Szabó Tibor

VÁLLALATI ÉS MAGÁN ESZKÖZÖK KETTŐS CÉLÚ FELHASZNÁLÁSÁNAK VESZÉLYEI

Absztrakt

Napjainkban a számítástechnikai eszközök nagy műveletvégzési kapacitással rendelkeznek, viszonylag kis fogyasztásúak, a többsége hordozható és internetre csatlakoztatható. Mindezek alapján magától értetődőnek tűnik a legújabb trend, miszerint „hozd a saját eszközöd a munkahelyedre és dolgozz azon”. Jelen cikkben sorra vesszük a mellette és az ellene szóló érveket.

A legelterjedtebb eszközök, az okostelefonok veszélyeztetettsége kerül elemzésre és értékelésre az operációs rendszerek és a frissítések szempontjából.

Kulcsszavak: BYOD, Android, okostelefon, patch-kedd, biztonsági intézkedés

THE DANGER OF DUAL-PURPOSE USE OF THE CORPORATE AND PRIVATE EQUIPMENTS

Abstract

Nowadays the computer equipment have large processing capability, relatively low power consumption. Much of computer can connect to the Internet and portable. Based on the above the latest trend seems self-evident to “bring your own device (BYOD) to your job and work on it”. In this article we look at the arguments in favor and against the BYOD.

The vulnerability of most common devices, the smartphones will be analysed and interpreted based on operating systems and upgrades.

Key words: BYOD, Android, smartphone, patch-Tuesday, safety action

1. MÉRETVÁLTOZÁSOK

A processzorok összetettségének növekedése és a gyártástechnológia számottevő fejlődése eredményezte az eszközök méretének, súlyának látványos csökkenését és a fogyasztói árak kedvező mérséklődését, amelyek a kisszámítógépek elterjedésének legfőbb mozgatórugói. Mindemellett, napjainkban a számítástechnikai eszközök nagy műveletvégzési kapacitással rendelkeznek, viszonylag kis fogyasztásúak, - szinte mindenki otthonában elérhető – internetre csatlakoztathatók és a többsége hordozható.

2. TÁVMUNKA

Mindezek alapján magától értetődőnek tűnik a távmunka gondolata a munkáltatók részéről, amely szerint a dolgozók otthon is képesek elvégezni feladataikat, felcsatlakozva a vállalat központi szerverére a világhálón keresztül. A legújabb trend szerint (BYOD - Bring your own device) hozd a saját eszközöd (okostelefon, laptop) a munkahelyedre és dolgozz azon. A tapasztalatok szerint az üzleti élet bizonyos területein ez váltotta ki a jelentős eredménynövekedést. Vegyük sorra a mellette és az ellene szóló érveket:

Mellette:

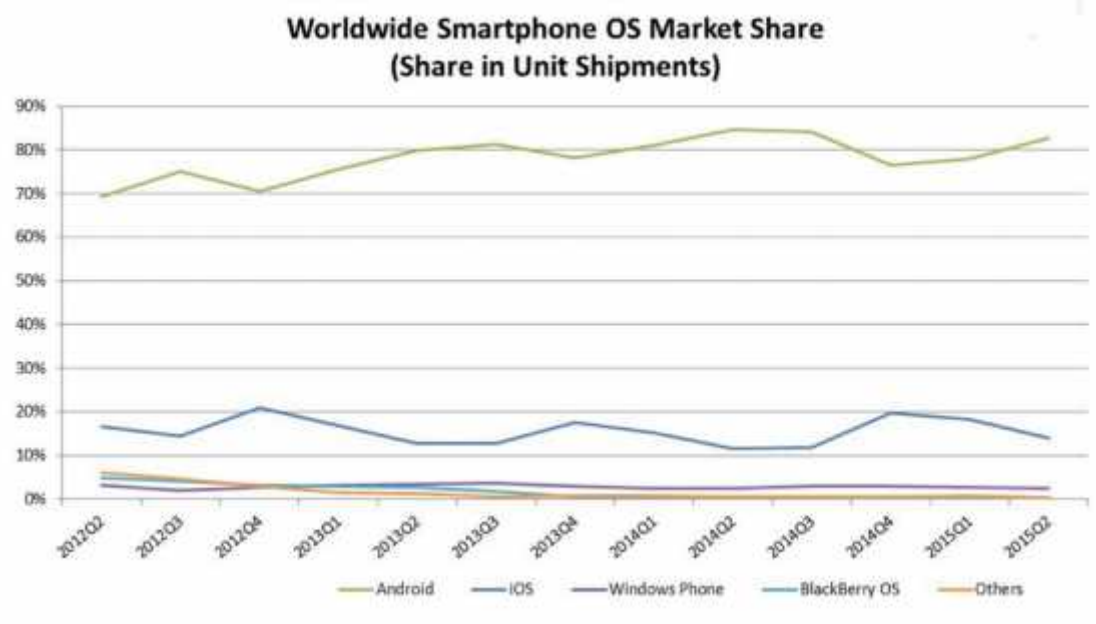
- A dolgozó saját igényeinek megfelelő eszközt és szoftver környezetet választ, amivel esetenként kiküszöböli a számára elavult és korlátozott képességekkel rendelkező vállalati eszközparkot.
- A dolgozó gyorsabb és flexibilisebb a feladat-végrehajtásban a számára ismerős eszközparkon – nem érzi korlátok között magát.
- Az alkalmazottak gyorsabban tudják követni a technikai fejlődést, modernebb eszközöket használnak, - mint egyes cégek, ahol ritkán van fejlesztés - ezért jobb arculati kép alakul ki a munkáltatóról.
- Pénz megtakarítást jelent a cégnek a dolgozói eszköz használata.
- Távmunka és rugalmas munkaidő beosztás lehetősége.

Ellene:

- A személyes eszközöket nehéz felügyelni, karbantartani és esetenként beilleszteni vállalati informatikai környezetbe.
- A minősített adatokhoz való hozzáférés, módosítás és másolás alapvető biztonsági kérdéseket vet fel - főleg, ha azzal is számolni kell, hogy a dolgozó elveszítheti eszközét vagy a rajta lévő érzékeny információkra illetéktelenek is ráláthatnak.
- A számítástechnikai eszközöket nem csak a biztonságtudatos alkalmazott, hanem családtagjai és ismerősei is használják, ezért a rosszindulatú program (malware) fertőzés veszélye sokkal magasabb.
- Az eszközök a vállalati hálózaton kívül fölcsatlakozhatnak közvetlenül az internetre is, ezért a saját eszközön használt – többnyire – „lazább" biztonsági irányelv miatt könnyebben ki lehet használni a sérülékenységeket akár egy malware telepítésére is.
- A vállalati hálózatba könnyebben be tudnak kerülni rosszindulatú programok a külső, határvédelmi rendszereket megkerülve.
- Megnövekszik az információs rendszerek – logikai és fizikai – védelmére fordított költség a cégnél.
- Új és egyben fokozottabb biztonsági szabályok bevezetésére van szükség.
- A dolgozó figyelme hamarabb elterelődik a munkáról, mivel kapcsolatait saját eszközén tartja fenn, ezáltal könnyebben is kaphat malware fertőzést.
- Csak bizonyos dolgozók engedhetik meg, hogy kövessék eszközeikkel a technikai fejlődést.
- Szoftver licencjogi, ill. biztonsági frissítésekkel kapcsolatos kérdések keletkeznek.
- Személyes adatok kiszivárgása vállalati rendszeren keresztül jogi kérdéseket vethet fel.
- Az alkalmazottak által használt eszközök sokfélék lehetnek, ezért halmozottan több sérülékenységgel kell számolni, tehát nagyobb teret biztosít a kihasználhatóság szempontjából.
- A keletkezett dokumentumok sokszínűsége komoly összefésülési és egyeztetési metodikát igényel az adatvagyon egységesítése érdekében.
-

3. POTENCIÁLIS CÉLPONTOK

Érdemes kiemelni az eszközök közül a magas használati aránnyal rendelkező okostelefonokat, amelyeknél a legelterjedtebb operációs rendszer (Android) frissítéseinek hiánya több százmillió felhasználót tesz potenciális célponttá a világon. (1. ábra)



1. ábra. Az operációs rendszerek megoszlása a piacon. [1]

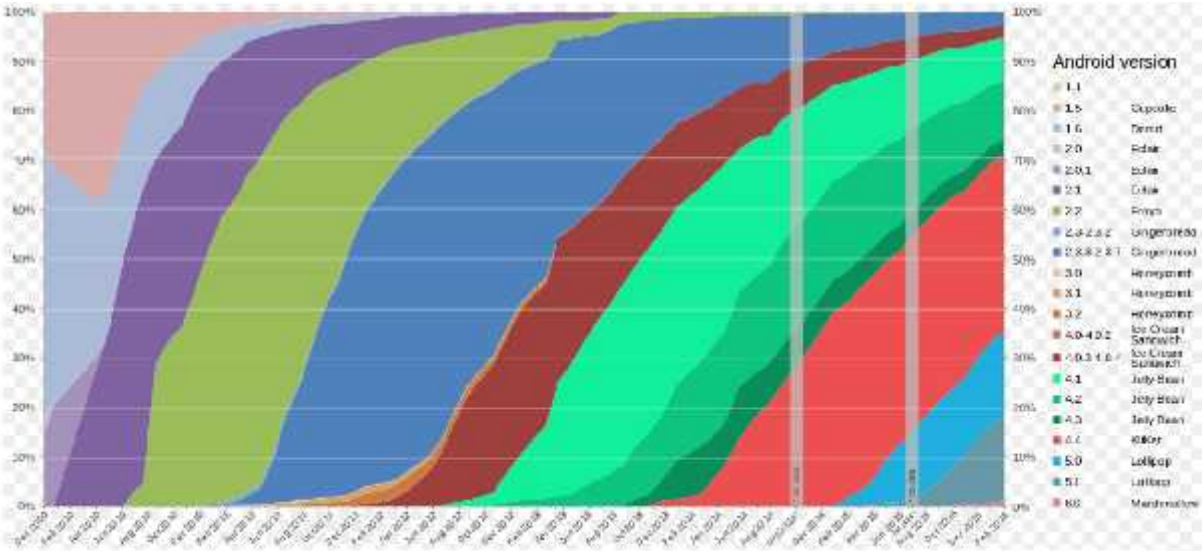
Az amerikai Szövetségi Kereskedelmi Bizottság és a Szövetségi Hírközlési Bizottság felismerte ezt a problémát és kérdőre vonta a gyártókat és a mobilszolgáltatókat, hogy milyen gyakorlatot követnek a frissítések kiadása kapcsán.

A Google által beindított "androidos patch-kedd" elnevezésű – rendszeres operációs rendszer frissítés – kezdeményezést a Samsung és az LG is támogatta, ellenben a többi gyártó (BlackBerry és Apple is) tartózkodik a módszer átvételétől.

További információk: [2]

Bizonyos Android verziók (1.0 – 2.3.2) támogatása megszűnt, ami további biztonsági kérdéseket vethet fel azoknál a vállaltoknál, ahol az alkalmazottak ilyen készüléket hordoznak nap, mint nap. (2. ábra) Amennyiben mindemellett figyelembe vesszük az okostelefonok mennyiségi növekedését, a mobiltelefon-függők arányának emelkedését, akkor az alábbiakban felsorolt biztonsági intézkedések megfontolása javasolt.

- Jelszavak esetén alkalmazandó szabályok (legalább 10 karakter; szám kis-, nagybetű és speciális karakterek együttes használata).
- Rendszeres operációs rendszer és alkalmazás frissítés.
- Anti-vírus szoftver telepítése.
- Személyes tűzfal telepítése.
- Csak megbízható, titkosított Wi-Fi hálózat használata állandó hardver azonosító figyeléssel.
- Olyan Wi-Fi csatlakozási pont alkalmazása, amely nem engedélyezi egy, már megszakított folyamat folytatását..
- Böngészés csak megbízható és lehetőleg https protokollal elérhető oldalakon.
- Alkalmazás telepítésének mérlegelése.
- Bluetooth, Wi-Fi kapcsolat megosztásának mellőzése.
- Mentések gyakoriságának fokozása, ill. egységes központi adatmentés megvalósítása.
- A legbiztonságosabb és leggyakrabban frissíthető böngésző használata.
- A világhálón elérhető alkalmazások helyettesítése saját (céges) készítésű, biztonságos megoldásokkal a dolgozók részére.



2. ábra Android verziók aránya az idő függvényében [3]

4. HIVATKOZÁSOK

[1] http://www.idc.com/prodserv/smartphone-os-market-share.jsp

[2] http://www.hwsw.hu/hirek/55582/android-biztonsagi-frissites-amerikai-vizsgalat-mobilgyarto-mobilszolgaltato.html

[3] https://hu.wikipedia.org/wiki/F%C3%A1jl:Android_historical_version_distribution_-_vector.svg

Szabó Tibor
tűzoltó őrnagy, kiemelt főreferens, BM Országos Katasztrófavédelmi Főigazgatóság Hatósági Főigazgató-helyettesi Szervezet
main rapporteur, organization of the Magisterial Deputy Director-general, National Directorate General for Disaster Management
tibor.szabo2@katved.gov.hu
orcid.org/0000-0001-9948-4460

A kézirat benyújtása: 2016.11.10.
A kézirat elfogadása: 2016.12.05.
Lektorálta:
Dr. Bognár Balázs PHD
Dr. habil. Vass Gyula PHD