IT Biztonságtudatosság

Készítette: Pethes Tamás Dávid /six/

Dátum: 2020.08.11.

Modern élet

Ha van pénzed, adatod vagy munkahelyed...

...biztos lehetsz benne, hogy célzott támadások fognak érni.

Az utóbbi hónapok során különösen igaz, hogy egy új, virtuális térben vagyunk kénytelenek mozogni nap mintnap, ahol intéznünk kell ügyeinket, kapcsolatot kell tartani másokkal. De a legfontosabb, amit meg kell tanulnunk - vigyázni magunkra és másokra is. Ezért fontos megismerni a rosszindulatú hackerek és rendszerek motivációt, gondolkodását és hogy mit tehetünk ellenük.

Célunk: a biztonságtudatosság növelése.

A támadók motivációi

Mindig vannak jók... és rosszak.

Kategóriák:

- Pénzszerzés
- Adatok megszerzése
- Elégedetlenség, bosszú, rosszindulat
- Szórakozás

A legtöbb támadás kintről érkezik, e-mailen, telefonon vagy sérülékenységek kihasználásán keresztül, de arányaiban, gyakran előfordulnak belső támadások is. Ilyenre lehet példa egy elbocsátott alkalmazott, aki magával viszi a céges adatokat. A védelem több szinten kell működjön (threat modeling szerint).

Rajtatok áll sikerül-e nekik!

Ha fura email-eket, üzeneteket kapnak ismerőseitek tőletek (vagy a nevetekben), amiket nem ti írtatok (☺), akkor valószínűleg kártékony kód fut valahol!

Belépés, jelszavak, problémák?

LastPass, KeePass és a **Yubico kulcs** remek megoldások.

Nem osztod meg őket

A jelszavak megosztása nem csak visszaélési lehetőségeknek ad teret. Amint kikerült jelszavunk, már nincs kontrollunk afelett, hogy milyen módon van kezelve és azonnal meg kell változtatni.

Jobb ha hosszabb

A rövid jelszavakat könnyű akár egy kezdő hackernek is feltörni. Javasolt mondatokat kitalálni és abból létrehozni a jelszót. Így 8-10 bonyolult karakter helyett lehet egy 20 karakteres, nehezen feltörhető, de könnyen megjegyezhető jelszavunk.

Titokzatos, nem hagyod el

Gyakori hiba, hogy valaki felírja papírra a jelszavát, vagy lementi titkosítás mentes helyekre, amit más is elérhet. Gondoljunk bele, hogy ha ott a jelszó a postit-en, akkor bárki láthatja még a szomszéd épületből is egy kis távcsővel vagy drónnal ☺

Gyakran váltod és mindig más

Azért fontos a jelszavakat megváltoztatni, mert kompromitálódhatnak idővel. Lehet csak hetekkel később vagy talán soha nem derül ki, hogy egy gépen ahol belépünk, már el is lopta a jelszavunkat. Ha már ellopták, akkor nem csak egy helyen, hanem mindenhol be fogják próbálni. Ezért legyen mindenhol más a jelszó!

Phishing és Vishing

Halászat emailen és telefonon keresztül

Demo video ☺ ...avagy így lopják el a mobil szolgáltatói fiókod egy rövid híváson keresztül:

https://youtu.be/fHhNWAKw0bY?t=85

Live Phishing Demo

Hogy dolgozik a hacker, hogyan küld neked levelet?

1. Phishing és böngészés
2. Levelezés, mire figyeljetek
3. Fizikai védelem fontossága

Böngészés és a linkek

Amikre figyeljünk mindig

- HTTPS és tanúsítványa – tehát titkosított az adatforgalom és nem látja bárki!
- Domain neve – amit beírsz, hogy megnyisd a weboldalt
- Link szerkezete – a domain körüli rész, például: https://v-space.hu/oldal
- Hova mutat a link valójában? – Kattintás előtt várjunk kicsit amíg kiírja

FireFox és Chrome böngészők: kiegészítőkkel biztonságosabb

HTTPS beállítások erősítése: HTTPS Everywhere

Tamadási felület csökkentése és reklámok tiltása: adblock kiegészítő

Tamadási felület csökkentése, javascript tiltás: NoScript és ScriptBlock

Tamadási felület csökkentése, nyomkövetők tiltása: EFF Privacy Badger

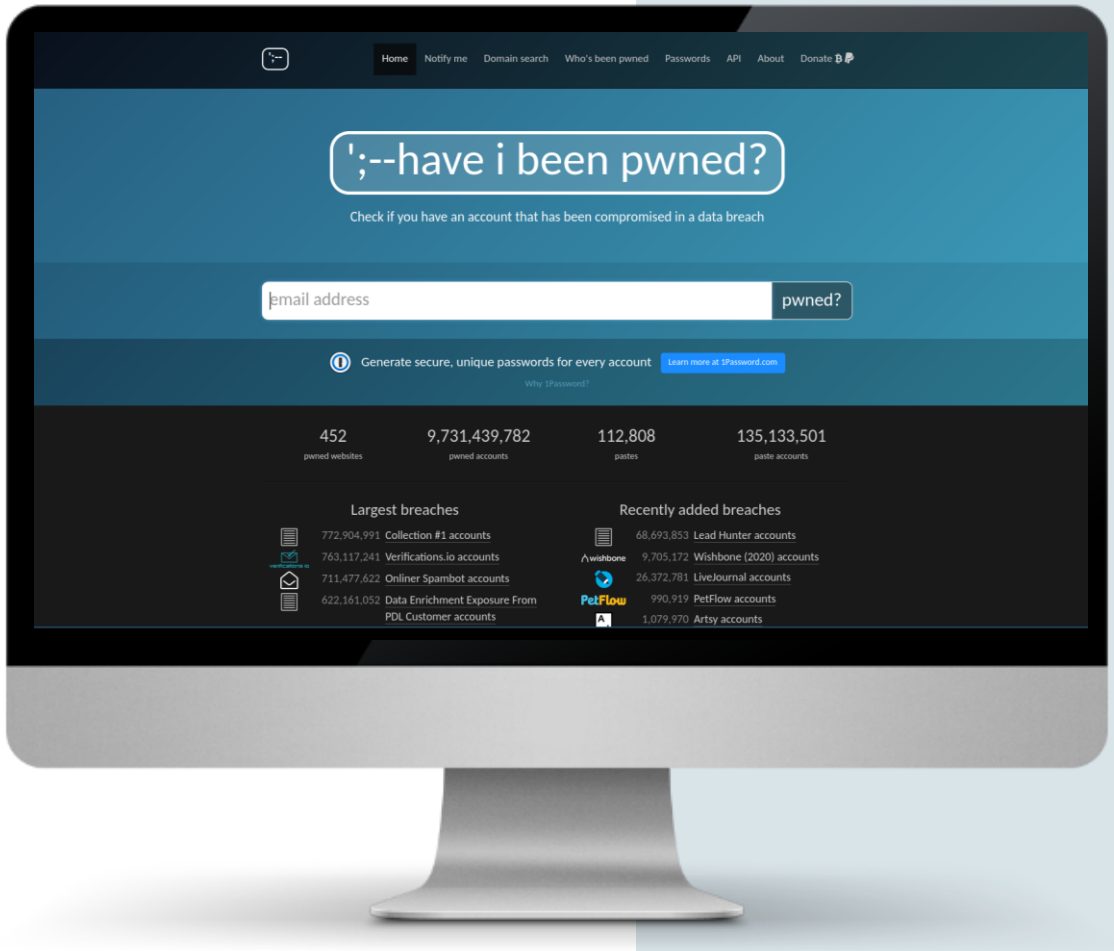
Tipp: inkognitó mód

History törlés: CTRL+SHIT+DEL

Have I been pwned?

https://haveibeenpwned.com/

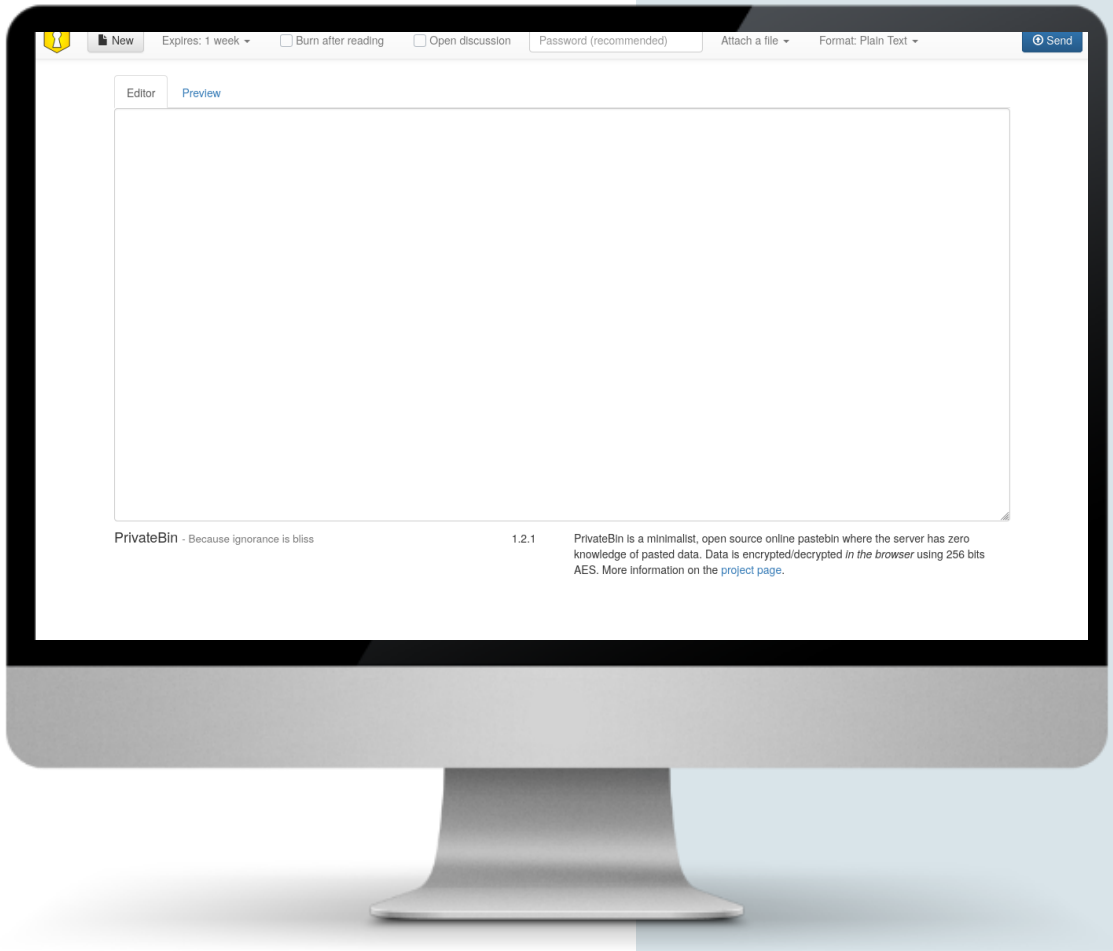
Ennek az oldalnak a segítségével megnézhetitek, hogy az e-mail címetek, amit használtok, benne van-e kompromitált, kiszivárogtatott adatbázisokban.



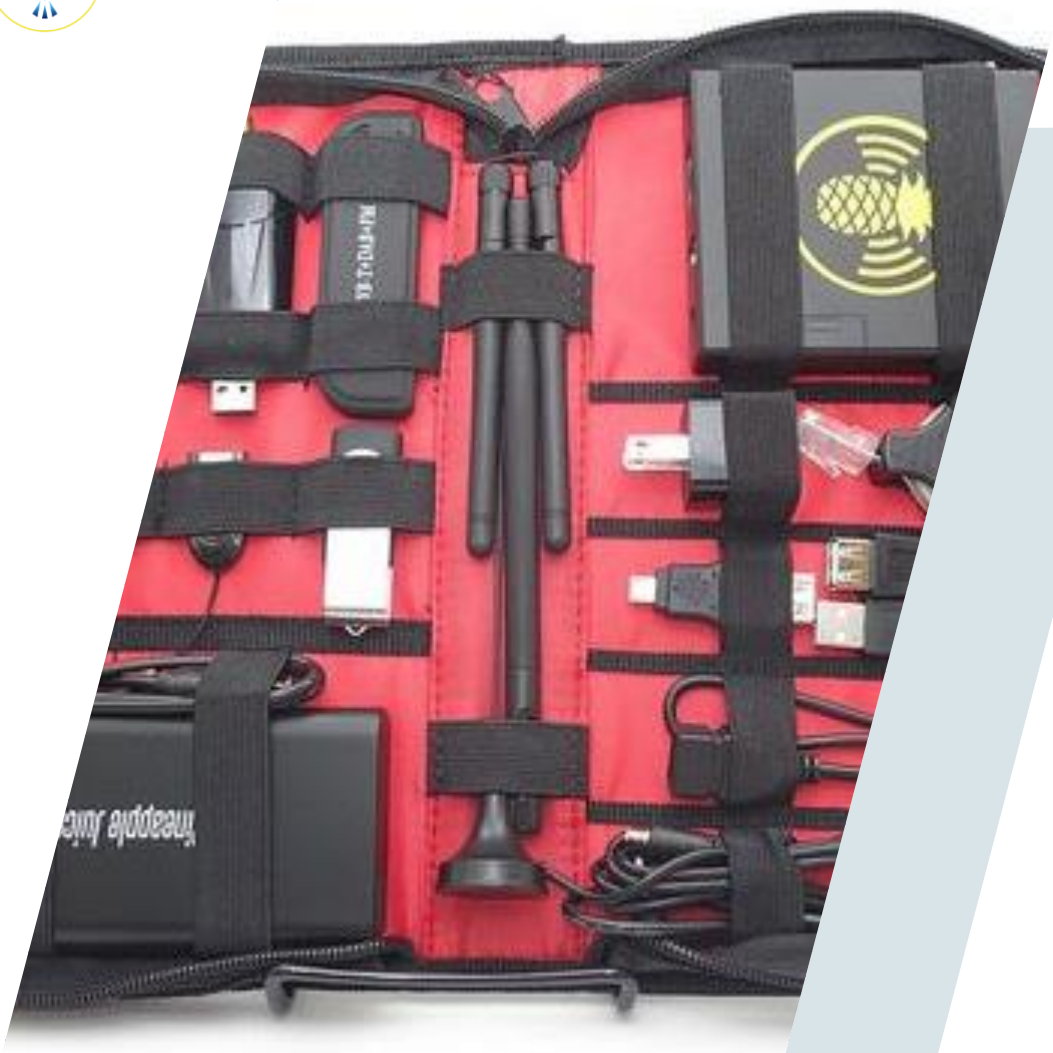
PrivateBin - a titkos küldő

https://bone9.hu/privat

1. Szöveg beillesztése (lehet jelszó is), opcionálisan file feltöltés
2. Beállítani a lejárat idejét
3. ”Send” gomb
4. Link másolása és elküldése (mondjuk e-mailen, Signal-on*)



*A Signal titkosít a két kommunikáló eszköz között és nem követ vagy raktároz el minden kis mozzanatot, hangot mint a Facebook vagy a Google.



Helyi (lokális) támadások

Az elvesztett pendrive

Ha találsz egy pendriveot, bedugnád a gépedbe? Nem tudhatod, hogy valaki nem direkt hagyta-e el, hogy vírust juttasson a gépedbe!

Hardware keylogger

Mindig ellenőrizzük az eszközeinket, hogy nem helyezett-e el valaki egy behatolásra alkalmas eszközt.

A nyitva felejtett ajtó

Az udvariasság fontos, azonban nem szerencsés, ha azt is beengedjük az épületbe, aki nincs felhatalmazva. Figyeljünk arra, hogy kit engedünk be. Badge rendszer esetén ne higgyük el, hogy „otthon felejtette”.

... és amikor nem lockoltad.

Ha nem zárod le a képernyőt (Win+L), az csak a jobbik eset, hogy valaki lecseréli a hátteredet David Hasselhoffra. De bármilyen adatot elvihet egy potenciális támadó a rendszerből, ha nincs lezárva.

Best practices

00. Gyakorlás, szinten tartás

Gyakoroljatok a mindennapi életben, és ne kerüljétek ki, hogy hasznotokra váljon!

Nem elég csak részt venni ezen a prezentáción, amit megtanultok, azt be kell építeni a hétköznapokba, hogy valóban hasznotokra váljon és biztonságosabban használjátok az eszközeiteket.

01. Frissítések

A frissítések segítenek megvédeni az ismert sérülékenységekkel szemben. Célszerű beállítani, hogy ezek automatikusan fussanak le.

02. Wifi és VPN

A nyílt (open) wifi használata VPN nélkül veszéles, mivel az adatforgalom mindenki számára nyíltan közlekedik a ”levegőben”. A VPN segít titkosítani az adatfolyamot.

03. Biztonsági mentések

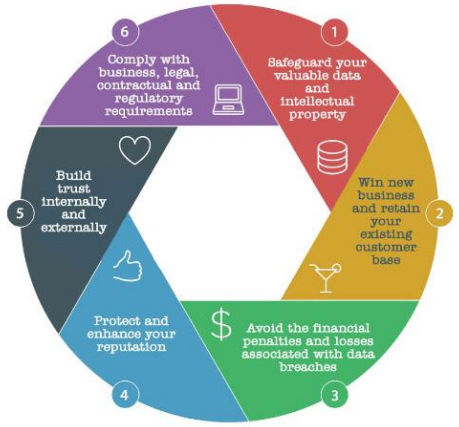
„Ami csak egy helyen van meg, az nincs meg.” Gondolj bele, mi történne ha az összes családi emlék csak egy pendriv-on lenne és az a pendrive elromlana... Készítsetek biztonsági mentéseket!

Az ISO 27001 szabvány

Komplex rendszerekkel és számos technikával, szokással kerülünk kapcsolatba nap mint nap. Ezeket az ISO 27001-es információ biztonsági szabvány keretek közé rendezi.

Az biztonságtudatosság témaköre

- A tudatosság jelentőssége és gyakorlati megközelítése.
- A céges szabályzatokat ismernie kell minden dolgozónak.
- Hol helyezkedik el a folyamatokba? Előnyök és hátrányok.
- Szabályok be nem tartásának lehetséges következményei.



ISO 27001 alapfogalmak

ISMS – Information Security Management System

CIA – Confidentiality, Integrity, Accessibility

Principle of Least Privilege (POLP)

Segregation of duties

Fiókok kezelése és az internet használata

Fiókok, jelszavak kezelése, több faktoros autentikáció bemutatása és gyakorlatba helyezése.

A böngésző bizontásgosabb használata, mire figyeljünk és milyen kiegészítők segíthetnek?

Fizikai védelem

Perifériák, hardware-k védelme.

A munkavégzés helyének védelme.

Titkosítás és biztonsági mentések védelme.

Hogy segíthetünk még?

Biztonságtudatosság program

Phishing kampány, dolgozók tesztelése és a tudatossági szint növelése, szinten tartása. Phishing tesztek akár havi rendszerességgel.

Behatolási tesztek (pentest)

A teljes rendszer vagy meghatározott részeinek vizsgálata, biztonsági szemptonból.

Hardening

A rendszer biztonságának technikai oldalról való megközelítése, biztonságosabb beállítások (konfigurálás) segítségével.

Konzultáció

Folyamatok, ISO27001 és kriptovalutákkal kapcsolatos konzultációs lehetőségek.

Köszönöm a figyelmet!

Elérhetőség

Pethes Tamás Dávid /six/

Signal: (+36) 20 256 4090

Email: hello@awalcon.org

Weboldal

https://awalcon.org/