történhet levélben, e-mailben, akár személyesen is vagy a szemetesből.

- 2. Kapcsolat kiépítése: ez lehet rövid távú, egyszeri segítségkérés például, de egy pszichopata elkövető akár arra is vetemedhet, hogy a célszeméllyel hónapokig tartó jó barátságot, vagy még többet alakít ki, hogy bizonyos adatokat meg tudjon szerezni, vagy be tudjon jutni valamilyen helyre.

- 3. Kapcsolat kihasználása: a kiépült kapcsolat révén alkalmat szerez, hogy a tervet végrehajtsa.

- 4. Támadás végrehajtása: a kapcsolat kihasználása révén például távoli hozzáférést szerez az elkövető bizonyos szerverekhez, számítógépekhez, eljött hát az aratás ideje.



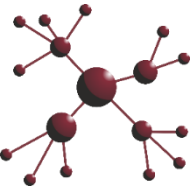
Social engineering - adathalászat

- A phishing, vagyis az adathalászat (az angol fishing szóból ered) a számítógépalapú Social Engineering módszerek egyik válfaja.

- Két fő típusa van célpontok szerint: az általános és a célzott adathalászat.

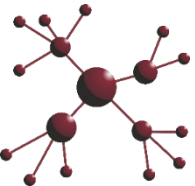
- Az általános esetén az elkövető nem konkrét természetes és jogi személyeket céloz, hanem minél több célpontot próbál meg elérni, míg a célzott esetén célzottan egy intézmény, intézménycsoport vagy szektor ellen irányul. A támadó célja, hogy a felhasználót megtévesztve felhasználói vagy személyes adatot szerezzen, vagy bármilyen más nem nyilvános információt megismerjen.

- Lényege abban rejlik, hogy az adathalaszok a felhasználókat, valamilyen elektronikus csatornán keresztül, – például e-mailben, azonnali üzenetben, vagy éppen szalagcím hirdetésekben – egy látszólag teljesen eredeti, valójában pedig egy hamis weboldalra irányítják, ahol arra kérik, hogy adja meg bizalmas adatait



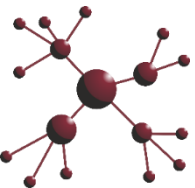
Social engineering - a WiFi sebezhetőségeinek kihasználása

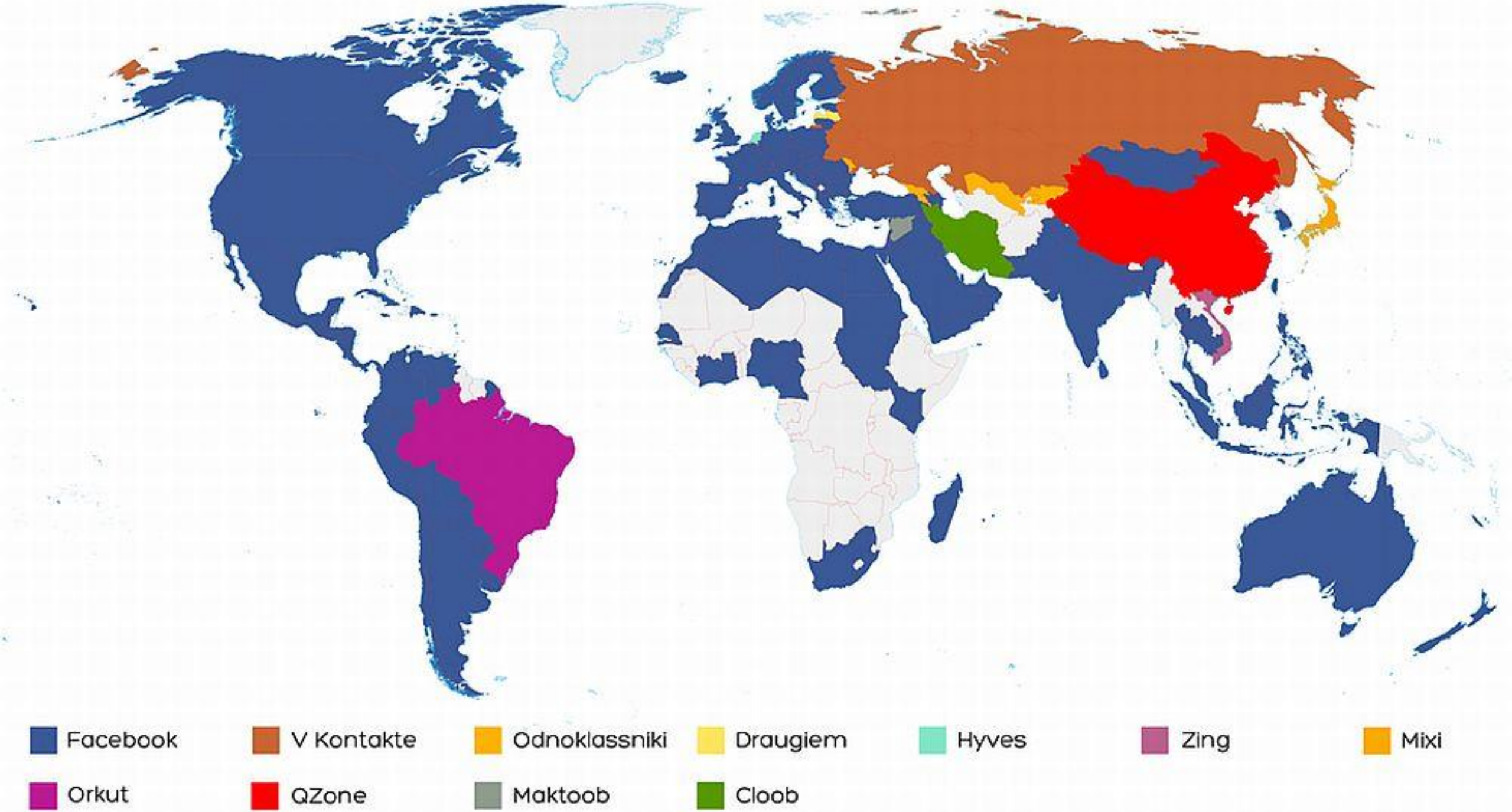
- A WiFi-hálózat gyengeségeinek kihasználása nemcsak a rosszindulatú szoftverek terjesztésére alkalmas, hanem további információk megszerzésére is. Ez megvalósítható többek között úgy, hogy azzal tévesztik meg a célszemélyt, hogy egy az eredetivel szinte teljesen megegyező, nagy jelerősségű hálózatot hoznak létre, ezáltal a felhasználó nem biztos, hogy meg tudja különböztetni a két hálózat közötti különbséget, igy automatikusan a nagyobb jelerősségű hotspothoz fog kapcsolódni a kényelmesebb internet elérés érdekében.
- Amint a gyanútlan felhasználó rácsatlakozik erre a csatlakozási pontra, már könnyeden megfigyelhetők és naplózhatók az általa küldött és fogadott adatok. Ez nemcsak azért rendkívül veszélyes, mert ennek segitsegevel számtalan bizalmas információ megszerezhető, hanem azert is, mert tökéletes alapként szolgálhat a profilozáshoz is.
- man in the middle támadás: a módszer lényege, hogy a támadó annak érdekében, hogy elfoghassa, lehallgathassa, esetleg módosíthassa a célszemélyek közötti kommunikációt, megszakítja vagy átirányítja, majd beékeli magát a kommunikációs csatornába, és mindkét fél irányába azt mutatja, hogy ő a másik fél, vele kommunikálnak

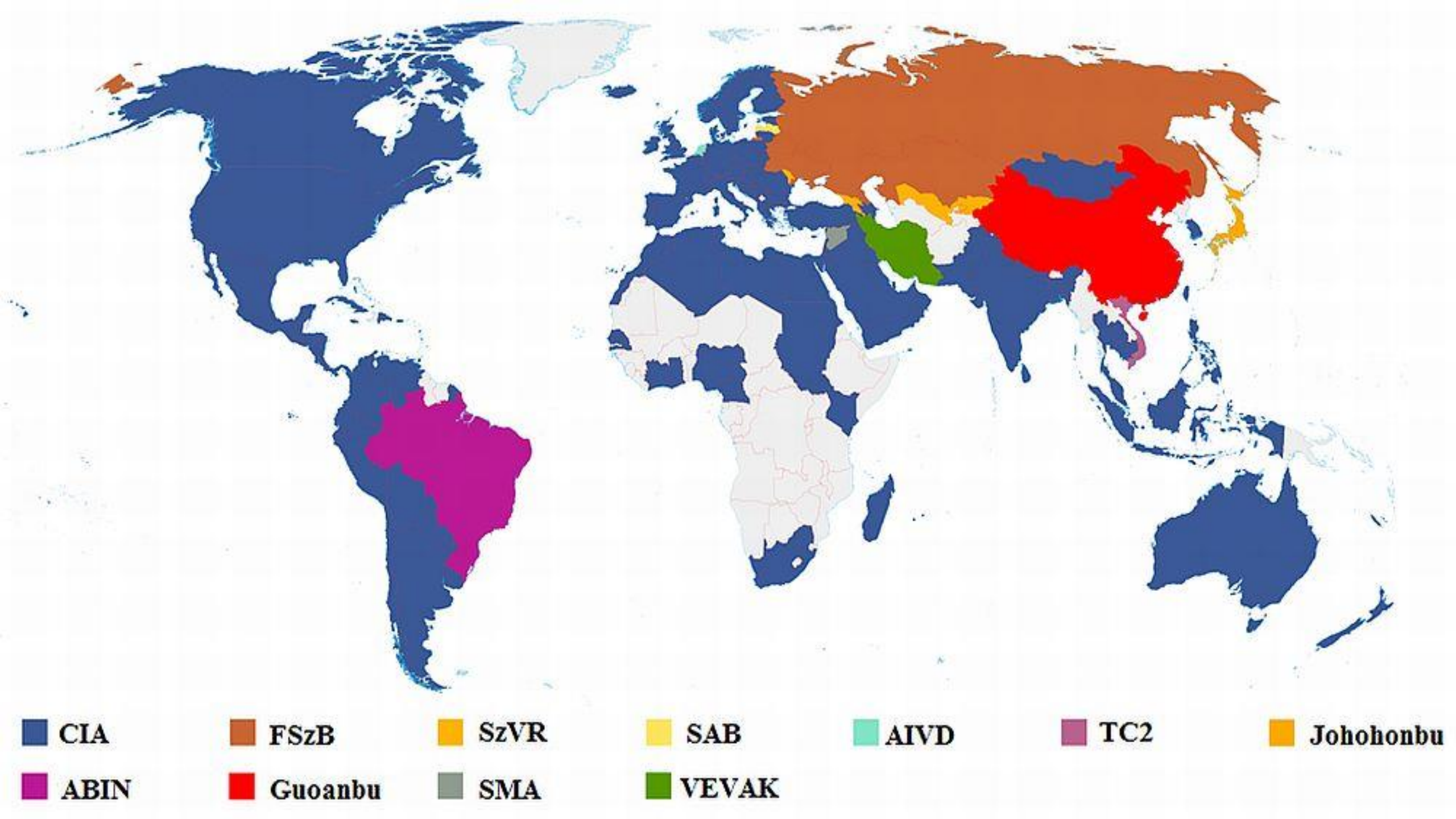


Social engineering – közösségi platformok általi információgyűjtés

- kis költséggel nagy mennyiségű információ szerezhető meg.
- a támadó nemcsak a célszemély személyes adatait és elérhetőségeit (e-mail cím, esetleg telefonszám, lakhely), hanem számos egyéb információt is megszerezhet.
- gyakran posztolnak a családtagjaikról, kedvenc háziállatukról, amelyek akár az áldozat jelszavára is utalhatnak




Facebook
V Kontakte
Odnoklassniki
Draugiem
Hyves
Zing
Mixi
Orkut
QZone
Maktoob
Cloob


CIA
FSzB
SzVR
SAB
AIVD
TC2
Johohonbu
ABIN
Guoanbu
SMA
VEVAK

„Amikor feltölt vagy valamilyen más módon elküld tartalmakat a Szolgáltatásainkba, világszerte érvényes engedélyt ad a Google-nak (és a Google-lal együttműködőknek) az ilyen tartalmak felhasználására, hosztolására, tárolására, reprodukálására, módosítására, származékos művek létrehozására […], megosztására, közzétételére, nyilvános előadására, nyilvános megjelenítésére és terjesztésére.”

google.com/dashboard

Mit tegyünk?

- A NIST keretirányelvei nevesítik az információs visszaélésekkel kapcsolatos teendőket, ezek a következők:

- • Azonosítás: az a lépés, melyben kijelölik azokat az adatokat és infrastruktúraelemeket, amelyek védelme a működés szempontjából szükséges.

- • Védelem: azon szabályok és tevékenységek összessége, amelyek segítségével az előző lépésben azonosított adatok védelme biztosítható.

- • Felismerés: a rendszert ért támadás felismerésének folyamata. Ez nem kizárólag véletlenszerűen történik, előre definiált folyamatokkal és adminisztratív intézkedésekkel az esetlegesen még passzív támadások is felismerhetők.

- • Reagálás: egy kiberbiztonsági eseményre megfelelő intézkedések és tevékenységek végrehajtása, válaszul az észlelt biztonsági incidensre. A folyamatban többnyire adminisztratív intézkedések végrehajtásáról beszélünk, de ez a szükséges műszaki eszközök és technológiák nélkül nem hatékony.

- • Helyreállítás: az a tevékenység, melynek segítségével a szervezet információs rendszerének normál működése egy incidens után vagy alatt visszaállítható. A helyreállítás a vonatkozó terv alapján történik.

Mit tegyünk?

- A 3 Vonalas Védelmi modell (Three Lines of Defense Model) az Belső Auditorok Intézete (IIA- Institute of Internal Auditors) által készített kiberbiztonsági ajánlás. Célja, hogy a biztonsági feladatokat, feladatköröket elhelyezze a menedzsment szintjein.

- Az ITIL (Information Technology Infrastructure Library – informatikai infrastruktúra könyvtár) átfogó módszertan és ajánlásgyűjtemény informatikai rendszerek üzemeltetésére és fejlesztésére.

- Az ISACA által készített COBIT (Control Objectives for Information and Related Technologies) az üzleti folyamatokra, valamint az ezeket támogató informatikai megoldások négy területére – tervezés és szervezés; beszerzés és üzembe állítás; informatikai szolgáltatás és támogatás; felügyelet – helyezi a fő hangsúlyt, és elsősorban nagyvállalatok informatikai megoldásainak támogatására készült.

- AZ IBIR a vállalatirányítási rendszer azon része, amely átfogja és szabályozza a teljes informatikai tevékenységet, kiemelten kezelve az adatbiztonsági és adatvédelmi területeket. Segítségével a vállalat működésének kockázatelemzésén és kockázatkezelésén keresztül kialakítható a magas szintű információvédelem.

- Magyarországon a legrelevánsabb jogszabályi megfelelés az Ibtv. – Az állami és önkormányzati szervek elektronikus információs rendszerek biztonságáról szóló 2013. évi L. törvény. Alapvetően a NIST által publikált kontrolljegyzék alapján dolgozták ki.

- A GDPR olyan összehangolt adatvédelmi jogszabályt jelent az uniós tagországoknak, amelynek alapvető célja az uniós polgárok személyes és magán adatainak védelme.

Mit tegyünk?

- **a biztonságnak mindig kockázatarányosnak kell lennie**