Információbiztonság-tudatosság fejlesztési és mérési lehetőségei vállalati környezetben

Kiberbiztonsági Szakmérnök képzés

Szántó Lajos

Témavezető:
Dr. Póser Valéria

Külső Konzulens:
Szarvák Anikó

Információbiztonság-tudatosság

- Az információbiztonság szerves része kell, hogy legyen, nem függ eszköztől
- Social engineering fogalma, jelentősége
- Fejleszteni kell, ez nem mindig egyértelmű és egyszerű feladat.
- Megoldási javaslatok. Védekezési, kockázat csökkentési módszerek.

Az ember jelentősége

- Adatkezelés
- Közösségi média
- Home office
- Az emberi természet jellemzői
- Jellemző támadási formák és védekezések

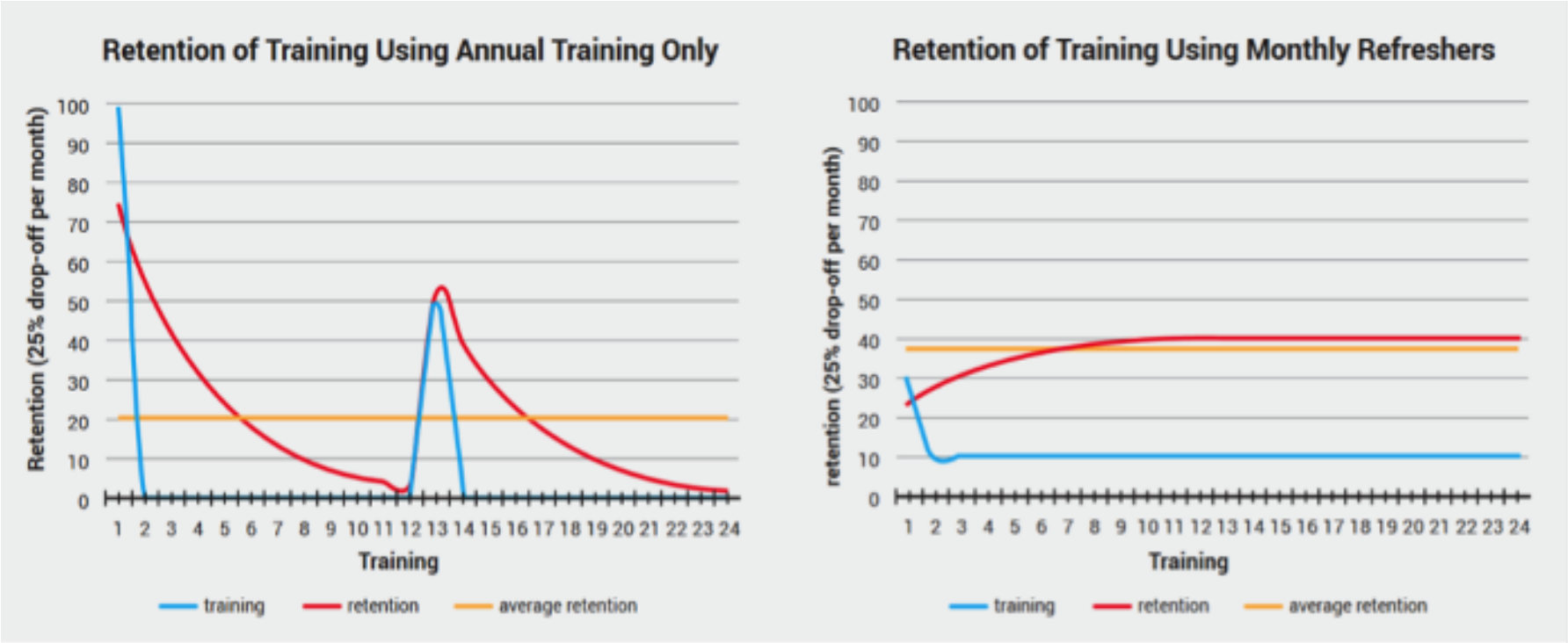
Emberi kockázat	Lehetséges social engineer támadási módszer	Oktatás segítségével a kockázat csökkentésének egy lehetséges módja
beléptető rendszer nem megfelelő használata	szoros követés besurranás	Példákkal, dokumentációkkal alátámasztva kell képezni a kollégákat az épületbe való belépés menetéről. A legjobb, videóval fotóval illusztrálva.
Ajtók záródására nem figyel	szoros követés besurranás	Az adatvédelem fizikai oldalát kell bemutatni képzés során
Nem figyel a képernyő, mobil eltakarására	rápillantás	El kell magyarázni, miért fontos eltakarni egy kijelzöt, amin kényes adatok jelennek meg, figyelni kell a körülötte lévő emberekre. Ez nem csak munkahelyi környezetre vonatkozhat (utazás).

Megoldási javaslat

A biztonságtudatosság fejlesztésének kulcsa:

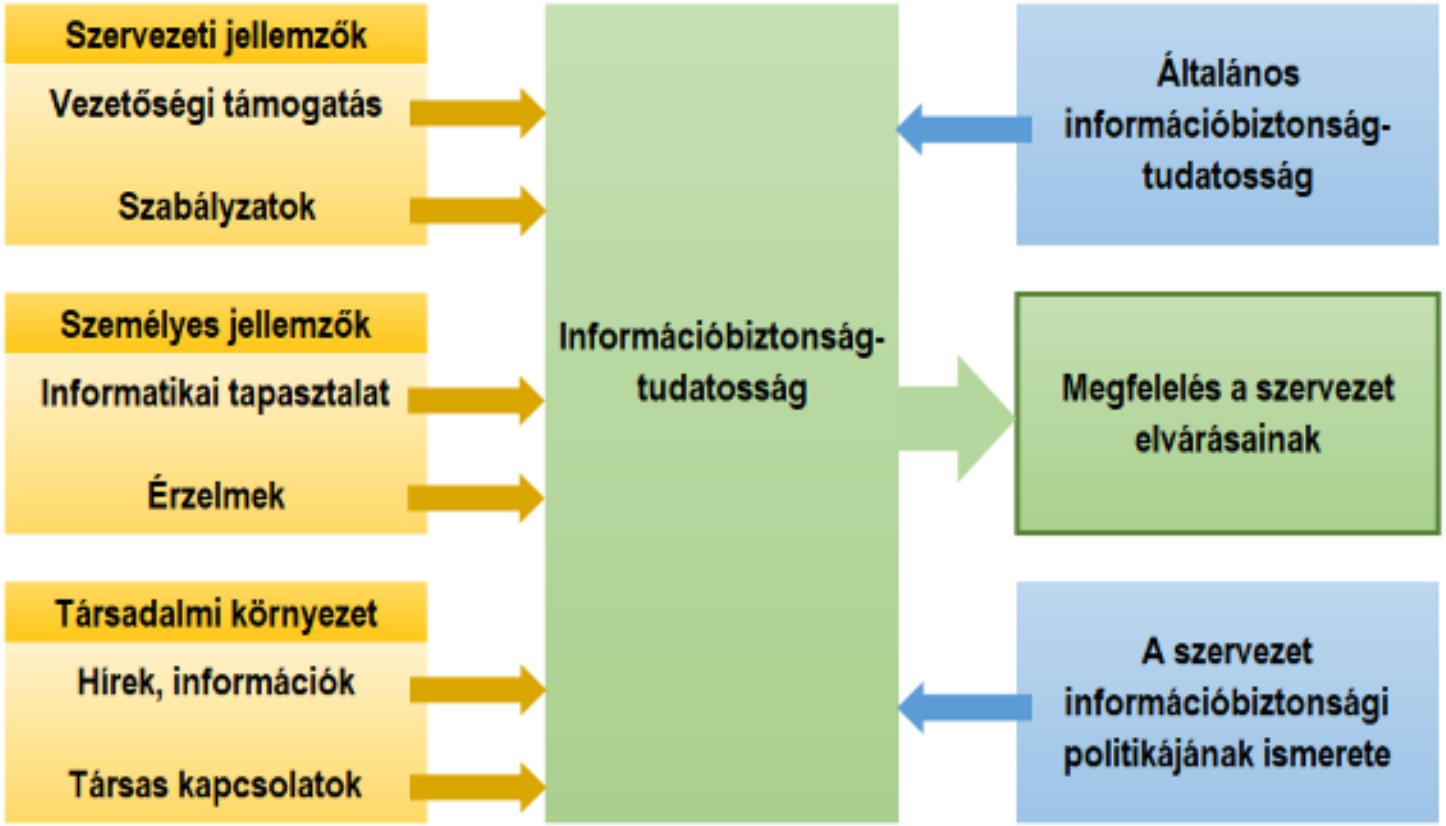
- Kockázatok
  kockázatok feltárása
- Szabályozási környezet
  belső szabályozások, szabványok
- Biztonságtudatossági oktatás
  sokfajta képzési forma, lényeges a célcsoport
- Biztonságtudatossági program
  források, használható eszközök, felelősség, visszamérés

Az eredmény egy magasabb szintű információbiztonsági-tudatosság



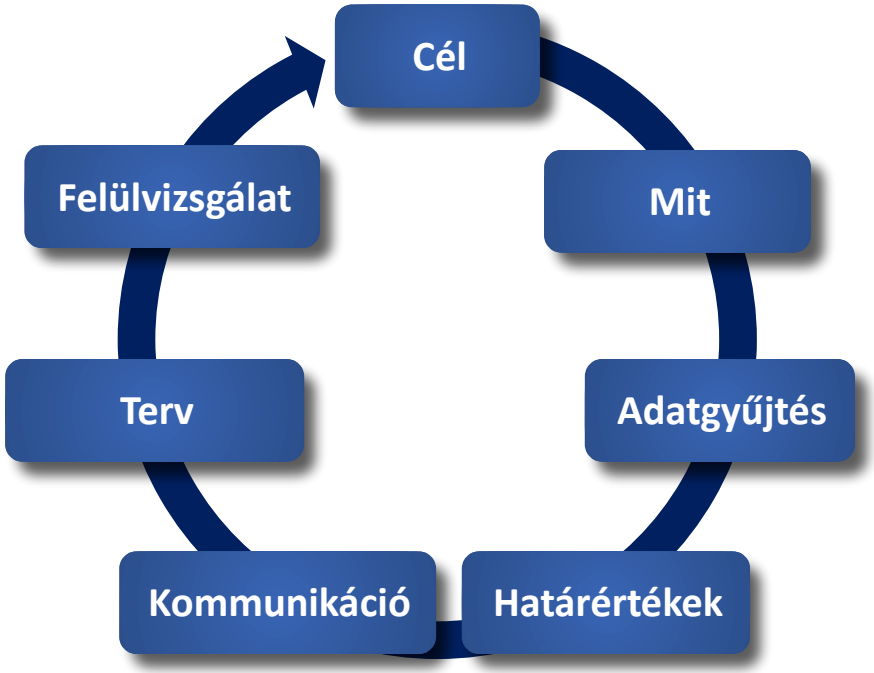
Forrás: https://resources.infosecinstitute.com/topic/building-serialized-phishing-simulation-and-security-awareness-campaigns/

Mi befolyásolja a biztonságtudatos magatartást?



Mérés

- Kirkpatrik-modell: oktatás hatékonyságának vizsgálata
- Mérőszámok meghatározása (SANS)
- Audit



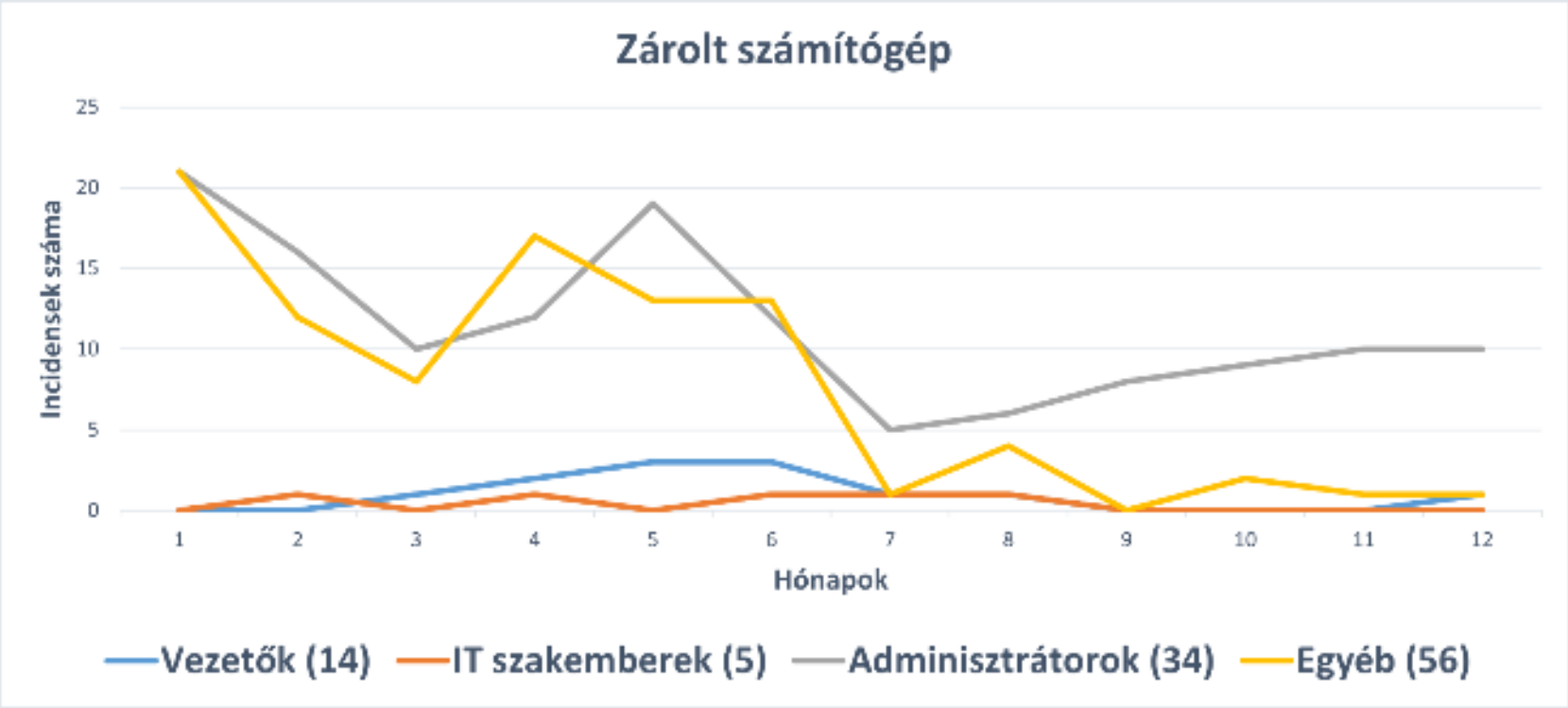
Mérés

- Nem könnyű mérni.
  - szabályzat követése?
  - szervezetet?
  - a programokat?
  - az oktatást?
- Egy lehetséges megvalósítás:
  - valós problémák számszerűsítése, összegzése
  - mi a fontos, mi jellemző a szervezetre?
  - rendszeres
  - csoportokat

Szervezet specifikus jellemzők

IT biztonság-tudatossági problémák Adatgyűjtés: 2021. év	Vezetők (14)												
	Jan	Feb	Már	Ápr	Máj	Jún	Júl	Aug	Sze	Okt	Nov	Dec	Átlag
Frissítések telepítésének engedélyezése	3	3	4	5	6	10	2	3	4	5	6	4	4,6
Zárolt számítógép	0	0	1	2	3	3	1	1	0	0	0	1	1,0
Kidobott érzékeny dokumentum	0	0	0	0	1	1	0	0	0	0	0	0	0,2
Kísérő nélküli személyek	0	0	0	0	0	0	0	0	0	0	0	0	0,0
Ellopott jelszó	0	0	0	0	0	0	0	0	0	0	0	0	0,0
Elküldött lánclevelek	0	0	0	0	0	1	0	0	0	0	0	0	0,1
Adathalász e-mailek	2	3	4	5	5	5	3	2	2	1	0	0	2,7
Megtévesztéses támadás	0	0	0	0	1	0	0	0	0	0	0	0	0,1
Beléptető rendszerek helytelen használata	3	4	4	5	3	4	5	6	4	3	3	3	3,9
Elvesztett adathordozó	0	0	0	1	0	0	0	0	0	0	0	0	0,1
Csali adathordozó használata	0	0	0	0	0	0	0	0	0	0	0	0	0,0
Szabályzatok ismeretének hiánya	1	2	2	1	1	2	2	2	2	1	3	1	1,7
Információmegosztás közösségi oldalon	0	0	1	0	0	1	0	0	0	0	0	1	0,3
Közös nyomtatóban hagyott dokumentumok	0	0	0	0	0	0	0	0	1	0	0	0	0,1

Szervezet specifikus jellemzők



Köszönöm a figyelmet!