

# **Az elektronikus információbiztonság-tudatosság és tudatosítás jelenlegi helyzete, lehetőségei és kihívásai a közzolgálatban**

**Legárd Ildikó**

Hétpecsét Információbiztonsági Egyesület  
Információvédelem menedzselése LXXXII. Szakmai Fórum  
Budapest, 2018. szeptember 19.  
Lurdy Konferencia-és Rendezvényközpont

# Az internetes támadások egyik leggyakoribb célpontja a közigazgatás

(Forrás: Dimension Data, Global Threat Intelligence Report 2018)



Az Európai Parlament 2018. június 13-i állásfoglalása a kibervédelmeről: felszólítja a tagállamokat, hogy erősítsék meg védelmüket az állami és nem állami szereplők kibertámadásai ellen.

(Forrás: <http://www.europarl.europa.eu/sides/getDoc.do?type=T&reference=P8-TA-2018-0258&language=HU&ring=A8-2018-0189> )

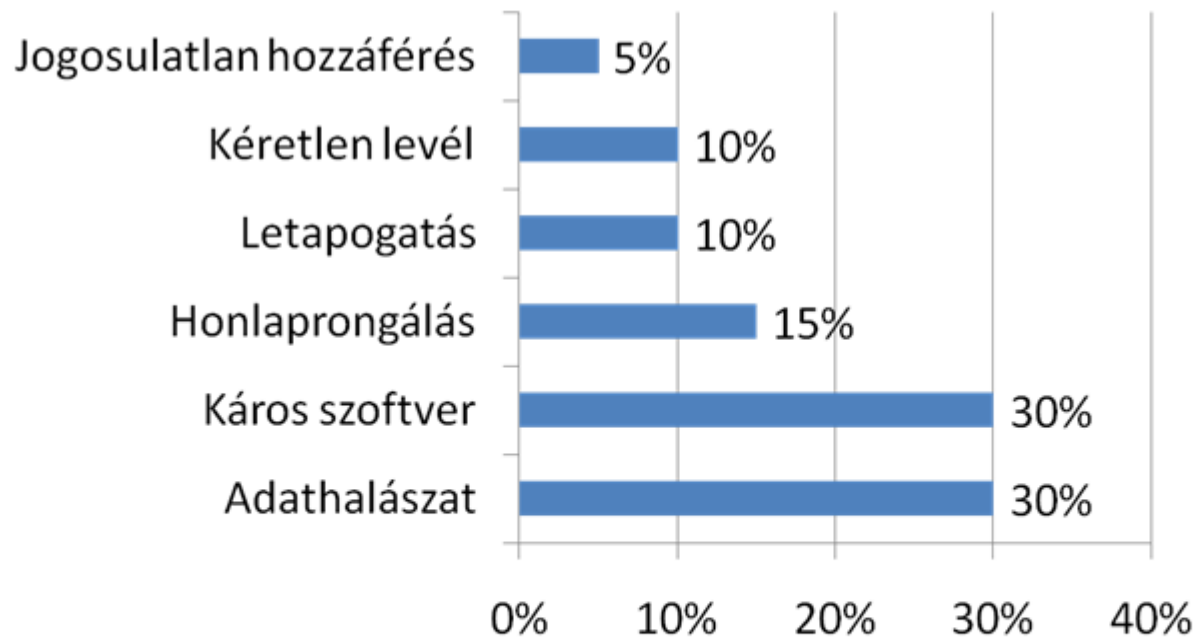


A Kaspersky Lab. Adatai alapján Magyarország a 37. a rangsorban a támadások száma alapján. (2018. 09.07. <https://cybermap.kaspersky.com/> )

## A támadás bárhonnán érkezheth!

Az NKI által kezelt, incidensekre vonatkozó statisztikai adatok (2018.08.31. - 2018.09.06.):

*(Forrás: Nemzetközi IT-biztonsági sajtószemle 2018. 36. hét)*



## A közigazgatás, mint célpont



Az állami és önkormányzati szervek munkatársai a támadók számára értékes és kiemelt célpontnak számítanak, hiszen általuk akár a nemzeti adatvagyon részét képező információkhoz is hozzáférhetnek, vagy akár megbéníthatják egy egész szervezet működését is.



**SOCIAL ENGINEERING**

# SOCIAL ENGINEERING



Humánalapú támadások



Számítógép-alapú támadások



**KÖZÖS** : az EMBER → a MUNKATÁRS!!!

# A MEGOLDÁS: TUDATOSÍTÁS



Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. Határozat

**2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)**

41/2015. (VII. 15.) BM rendelet

2 szereplőt nevesítenek:

**Felhasználó:** egy adott elektronikus információs rendszert igénybe vevők köre  
(Ibtv. 1. § (1) 18.)

**Az elektronikus információs rendszer biztonságáért felelős személy** – IBV / IBF  
(Ibtv. 13. §)

# VIZSGÁLAT

2018. február 27.- április 12.

Állami és önkormányzati szervek

Nem reprezentatív felmérés: kérdőíves módszer, statisztikai elemzés  
Eredmények összehasonlítása (2011, 2014, 2015, 2016)

## „FELHASZNÁLÓK”

112 fő

62,4% állami szerv

37,6 % önkormányzat

?:

- Felhasználó és munkahelye
- Információbiztonsági tudatosítás
- Információbiztonsági tudatosság
- Jelszóhasználat és elektronikus levelezés

## „SZAKÉRTŐK”

14 fő

11 fő állami szerv

4 fő önkormányzat

?:

- Kötelező továbbképzés
- IBV-k tevékenysége (tudatosítás, hatékonyság stb.)
- Incidensek gyakorisága és típusai
- Felsővezetői képzés és támogatás

# Szakértői tapasztalatok 1.

## Elektronikus információbiztonsági események

A szervezetek többségénél **évente 1-5 alkalommal** (leggyakoribb: emberi tényező által okozott incidens és a zsarolóvírus)

**Okok:** tudatlanság, képzetlenség, gondatlanság, hanyagság + kényelem, bosszú, sértettség

**Megelőzés:** tudatosító tevékenység („hittérítés”), adminisztratív eszközök + fizikai védelem növelése

## Tudatosítás

**Formái:** belső képzések; elektronikus tájékoztató, figyelemfelhívó körlevelek; egyéni tájékoztató e-mailek küldése

57% - elégedett, 43%  nem

- tananyag, képzési rendszer fejlesztése, gyakorlatiasabbá tétele;
- szankciók;
- a vezetői elkötelezettség növelése;
- „több forrást kellene biztosítani”



## Szakértői tapasztalatok 2.

### Felhasználói tudatosság

Sokkal felkészültebbek az utóbbi években! De! Szükséges:



- **Humán faktor megerősítése (71%)** „ *Az informatikai biztonsági terület a felhasználók körében (sem) nem slágerterület, a biztonság jellemzően a probléma felbukkanása után kerül csak előtérbe. A felhasználók közül sokan gondolják úgy, hogy velük nem történhet meg pl. egy jelszó kompromittálódás és nem érzik a súlyát.*”

- **Vezetői elkötelezettség és példamutatás (30%)**

**Szabálykövetés:**

78,6% szerint a felhasználók ismerik hatályos IBSZ-t, **azonban csak 50%-uk gondolja úgy, hogy azt követik is az állomány tagjai!**

# Felhasználók 1.



91% felismeri az **információbiztonság jelentőségét + tudatosabb viselkedés** (spam, adatvédelem, alkalmazás telepítés, zárolás stb.);



93,8% szerint a szervezet elektronikus **információbiztonságának** garانتálása az elektronikus **információbiztonságért és az adatvédelemért felelős részleg, valamint a munkatársak közös felelőssége**



76,6%-a a belépő új munkatársaknak nem részesült **információbiztonsági képzésben /oktatásban, 36% egyáltalán nem részesül kifejezetten ilyen jellegű oktatásban;**



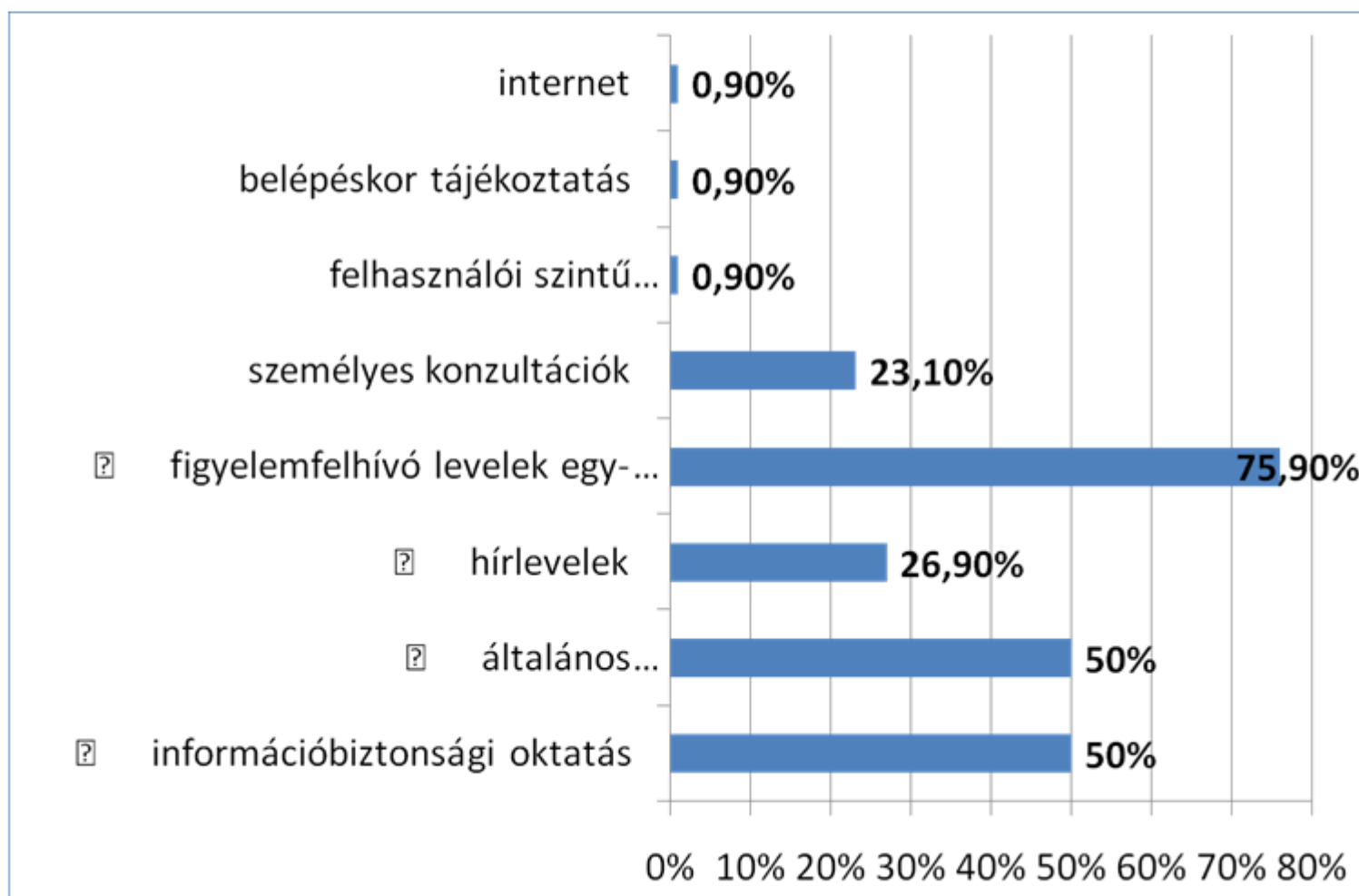
„Kerülőutak”:

saját **adathordozók csatlakoztatása, számítógép zárolása, jelszóhasználat**

## Felhasználók 2.

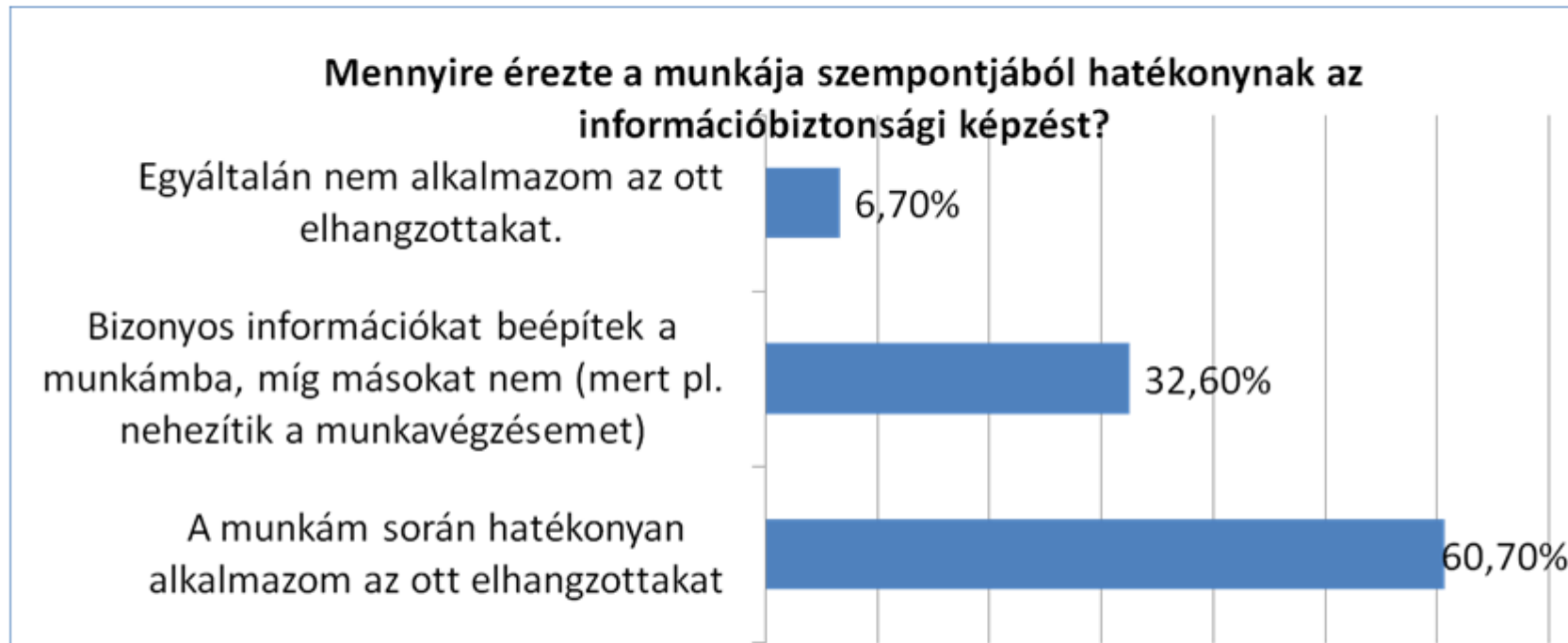
### Információbiztonsági tudatosítás:

Valamilyen formában minden szervnél megvalósul:



## Felhasználók 3.

### Információbiztonsági képzések hatékonysága



**Miért nem hatékony??** „a képzés nagyon **általános**”, „**semmire sem emlékszem belőle**”, „**nem érinti a munkavégzésüket**, mivel az oktatás csak az internet és a levelezés helyes használatára vonatkozik”, „**hanyagosság**”, „**Nyűgös alkalmazni a biztonsági szabályokat.**”

## Felhasználók 4.



Az einfobiztonság mely területén tapasztal hiányosságokat?

- *„Túlzottak a biztonsági beállítások, a gyakori jelszócserek, ahány program, annyi féle jelszó és felhasználónév. A jogosultságigények nehézkesek, szigorúak, redundánsak. Lassan nehezebb eljutni az adatokhoz, mint az adatokkal dolgozni.”;*
- saját eszközök használata a hivatali rendszerben;
- naprakész vállalati szoftverek és az ezek közti átjárás hiánya;
- **„a kollégák még mindig nem veszik eléggé komolyan”;**
- **„Annyira hiányos az ismeretem a témában, hogy azt sem tudom, hogy mi segítene ...!”**



Milyen típusú tudás segítené a legjobban a mindennapi munkáját?

- A mindennapi munkavégzéshez szükséges felhasználói szintű ismeretek;
- alapvető ismeretek, mint vírusvédelem, tűzfal, phishing, egyéb veszélyforrások;
- a mobiltelefon használat, WIFI használat veszélyei;
- a napi rutinon túlmutató esetek ismertetése;
- személyes adatok védelme;
- Kriptográfia 😊;
- etikus hacker ismeretek 😊.

# Következtetések, javaslatok 1.

## Gyakorlatorientált képzés

- Fókuszban: a napi munkahelyi rutin során jobban alkalmazható, gyakorlatias tudás;
- Incidensek esettanulmány-alapú feldolgozása;
- Kommunikáció
- „Nemzeti minimum tananyag és ellenőrzési rendszer” (Ibtv. hatálya)



NKE, NKI + szakértők bevonása  
Folyamatosan frissülő, naprakész  
anyag  
Oktatása Ibtv. Hatálya alatt kötelező

## Újabb módszerek, csatornák alkalmazása

**Kritérium: nem vesz igénybe sok időt, figyelemfelhívó, gondolatébresztő, ÉLMÉNYALAPÚ TANULÁS!!!**

- Hírlevelek (pl. NKI)
- Intraneten tájékoztató anyagok
- Kérdőívek, egyszerű játékok -> gamifikáció (játékosítás)!!
- Figyelemfelhívó videók
- Rendkívüli eseményekről tájékoztatás
- Tájékoztató brosúrák, plakátok (pl. ENISA „Keep updating” c. posztere\*, SANS Intézet „Célpont vagy” posztere)

\*<https://www.enisa.europa.eu/media/multimedia/posters/cybersecurity-education-posters-2016/enisa-eduposters-en.pdf>



# You are target – „Célpont vagy” kampány, SANS Intézet

Forrás: <https://www.sans.org/security-awareness-training/resources/posters/you-are-target>



## CÉLPONT VAGY



### Felhasználói nevek és jelszavak

Miután sikerült illegális hozzáférést szerezniük, a kiberbűnözők olyan káros programokat telepíthetnek a számítógépedre, amelyekkel figyelik billentyű leütéseidet, beleértve a felhasználó neveid és jelszavaid. A megszerzett adatokat olyan online felhasználói fiókjaidba történő bejelentkezéshez használják fel, mint például:

- Banki és egyéb pénzügyi számláid, ahonnan megszerezhetik illetve elutalhatják a pénzedet.
- iCloud, Google Drive vagy Dropbox felhasználói fiókjaid, ahol hozzáfuthatnak minden ott tárolt bizalmas adatodhoz.
- Az Amazon, Shopline vagy más online áruházi felhasználói fiókjaid, amelyekkel a nevedben tudnak vásárolni.
- Futárszolgálatokhoz köthető (UPS, FedEx) online fiókjaid, így a nevedben akár lopott árukat is küldhetnek.

### E-mail címek megszerzése

Miután sikerült illegális hozzáférést szerezniük, a kiberbűnözők olyan adatokat szerezhetnek meg a levelező rendszeredből, amelyeket értékesíthetnek másoknak, mint például:

- A címjegyzékedben szereplő nevek, e-mail címek és telefonszámok.
- A személyes és a munkádral kapcsolatos elektronikus leveleid.

### Virtuális értékek

Miután sikerült illegális hozzáférést szerezniük, a kiberbűnözők olyan virtuális javakat másolhatnak le és lophatnak el, amelyeket értékesíthetnek mások számára, mint például:

- Online játékbeli karaktereid, -értékeid vagy a játékhöz kötődő fizetőeszközöid.
- Szoftver licenzek, operációs rendszer licenzek, kulcsok vagy játék licenzek.

### Botnet

Miután sikerült illegális hozzáférést szerezniük, a kiberbűnözők hozzákapcsolhatják a számítógéped egy feltört eszközökből álló hálózathoz, amelyet ők vezérelnek. Az ilyen hálózatokat nevezzük botnet hálózatoknak, melyeket például a következőkre is használhatják:

- Kéretlen levelek (spam) küldése emberek millióinak.
- Szolgáltatás megtagadásos (DoS - Denial of Service) támadások végrehajtása.

Talán észre sem veszed, de kiberbűnözők célpontja vagy. Számítógéped, mobil eszközeid, felhasználói fiókjaid mind óriási értéket képviselnek. Ez a poszter bemutatja a különböző módszereket, ahogy a kiberbűnözők pénz csinálnak az adataidból. Szerencsére, néhány egyszerű lépés megtételével megvédheted magadat és családot. Amennyiben szeretnél többet megtudni, iratkozz fel az OUCH-ra, ami egy biztonsággal foglalkozó hírlevél azzal a céllal, hogy segítsen a hétköznapi felhasználóknak, így például neked.

[www.securingthehuman.org/ouch](http://www.securingthehuman.org/ouch)



### Személyazonosság lopás, megtévesztés

Miután sikerült illegális hozzáférést szerezniük a számítógépedhez, a kiberbűnözők megszerezhetik online személyazonosságodat, hogy a nevedben csúcsokat kövessenek el vagy további értékesítsék az olyan személyazonosságokat, mint például:

- A Facebook, Twitter vagy LinkedIn felhasználói fiókod.
- E-mail fiókjaid.
- Skype vagy más IM (Instant Messaging) felhasználói fiókjaid.

### Webszerver

Miután sikerült illegális hozzáférést szerezniük a számítógépedhez, a kiberbűnözők webszerverre alakíthatják, amit ezután felhasználhatnak:

- Adathalász weboldalak kiszolgálására, más emberek felhasználó neveinek és jelszavainak megszerzéséhez.
- További támadáshoz használt eszközök kiszolgálására, amelyek mások számítógépeit fogják megfertőzni.
- Peddől tartalmak, képek videók és kópiát zenei anyagok terjesztése.

### Pénzügyi információk

Miután sikerült illegális hozzáférést szerezniük a számítógépedhez, a kiberbűnözők olyan értékes adatokat kereshetnek a rendszereden, mint például:

- Bankkártya adatok.
- Jövedelem és adónyilatkozatok, korábbi adóbevallások.
- Pénzügyi, befektetési és megtakarítási kimutatások.

### Zsarolás

Miután sikerült illegális hozzáférést szerezniük, a kiberbűnözők átvehetik a számítógéped irányítását és pénzt követelhetnek tőled a következőkért:

- Fényképeket készíthetnek rólad a számítógéped kamerájával és pénzt követelnek azok megsemmisítéséért vagy azért, hogy ne tegyék közzé azokat.
- A tárolt adataidat titkosítják és pénzt követelhetnek a titkosítás feloldásáért.
- Nyomon követik az általad megkért weboldalak és megfigyelhetik azzal, hogy közzétesz azokat az adatokat.

A poszter Brian Krebs eredeti munkáján alapszik. Az alábbi blogon további információk érhetőek el a kiberbűnözéssel kapcsolatban: <http://krebsonsecurity.com>

## Következtetések, javaslatok 2.

### Megengedőbb belső szabályozás

pl. külső adathordozó, jelszó átadás,  
túlzott biztonsági beállítások (IBSZ)



„kerülőutak”

### Motiváció – Szankció

- Belső motiváció (visszacsatolás)
- Külső motiváció (játékos „jutalmazó”rendszer)
- Szankció ????

### Felsővezetői elkötelezettség

Felsővezetői példamutatás,  
elkötelezettség, tudatosság



Tudatos dolgozói magatartás

**KÖSZÖNÖM A FIGYELMET!**