DOMÉNPORTFOLIÓ-MENEDZSMENT

A vállalat összes doménének egységes és átfogó kezelése, menedzsmentje, védelme

(akkor is, ha csak egyetlen doménneve van cégünknek!)

A fő problémák és veszélyforrások:

emberi és menedzsment hibák.

Károk okozói:

1. 'nem szándékos hibák' (tudatlanság, átgondolatlanság, gondatlanság)
2. visszaélések,
    a. főként csalások
        i. social engineering (megtévesztés, okirathamisítás, identity lopás stb.)
3. technikai problémák
4. technikai visszaélések.

Problémák

- Nem hosszabbított **fenntartás**.
- **Névszerver doménnevének fenntartása** nem lett meghosszabbítva.
- A doménhasználó elvesztette 'accountját' a regisztrátornál.
- A doménhasználó részéről megadott jogosult(ak) már távozott munkatárs(ak).
- A doménhasználó nem tudja ki jogosult intézkedni, nem tudja kit hatalmazott fel jogosultnak.
- A tényleges doménhasználó és a formai doménhasználó más: ez komoly komplikációkhoz vezethet.
- Illetéktelen hozzáférés vagy nem kívánt változtatás:
  - a domén zónájában,
  - a domén authoritatív névszervereiben,
  - a regisztrációs adatokban (pl. domén lopás /domain hijcacking/).
- Regisztrátor problémák;
- DNS-szolgáltató problémák.
- Sokféle más probléma is lehetséges :-(

Doménhasználó:

- **tényleges**,
- **whois szerinti**.

Miért is jó és nem jó, ha ezek eltérnek?

A vállalati doménmenedzsment, illetve menedzseletlenség jellemzői:

1. átgondolatlanság,
2. elhanyagoltság,
3. tervezetlenség,
4. szabályozatlanság,
5. felelősök kinevezésének hiánya,
6. dokumentálatlanság
7. szervezeti problémák,
8. védelmi eszközök (pl. MFA, DNSSEC), lehetőségek és szolgáltatások nem alkalmazása,

ezek eredendő oka

9. ismeret és tudás hiánya; szolgáltatói segítség hiánya,
10. ajánlások nem ismerete vagy elhanyagolása,
11. gondatlanság, hanyagság,
12. alulértékelés, a domének fontosságának/jelentőségének alábecsülése.

Registry Lock - a Szent Grál?

Registry Lock - egy könnyen rosszra vezető eszköz.

Mi az Registry Lock? Miért jó, miért rossz?

És amikor megbántuk, hogy registry lockot alkalmaztunk :-(

És amikor megbántuk, hogy nem alkalmaztunk :-(

Registry Lock és Registrar Lock

Registrar Lock - bizonyos nem kívánt műveletek ellen véd

Domain Status: **clientDeleteProhibited** https://icann.org/epp#clientDeleteProhibited
Domain Status: **clientTransferProhibited** https://icann.org/epp#clientTransferProhibited
Domain Status: **clientUpdateProhibited** https://icann.org/epp#clientUpdateProhibited

Registry Lock - bizonyos nem kívánt műveletek ellen véd

Domain Status: **serverDeleteProhibited** https://icann.org/epp#serverDeleteProhibited
Domain Status: **serverTransferProhibited** https://icann.org/epp#serverTransferProhibited
Domain Status: **serverUpdateProhibited** https://icann.org/epp#serverUpdateProhibited

Registrar Lock - regisztrátor szintjén véd, illetve regisztrátor váltás ellen is védhet

Registry Lock - regisztrátor szintje felett implementált védelem

Részleges és teljes zárolás ('zár', 'lock')

Példa: **teljes** registry lock: **.HU domainzár** (**2F**)
részleges registry lock: (ún. 1F, illetve 2F, azaz **1-, illetve 2-faktoros**) **megerősítéses eljárás** a .HU regisztrációs rendszerben

"The Domain Name Server (DNS) is the Achilles heel of the Web. The important thing is that it's managed responsibly." Tim Berners-Lee

Gondolatok a DNS-szolgáltatásról

és a domén és DNS-biztonságról

DNS service	**-**	**'afterthoughted'**
name servers	**-**	**'set and forget'**
domain and DNS security	**-**	**'neglected'**
	-	**'Terra incognita'**

Felelősök

Kontaktok (értesítési kontaktok)

Jogosultak (változtatásra jogosultak - jóváhagyók)

Értesítendők köre **ésszerűen tág és szerepkörökhöz kötött**,

Jóváhagyók köre **ésszerűen szűk és személyhez kötött**.

Kommunikációs szervezettség

- csoportcímek
- ticket kezelő

versus

- szenzitív információk gondos kezelése

Problémás megoldások, hibák, szarvashibák
- néhány példa -

- domen.hu domain értesítési címe valami@domen.hu
- megszűnt címekre menő értesítések
- alvó accountok
- spamfolderbe került értesítések
- rossz vagy hiányzó adminisztráció
- kifizetetlen számlák (lásd még: feleslegesen kifizetett /ál/számlák)

Ötletek, megoldások

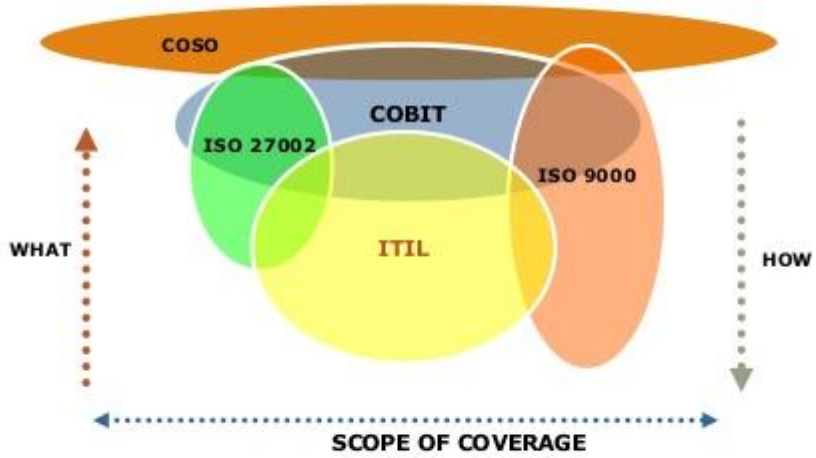
- regisztrációs 'szervizdoménnév' és speciális email címek
- külső felügyelet
- monitorozás
- határozatlan időre szóló doménfenntartás
- hosszú időre (10 évre) kifizetett doménfenntartás
- különös értesítési kívánságok (klasszikus megoldások: postai értesítés, telefonhívás stb.)
- BCP és DRP-be beemelni a domén és DNS védelmet

Doménbiztonság

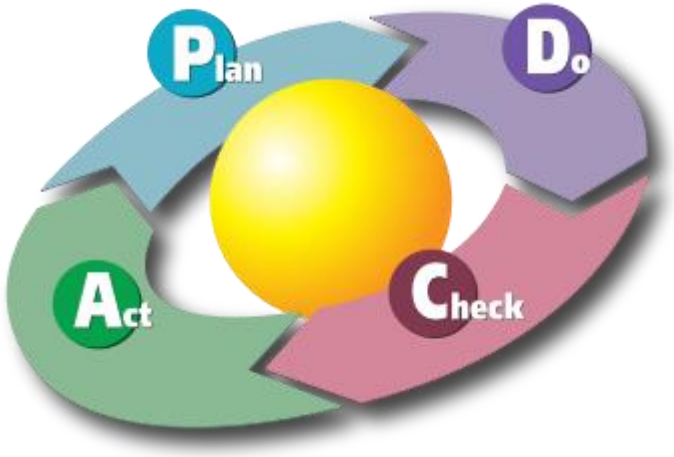
- Doménfenntartás folytonossága
- Domén lopás elleni védelem
- Authoritatív névszerver módosítás elleni védelem
- menedzsmentfelületek hozzáférésének biztonsága (MFA stb.)
- regisztrátor és más szereplők gondos és jó megválasztása

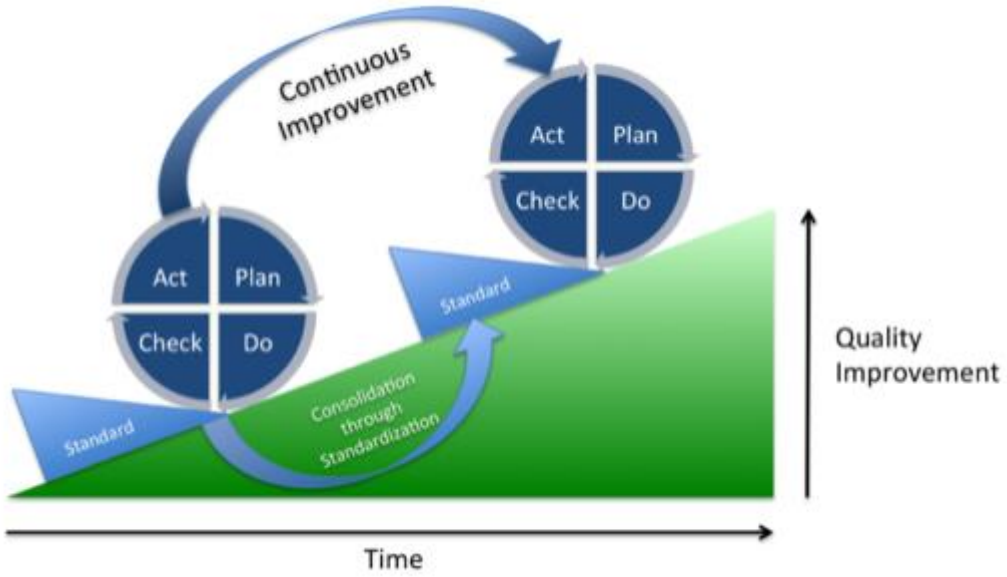
- **DNS-biztonság**
- DNSSEC
- menedzsmentfelületek hozzáférésének biztonsága (MFA stb.)
- jó DNS szolgáltatás/jó DNS szolgáltató(k)

COBIT and Other IT Governance Frameworks



8





https://en.wikipedia.org/wiki/PDCA

Domain Portfolio Management as a Service

- Determine corporate objectives for domain management
- Adopt enterprise-wide policies and procedures
- Work with corporate subsidiaries and divisions to consolidate domain names
- Access and authorization management, contact management
- Domain Name Registrations and Renewals
- Domain Name Registration Modifications and Transfers
- Domain Name Acquisitions & Disposals
- Domain Name Portfolio Audits and Gap Analysis
- Risk assessment
- Risk management
- Domain Name Security
- Secure and protect valuable domains
- Portfolio evaluation and cleaning
- Intellectual property infringement
- DNS Services
- DNS Security
- Domain Name Monitoring
- Alerting
- Incident management and emergency help
- Domain Name Recovery
- Accounting, payments
- Support
- Training
- …

A legjobb eszközök is vezethetnek problémához, ha nem jól alkalmazzuk őket:

ilyenek pl. a DNSSEC és a Registry Lock.

Major DNSSEC Outages and Validation Failures
https://ianix.com/pub/dnssec-outages.html

A biztonság érdekében azonban ezen eszközökre szükségünk lehet, és sokszor esetben van is.

Saját erőre és tudásra nem elég támaszkodni.

Szolgáltatók tudása rendszerint nem univerzális, szükségünk lehet speciális szolgáltatókra.

Domén biztonság a gyakorlatban

Kockázat értékelés	Mit ér meg nekünk egy domain biztonsága?
Kockázat kezelés	Ignoráltuk a kockázatot.
Domain portfolio management	Kinek van ilyen?
Szervezeti szabályozás	Domainnevek ebből kimaradtak.
Személyi felelősségek	nem hosszabbított domain nevek névszerver nem hosszabbított domainneve
Üzletfolytossági terv (BCP) **Katasztrófaterv (DRP)**	minden működik, csak éppen semmi
Contingency Planning	Mit kezdjünk most ezzel?
Biztonsági tervezés, biztonsági politika	Hallotunk már a DNS spoofingról meg az DNS amplifikációs támadásról is. De erről még nem. - Erre nem gondoltunk. Ezt is védeni kellett volna?
Dokumentáció	Fogalmunk sincs ki a felelős, honnan tudjuk?
Monitorozás, riasztások	Valami baj van, de nem tudunk róla. Rendszerünk észleli, de nincs intézkedés.
Ellenőrzés, audit	Erre nem is gondoltunk! Ezzel nem számoltunk! Ez nem úgy van, ahogy kéne!