Nemzetközi távközlési adatvédelmi munkacsoport	International Working Group On Data Protection in Telecommunications

Munkadokumentum a „saját eszközökkel" kapcsolatos adatvédelmi és biztonsági kockázatokról[*]

56. értekezlet, 2014. október 14-15. Berlin (Németország)

Hatály

Ez a munkadokumentum megvizsgálja a végfelhasználók tulajdonában lévő mobileszközök használatával kapcsolatos biztonsági és adatvédelmi kockázatokat, például a tabletekét az okostelefonokét, ezek alkalmazásaihoz és adataihoz való hozzáférést, ide értve a társaságok hálózatán tárolt személyes adatokat. Több ilyen kockázatot a munkacsoport korábbi dokumentumaiban, például a „Személyes adatok mobil feldolgozása és kockázata[1]" és a „Számítástechnikai felhő[2]" címűben, de vannak újabb, a saját, társasági hálózatokban használt eszközökkel kapcsolatos.

Háttér

A „hozd a saját eszközödet" (hase) gyakorlata sok üzleti környezetben uralkodóvá vált, és használatuk növekvő nyomás alatt áll. Mindazonáltal e politika alkalmazásának a biztonságra és az adatvédelemre gyakorolt hatása tekintetében nő az aggodalom[3]. A szervezetek a hasét úgy tekintik, mint amelyet egyre gyakrabban használnak azok az alkalmazottak és szenior vezetők akik ezt az eszközt jó munkaeszköznek tartják, és mozgás közben, otthon is használják, s akik gyakran szükségük van arra a növekvő funkcionalitásra és alkalmazhatóságra, amit saját okos eszközük kínál. A lehetséges előnyökkel azonban a társasági információ feldolgozó rendszerek bizalmas voltát és integritását növekvő veszélyek is fenyegetik, amelyek azzal járnak, hogy e rendszerekben tárolt személyes adatokat többé nem lehet megfelelően védeni. Annak a szervezetnek, amely a hasét használja, megfelelő védelmi intézkedéseket kell foganatosítania annak érdekében, hogy a társaság által feldolgozott adatokat védje. A szervezeteknek arról is gondoskodniuk kell, hogy ezeket az óvintézkedéseket az egyes felhasználók esetében minimalizálják[4].

A hasék felhasználói azonban aggódhatnak amiatt, hogy a szervezet a kockázatok csökkentése érdekében szorosan megfigyeli ezt a használatot, például a társasági hálózat adminisztrátorait (ide érve a személyes adatokhoz való hozzáférést). Ha az eszköz elvész vagy azt ellopják, az adatok távolról való letörlése azzal járhat, hogy az eszközön tárolt személyes adatok véglegesen törlődnek. Ennek megfelelően a hasék a felhasználók személyes adatait tovább veszélyeztetik. A mobileszköz menedzsmentjének korrekt használata megvédheti a hasék felhasználóinak adatait, míg védik a társasági adatok bizalmasságát és integritását.

---

[*] Könyves Tóth Pálnak a Munkacsoport angol és német nyelvű dokumentumáról készített fordítása. Letölthető: http://www.datenschutz-berlin.de/content/europa-international/international-working-group-on-data-protection-in-telecommunications-iwgdpt/working-papers-and-common-positions-adopted-by-the-working-group

[1] http://www.datenschutz-berlin.de/attachments/886/675.41.18.pdf

[2] http://www.datenschutz-berlin.de/attachments/875/Sopot_Memorandum.12.6.12.pdf

[3] http://enterprise-mobile-solutions.tmcnet.com/articles/359879-growth-byod-compels-companiesrevisit-security-basics.htm

[4] For example by employing sandboxing techniques where a device contains two distinct sandboxes, one personal and one professional

A Fehér Háznak[5] a szövetségi ügynökségeknek szóló útmutatása támogatja ugyan a hasét, figyelmezteti őket: *A hase programok alkalmazása az ügynökségeknek biztonsági, döntési, technikai és jogi kockázatot jelent, és nem csak a belső kommunikációban, hanem az üzleti és kormányzati partnerek viszonyát és beléjük vetett bizalmat illetően is."*
Az Egyesült Királyság kormányának osztályaihoz [6] intézett útmutatás óvatosabban ezt javasolja: *„Szükséges, hogy az eszköz használata teljes időtartamában a vállalkozás menedzsmentjének a felügyelete alá helyezzék, hogy hivatalos adatokhoz ne lehessen hozzáférni. Így olyan hase modell alkotható, amely, ámbár azt technikai és nem technikai okokból nem ajánlják, amely jól tükrözi használatának szerkezetét."*

Jelenleg a Francia Biztonsági Ügynökség óv a hase használatától[7].

Az Egyesült Királyság Információs biztosának útmutatása[8] azt hangsúlyozza, hogy: *„Ha megengedjük, hogy egy, a használója által nem ellenőrzött eszközt a társaság informatikai rendszeréhez kapcsoljanak, az számos biztonsági és más adatvédelmi problémával jár, ha nem megfelelően menedzselik."*

A Német Informatikai Biztonsági Szövetségi Hivatalnak a hase felhasználását áttekintő dokumentumait azt hangsúlyozza[9], hogy: *A magántulajdont képező végfelhasználói eszközök általános használata azt eredményezheti, hogy az információbiztonság és az adatvédelem több kockázatnak lesz kitéve. Ezt stratégiai kihívásnak kell tekinteni, amelyre az intézmények felső vezetésének kell a megfelelő választ megadnia (…). A technikai intézkedések önmagukban nem elegendők, azokat az intézménye általános szervezeti intézkedésekkel is támogatni kell",* ha a homokzsák bokszolási technikát alkalmaznak, s az eszköznek két különböző homokzsákot kell tartalmaznia.
Ontario és Kanada Információs és adatvédelmi Biztosának Hivatala egy, a TELUSsal közösen közzétett dokumentumban [10] megvizsgálta az információmenedzsment kockázatait, azok mérséklésére szolgáló útmutatást adott. Az saját eszközök használata nem korlátozódik a haséra, melyek felölelik azokat a végfelhasználói készülékeket is, amelyet harmadik felek, például szerződéses ügyfelek és alvállalkozók használnak. Ha azonban korlátozzák a személyes adatoknak a társaság által menedzselt eszközök használatát, úgy az nem küszöböli ki azoknak a kockázatok mindegyikét, mely kockázatokat a mobilis munkaerők növekvő száma, valamint a nem szankcionált szoftver alkalmazásokkal vagy az online szolgáltatások igénybevételével járnak, melyek „hozd magaddal saját alkalmazásodat", „hozd magaddal saját szoftveredet" vagy „hozd magaddal saját bármidet[11]" révén hasonló adatvédelmi és biztonsági kockázatokkal járnak.

Adatvédelmi és adatbiztonsági kockázatok

E kockázatok jelentős része a társaság tulajdonát képező hasék használatával kapcsolatos, ide értve a következőket is:

[5] http://www.whitehouse.gov/digitalgov/bring-your-own-device#key-considerations
[6] https://www.gov.uk/government/publications/end-user-devices-security-guidance-introduction
[7] http://www.ssi.gouv.fr/IMG/pdf/Communique_de_presse_Assises_de_Monaco_2012_v2.pdf
[8] http://www.ico.org.uk/for_organisations/data_protection/topic_guides/online/byod
[9] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/Ueberblickspapiere/Ueberblickspapiere_node.html
[10] http://www.ipc.on.ca/site_documents/pbd-byod.pdf
[11] https://byox.eq.edu.au/SiteCollectionDocuments/byox-project-research-report.pdf

a) A hasék általában kicsik és mobilak, ezért a haséhoz továbbított adatok esetleg elvesznek, ellopják őket vagy illetéktelenül hozzájuk férnek;
b) a hasék az alkalmazások között megoszthatják az adatokat és a technikai adatvédelmi ellenőrzést;
c) a hasék kilehetnek téve észrevétlen külső támadásoknak és nyomkövetésnek (pl. a Wi-Fivel való visszaélés és az Internet helyekhez való nem biztonságos hozzáférés következtében). Ez felölelheti a közmédia használata miatt bekövetkező pszichológiai manipulációs támadásokat vagy más online szolgáltatásoknak a munkavégzés céljára való használatát.
d) a hasék operációs rendszerét különösen nehéz úgy kialakítani, hogy a társaság eszközeivel közös funkcionalitásuk csökkenjen és biztonságuk növekedjen, melyek menedzsmentje a szervezet feladata;
e) a hasék gyakran esetleg kevésbé biztonságos, különféle környezetben vagy hivatalban, otthon, hazai vagy külföldi közterületen működő kommunikációs hálózatok szélesebb körének alkalmazására képesek, melyekhez azok a társasági eszközök nem férhetnek hozzá, amelyek rendszerint a társaság által menedzselt kommunikáció hálózatokat használnak, például huzalos helyi hálózatokat, amelyek biztonságos hivatali környezetben működnek;
f) a létező társasági alkalmazásokat és hálózati infrastruktúrákat esetleg nem úgy tervezték, hogy a hasék által biztonsággal hozzáférhetők lehetnének;
g) a társaság által elfogadott Internet hozzáférési és világhálózati, vagy levelezési rendszereknek az alkalmazottak által való használatát nehezebb lehet kikényszeríteni, ha az alkalmazottak hasékat használnak;
h) a hasék operációs rendszerei esetleg nem olyan fejlett, mint a hagyományos társasági eszközöké, és esetleg sok támadásnak vagy sérülésnek vannak kitéve. Melyek egy megfelelő időskálába nem illeszthetők be, és a saját eszközök aktualizálása általában a felhasználó feladata;
i) a hasék használatának jelentős része személyes, és az eszközt a tulajdonos családtagjai vagy a háztartás más tagjai is használhatják;
j) az automatizált háttérszolgáltatások vagy a felhasználó által installált, harmadik féltől származó szoftver a hasék váratlan vagy illetéktelen használatához vezethet;
k) a hasék felhasználója esetleg kevésbé éber vagy a hase nagyobb biztonsági kockázatait figyelmen kívül hagyja;
l) a személyes adatokat, mielőtt azokat mások rendelkezésére bocsátanák, eladnák, esetleg kevésbé biztonságos módon törlik;
m) a mobil eszközmenedzsment eszközök helytelen használata, az alkalmazottak túlzott megfigyelését eredményezheti.

Ajánlások

Az adatvédelmi és az információbiztonsági kockázatokat figyelembe véve minden szervezetnek meg kell vizsgálnia, hogy a hasék megengedett használatát megelőzően, mielőtt egy ilyen rendszer alkalmazásáról döntenek, értékelni kell a használatnak az adatvédelemre gyakorolt hatását. Az is elengedhetetlen, hogy az adatvédelemre gyakorolt hatáselemzés során figyelembe vegyék a hase használóinak és a vállalkozások személyes adatainak kockázatát. Az adatvédelemre gyakorolt hatáselemzés során azt is figyelembe kell venni, hogy a hasék által feldolgozandó személyes adatoknak, az adatok érzékenységének sérelme és az adatvesztés vagy az adatok felfedése rontja az adatalany jó hírnevét.

Először a nem különleges és nem bizalmas információk feldolgozását kell óvatos, kis lépésekben végrehajtani. A különleges adatok feldolgozása további aggodalmakkal jár és további védelmet kíván[12].

Minden szervezetnek, amelyik úgy dönt, hogy megengedi a hasék használatát, további védelmi intézkedéseket kell tennie, amelyek felölelik a következőket, de nem korlátozódnak azokra:

a) a szervezet által feldolgozott személyes és bizalmas adatok értékelése annak figyelembe vételével, hogy az adatok a hasékkal feldolgozhatók-e vagy sem. Az általános szabály szerint különleges adatok hasék által való feldolgozása csak akkor tekinthető megfelelőnek, ha a feldolgozás kockázatai az elfogadható minimumra csökkenthetőek; (Vesd össze a számítástechnikai felhő adatvédelmi vonatkozásairól szóló munkadokumentummal. Sopot memorandum, Sopot, Lengyelország 2012. április 23-24., 2. lábjegyzet.)
b) A lehetséges adatvédelmi és adatbiztonsági kockázatoknak, az adatok érzékenységének és az adatok elvesztésének, vagy felfedésének az adatalanyok jó hírére gyakorolt hatásának értékelése.
c) A vállalati alkalmazások meghatározását a hasék értékelésével kell eldönteni.
d) Azoknak az adatkategóriáknak a meghatározása, amelyekhez a személyzet a hasék használatával hozzáférhet.
e) Az alkalmazottak kötelességeire vonatkozó, a hasék használatára vonatkozó döntéseket írásba kell foglalni, ide értve legalább a következőket:
    (1) A hasékon tárolt személyes adatok törlése időpontjának meghatározására vonatkozó szabályok.
    (2) Az alkalmazottaknak a vállalkozás tájékoztatására vonatkozó kötelessége, ha a hasén tárolt vállalati személyes adatokat ellopták vagy meghamisították.
    (3) A vállalkozás személyes adatainak vagy hasék által való hozzáférésének védelme jogosulatlan hozzáféréssel szemben, ide értve azt is, hogy a hasékat felhatalmazott harmadik felek, például családtagok is használhatják.
f) hasék egyéni felhasználóinak folyamatos támogatása a véletlen eseményekkel, a jelentések kibocsátásával és az általános részvétellel szemben.
g) A szervezetnek hasékhoz való hozzáférést illető biztonsági politikája és technikai infrastruktúrája fejlesztési szempontjainak a meghatározása, mint:
    (1) A felhasználó felhatalmazása folyamatának és a hasékhoz való kommunikációs módszerekkel való hozzáférés biztosítása.
    (2) Azoknak a vállalati alkalmazásoknak a fejlesztése, amelyek a hasékkal hozzáférhetők.
    (3) A kommunikációs infrastruktúra fejlesztése a hasékkal való kommunikáció végfelhasználói adatinak titkosítása céljából.
    (4) Az elfogadott hasék és azok elfogadott felhasználói nyilvántartásának létrehozása.
    (5) A hozzáférést ellenőrző mechanizmusok létező eljárásainak kiterjesztése, például akkor, ha egy felhasználó kilépett a szervezetből vagy már nem igényel hozzáférést.
    (6) A hasékban tárolt adatok másolatának rendszeres mentése.
    (7) A vállalkozás hasékon tárolt adatinak távoli törlésének feltételeire vonatkozó világos szabályok megállapítása, ha azok elvesztek, ellopták őket vagy a

[12] Cf. the Working Paper on Cloud Computing – Privacy and data protection issues – "Sopot Memorandum" (Sopot (Poland), 23./24. April 2012), footnote 2 above.

vállalkozás hálózatában tárolt adatokhoz felhatalmazott módon már nem lehet hozzáférni.

(8) Azoknak a hibás szoftvereknek a törlése vagy azoknak a szűk keresztmetszetek megszűntésére vonatkozó döntések meghozatalának módja, amelyek befolyást gyakorolhatnak a vállalkozás hálózatára (például a hálózat hatékony felosztása vagy hozzáférési jegyzőkönyvek), ha az adatok sérelme feltételezhető és gondoskodtak megfelelő, a veszélyeket csökkent intézkedésekről.

(9) Megfelelő adatvédelmi, bizalmassági, gyakorlati intézkedések oktatása, melyekről a vállalkozás gondoskodott, ide értve a megnövelt biztonságtudatosságot és a hasék felhasználóinak további oktatását is.

(10) A haséknak egy elkülönített hálózaton való használata.

(11) A saját eszközök alkalmazása, tesztelése és a velük kapcsolatos technikai intézkedéseknek, ideértve a tűzfalakat és a hasék homokszákos védelmét is, értékelése, mely intézkedések azt szolgálják, hogy a vállalkozás adatait védjék az egyéb alkalmazásokkal való hozzáféréstől, miközben tiszteletben tartják a felhasználó magánéletét.

(12) A hasékon folyó feldolgozások megfelelő, releváns és arányos védelme, különös tekintettel a felhasználó személyes adatait tároló helyhez való hozzáférésre és a hasék munkaidőn kívül használt helyének megfigyelésére. Parancsoló szükségszerűség, hogy a szervezet adatait védő biztonsági intézkedések ne sértsék azoknak a felhasználóknak vagy bárki másnak (egy harmadik félnek) a magánéletét, akiknek az adatait a felhasználó a saját eszközén tárolja (például címjegyzékében, e-mail fiókjaiban, családi fényképeiben, stb.)

(13) A hasék integritását értékelő folyamatok és hogy megfelelnek-e az elfogadható feltételeknek, például a minimális operációs rendszerváltozatnak, az eszköz típusának, a beléptető szó védelmének, a titkosításnak) és az aktuális hibás szoftver elleni védelmeknek.

(14) A szervezeti politikával tiltott szoftverek használatának felfedésére és megakadályozására vonatkozó eljárások, például a fájlmegosztó alkalmazások, az adatáramlás és a végponttól végpontig terjedő alkalmazások megállapítása.

****