Informatikai biztonság és Bizalom

A két fogalom viszonya – kicsit körbejárva.

Horváth Gábor (civil felhasználó)

Bizalom: hit a saját pozitív elvárásainkban, hogy személyek, szervezetek, rendszerek, stb. a számunkra elvárt kedvező módon fognak viselkedni.

Könnyű elveszíteni, nehéz visszaszerezni, a "hit" szó ellenére hosszú távon racionális fogalom.

1, **Trivialitások**

Információbiztonság

- üzembiztonság: a rendszerem működni fog, azok és csak azok számára használható, akiknek szánva van
- adatbiztonság: az adataim elérhetőek, azok és csak azok számára érhetők el, akiknek szánva van

Ebben szeretnék bízni. A bizalom akkor sérül, ha ez nem teljesül.

Kikben is kell(ene) bíznom?

- A felhasználóimban, kollégáimban,
- A rendszerek gyártóiban (hardware és software)
- Az alkalmazott algoritmusokban,
- A felhasznált szolgáltatások szolgáltatóiban,
- Akikben a szabályozási környezet miatt bíznom kell.

2. **Kis kitérő – az egyik véglet: a fundamentalisták**

"Ne bízz meg senkiben! Ez volt az első szabály, amit megtanultunk."

A keményvonalasok szerint a bizalomnak az informatikai biztonságban
semmi szerepe sincs:

- a kritikus pontokon (pl. titkosítás):
  - csak matematikai módszerekkel igazolt algoritmusok
  - csak eseménytér-tesztelt, nyílt forráskódú implementációk

- csak a személyes azonosítás lehet egy tanúsítványlánc eleje
  (PGP kulcs cserélő parti)

BitCoin:
- csak a megismételhetetlen mennyiségű számítás lehet az időbeli folytonosság garanciája
- csak az tarthat össze egy közösséget, hogy a többségnek nem érdeke a feloszlás

3. Kis kitérő - a másik véglet: az egységsugarú felhasználó

Mindenkiben bízunk, mindenki értünk van, ha mégis van itt rossz ember, akkor Állam bácsi megvéd, meg különben is, a gyártók nem hülyegyerekek, nekik is érdekük, hogy menjen a szekér rendben.

Nem alap nélküli a hit, pl. a repülés biztonságban, stb valami ilyesmi tapasztalható - még.

Mindenre ráklikkel, mindent kiposztol, letölt, kipróbál és elhisz. Ha néhány nap (óra?) alatt nem válna a gépe működésképtelenné, nem veszítené el az adatait (jobb esetben a bankszámlája és a lakása érintetlen marad) akkor ez az előadás érdektelen lenne.

Ő egyébként a social hacking tipikus célpontja is, az is az indokolatlan bizalom következménye...

Ha figyelmezteted: „nekem nincsenek titkaim, becsületes embernek nincsen félnivalója”

4, **Akikben bíznom kellene : a Felhasználók - I.**

Mi veszélyezteti a bizalmat?

a, Szándékos rosszindulat - pl. kiszivárogtatás, visszaélés

> Jogi következményekkel biztosíthatom magam.
> A "tettes" szükségszerűen kiderül, ezt tudatosan vállalja az elkövető – már elég rossz a helyzet, ha ilyen előfordul...

b, A felhasználó hanyag magatartása

- próbálok képzéssel kevésbe hanyag felhasználót csinálni és megbízok benne

- nem bízok meg benne. Technikai megoldást keresek a problémára.

5, **Akikben bíznom kellene : a Felhasználók - II.**

Tehát nem bízok meg benne. Mit tehetek?

-majd a rendszer policy kikényszeríti a felhasználói fegyelmet
(de egy hosszú és gyakran változó jelszót mindenki felír és nem megjegyez – romlik a biztonság)
- kisebb hibalehetőségű megoldásokat használok (pl. biometrikus azonosítás)
- olyan munkaszervezést, munkafolyamatok találok ki, amik az egy emberes visszaéléseket nem teszik lehetővé, és ezeket a folyamatokat implementálom a rendszereimben. Ide tartoznak:

-- banki rendszerekben egy felhasználó nem tud végigvinni egy sikkasztáshoz vezető tranzakciót,
-- éles adatot csak az lát, akinek a munkaköréhez tartozik az adott adathalmaz (alkalmazásokban belső hozzáférés ellenőrzés, adat deperzonalizáció a fejlesztői rendszerekben, ...)
-- olyan területre logolás, amit az elkövető nem tud utólag befolyásolni
-- kilépett felhasználó jogosultságainak egy lépésben történő azonnali visszavonása

6, **Akikben bíznom kellene: a Gyártók - I.**

Most komolyan: kapok egy levelet, abban van egy link valami érdekes szöveggel. Ráklikkelek, mire minden figyelmeztetés nélkül elindul egy progi, ami:
- kémprogramot telepít a gépemre, ami minden linket, billentyűleütést továbbít,
- titkosítja a file-jaimat és csak pénzért cserébe kódolja vissza őket,
- leveleket küldözget szanaszét a nevemben,
- erőforrás-igényes számításokat futtat a gépemen, ...

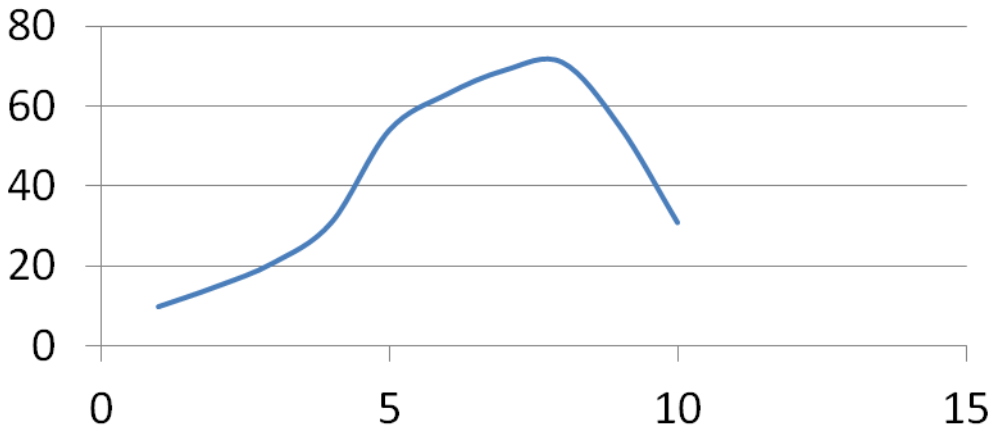
EZ NORMÁLIS? NEM.

Mondjuk ki: ez egy piszok nagy tervezési hiba! Amit azonnal, ingyen és sűrű bocsánatkérés közben kellene javítani.

Helyette: ez egy természetes jelenség, használjunk malware, spyware meg mindenféle vírus irtót és detektort, personal ids-t meg tűzfalat - és fizessük elő a minél gyakoribb frissítéseket is!

7, **Akikben bíznom kellene: a Gyártók - II.**

Megfogalmazódik egy csúnya gyanú: nézzük csak pl. a vírusbusiness bevételeit az okozott károk függvényében:



Ha kicsi a víruskár, senki nem vesz vírusirtót.
Ha nagy a víruskár, kihátrálnak a nagy megrendelők a platform mögül.

A maximum körül mozgunk. Sok év óta, stabilan. Valami ott tartja a rendszert ...
Lehet, hogy nem a véletlen.

8, **Akikben bíznom kellene: a Gyártók - III.**

Nézzünk egy másik dolgot - két hasonló gyártó, két hasonló termék,
fele-fele piaci részesedés – két játékelméleti stratégia:

1. gyártó: a nyereséget a minőségbe forgatja vissza – így akarja legyőzni a másikat.

2. gyártó: a nyereséget az árfolyam felfuttatására fordítja, hitelt vesz fel, megveszi az 1. gyártót és bezárja. Monopolhelyzete lesz, a hitelt a termék árának növeléséből fizeti vissza. A monopolhelyzet és a fejlesztéstől elvett pénz szükségszerűen a minőség romlását eredményezi.

2. gyártó B verzió: a nyereséget korrupcióra fordítja, megnyeri az államigazgatást, a nagy vásárlókat, a többiek meg mennek utána...

Az offshore tulajdonláncok a 2. gyártó helyzetét nagyon megkönnyítik,
szinte erre a pályára kényszerítik! Ez a szabályozási környezet felelőssége.

9, **Akikben bíznom kellene: az algoritmusok**

Vannak elég jó algoritmusok, azonosításban, titkosításban, de a munkaszervezésben vagy a logolásban is! A matematikában és a logikában lehet bízni....

Sajnos ehhez képzett és fegyelmezett programozók kellenek és olyan munkakörnyezet, ahol lehetővé teszik az igényes munkát. A rossz és a jó titkosítás elsőre ugyanúgy néz ki. Ahol az a cél, hogy úgy nézzen ki, mintha - ahol az a fő cél, hogy a user fizessen, aztán mindegy, hogyan érzi magát a használat során - ott nem fognak korrekt algoritmusokkal és korrekt programozókkal dolgozni.
De ez már a gyártói bizalom.

A tapasztalat azt mutatja, hogy a fejlődő világ gyorstalpalón kiképzett, olcsó programozói a grafikus fejlesztőrendszerekben összeklikkelt alkalmazásaikkal nettó informatikai szemetet termelnek. Erőforrás-pazarló, megbízhatatlan megoldások születnek, amik a csilivili külső dacára belül gyakran meghaladott, célszerűtlen megoldásokat tartalmaznak.

10, **Akikben bízni kellene - a szolgáltatók**

Kettős fronthatás érvényesül:

1, A szabályozási környezet ide keményen belenyúl: kötelezve vannak bizonyos adatok gyűjtésére, átadására, kereshetővé tételére, fekete dobozok elhelyezésére ...
Konkrét adatok kiadása csak bírói engedélyre. Elvileg. Gyakorlatilag nem.

Üzembiztonság: amit a verseny kikényszerít.

2, A felhasználók adatainak saját célú felhasználása

Amit beismernek (és jóváhagyólag alá is íratnak): a felhasználók adatainak felindexelése és célzott reklámokban való felhasználása.

Amitől tartunk: ipari kémkedés. Magánemberként akár meg is bízhatunk bennük, de olyan cégként, amelyiknek vannak kutatási, fejlesztési eredményei: nagyon nagy hiba volna.

11, **Akikben bízni kellene - a szabályozási környezet**

A sokféle titkos, egyenruhás, civil, stb. állami és állam közeli szervezetre gondolok.

Akik egytől egyik hivatalosan minket védenek, értünk vannak. Akkor mi itt a bibi?
Ezzel két bibi van:

1, Ha felsorolnánk, hogy hányszor buktak le csúnyán, hogy pénzért vagy politikai nyomásra is felhasználták a "terrorizmus elleni küzdelem" jelszavával kapott lehetőségeiket, akkor még 3 nap múlva is itt ülnénk. És itt még van rosszabb hírem: általában nem kísérte semmilyen felelősségre vonás ezeket a botrányokat. Tehát nem az volt a „baj”, hogy így történt, hanem hogy kiderült. Tehát a bizalom mérhetetlenül kicsi.

2, A nekik adott informatikai lehetőségeket még ketten használják saját céljaikra:
boldog és boldogtalan.
Sőt, árulják is. Aztán néha annyira balfácánok, hogy az egész ki is derül. (pl. Hacking Team)
Már egy ilyen cég puszta léte is felveti, hogy maga a szabályozási környezet rossz.
(A legális vásárlók között voltak hivatalosan terroristaként nyilvántartottak is.)

Szóval a bizalom a szabályozási környezetben (és annak résztvevőiben is)
teljesen indokolatlan.

De miért beszélünk erről? I.

(mint a két öreg a Muppet show páholyában ...)

Mert a modellszámítások azt mutatják, hogy előbb-utóbb probléma lesz.
A megbízhatatlanság irányába a rendszer letörési karakterisztikával rendelkezik.
A visszacsatolás (pl. automatikus update eljárások) egyre erősebb oszcillációt okozhatnak – már eddig is csak a mázli segített egy-két esetben.

Készüljünk fel, hogy:
- probléma esetén nálunk lassabban jelentkezzen, vagy gyengébb legyen a hatás,
- legyenek készen eljárásaink, hogyan fogunk talpra állni – ne akkor töprengjünk.

A mi gondolataink, szemléletünk az a „katasztrófa-biztos génbank”, amiből a talpra állás lehetséges. Ha meg valaki már előtte komolyan vesz minket és szabályozási módszerekkel megállítják a megbízhatatlanság felé vezető úton a rendszereket, annál jobb.

De miért beszélünk erről? II.

Amikor vásárolunk egy megoldást, egy rendszert, akkor mi alapján döntünk?

1, Tudás
2, Ár
3, Bizalom.

Az téves gondolkodás, hogy a bizalmat egy márkával azonosítjuk. Hogy ha „márkát” veszünk, akkor az megbízható, ha meg nem márkát veszünk, akkor az lutri.

A tények azt mondják, amit a józan ész (amire egyébként nem hallgatunk):

- vannak márkák, amik a megbízhatóságra építették fel az image-et, és egy-egy baleset, botrány, nem hízelgő teszt esetén az elvárt belső korrekciók megtörténnek,
- és vannak márkák, akik agresszív marketinggel próbálják elnyomni a kritikus hangokat, esetleg egy 4. tényezőt is beviszek az értékesítésbe (korrupció, márkára szabott beszerzés, informatikai vezetők meggyőzése)

Ne féljünk kimondani, hogy egy nagy név, egy divatos technológia pocsék minőséget is takarhat – a saját érdekünk és a cég érdeke is, ha nem hiszünk el mindent.

Mit tehetünk?

Legyen kicsit erősebb a zár, mint a szomszédnak. Pár ötlet:

-legyünk tudatos vásárlók, nézzük meg a független teszteket döntés előtt,

-vegyük komolyan a központi desktop kezelést, Micike ne legyen admin a gépén

-vegyük komolyan a mentéseket, a visszatöltési tesztek 40%-a végződik hibára

-ne bízzunk meg vakon az automatikus update-ekben. Először a support nézze meg, hogy jól sült-e el, aztán engedje csak rá a cég termelő gépeire

-ne bízzunk meg a külső adattárolókban és levelezőkben (ingyen ebéd meg pláne nincsen, ilyet megbízhatóan nyújtani drága mulatság, kifizetjük ezt mi, csak nem tudjuk)

-képezzük a munkatársakat, mondjuk el nekik, hogy mi az a céges adatvagyon is mit nem szabad vele csinálni.

-képezzük az informatikai vezetőket, és mondjuk el nekik, hogy a kockázatvállalás is pénzbe kerül. Lehet, hogy egy kis takarékosság végül nagy extra kiadással jár majd.

Végül…

Egy ismert tanácsadó cég előrejelzésében azt a valószínűséget, hogy a következő 5 évben világméretű adatvesztés vagy működési zavar fordulhat elő az informatikai rendszerekben, a Windows10 piacra kerülésével 20%-ról 40%-ra módosította.

Egy feltétellel: ha nem jelenik meg új szereplő a desktop piacon.

De miért ne jelenne meg? Már az ipari területeknek (erőművek, közművek, légiforgalom, hadsereg, banki tranzakciókezelés, stb) is szüksége van gyors és tetszetős grafikus felületekre. Nagyon megbízható platformon. Miért ne lehetne azt máshol is, akár otthon is használni?

Köszönöm a figyelmet!