

INFORMATIKAI BIZTONSÁG ALAPJAI

8. előadás

Göcs László

főiskolai tanársegéd

Neumann János Egyetem GAMF Műszaki és Informatikai Kar

Informatika Tanszék

Az emberi tényező az IT biztonságban



Az ember szerepe az IT biztonságban

Az információbiztonság sokszor **elfelejtett tényezője** az ember, vagyis a

- vállalat munkatársai,
- partnereinek alkalmazottjai,
- beszállítói,
- ügyfelei,
- egyéb látogatói.

Az ember szerepe az IT biztonságban

A védendő értékre **közvetlen hatással van**, hiszen a vállalat alkalmazottjai

- kezelik a számítógépeket,
- futtatják a programokat és
- dolgoznak a cég adataival.

Az ember szerepe az IT biztonságban

Az informatikai jellegű meghibásodások, károk oka majdnem 60%-ban valamilyen **emberi mulasztás** következménye.

Gyakori veszélyforrás az **emberi hanyagság**, a munkatársak figyelmetlensége.

A felhasználók nincsenek tisztában azzal, hogy az őrizetlenül hagyott vagy **nem megfelelően kezelt** hardver eszközök, adathordozók mekkora veszélyt is jelenthetnek információbiztonsági szempontból.

Az ember szerepe az IT biztonságban

- Számítógép
 - Távollétükben jelszó nélküli adathozzáférés
 - Laptop eltulajdonítása, szervizbe adása
- Hordozható adattárolók elvesztése
 - Pendrive, memóriakártya
 - Mobiltelefon
 - CD/DVD lemez
- Eszközök leselejtezése, adatok megsemmisítése
 - Szoftveres törlés
 - Hardveres megsemmisítés

Kihasználható emberi tulajdonság

- **Segítőkézség**

Az emberek legtöbbször **szívesen segít** az arra rászorulóknak, különösen ha az egy munkatársnak tűnik.

- **Hiszékenységgel, naivsággal**

A munkatársak segítenek egy támadónak, mert naivan elhiszik, hogy **tényleg bajban van**, de nyugodt szívvel rendelkezésre bocsátanak bizalmas információkat olyan illetéktelen személyeknek, akik valódi munkatársnak tűnnek, holott lehet, csak ismerik az adott területen használt szakzsargont.

Kihasználható emberi tulajdonság

- **Befolyásolhatóság**

Meggyőzés, megvesztegetés, vagy akár megfélemlítés is. A munkatársak befolyásolhatóságának sikerességéhez több tényező is hozzájárulhat, ezért mindig célszerű figyelmet fordítani a kiszemelt alkalmazott **munkahelyi körülményeire, életszínvonalára.**

- **Bosszúállás**

A támadók legtöbbje **belülről**, a cég munkatársai közül, vagy legalábbis a segítségükkel kerül ki. Ha az alkalmazott már különösen **negatív érzéseket** táplál munkahelye iránt, vagy esetleg éppen önként távozik vagy elbocsátják, akkor a befolyásolhatóságon túl felmerülhet a bosszúállás lehetősége is.

„Az amatőrök a rendszereket hackelik, a profik az embereket.”

Social Engineering



Pszichológiai manipuláció

Amikor egy **jogosultsággal rendelkező** felhasználó **jogosulatlan** személy számára bizalmas adatokat ad át, vagy lehetőséget biztosít a rendszerbe történő belépésre a másik személy **megtévesztő viselkedése** miatt.

Informatikai rendszerek biztonsága ellen indított támadások.

Social Engineering

Az emberi természet két aspektusát igyekeznek kihasználni:

- a legtöbb ember **segítőkész** és igyekszik segíteni azoknak, akik segítséget kérnek.
- az emberek általában **konfliktuskerülők**.

Social Engineering

Ha egy hacker be kíván törni egy informatikai rendszerbe, vagy egy programot akar feltörni, hibából fakadó **sebezhetőségeket** kell keresnie (pl. forráskód).

Ha az efféle hibáktól mentes az adott szoftver, más utakon kell elindulnia.

További információkat kell szereznie a rendszerrel kapcsolatban.

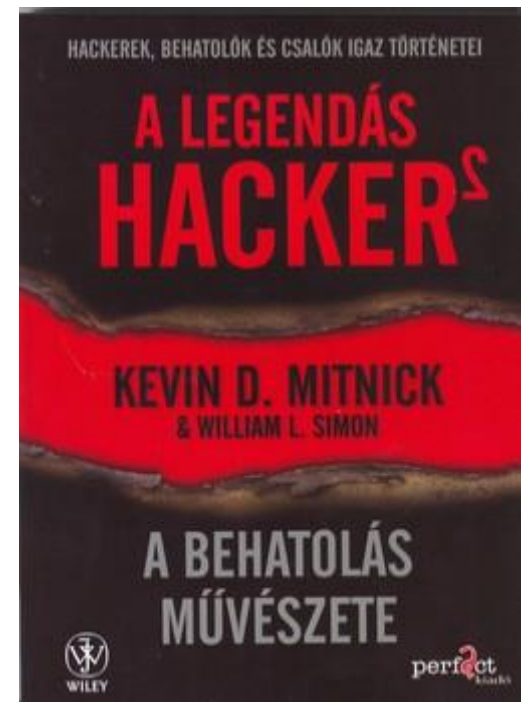
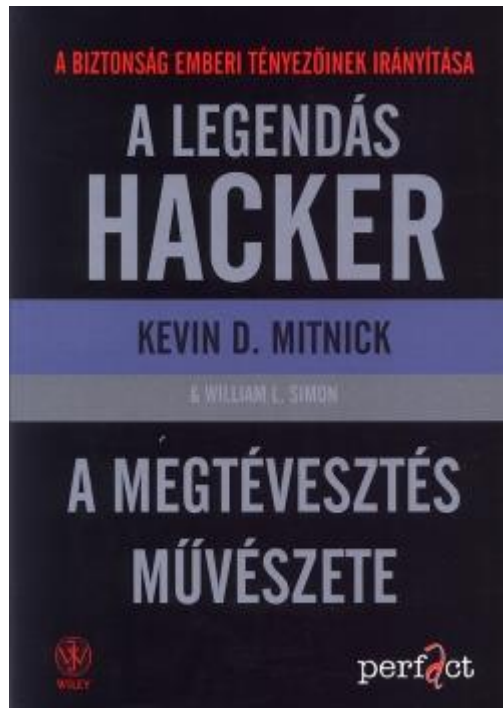
A biztonsági rendszerek mindenkori leggyengébb láncszemére, magára az **emberi tényezőre** összpontosít.

Egy social engineernek tudnia kell

- álcázni magát,
- hamis indentitással mutatkozni,
- raffinált technikákkal sarokba szorítani a kiszemelt áldozatot **információszerzés** szempontjából,
- egyszóval tudnia kell hazudni.

Social Engineering

Kevin David Mitnick



Social Engineering

„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.”

(Kevin D. Mitnick – A megtévesztés művészete, borító)

Humán alapú social engineering

- **Segítség kérése**

- HelpDesk átverése
- Új alkalmazott megszemélyesítése
- HelpDesk kér segítséget
- Piggybacing – más jogosultságának a használata (open wifi)

- **Segítség nyújtása**

- hibát generál, majd az illetékeseket megelőzve tűnik fel a megoldást jelentő
- szakember szerepében.

Humán alapú social engineering

- **Valamit valamiért**

- A social engineer azt próbálja elérni, hogy az áldozat tegyen meg neki valamilyen szívességet, jellemzően mondjon meg neki valamilyen felhasználható információt egy későbbi támadáshoz.

- **Fontos ember megszemélyesítése**

- A támadó a főnököt megszemélyesítve garantáltan megkap minden kért információt.

- **Felhatalmazás**

- Ha a támadó a főnököt nem tudja megszemélyesíteni, mert például a kieszemelt kolléga ismeri valamennyire.

Humán alapú social engineering

- **Reverse Social Engineering**

- a social engineer olyan kérdéseket tett fel magának, amelyekben benne vannak a számára szükséges információk.

- **Dumpster Diving – kukaátvizsgálás**

- Szemetesbe kerülhetnek a monitorról leszedett jelszavas cetlik, másrészt az alkalmazott olyan személyes adatai, amelyek segítséget nyújthatnak az illető személyazonosságának felvételéhez.

Humán alapú social engineering

- **Shoulder Surfing – „váll szörf”**
 - valamilyen módon az áldozat közelébe kell férkőzni, ami történhet konkrét céllal, úgy hogy nem kell semmi hazugságot kitalálni (például ügyfélként) vagy valamilyen más social engineering módszerrel kombinálva valaki mást megszemélyesítve.
- **Tailgating – szoros követés**
 - támadó úgy tesz, mintha egy vendég- vagy munkás csoport tagja lenne, majd hozzájuk csapódva egyszerűen besurran az épületbe és ott szabadon járkálva kutathat az információk után.

Számítógép alapú social engineering

- **Ál weboldalak**
 - Regisztráció ellenében kínálunk valamilyen ingyenes tartalmat, vagy sorsolunk ki valamilyen nyereményt. A felhasználók legtöbbször ugyanis több helyen is ugyanazt a karaktersorozatot használja, vagy valamilyen nagyon hasonlatosat.

1. figyelem felkeltés, megtévesztés

2. Az adatlopás felülete – egy álweboldal

facebook [Regisztráció](#)

Facebook-belépés

Ki lettél léptetve, kérjük jelentkezz be újra!

Az általad megtekintett hivatkozás nem biztonságos ezért rendszerünk automatikusan kiléptetett.

Elfelejtetted a jelszavadat? [Új jelszó igénylése.](#)

E-mail vagy telefon:

Jelszó:

☐ Bejelentkezve maradok

[Bejelentkezés](#) vagy [Regisztrálj a Facebookra!](#)

[Elfelejtetted a jelszavadat?](#)

Magyar English (US) Deutsch Français (France) Italiano Русский Español Română Português (Brasil) العربية ...

Regisztráció

Játékok

Felkérlek

Bejelentkezés

Helyek

Súgó

Messenger

Rólunk

Facebook Lite

Hirdetés létrehozása

Mobil

Oldal létrehozása

Ismerősök keresése

Fejlesztők

Névjegyek

Álláslehetőség

Emberek

Adatvédelem

Oldalak

Sútk

Helyek

AdChoices

Facebook © 2015
Magyar

Számítógép alapú social engineering


- **Phishing – adathalászat**

- Smishing - pénzügyetnél az utalás elengedhetetlen feltétele az SMS-ben érkező jelszó begépelése.
- Hamis bannerek, reklámok
- Hamis e-mailek és weboldalak

- **Pharming**

Nem a felhasználót, hanem a DNS-szerverek sebezhetőségeit és a böngészőprogramok befoltozatlan biztonsági réseit kihasználva az adott weboldal tényleges címét módosítják az alábbi módszerek valamelyikével.


Adathalászat felhívás



OTPdirekt internetbank
Belépés az internetbankba.
Számkezelés a nap 24 órájában

Mi az OTPdirekt?
Minden OTPdirekt szolgáltatás
egy helyen: ismerje meg őket!

Internetbank demó
Ha még nem ügyfelünk, itt
kipróbálhatja szolgáltatásunkat.



Adathalász kísérlet (2017.03.20.)


Egy, az interneten terjedő adathalász (phishing) levélben ismeretlenek az OTP Bankra hivatkozva próbálnak meg személyes, internetbanki belépéshez szükséges adatokat kicsalni ügyfeleinktől. Felhívjuk figyelmüket, hogy **a levél hamis** és a levélben található hivatkozásra kattintva egy **adathalász** oldalra jutnak.

[További részletek](#)

Belépés

Belépés saját azonosítóval

OTPdirekt belépés



Azonosító

Azonosító

Számla 117

Számlaszám

Jelszó

Jelszó

☐ Tranzakciónkénti azonosítás


☐ Azonosító, számlaszám megjegyzés

Belépés →

→ [Először használná?](#)

→ [Teendők elfelejtett jelszó esetén](#)


OTP SmartBank




Az OTP SmartBankkal
kényelmesen elérheti
internetbankunk fő funkcióit, sőt,
többet is!

Töltse le most és próbálja ki,
szeretni fogja!

Available on the
App Store

Google play

Windows Store

Az alkalmazás megújult külsővel, egyszerű PIN
kódos belépéssel és további új, hasznos
funkciókkal bővült.

Megnézem →

BIZTONSÁGOS BÖNGÉSZÉS

- HTTPS:// böngészés

  OTP Bank Nyrt. (HU) | <https://www.otpbank.hu/portal/hu/fooldal>


  | <https://netbank.erstebank.hu/erste-netbank-eloszto/erste-ne>

  | <https://accounts.google.com/ServiceLogin?service=mail&contin>

  | <https://www.facebook.com>

Kétfaktoros autentikáció

1. Azonosító + Jelszó

OTPdirekt belépés 

Azonosító

Számla 117

Jelszó

☐ Tranzakciónkénti azonosítás

☐ Azonosító, számlaszám megjegyzés


Belépés 

2. SMS

Kérjük, adja meg az alábbi adatokat!

SMS-ben kapott azonosító

Tovább

Sign in 

Email

Password

Sign in

☐ Stay signed in


[Can't access your account?](#)

Enter the verification code sent to your phone number ending in **65**.

Enter code:

Verify

☐ **Trust this computer**
We won't ask you for a code again when we recognize one of your trusted computers. [Learn more](#)



Elektronikus levelezés veszélyei

- Kéretlen levelek, reklámok
- Megtévesztő információk
- Adatkérés -> adatlopás
- Veszélyes mellékletek (vírus, kémprogram)

Kéretlen levél /spam/ - Kéretlen levél minden olyan elektronikus levél, amelyet a címzett nem kért. Leggyakoribb előfordulási formája a kéretlen reklám. Az ilyen küldemény gyakran még kéretlen betolakodót (vírust) is hordoz. A levél feladója, tárgya és szövege olyan gyakran változik, hogy ezen **levelek szűrése, egyszerű minta alapján nem lehetséges.**

Beugrató levél /hoax/ - Hamis levélriasztás, mely az emberek jóhiszeműségére építve, hatalmas levélforgalmat generál, ezzel a **levelező rendszereket lassíthat, vagy béníthat meg.** Kártékony programot nem tartalmaz, ha tartalmaz, akkor már vírusnak /malware/ hívják.


Támadás jelei, formái





- A feladó neve, és maga az email cím valódisága
 - Komoly megrendelés -> telefon
- Hivatalos levél nem jön @gmail.com, @freemail.hu stb címről
- Mellékletek


Megtévesztő feladó, veszélyes melléklet




Adathalászat

**Dear Account User**



Feladó **Admin** 

Címzett **Recipients** 

Dátum **2016-07-14 13:15**

Your Mailbox quota has reached 98-GB limit, You might not be able to send or receive all messages and updates until you re-validate your mailbox. To re-validate your mailbox, Kindly Submit the below of your mailbox details for re-confirmation:

{user-name :
{Password :
{Confirm Password :

Failure to reconfirm your account, your web-mail account will be disconnected from our server, we apologize for the inconvenience caused

Best Service
Web-mail Team

Magyar változatban (Telekom logo)

We've Disabled Your Account Access

Spam x



Apple Support <no-replay@server2.sashianceit.com>
címezett saját magam



Miért van ez ez üzenet a Spam mappában? Az üzenet hasonló a spamszűrőnk által korábban észlelt üzenetekhez. [További információ](#)



angol



magyar

[Üzenet lefordítása](#)

Update Your Information Within 48 Hours.

Dear Customer,

We have changed our policy tems, so we need from you to confirm you ID Apple and accept our new tems. **Policy Update.** To learn more about what's been changed, simply **Log in** to your ID Apple and click on policy updates under the notifications section.

[Update Your ID Apple](#)

Sincerely,
Apple Support

<http://rossignol.kiev.ua/skin/test.php>

Veszélyes melléklet

- **Keylogger**

- Minden billentyűzet leütést rögzít, továbbít emailre
- Kategóriákba szedi (böngésző, gépelés, programok indítása...)
- Már nem csak **exe** fájlként hanem **jpg** fájlban is terjed



Számítógép alapú social engineering

- **Keyloggerek**

Olyan billentyűzetnaplózó programok, amelyek a felhasználó által begépelte karaktereket naplózzák, majd elküldik a támadónak.

- Szoftveres
- Hardveres

2012. évi C törvény XLIII. Fejezet

422. § (1) ...

d) elektronikus hírközlő hálózat - ideértve az információs rendszert is - útján másnak továbbított vagy azon **tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti**, bűntett miatt **három évig** terjedő szabadságvesztéssel büntetendő.

424. § (1)...

a) **jelszót** vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, **megszerez**, vagy forgalomba hoz

...

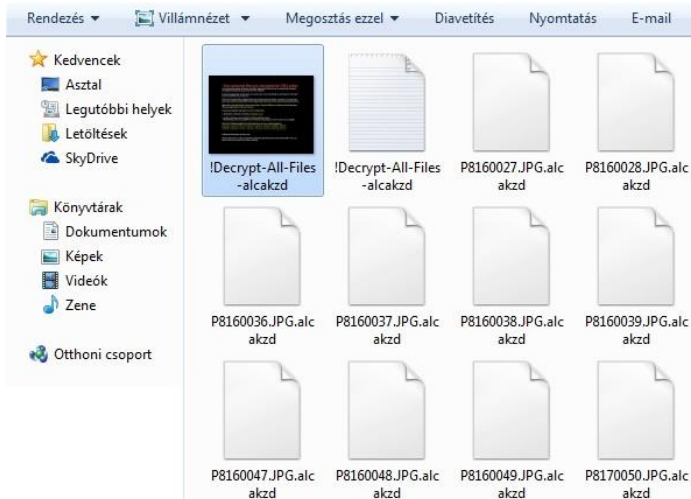
vétség miatt **két évig** terjedő szabadságvesztéssel büntetendő.



Fájlok ellen irányuló támadás

- Helyi számítógépen: Vírus által törölődnek vagy kódolva lesznek
- Felhő alapú tárolásnál: adathalászat következtében -> hozzáférés
- Elhagyott adathordozó

CryptoLocker támadás



Asztal	tételek	2015.02.05. 19:13	Fájlmappa	
Legutóbbi helyek	e_tortma_14maj_ut.PDF.alcakzd	2014.07.10. 6:33	ALCAKZD fájl	279 KB
Letöltések	feladat sor 1 jav kulcs.PDF.alcakzd	2014.07.10. 6:27	ALCAKZD fájl	283 KB
SkyDrive	feladatsor 1.PDF.alcakzd	2014.07.10. 6:26	ALCAKZD fájl	1 970 KB
	feladatsor 2 javító kulcs.PDF.alcakzd	2014.07.10. 6:36	ALCAKZD fájl	279 KB
Könyvtárak	feladatsor 2.PDF.alcakzd	2014.07.10. 6:33	ALCAKZD fájl	3 085 KB
Dokumentumok	tortenelem_vk.PDF.alcakzd	2014.07.10. 6:23	ALCAKZD fájl	177 KB

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

If you see the main locker window, follow the instructions on the locker. Otherwise, it's seems that you or your antivirus deleted the locker program. Now you have the last chance to decrypt your files.

Open <http://fizxfsi3cad3kn7v.onion.cab> or <http://fizxfsi3cad3kn7v.tor2web.org> in your browser. They are public gates to the secret server.

If you have problems with gates, use direct connection:

1. Download Tor Browser from <http://torproject.org>
2. In the Tor Browser open the <http://fizxfsi3cad3kn7v.onion/>
Note that this server is available via Tor Browser only.
Retry in 1 hour if site is not reachable.

Copy and paste the following public key in the input form on server. Avoid missprints.
JG4ZBMJ-R72YVDJ-WIDYVXP-MLN4TDI-KETQEJ6-H2WYKWC-KSQHQME-ANEATA5
MNMQFEN-CB4XK6M-Z5HCF24-E3ADUIK-5BW7JUK-4TUNYDH-J2WLTQA-RHS3OI4
SVQWCKN-5RB6PWQ-C2H5O27-VXL5RN3-IC5QLH2-0O22DVX-DTEKOEW-NSPCK4S

Follow the instructions on the server.

<https://www.youtube.com/watch?v=Gz2kmmsMpMI>

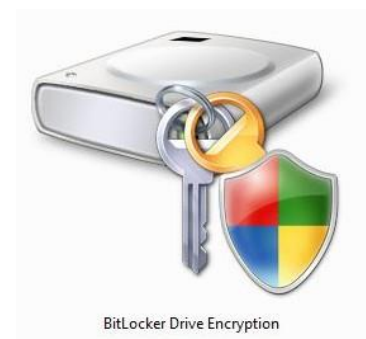
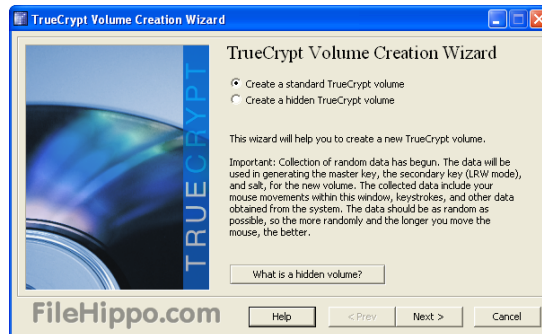
ADATMENTÉS KÜLSŐ TÁROLÓRA!

- Fontos adatainkat, munkáinkat időközönként mentjük külső adathordozóra, amit csakis az adatmentéskor csatlakoztassunk a gépünkhöz.



TITKOSÍTÁS

- Az adathordozót, partíciót, teljes merevlemezt titkosítani.



Számítógép alapú social engineering

- **Pharming**

- Szerver alapú DNS Poisoning
 - DNS szerver támadás – a letárolt URL mellé saját IP
- Cross-Site Scripting (XSS)
 - Idegen parancsok végrehajtása – valódi weblap kódjába való betörés

- **Trójai programok**

- Letöltő oldalakról
- Email mellékeletek
- Road Apple (direkt elveszít egy adathordozót)

Támadások felépítése

- Információ szerzés
- Kapcsolat kiépítése
- Kapcsolat kihasználása
- Támadás végrehajtása

Védekezés

- **Sebezhetőségek feltérképezése**

Alkalmazott megoldások, eljárások időnkénti ellenőrzése, felülvizsgálata, hogy ezáltal fény derüljön az újonnan keletkezett vagy eddig figyelmen kívül hagyott sebezhetőségekre.

- **Audit, felülvizsgálat**

A vállalat fizikai védelmének, az informatikai eszközök és adathordozók kezelésének, a hozzáférés-védelemnek valamint a vállalati kultúra és a felhasználók képzésének vizsgálata is

Védekezés

- **Penetration teszt**

Behatolási teszt. A behatolási teszteket információbiztonsági cégek szakértői hajtják végre, és munkájuk során csak olyan módszereket alkalmaznak, amelyeket a megrendelő kér, illetve engedélyez.

- **Audit, felülvizsgálat**

A vállalat fizikai védelmének, az informatikai eszközök és adathordozók kezelésének, a hozzáférés-védelemnek valamint a vállalati kultúra és a felhasználók képzésének vizsgálata is