HONNAN ÉRHET TÁMADÁS, ÁRTALOM?

Mitől is félhetünk?

El akarják lopni a doménnevünket?

Nem ettől kell igazán félnünk. Inkább attól, hogy átmenetileg

- **megszerzik doménünk felett a hatalmat**,
  - **authoritatív névszereinket módosítják**
- vagy **DNS zónánkban nem kívánt változtatás** történik;

valamint attól, hogy

- **doménünk működésképtelenné válik** (**nem hosszabbítjuk a fenntartását** stb.).

Kockázat, sérülékenység

ICANN

Nyilvántartók (Registries) (pl. com: VERISIGN, hu: ISZT Nonprofit Kft., eu: Eurid)

Regisztrátorok (Registrars)

Közvetítők (Resellers)

Doménigénylők/használók (Registrants)

Tényleges doménhasználók[1] + harmadik felek (pl. felhasználók)

Más szereplők:

- **Authoritatív DNS-szolgáltatók**
  - **felsőbb szintű DNS-szolgáltatók (hu: ISZT Nonprofig Kft. + CDNS és Rcodezero)**
- Távközlési szolgáltatók, hálózatüzemeltetők
- Hoszting szolgáltatók
- Más szolgáltatók (tűzfal, IDS, DDoS védelem, monitoring stb.)
- További szereplők: tanácsadók, auditorok stb.
- Hatóságok, bíróságok, jogalkotás.

[1] akik konkrétan saját célra használnak adott domaint

DNS-biztonság

Authoritatív DNS és DNS-feloldás:

authoritatív és resolver (rekurzív) DNS szerverek

Jelen esetben csak az authoritatív DNS szolgáltatás és a doménbiztonság kérdésével foglalkozunk!

DNS	Domain
1. Root DNS zóna ('.') 1.1. TLD zóna (pl. hu.) 1.1.1. domain zóna (pl. domen.hu) 1.1.1.1. zónaadatok (esetleg delegált zónák) (pl. A, MX, CNAME, TXT stb. rekordok)	1.) ICANN 2.) Registry 3.) Regisztrátor 4.) Közvetítő (opc.) 5.) Tulajdonos

HOGYAN LOPJUNK EL DOMÉNNEVET?

Mi a célunk?

- A doménnév ellopása?
- A domén alatti szolgáltatásokkal visszaélés?

Mi felett szeretnénk átvenni a hatalmat?

- A domén feletti teljes rendelkezés felett?
- A domén authoritatív névszervereit módosítsuk?
- A domén DNS zónája felett?

Kitől szerezzük meg a hozzáférést?

- Tulajdonostól?
- Közreműködőtől?
- Regisztrátortól?
- Nyilvántartótól?

Doménbiztonság:

Domén nyilvántartásban történő nem kívánt módosítás (jogosultságok megszerzése, tulajdonosváltás, regisztrátorváltás) elleni védelem.

Működő domén esetén a legkritikusabb

- az **authoritatív névszerverek módosítása** felett megszerezni a hatalmat.

DNS-biztonság:

Domén zónájának védelme.

Gyenge pontok keresése – leggyengébb láncszemek

- Felhasználók, felhasználói accountok
- Felhasználói (webes) felületek [pl. szoftveres gyengeségek]
- Social engineering [pl. hamis okirattal visszaélés, más személyével történő visszélés]
- Nem kellően biztonságos authentikáció [MFA hiánya]
- Regisztátor szintjén történő visszaélés (csalás, megtévesztés, illetéktelen behatolás a regisztrátor rendszerébe, illetéktelen hozzáférés) [Registry Lock]
    - Hasonló veszély: DNS-szolgáltatónál történő visszaélés
- Belső információk megszerzése, belső visszaélés
- Gondatlanság, hanyagság, tájékozatlanság, tudatlanság
- Adott felső szintű domén (TLD) szabályozásával, rendszerével, működésével, gyakorlatával specifikus problémák-sérülékenységek.

Egy halovány, de akár sikerre vezető próbálkozás

Első forgatókönyv visszaélés elkövetéséhez:

Telefonon hívjuk a regisztárort:

- Informálódunk, tervezünk, felkészülünk,
- ‘nagy gáz van’ – azonnali segítséget kérünk,
- trükkösködünk: írtunk e-mailt …, az ügyfél (illetékes) telefonszámáról hívunk …

Jó esetben az eredmény: **átírják nekünk a domén névszervereit[2] – GYŐZTÜNK**.

[2] Authoritatív DNS-szervereit

Egy erőteljesebb próbálkozás

Második forgatókönyv: **CSALÁRD REGISZTRÁTORVÁLTÁS**

A totalbank.hu tulajdonosa a Totál Bank Zrt. regisztrátora X Nyrt.

- A totalbank.hu doménnevet átkérjük Y regisztrátorhoz [REGISTRY LOCK (DOMAINZÁR) NINCS BEÁLLíTVA],

- hamis okiratot (egy másolatot) benyújtva az új regisztrátorhoz.

Jelen regisztrátorunk nem tud megvédeni a visszaéléstől!!!

Figyelem: nem kell, hogy nevünkre irassuk a totalbank.hu domént, sőt, ne próbálkozzunk ezzel, mert ezzel kifejezetten gyanút kelthetünk.

Amiről még ne feledkezzünk meg: névszerver TTL-k megemelése.

Eredmény:

totalbank.hu új névszerverei

- hamis hosztnevekre (pl. https://www.totalbank.hu/, online.totalbank.hu),
- hamis mailszerverekre mutatnak,

és még azután is, hogy az authoritatív névszerverek helyre lettek állítva, még jó ideig nem sikerül minden resolverből a hamis adatokat eltávolíttatni a banknak.

Ha kellően szofisztikáltan jártunk el, akkor

- sok pénzt utalhattunk át hamis számlákon keresztül magunknak,
- de az sem semmi, ha csak személyes adatok tömegét, köztük nagyszámú jelszót szereztünk meg.

Milyen esélyünk van a sikerre?

Megjegyzések az okiratokról

Okirat lehet

- fizikai (papír)alapú,
- ennek papíralapú vagy elektronikus másolata,
- elektronikus okirat.

Okirat lehet

- aláíratlan,
- aláírt (kézjeggyel vagy kriptográfiai eljárással digitális aláírással ellátott),
- aláíratlan, de aláírásképet tartalmazó (kézzel történt aláírás másolatát tartalmazó),
- hamis aláírással (illetve hamis aláírás másolatával) ellátott.

Teljes bizonyító erejű magánokirat, közokirat (Polgári perrendtartásról szóló törvény)

Cégszerű aláírás

Példa teljes bizonyító erejű magánokiratra:

- sajátkezűleg írtam és írtam alá,
- aláírtam és két tanú hitelesítette az aláírásomat,
- cégszerűen aláírtam.

Példa nem teljes bizonyító erejű magánokiratra:

- nem sajátkezűleg írtam vagy nem írtam alá,
- nem én írtam alá, valaki más odahamisított egy én aláírásomnak látszó valamit,
- hamis valamely tanú aláírása.

Elektronikus aláírás jobb, de hamis elektronikus aláírás még megtévesztőbb lehet, mint egy hagyományos hamis aláírás.

Minősített elektronikus aláírás

- Ha nevünkben más ír alá minősített aláírással, akkor az bizony elég kellemetlen lehet.
- Ha igazán profik vagyunk, akkor minősített aláírással csalunk☺

Csalás tárháza: Hogyan is csaljunk minősített aláírással?

Tippek, tanácsok az elektronikus világban még kezdő okirathamisítóknak ☺

☹ Mi hitelesebb?

- Ha inkább csak fenekünket akarjuk védeni (egy esetleges bírósági jogvitában),
- vagy ha valóban meg akarunk győződni arról, hogy
  - valóban ügyfelünk
  - egy valóban arra jogosult felhasználója,
  - jogosultan és helyesen akar egy változtatást kezdeményezni vagy végrehajtani?

A legerősebb, legjelentősebb védelmi megoldások

- megfelelő tervezés, szabályozás, szervezettség, menedzsment
- megbízható szolgáltatók választása
- MFA
- Registry Lock
- DNSSEC

Registry Lock

Regisztrátor szintű hibáktól véd
és plusz authentikációs és authorizációs szint.

Registry Lock elterjedtsége és használata.

DNSSEC

DNS adatok meghamisítása ellen véd

DNSSEC elterjedtsége és használata.

http://www.domain.hu/statisztika/domain-counter.xml

Domain counters

TLD:	hu
timestamp:	2020-11-17T08:01:00
Current total:	804263
Current total DNSSEC:	159622
Current total IDN:	24521
Current total lock:	5

https://www.internetsociety.org/deploy360/dnssec/statistics/
https://stats.labs.apnic.net/dnssec