



Adatbiztonság, Adatvédelem

Adatvédelem bitek szintjén és
adatvédelmi alapok



Adatvédelem a mindennapokban

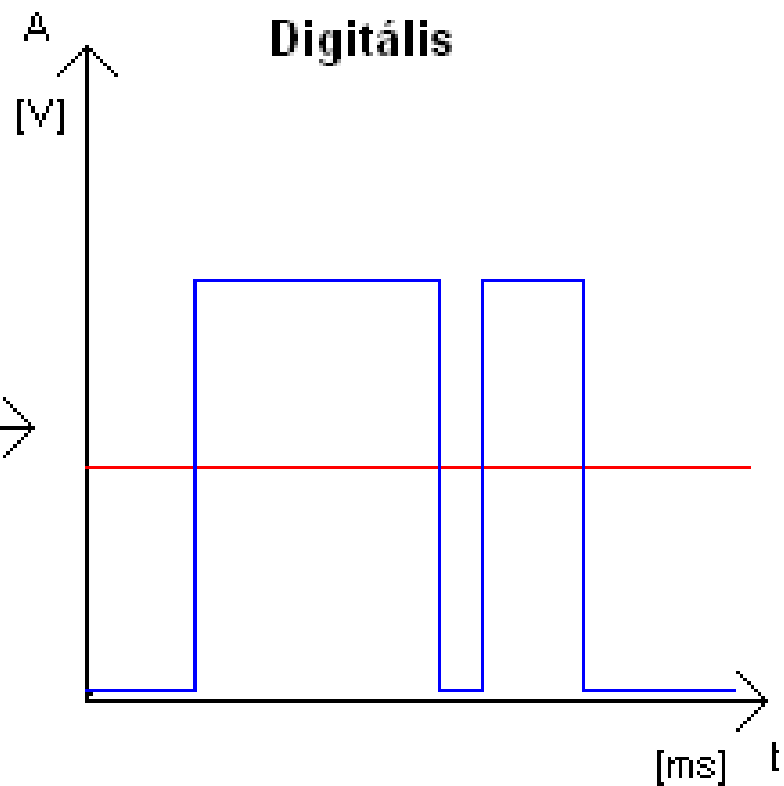
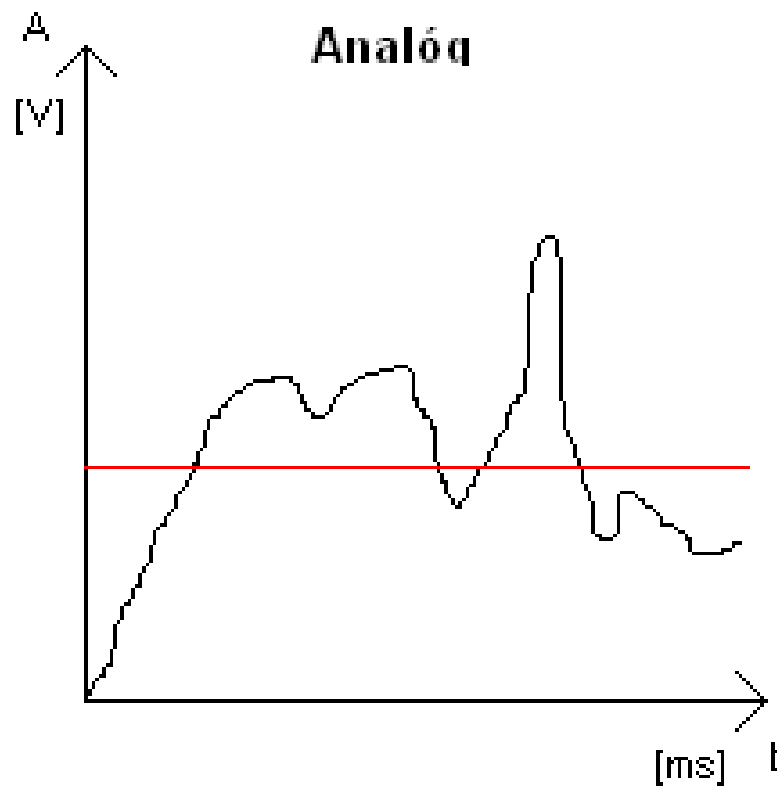
- Minden digitális kommunikációra alkalmas eszköz rendelkezik adatvédelmi megoldásokkal.
- Erre azért van szükség, mert a való világ (nem a műsor!) inkább analóg természetű, így a bináris jelsorozatunkat valamilyen „kézzel” fogható fizikai mennyiséggé kell konvertálnunk.
- Ez átvitel során megsérülhet.



Analóg jel vs. Digitális jel

- Az analóg jel egy folyamatosan változó jel, idő és amplitúdó szerint egyaránt.
- Leginkább abban különbözik a digitális jeltől, hogy az apró ingadozásoknak, hullámzásoknak is van jelentésük.
- A digitális jel valamely változó jelenségnek, vagy fizikai mennyiségnek diszkrét (nem folytonos), megszámlálhatóan felaprózott, s így számokkal felírt értékein alapul.

Analóg vs. Digitális Jel





Bináris adatátviteli csatorna

- A bináris adatátviteli csatorna egy olyan csatorna, ahol a digitális jelsorozatunk közlekedik valamilyen fizikailag is mérhető módon.
- Jelsorozat: feszültség változás, frekvencia, amplitúdó moduláció, egyéb megoldások...
- Legalapvetőbb megoldás: feszültség szint változtatás.

Feszültség alapú átvitel

- ▶ 3 logikai jelszint család: TTL; CMOS; CMOS 3,3v

Paraméter	TTL	CMOS	CMOS 3,3V
U_{beL}	$\leq 0,8 \text{ V}$	$\leq 1,5 \text{ V}$	$\leq 0,99 \text{ V}$
U_{beH}	$\geq 2 \text{ V}$	$\geq 3,5 \text{ V}$	$\geq 2,31 \text{ V}$
U_{kiL}	$\leq 0.4 \text{ V}$	$\leq 0 \text{ V}$	$\leq 0 \text{ V}$
U_{kiH}	$\geq 3.6 \text{ V}$	$\geq 5 \text{ V}$	$\geq 3,3 \text{ V}$

Feszültség alapú átvitel

- „Piece of cake” nehézségű implementálni
- Beépítetten van némi tolerancia
- Kábelhossz és illesztési problémák miatt azonban érzékeny a rendszer.
- Halmozottan igaz a dolog 3,3V rendszereknél.
- További hibavédelem szükséges, amely megvalósítását a protokollban kell(ene) megoldani.
- Ez minden átviteli rendszerre igaz

Mennyi védelem szükséges?

- Mondóka:
 - Egy védelem nem védelem
 - Két védelem fél védelem
 - Négy védelem egy védelem
 - Egy védelem nem védelem...☺
- Végtelenségig folytatható, mindig a szituáció határozza meg. Univerzális szabály nincs.



Hibavédelmi eljárások

- Rossz kódszó felismerése, majd jelzés a küldőnek, hogy küldje újra az adatot
- Felismerés: speciálisan megválasztott kódszavakkal
- Hibajavító kódolással.
- Kódszó: átvitelre szánt adat egy részlete. Lehet változó és fix hosszúságú.

Speciálisan megválasztott kódszavakra példa

➤ Példa:

- 3 állapotot akarunk megkülönböztetni.
- 3 állapothoz 2 bit kellene minimum.
- Hibavédelem miatt használunk 4-et. Ekkor a kódszavaink:
 - 0000 -> 1. állapot
 - 1111 -> 2. állapot
 - 0110 -> 3. állapot.

Dr. Zoidberg véleménye a példámról





Speciálisan megválasztott kódszavakra példa

- Előny:
 - Egyszerű módszer
- Hátrány:
 - Túl nagy a „veszteség”, mivel n bit adat esetén 2^n kódszavak kellene.
- Vannak jobb megoldások...

1-az N-ből kód

- N állapot esetén N bites kódszavak
- Minden kódszóban csak egy darab 0 van
- Ez a 0 a legkisebb helyi értéken helyezkedik el.
- Példa 1-a 4-ből kódra:
 - 1110
 - 1101
 - 1011
 - 0111
- Gond: Nem éppen takarékos. 32 állapothoz 32 bites kód

Paritás bit bevezetésével

- Paritás: párosság vizsgálata.
- A kódszavakat kiegészítjük +1 bittel
- A +1 bit a kódszóban található egyesek párosságáról hordoz információt.
- 0-val vagy 1-el jelölt párosság eldöntése a felhasználón múlik.
- A paritás bit általában az információ végén helyezkedik el.

Példa 3 bites rendszerre

- 1-el jelöljük a páros darab 1-et tartalmazó kódokat.
- A csupa 0-át tartalmazó kód páros

Eredeti szó	Paritás	Kiegészített
000	1	0001
001	0	0010
010	0	0100
011	1	0111
100	0	1000
101	1	1011
110	1	1101
111	0	1110



Paritás

- +1 bit bevezetése „csak” 1 bit eltérés jelzésére jó
- További paritás bitek adhatóak tetszés szerint a kódhoz.

Ciklikus redundancia vizsgálattal

- CRC
- Redundancia: küldött bitek és ténylegesen fogadott bitek különbsége.
- Különböző HASH (ellenőrző összeg) algoritmusokkal valósul meg.
 - Népszerű algoritmusok: MD5, SHA1, SHA256, CRC32
- Részletesen ezekről később lesz szó



Vissza egy kicsit az analóg jelekhez

- Átviteli rendszerek esetén ritkán jelenti a 0 V a nullát, az 5 V pedig az 1-et szimplán.
- Ennek oka nem meglepő módon a hibavédelem.
- Ha szakadás lép fel és 0 V jelöli a nullát, akkor nem tudjuk megkülönböztetni az átvitel hiányát a 0 állapottól.

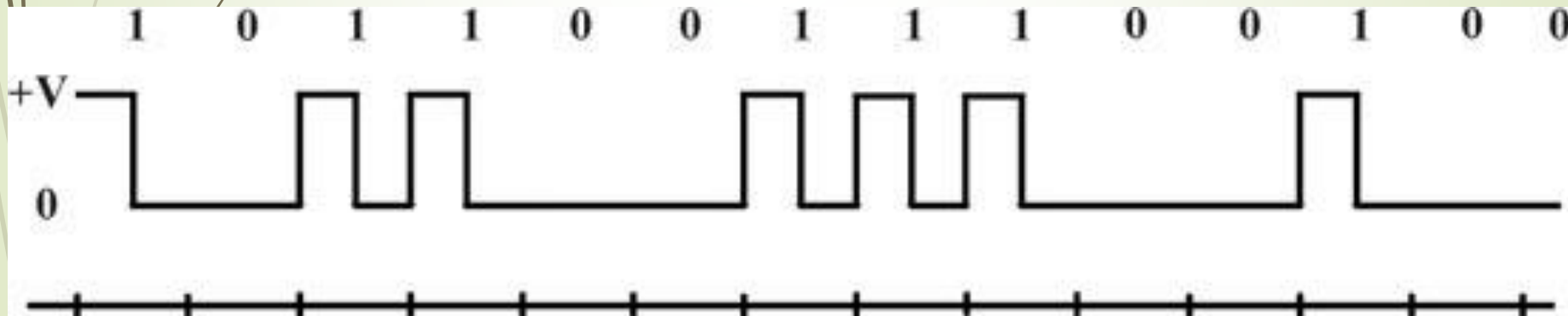
Vissza egy kicsit az analóg jelekhez

- Megoldás: Olyan feszültség jelsorozat használata, ami ezt kivédi.



RZ – Nullára visszatérő kódolás

- A 0 szintet $0V$, az 1 szintet viszont a bitidő egyik felében $+V$, a másik felében pedig $0V$ jelenti.



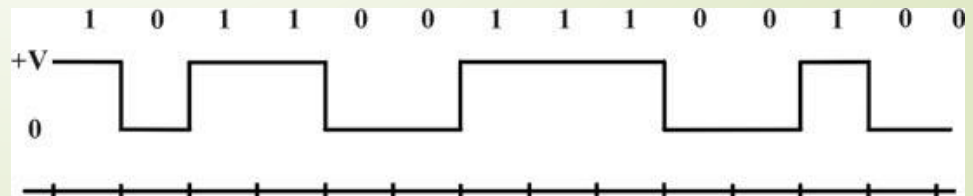


Megoldások

- Rengeteg megoldás lehetséges.
- Szituációfüggő, hogy melyiket érdemes alkalmazni.
- A teljesség igénye nélkül ezek lesznek most tárgyalva:
 - RZ (nem jó)
 - NRZ
 - Manchester
 - DVS, LVDS

NRZ - Nullára nem visszatérő kódolás

- Mindig az a feszültség szint van a vonalon, amit az adott bit meghatároz. Pl: 0 állapot 3V, 1 állapot: 5V
- Egyszerűen megvalósítható, akkor jó, ha a jel sok váltást tartalmaz.
- Azonban, ha a sok egyforma bit van egymás után, akkor a vonal állapota is azonos szinten marad.

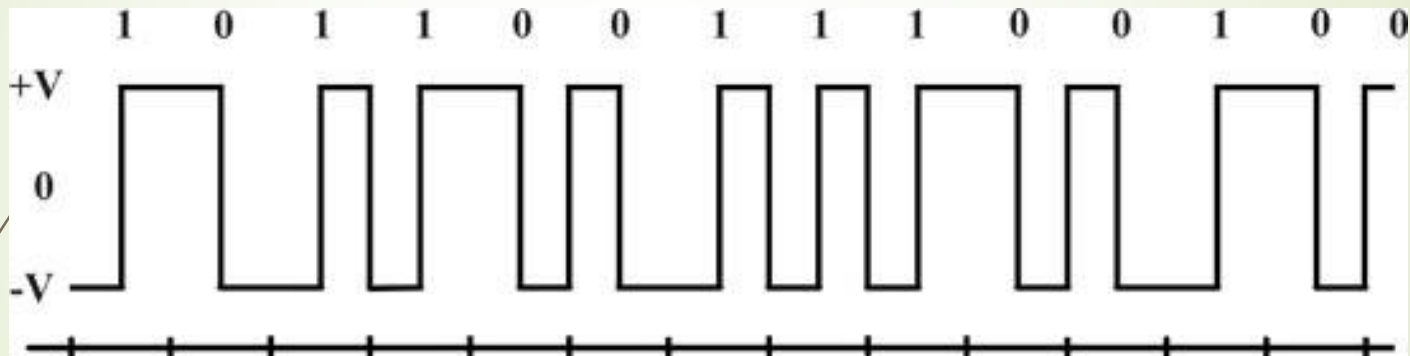




Manchester kód

- Ethernet hálózatok kódolása
- A biteket nem jelszintek, hanem a jelváltások iránya határozza meg.
- A lefutó él a logikai 0
- A felfutó él a logikai 1
- Amennyiben az egymást követő bitek azonos értékűek, akkor a jelnek a bitidő felénél vissza kell térnie az előző szintre.

Manchester kód



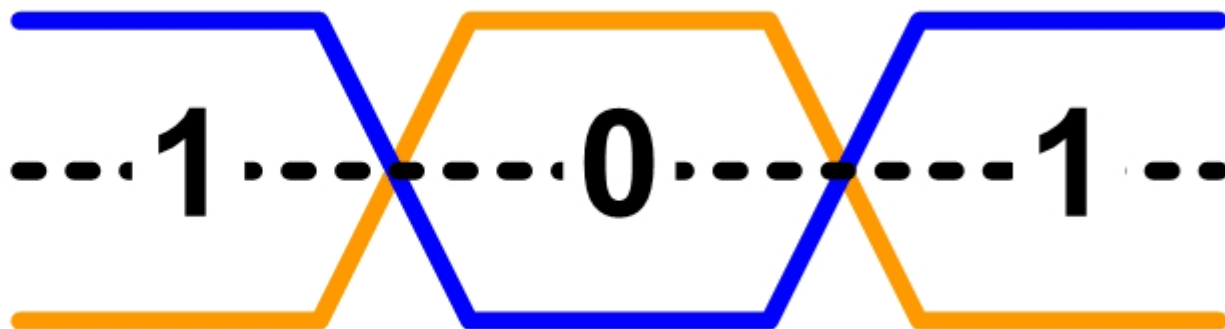
DS – Differenciált jelzés

- Nagy sebességet tesz lehetővé alacsony feszültség szintű rendszerek mellett.
- Használt:
 - USB, SATA, PCI-E, LCD kijelzők

$$V_{OH} = 1.375V$$

$$V_{CM} = 1.2V$$

$$V_{OL} = 1.025V$$





Az Adatbiztonság

Mai második fő témánk



Mi is az adatbiztonság?

- Azon fizikai és algoritmikus megoldások összessége, amelyek segítségével a véletlen adatvesztések, szándékos adatrongálások és adatkiszivárgások megelőzhetőek vagy megnehezíthetőek.



Az adatbiztonság, a játékelmélet szerint

- Két játékos játssza: védő és támadó.
- A védő mindenképpen veszít, még akkor is, ha nyer.
- Hogy is van ez? – egyszerű példa:
 - A védő költ lakatra, biztonsági zárra. Ez példaként legyen most 60 ezer forint.
 - A támadó vesz feszítővasat, ez kerül 5 ezer forintba.
- Szóval a játék alapkérdése, hogy a védő konkrétan mennyit is veszít.



Fizikai adatvédelem

- Az adatok megóvása a külső behatásoktól, valamint az eszközök közelébe jutás megnehezítése lenne a fő cél.
- Informatikai szemszögből nézve a következő dolgokra kell ügyelnünk a betörésvédelem mellett:

- 
- 
- Villamos hálózat helyes kialakítása és szünetmentes tápegységek használata.
 - A nem megfelelő villamos hálózat tűzveszélyes, valamint az adatvesztések közel 50%-a a nem megfelelő tápellátás miatt következik be.
 - Megfelelő legyen a szerverkörnyezet: klimatizálás, füstérzékelés, stb...



Ügyviteli, adminisztrációs adatvédelem

- Ez nem más, mint az adatokkal való kapcsolatba kerülés megnehezítése adminisztratív eszközökkel.
- Példák erre:
 - Feladatok, jogkörök, felelősségek szétválasztása
 - Személyazonosítás
 - Hozzáférések és tevékenységek naplózása

Algoritmikus adatvédelem

- Olyan programok és eljárások alkalmazása, amelyek segítik az előző két terület feladatait, és létrehozzák azokat a számítógépes védelmi funkciókat, amik ezen a területen meggátolják az adatokhoz való illetéktelen hozzáférést és módosítást.
- Pl.:
 - Hálózati azonosítás, automatikus biztonsági mentés, titkosítások, stb..

Az adatvesztés elkerülése

- „Kétféle ember létezik. Aki már veszített el fontos adatot és aki fog.” - Murphy
- Cél a megelőzés. Ha megtörtént a baj, akkor igen kicsi az esélye a helyreállításnak, ha nincs biztonsági másolat.
- Ezért legyen mindig biztonsági másolat.

Az adatvesztés elkerülése

- Jó megoldást a RAID üzemmódok biztosítanak.
- Elv: Két vagy több lemez egyidejű elhalálózása kisebb valószínűséggel következik be, mint egy lemez elhalálózása.
- Fontos RAID módok:
 - RAID 0
 - RAID 1
 - RAID 5 vagy 6

Az adatvesztés elkerülése

➤ RAID 0:

- „RAID 0 esetén a 0 a visszaállítható fájljaid számát jelzi, ha valami gebasz történik” – internetes hozzászólás.
- Két lemez párhuzamosan kötve, a vezérlő egy csíkot az egyik lemezre, másik csíkot a másik lemezre írja.
- Dupla kapacitás és sebesség az előnye.
- Gond akkor van, ha egy lemez meghal.

Az adatvesztés elkerülése

➡ RAID 1:

- ➡ Két lemez párhuzamosan. A lemezre írandó adatot a vezérlő egyszerre két lemezre írja ki, így ha egy lemez meghal, van egy tükörmásolat.
- ➡ Sebességben és kapacitásban nem jelent előnyt.
- ➡ Olyan rugalmatlan, mint a RAID0.
- ➡ Menet közben nem bővíthető a kapacitás ☹

Az adatvesztés elkerülése

- RAID 5/6:
 - Minimum 3 lemez kell.
 - Két lemezen tényleges adat tárolása, a harmadikon pedig helyreállító információk tárolódnak.
 - Ha egy lemez kiesik, akkor az adatoknak nem lesz baja.
 - Rugalmasan bővíthető az adattároló és a helyreállító lemezek száma is.
 - Level 6 nagyobb biztonságot nyújt, több a helyreállító adat.

Az adatvesztés elkerülése

- Van ami ellen ez sem véd:
 - Villámcsapás, Chuck Norris, Darth Vader, stb...
- Ezért kellene, hogy legyen biztonsági másolat is.
- Önmagában a biztonsági másolat sem ér sokat, ha nem állítható vissza, vagy nagyon régi.
- Rendszeres mentést kell alkalmazni. Napi és heti bontásban minimum.

Az adatvesztés elkerülése

- Napi mentés: csak a nagyon fontos, naponta használt adatokról, akár inkrementális megoldásban (Egy bázis változathoz képest csak a módosítások külön tárolása. A bázis változat lehet mondjuk a heti mentés.).
- Heti mentés: mindenről.
- Célszerű időközönként tesztelni a rendszert a visszaállíthatóság miatt.

Az adatvesztés elkerülése

- Legalább két helyre legyen mentés, biztos, ami biztos alapon.
- Ebből az egyik ne ugyan ott, ahol a szerver van.
- Ennek oka igen egyszerű: hiába volt mentés, ha a betörő azt is ellopta...
- Ennek a profi kivitelezése megoldástól függően igen sokba is kerülhet.

Biztonsági másolatból sosem
elég 😊





Ha megtörtént a baj...

- Tény: A normális biztonsági másolat költsége kisebb, mint bármilyen helyreállítás költsége.
- Fizikai lemez sérülése esetén mindenképpen borítékolható valamekkora adatvesztés.
- Speciális szakemberi segítséget igényel a dolog, ez viszont nem olcsó mulatság.
- Magyarországon specialisták: Kürt KFT.



Ha megtörtént a baj...

- Ha a fájlok törlődtek és nem íródtak felül, akkor van esély a visszaállításra.
- Erre vannak programok szép számmal.
- A profi programok fizetősek, nem olcsóak.
- Nehéz megtalálni a megfelelő programot, valamint lehet, hogy csak több kárt okozunk.
- Szakemberi segítség ajánlott ekkor is.

Hálózati biztonság

- Törekedjünk a WLAN hálózatok használatának kerülésére, mivel ezek feltörhetőek*, illetve a nagyobb gond az, hogy könnyen lehallgathatóak.
- Szintén ez vonatkozik a vezeték nélküli billentyűzetekre is. Ezek használata kerülendő (később lesz szó róla, hogy miért)!
- Csak és kizárólag felhasználói azonosítóval lehessen hozzáférni bármilyen adathoz.



Hálózati biztonság

- A felhasználókat rá kell kényszeríteni a jelszavaik cseréjére időközönként.
- Ne minden felhasználó férhessen hozzá mindenhez. Pl.: Egy takarító ne férhessen hozzá a könyvelési adatokhoz, mert nem kell neki.



Szoftveres oldalról megközelítve

- Tűzfal alkalmazása
- Antivírus program alkalmazása*
- **Rendszeres program- és rendszer frissítés**
- A rendszeres frissítések elmulasztása olyan, mintha szándékosan lábon löpnénk magunkat.
- Egyeseknek lehet ez élvezetes, de a többségnek igen kellemetlen.



Antivirus, jó, de mégis mit?

- A legtöbb esetben elég a Windows Defender.
- A legtöbb antivirus rendszergazdai jogokkal fut és bőven többet tud, mint kellene neki.
- Ez lehet gyenge pont a védelemben, mivel csak az antivirust kell kiiktatni.



Antivirus, jó, de mégis mit?

- Igazából tökéletes megoldás nincs.
- 0day exploittal a legtöbb megoldás nem tud mit kezdeni.
- Így védelemben a legtöbb megoldás ugyan ott van, mint a gyári Defender.
- Érdemes átgondolni, hogy kell-e, vagy érdemes-e fizetni külön védelmi szoftverért.



Antivirus, jó, de mégis mit?

- Tört, crack-elt, nem jogtisztta vírusirtót alkalmazni olyan, mint szándékosan lyukas övszert használni.
- Sosem tudhatod, hogy a crack mit csinál ténylegesen a szoftveren belül.
 - Lehet kiiktatja a védelem egy specifikus részét, ezáltal a biztonság csak látszat.
- Az egyéb nem jogtisztta megoldások pedig egyszerűen etikátlanok.

Összefoglalva





Komolyan összefoglalva...

- A nem megfelelően ellátott adatvédelmi feladatoknak komoly következményei lehetnek a felelős felé:
 - Jogi
 - Anyagi
- Továbbá borítékolható, hogy a felelősnek új állást kell keresnie...



Köszönöm a figyelmet!