

EIVOK 35.

(-2023 április 27-)

(B)usiness (E)mail (C)ompromise –
(mint a vezetői elköteleződés és motiváció eszköze)

Inspiráció - ötletadók

WITSEC szakmai nap 2022.10.26 - **dr. Ambrus Orsolya** (Bonafarm Zrt.)

(<https://www.youtube.com/watch?v=2LgrhZB9Z54>)

EIV 2018 – Orosz Lajos – (tanár, az NKE Minőségügyi Bizottság elnökhelyettese volt)

válasza egy kollégának, aki kevésnek tartotta a konzultációs gyakorlat végén a beszámolóra kapott időkeret:

„ha a szervezet vezetőjével egyszerre szálltok be a liftbe és kevesebb, mint 5 perced van, hogy udvarias érdeklődésére válaszul felkeltsd az érdeklődését és ilyenkor hosszas szakmai fejtegetésekbe bonyolódsz, akkor elszalasztottál egy lehetőséget, amelyet felkínált a sors...”

Bemutakozás

Dr. Muraközi Gergely (*Dr. Bakos - Dr. Smied - Dr. Muraközi Ügyvédi Iroda*)

dr.mura@t-online.hu

Jerabek György (*Hétpecsét Információbiztonsági Egyesület – titkár*)

titkar@hetpecset.hu

(B)usiness (E)mail (C)ompromise

Inspiráció: - **Dr. Ambrus Orsolya – Bonafarm Zrt.** - Előadás elhangzott: WITSEC – 2022,

illetve: <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise>

és még: <https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec>

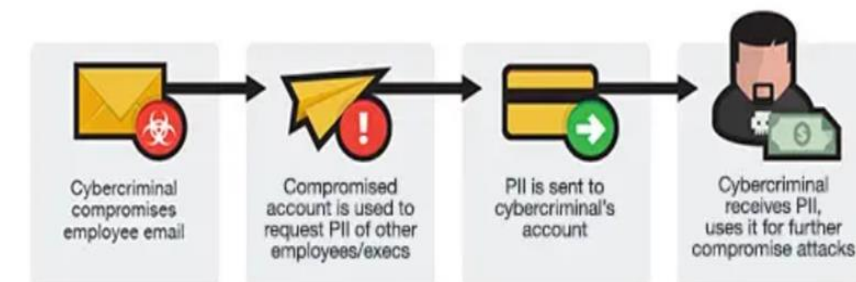
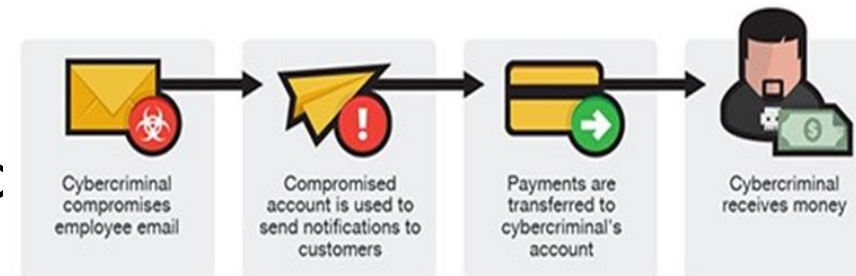
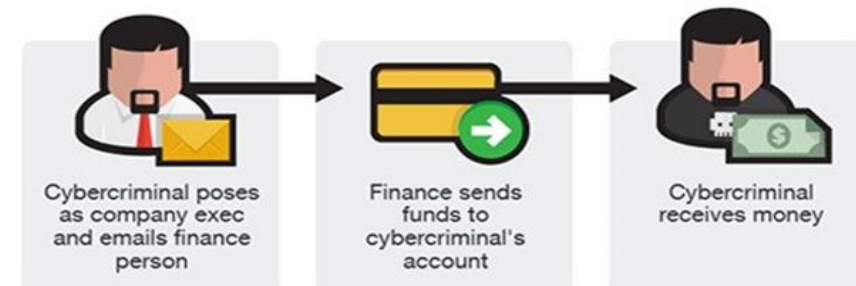
Miért éppen a „BEC” érdekes? (4/1)

- A legjövedelmezőbb elkövetési forma (átszoktak a zsarolóvírusban edzett bűnözői csoportok)
- IC3 (FBI Internet Crime Complain Center) – 2013 óta követi nyomon – globális kár közel 43,3 milliárd \$ (2016. július és 2021 december között)
- A kitettség egyre nő – és ebben az MI is segít... 😞

(B)usiness (E)mail (C)ompromise

Hogyan „működik” (4/2) – legnépszerűbb formái

- vezérigazgatói csalás (CEO Fraud)
- alkalmazotti postafiók kompromittálása (account compromise)
- hamis számlázási adatok – szállítói csalás (false invoice scheme)
- adatlopás (data theft)

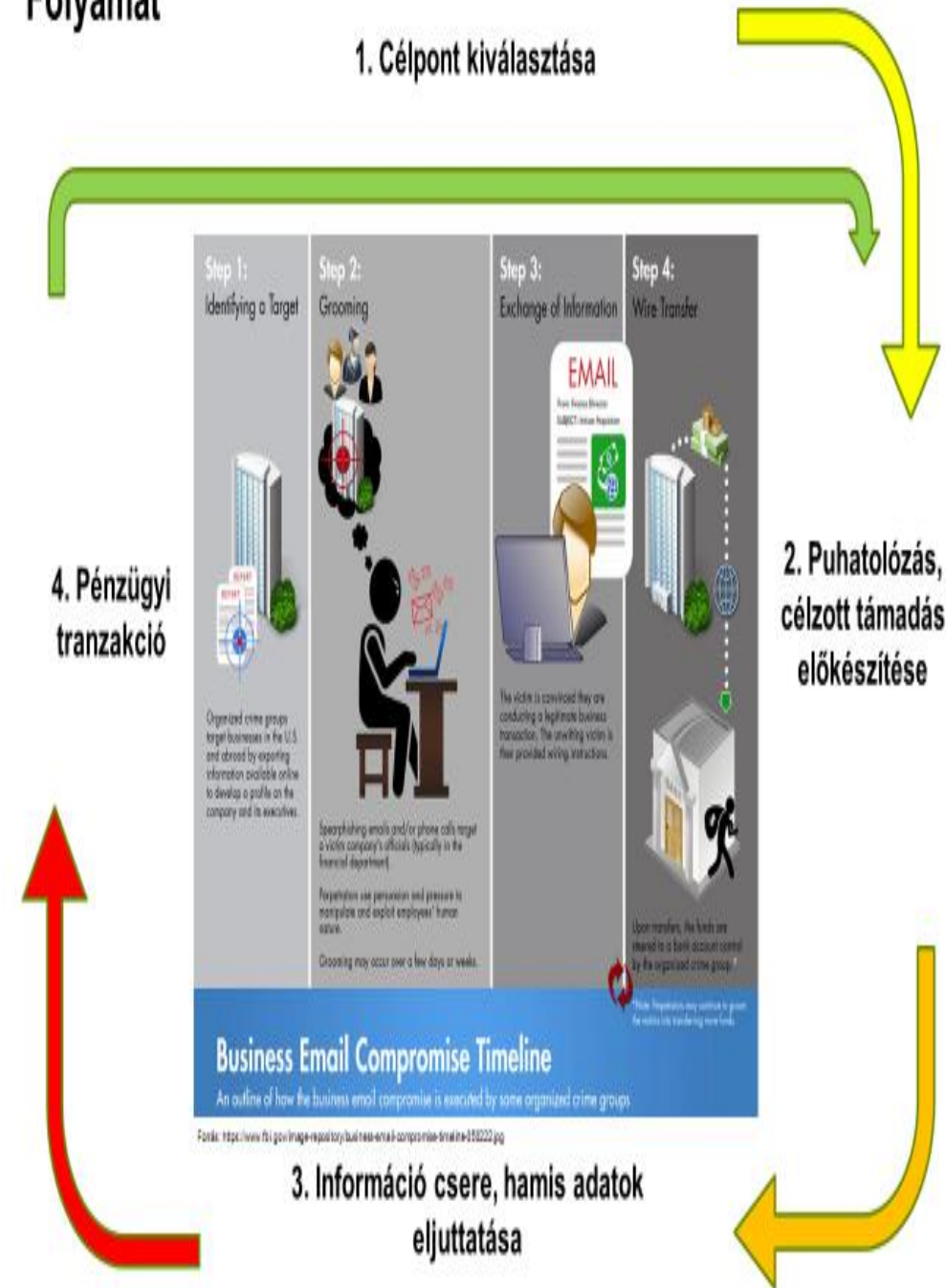


(B)usiness (E)mail (C)ompromise

Hogyan „működik” (4/2) – a „folyamat”

- célpont kiválasztása
- „puhatolózás” (OSINT) – támadás előkészítése
- információcsere, hamis adatok eljuttatása
- pénzügyi tranzakció

Folyamat

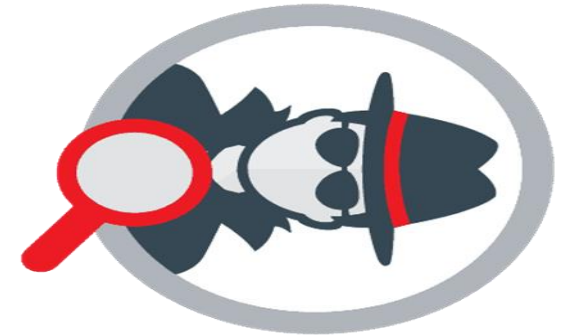


(B)usiness (E)mail (C)ompromise

Ki a felelős? (4/3) – jogi és IT vonatkozások

- Btk. 373. § - Csalás
- Btk. 422-424. § - IT rendszereket érintő cselekmények
- Btk. 399-400. § - pénzmosás

- Szerződés teljesítése, károkozás, szerződésszegés
- 6:525 § - károkozás, **károsulti közrehatás**
- Ptk. LXIII. 6:439 § - kárbiztosítás
- Ptk LXIII. 6:470 § - felelősségbiztosítás



(B)usiness (E)mail (C)ompromise

Ki a felelős? (4/3) – jogi és IT vonatkozások

- OSINT – mi deríthető fel? - („*passzív*” keresés)
- Social Engineering (Phishing, Whale, Scam) - (*felhasználói „interakció” szükséges*)
- Malware (trójai, spyware) - („*aktív*” felhasználói „*interakció*” szükséges)
- információbiztonság (infrastruktúra, hálózat, levelezés) – (*rendszergazdák, beszállítói lánc, IBF...*)
- Adatvédelem (*DPO, Compliance, etc.*)



(B)usiness (E)mail (C)ompromise

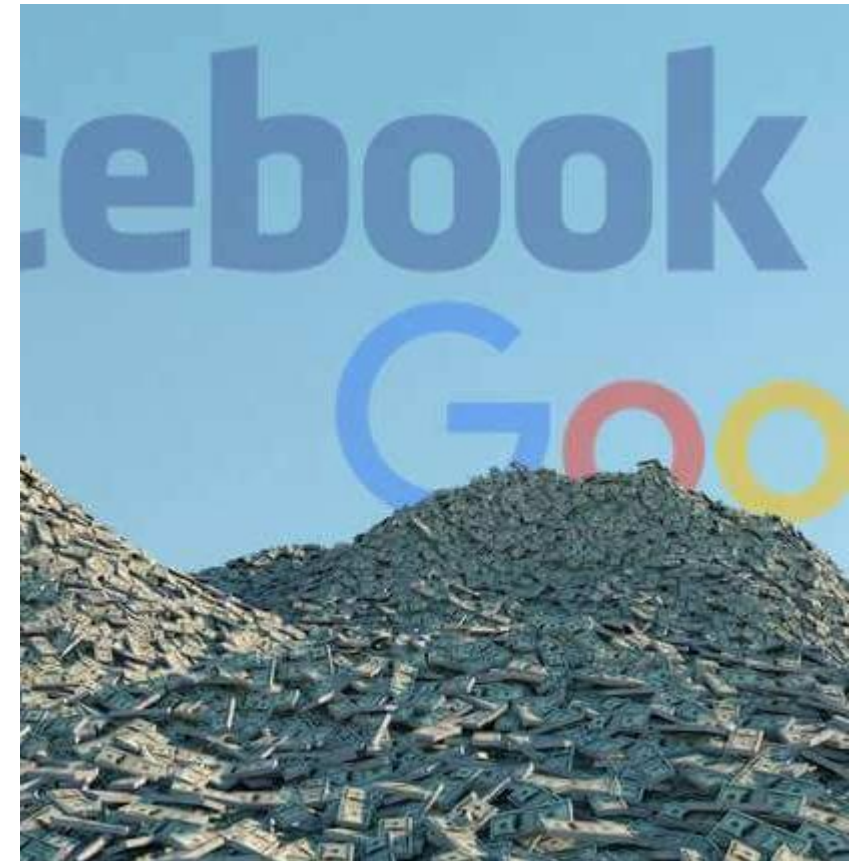
Hazai és külhoni példák... (4/4 - 1)

„Elismerte a pólószövetség: 54 millió forintot utalt rossz számlára, nincs meg a pénz”

(<https://telex.hu/sport/2022/11/22/vizilabda-teves-utalas>)

„From 2013 to 2015, Evaldas Rimasauskas carried out a series of BEC scams, leading him to a 5-year sentence in federal prison. This guy set up a fake company impersonating a Taiwanese hardware supplier Quanta Computer.”

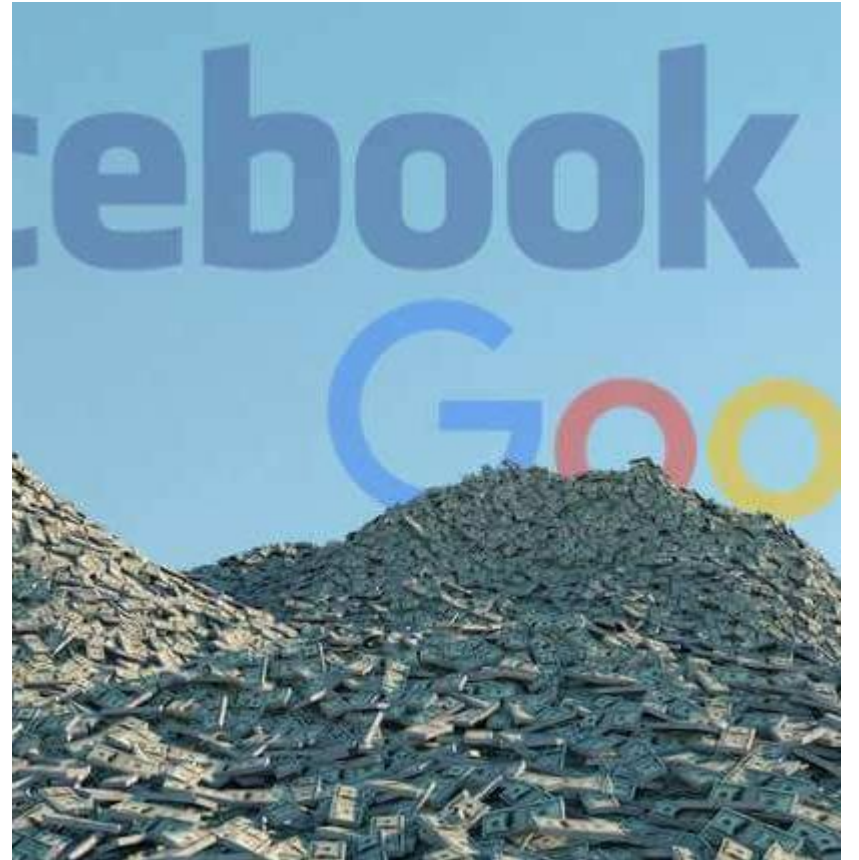
„Puerto Rico Government - In early 2020, the government of Puerto Rico was still recovering from a 6.4 magnitude earthquake when they found that they had fallen victim to a BEC scam. The victim was the director of Puerto Rico’s Industrial Development Company, Ruben Rivera, who mistakenly made the transaction of \$2.6 million to a fake bank account.”



(B)usiness (E)mail (C)ompromise

Hazai és külhoni példák... (4/4 - 2)

1. Holland eladó, német vevő, közel 500e EUR összeg
 - Magyarországon, szerb állampolgár által alapított cég
 - profi e-mail és telefonos kommunikáció angolul és németül
 - 1 nap után észlelték, ekkor gyorsan felvették velünk a kapcsolatot
 - BRFK Korrupció és Gazdasági Bűnözés Elleni Osztály és Pénzmosás és Terrorizmusfinanszírozás Elleni Iroda (FIU, Financial Intelligence Unit) hatathós segítségével az összeg kb 1/3-a meglett, a maradék eltűnt a nemzetközi bankok útvesztőjében

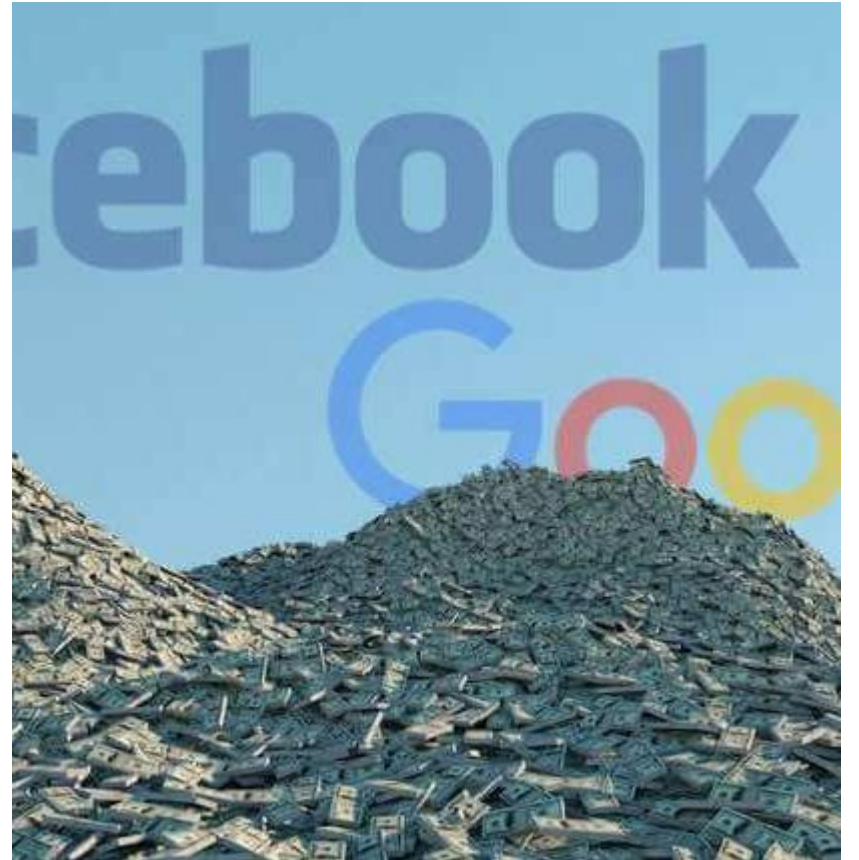


(B)usiness (E)mail (C)ompromise

Hazai és külhoni példák... (4/4 - 3)

2. Magyar eladó, osztrák vevő, közel 100e EUR összeg

- lengyel magánszemély által Magyarországon nyitott számlára eltérített összeg*
- profi e-mail kommunikáció németül*
- hosszabb idő után észlelték*
- nem volt már lehetőség az összegből semmit megtalálni*
- a felek között polgári jogi vita alakult ki a felelősség kérdésében, amely mai napig is tart*

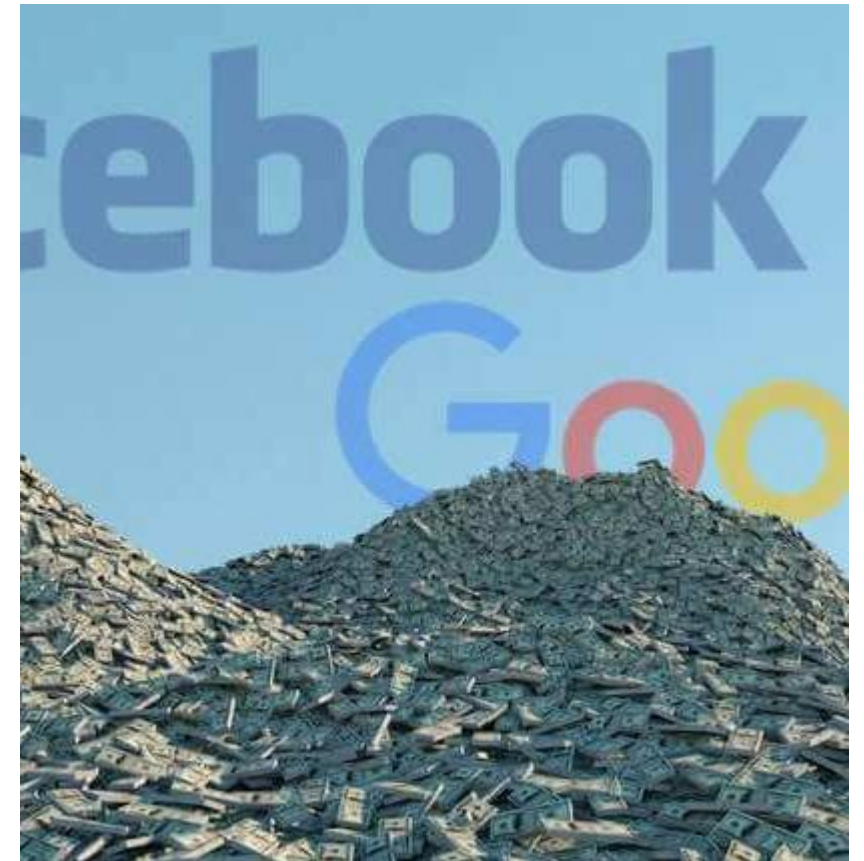


(B)usiness (E)mail (C)ompromise

Hazai és külhoni példák... (4/4 - 4)

3. Magyar ügyvéd, magyar ügyfél, ismeretlen összeg

- magyar ügyvéd a magyar ügyféltől letéti számlán fogadott volna összeget*
- az ügyfelet telefonon arról értesítette ismeretlen személy, hogy változott a letéti számla száma*
- az ügyfél – nagyon helyesen – közvetlenül felvette a kapcsolatot az általa személyesen ismert ügyvéddel, és tisztázták, hogy semmiféle számlaszám változás nem volt*
- a csalási kísérlet meghiúsult*



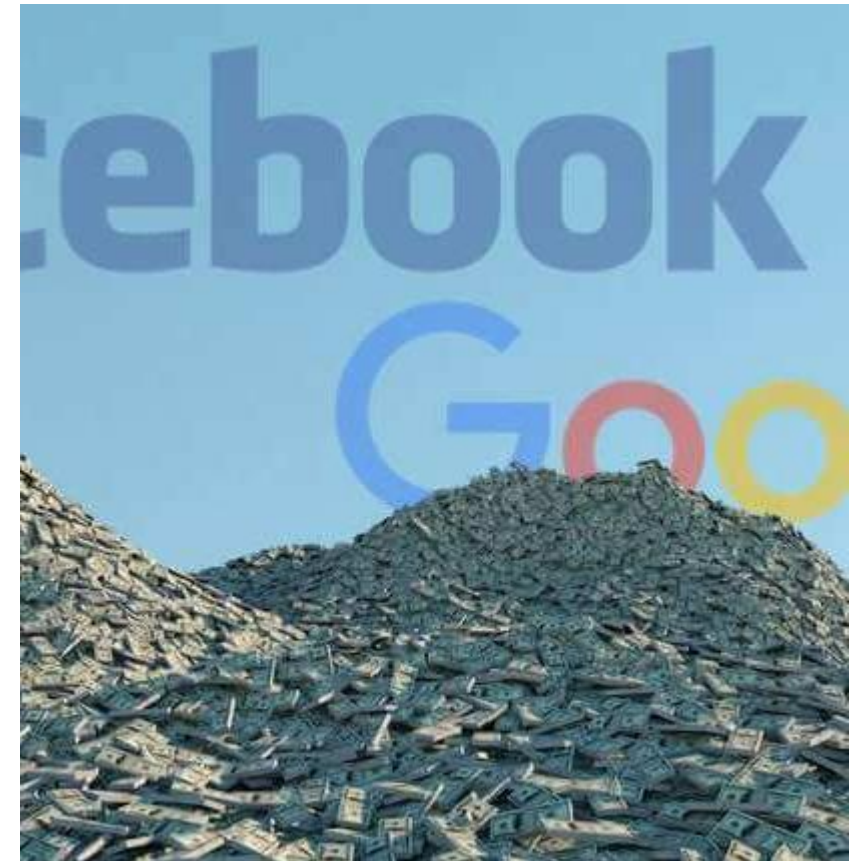
(B)usiness (E)mail (C)ompromise

Hazai és külhoni példák... (4/4 - 5)

4. Der große Hintergrundbericht:

DSGVO und Business E-Mail Compromise lassen Cyber-Schäden hochschnellen

„Business E-Mail Compromise (BEC) überholt zum ersten Mal Ransomware und Datenschutzverletzungen als Ursache von Cyber-Schäden, so der aktuelle AIG EMEA1 Cyber-Schadenreport. Nahezu ein Viertel der gemeldeten Schäden aus dem Jahr 2018 ließ sich demnach auf Business E-Mail Compromise zurückführen. Im Vergleich zum Vorjahr (2017) bedeutet dies einen Anstieg um 11 %. Ransomware, Datenschutzverletzungen durch Hacker und durch Fahrlässigkeit von Mitarbeitern sind dem Bericht zufolge die anderen hauptsächlichen Ursachen von Cyber-Sicherheitsvorfällen.“



EIVOK 35 – 2023.04.27

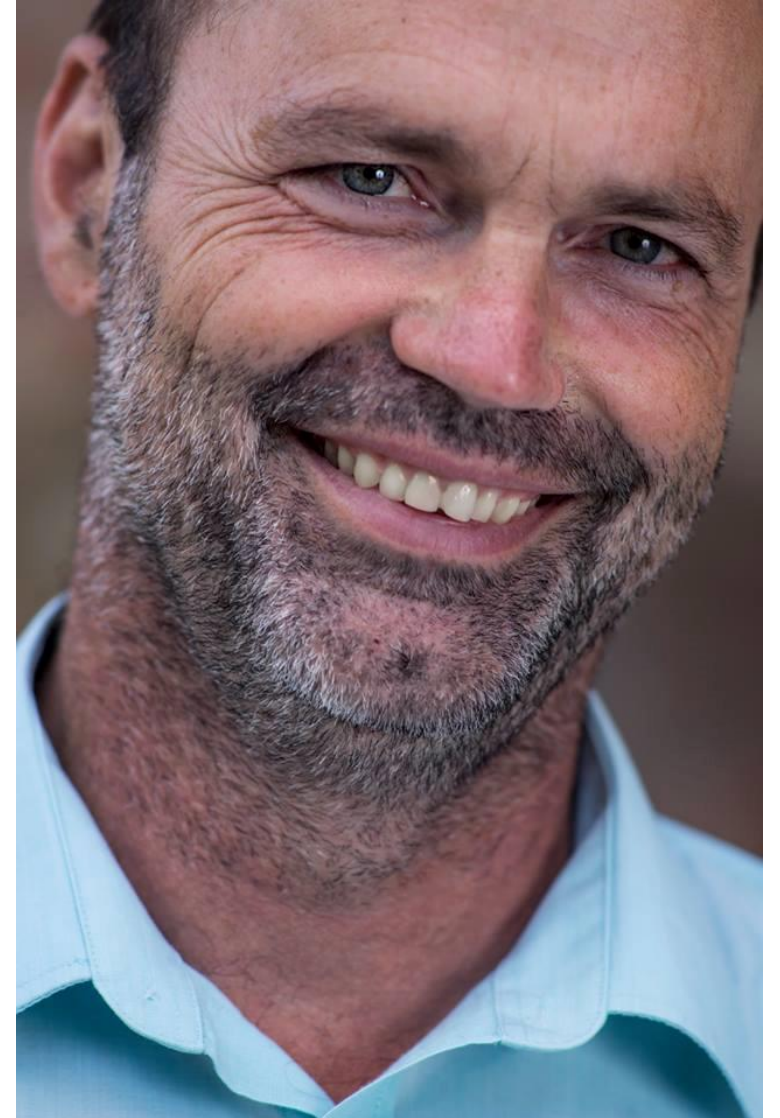
Jerabek György

titkar@hetpecset.hu

<https://www.linkedin.com/in/gyjerabek/>

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

+36 30 9847 860



EIVOK 35 – 2023.04.27

Dr. Muraközi Gergely

Dr. Bakos – Dr. Smied – Dr. Muraközi Ügyvédi Iroda

dr.mura@t-online.hu

+36 20 992 4675