Biztonságos architektúrák

Különvélemény a nagyvállalatok biztonságáról

László István
Információbiztonsági kockázatmenedzser
istvan.laszlo@kh.hu

Biztonságos architektúra – mi célból?

Kockázatok leghatékonyabb menedzseléséhez találjuk meg a legjobb utat, a legjobb megoldást a lehetségesek közül.

- a védekezés nagyon idő- és erőforrásigényes
- amit megspórolunk a biztonságon, azt csak áthárítjuk. De a költségek és a felelősség a szervezeten belül maradnak.

Biztonságos architektúra – hogyan?

- a biztonsági architektúrák is gyenge lábakon

- a királyok meztelenek: nincsenek elég jó termékcsaládok, de vannak nagyon jó alapeszközök.
- mindig van a megoldásainknak achilleszi sarka, pl. az érzékeny fájlok védelme. Fontos hangsúlyozni, hogy egy védelmi bástya eleshet, de nem mindegyik. Ennek előfeltétele a szoftver és architektúra összetétel-elemzés alapján alkalmazott kontrollkörnyezet.

Miért nem szereti az IT az IT biztonságot?

Telepítéskor

- IT: mindent kinyit, alapértelmezett telepítés, azonnal működjön!
- IRM: először minimumot, utána ami szükséges. Minimum konfiguráció, szabványok betartása, CIS, tanúsítványok és kulcsok, rejtjelezés. Hardening, hardening, hardening, majd teszt, dokumentáció és bekapcsolni, ami még szükséges.

Kapcsolatok kiépítésekor

- IT: nyisd ki ezt a port-ot!
- IRM: milyen szolgáltatást veszel igénybe és kitől?

Miért nem szereti az IT az IT biztonságot?

- Felelősségek értelmezése

  „Nem te, hanem a te nevedben”

Fordított logika

- IT: sakk
- Információ biztonság: francia sakk

Biztonságos architektúrák - üzemeltetés

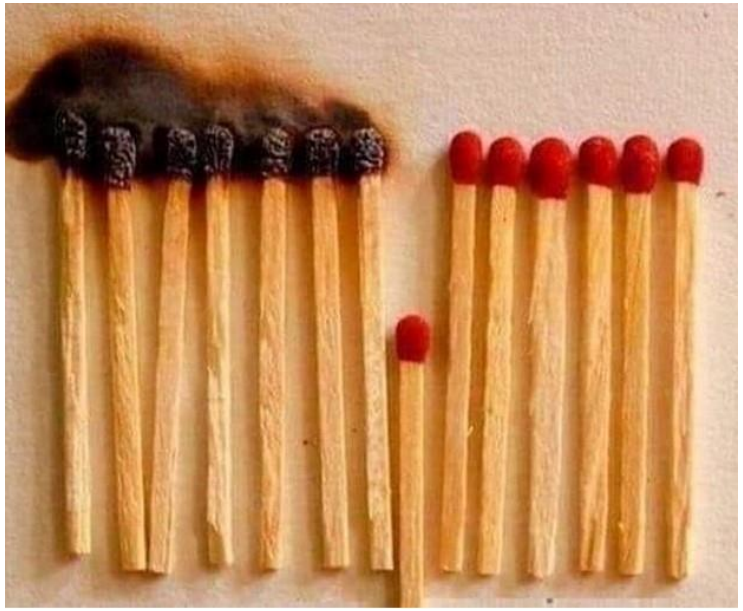
- Support - nem véd meg a sérülékenységektől és azok kihasználásától

- Frissítés vs. maintenace release - azonnal telepíteni?
- Release stratégia, major/minor release-ek tervezése

- Hogyan frissítenek a nagyok? Melyek a legjobb gyakorlatok?

Biztonságos architektúra - alapelv

Minden katasztrófához vagy incidenshez több hibán, hatástalan kontrollon keresztül vezet az út.



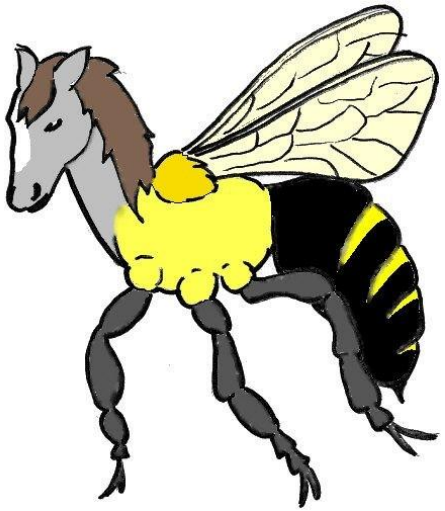
Többszörös, egymástól független kontrollok beépítése hatékony.

Biztonságos architektúra - alapelemek

- **architektúra elemek biztonsági funkciói**: diódák, adat proxy-, CDR, XML processzor, átjárók (WAF), naplózás és monitorozás, biztonságos API fejlesztés, többfaktoros authentikáció stb.

- **milyen kontrollokat valósítanak meg ezek a fogalmak**?

mi az, hogy gateway, WAF, proxy? Sztenderdek, protokollok granulált kikényszerítése pl. TLS, SMTP, input validáció, erőforrás és munkamenet menedzsment, OWASP csúcs-sérülékenységek elleni védelem?



Biztonságos architektúra - jellemzői

1. átlátható minden pillanatban meg tudjuk mondani mi történik a rendszerben kinek és minek a hatására, milyen eredménnyel.

2. van immunrendszere eredményesen gátolja meg, hogy 0. day, vagyis ismeretlen támadások kárt okozhassanak. Önmaga képes a védelmet ellátni, nem külső biztonsági elemekre támaszkodik kizárólag.

Alkalmazás szerves részeként van kezelve minden komponens.

3. egyszerű elemekből áll (SOA felépíthető komplex elemekből is) olyan elemekből épül fel, amelynek ismertek a szoftver függőségei, pl. frissíthető a db alatt egy library, ehhez rendelkezésre áll „maintenence release”.

Köszönöm a figyelmet!

László István, Információbiztonsági kockázatmenedzser

istvan.laszlo@kh.hu