BUDAPESTI GAZDASÁGI EGYETEM
PÉNZÜGYI ÉS SZÁMVITELI KAR

Bekövetkezett információ- technológiai incidensek és hatásuk a tőzsdei árfolyamra

Orbán Éva
Nappali munkarend
Gazdálkodási és menedzsment szak
Statisztikus elemző szakirány

Belső konzulens: Dr. Sugár András
Külső konzulens: Tamásné Dr. Vőneki Zsuzsa

2019

NYILATKOZAT

Alulírott .....Orbán Éva..... büntetőjogi felelősségem tudatában nyilatkozom, hogy a szakdolgozatomban foglalt tények és adatok a valóságnak megfelelnek, és az abban leírtak a saját, önálló munkám eredményei.

A szakdolgozatban felhasznált adatokat a szerzői jogvédelem figyelembevételével alkalmaztam.

Ezen szakdolgozat semmilyen része nem került felhasználásra korábban oktatási intézmény más képzésén diplomaszerzés során.

Tudomásul veszem, hogy a szakdolgozatomat az intézmény plágiumellenőrzésnek veti alá.

Budapest, 2019. év .....12. hónap ...11 nap

.....

hallgató aláírása

Tartalomjegyzék

Bekövetkezett információ- technológiai incidensek és hatásuk a tőzsdei árfolyamra

1. Az IT incidensek vizsgálatának fontossága

Az elmúlt években nem csak a pénz- és tőkepiacokon, hanem minden iparágban egyre magasabb technikai, technológiai szinten történik a termelés és a szolgáltatások nyújtása. Ezzel egyidejűleg folyamatosan változik a jogi, szabályozási környezet, ennek következtében a cégek szervezeti struktúrája is.

A változó környezetben és az állandó éles versenyhelyzetben szükségszerűen fontossá vált a kockázatok feltérképezése, kezelésükre működő módszertanokat kellett kialakítani mind a szigorú jogi szabályozás miatt (például Baseli tőkeegyezmények), mind az egyes vállalatok saját érdekében: a cég vásárlók általi pozitív megítélése, bizalom megszerzése és megtartása, a visszaélések következtében történő veszteségek minimalizálása, így a kockázatok kezelésének fontossága is előtérbe került. Ezen veszteségek lehetnek anyagiak és nem anyagiak egyaránt:

Nem anyagi veszteség érheti a vállalatot reputációs kár formájában, ha egy bekövetkezett esemény miatt megromlik a cég hírneve, megítélése, az ügyfelek/ potenciális ügyfelek elveszítik bizalmukat. Anyagi veszteség lehet az esemény miatt kiszabott bírság, tőzsdei árfolyam csökkenése, vagy közvetlenül eltulajdonított összeg.

A technológiai fejlődés, a felgyorsult világ új problémák elé állít minden vállalatot. A kockázatok forrása kibővült, a cyberbűnözés: zsarolások, vírusok, jogosulatlan hozzáférések, adatok módosítása stb. nagyléptékű, nagy veszteségekkel járó károkkal fenyegetnek. Ilyen esetek nap, mint nap történnek a világon, melyek során az eltulajdonított adatokkal a nevünkben hitelkérelmeket indíthatnak el, hozzáférhetnek a bankszámlánkon levő összegekhez, új számlákat nyithatnak a nevünkben, vagy akár a teljes személyiségünket eladhatják a feketepiacon.

1.1. A cyberbűnözés definíciója:

A cyberbűnözésnek számos definíciót próbáltak adni, de mivel az egész terület széleskörű és megfoghatatlan, ezért nincsen egyetlen, világszerte elfogadott megfogalmazás:

A Brit Cyberbiztonsági Központ (National Cyber Security Center) megfogalmazása szerint:
A cyberincidens egy olyan csalás vagy csalási kísérlet egy rendszer biztonsága ellen, amely megsérti annak integritását vagy hozzáférhetőségét, és/vagy jogosulatlan hozzáférést kezdeményez az ott található adatokhoz. Általánosságban elmondható, hogy a leggyakrabban észlelt csalások az alábbi típusokba sorolhatók: *(NCSC)*

1. Jogosulatlan hozzáférési kísérlet egy rendszerhez és/vagy annak adataihoz
2. Egy rendszer jogosulatlan felhasználása adatainak feldolgozása, vagy tárolása érdekében
3. Egy rendszer firmware, szoftver, vagy hardvereinek módosítása a rendszergazda hozzájárulása nélkül
4. A szolgáltatás kártékony célú megszakítása és/vagy megtagadása

1.2. Az Európai Unióban hozott rendeletek:

Az Európai Bizottság (European Commission) több rendelettel is küzd a cyberbűnözés ellen:

„A cyberbűnözés elleni küzdelem érdekében az EU -cyberbiztonsági stragégiája keretén belül- jogi szabályozásokat hoz és támogatja a tagállamok együttműködését. Ennek részleteit az **Ellenállóképesség, elrettentés és védelem: az erős EU cyberbiztonság megalkotása** című kommünikéjében fejti ki. Az Európai Bizottság többek között határon átnyúló, a bűnügyi nyomozásokat megkönnyítendő információmegosztási rendszert hoz létre.” *(EC)*

Az Európai Bizottság kulcsszerepet játszott az EC3 (Europian Cybercrime Center) létrehoztásában. A központ 2013 januárjában kezdte meg működését a cyberbűnözés elleni küzdelem központjaként, összegyűjtve a tagállamok bűncselekmények elleni nyomozásainak dokumentumait és európai szintű összefogást tesz lehetővé a törvényhozás és végrehajtás területén.

Legújabb intézkedés:

„A 2013-as információs rendszerek támadásait megakadályozó szabályozás (Directive on Attacks Against Information Systems) fő célja a nagy volumenű cybertámadások megfelelő kezelése, amely a tagállamok számára előírja a megfelelő nemzeti büntetőjog erősítését, valamint erőteljesebb szankciók meghozatalát. 2017-ben a Bizottság kiadott jelentésében összefoglalta az egyes tagállamok által megtett szükséges intézkedéseket annak érdekében, hogy a direktívának meg tudjanak felelni." *(EC)*

Véleményem szerint 2013 óta az EU és a teljes világ is számos változáson ment keresztül, a hackertámadások, információtechnológiai hadviselés, adatszerzési technológiák is rengeteget változtak, ezért szükség lenne az intézkedések sűrűbb frissítésére, új intézkedések beiktatására, mivel csak ilyen módon lehet lépést tartani a nagymértékű változással.

2. Az IT incidensek megjelenése a szakirodalomban

(Böhme 2013) tanulmányában foglalkozik a kérdéssel, ahol megfogalmazza azt, hogy miért fontos a hagyományos és a cyberbűnözést elkülöníteni.

„Átmeneti" bűncselekménynek nevezi azokat, amelyeket az online tér megjelenése miatt a hagyományos felületek helyett ma már az interneten követnek el- ilyenek például a bankkártyacsalások, az új bűncselekmények közé pedig azokat sorolja, amelyek csak az új felületek megjelenésével kezdtek elterjedni és függnek az online tértől. Utóbbiak közé tartoznak a platform- bűncselekmények, például a botnetek használatával történő visszaélések, melyre az általam vizsgált esetek között is olvashatunk majd konkrét példát.

Böhme tanulmányában arról is ír, hogy ugyan a hagyományos bűnözés közvetlenül nagyobb összegű károkat okoz, de a cyberbűnözés miatti közvetett felmerülő költségek (például a támadások elleni védelemre fordított erőforrások, a hírnévromlás miatti üzletvesztés stb.) sokkal magasabbak ennél. Példának pedig azt írja, hogy amíg 2010-ben a világon az összes spam egyharmadát küldő botnet tulajdonosai ezzel 2,7 millió USD-t nyertek, a vállalatok spam- prevenciós kiadásai összességében egymilliárd dollárt is meghaladták- a spamek küldése pedig a cyberbűnözés egyetlen kis szelete csupán.

A probléma az, hogy míg az eboláról napi szinten olvashattunk cikkeket, vagy a migrációs hullámról hallunk nap, mint nap minden kommunikációs csatornán, addig a bekövetkezett cyber károk, amelyek mindenkit (vállalatokat és magánembereket egyaránt) közvetlenül érinthetnek, a következményeikhez képest meglehetősen alul reprezentáltak a médiában, így sem a hétköznapi emberekben, de gyakran a nagyvállalati vezetőkben sem tudatosul eléggé, hogy a XXI. század információs technológiai fejlettsége mennyire behálóz mindent, és ez milyen veszélyeket hordoz magában, így a minket fenyegető veszélyek ellen nincsenek megfelelő intézkedési tervek kidolgozva.

A Price Waterhouse 2014 évi jelentésében Juan Pujadas, a vállalat elnökhelyettesének tanácsadója az alábbi módon hangsúlyozza a téma fontosságát a befektetők számára:

„A cyber biztonság és az adatok illetve adat elemzések növekvő fontossága jó példa a napjainkban tapasztalható diszruptív (a szakdolgozat író megjegyzése: ezek olyan, a meglévő rendszereket szétziláló új szervezetek, formák, mint pl. a Barion, PayPal, stb.) változásoknak. A folyamatosan növekvő cyber fenyegetéseket a világ egyik iparága, egyik cége sem hagyhatja figyelmen kívül. A top menedzsmentek elé kerülő adatbiztonsági kihívások és lehetőségek pedig elkerülhetetlenné teszik az adatok megfelelő értékelését.” *(PWC 2014)*

3. A hazai információtechnológiai környezet

Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hatóság adott ki ajánlást az internettel összefüggő adatkezelések egyes kérdéseiről 2011-ig, amelyben az alábbi területeket érintette:

-külföldre történő adattovábbítás

-kéretlen, üzleti célú spam- üzenetek jogi szabályozása

-nyilvános kulcsú kriptográfia használata

-elektronikus információszabadság

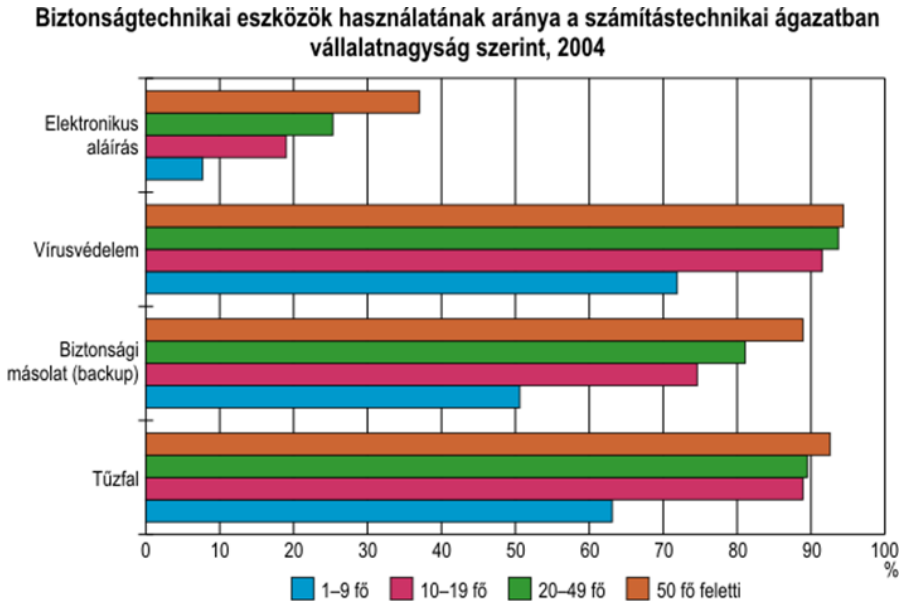
-törvényi szintű szabályozás igénye

-felhasználók és szolgáltatók adatvédelmet illető jogai és kötelezettségei *(Adatvédelmi biztos)*

2011 után azonban Magyarországon megszüntették az önálló adatvédelmi biztosi működést (2011. évi CXII. törvény) és ezután a feladatot az államigazgatási hierarchiába tartozó Nemzeti Adatvédelmi és Információszabadság Hatóság látja el. (Magyar Közlöny, 2011/88. szám, 2011. július 26.)

A törvényt bírálat fogadta, a Társaság a Szabadságjogokért szervezet az alábbiak szerint fogalmazott:
„A változás egyértelmű gyengülést jelent, hiszen a személyes adatok védelmét és közérdekű adatok nyilvánosságát elsősorban éppen azzal végrehajtó hatalommal szemben kell majd biztosítania a hatóságnak, amelytől a léte függ. „ *(TASZ)*

Magyarországon számítógépet a vállalkozások több, mint 90%-a használ, és a cégek nagy része rendelkezik saját honlappal. Az IT biztonság legfontosabb eszközeként ennek ellenére tűzfalakat, vírusirtókat alkalmaznak. Természetesen a nagy cégek - különösen a pénzintézetek – erősebb, komolyabb és szélesebb körű védelmet alkalmaznak, míg a kis és közepes cégeknél akár a biztonsági rendszerek alacsony szintje vagy akár hiánya is előfordul.



1. ábra Biztonságtechnikai eszközök használatának aránya, 2004

(Pergel 2001)

A világ legnagyobb forgalmú szoftvergyártóit tömörítő szervezet, a jogosulatlan szoftver felhasználás ellen küzdő Business Software Alliance elemzése alapján Magyarországon az illegálisan használt szoftverek aránya meghaladja a 44%-ot (2006-os adat), ami magasabb az Európai Uniós átlagnál. Hazánk a bankkártya csalásokban is élen jár a régióban.

AZ OECD már az 1970-es években megfogalmazta európai tagállamaira kiterjedő ajánlását az információbiztonság érdekében és az adatokhoz való illetéktelen hozzáférés ellen. Előterjesztésében a szervezet a számítógépes bűncselekmények négy csoportját határozta meg: csalás, adatokhoz való jogosulatlan hozzáférés, adatok jogosulatlan kezelése / módosítása és a megtámadott cégek, intézmények működésének

megakadályozása. A hackerek új generációjának felnövekedésével egyre nagyobb károkat okoz a zsarolás is. A fiatal számítógépes bűnözők fő motivációja „elsősorban nem az anyagi haszonszerzés, hanem szórakozás, figyelemfelhívás (…). Ezek egy része felelősségtudattal, illetve vétőképességgel, azaz büntetőjogi felelősségre vonás képességével nem rendelkező gyerek vagy fiatalkorú". *(Pusztai, 1989)*

Magyarországon a hatóságok az 1980-as évek első felében kezdtek el komolyabban foglalkozni a számítógépes bűncselekményekkel, és 1964 óta működik egységes rendőrségi – ügyészségi bűnügyi statisztikai adatgyűjtés, amely kiterjed a számítógépes bűncselekményekre is. Ezen új típusú bűncselekmények törvényi tényállását azonban a hatályos BTK nem tartalmazta, a számítógépes csalás „számítógéphez kötött bűncselekmény" néven csak 1994-ben került be a BTK-ba, amelyet pár évvel később, 1999-ben szigorítottak, a változó környezet hatására – ezen időszak alatt a gazdasági bűncselekmények száma ötszörösére, a számítógépes csalások száma négyszeresére nőtt. Ezzel párhuzamosan növekedett a különösen nagy kárt okozó bűncselekmények aránya is *(BM Központi Hivatal).* A csalások azonban a számítógépes bűncselekmények egy részét teszik csak ki, a többi, új típusú bűncselekmény pedig nem az általános „számítógépes", hanem specifikusabb címszóval került be a BTK-ba, pl. bankkártyával kapcsolatos csalásként vagy már eddig is létező címszavak alá, mint pl. szellemi termékhez fűződő jogok megsértése.

Ami ezen bűncselekmények területi elterjedtségét illeti, jóllehet számítógépes csalók mindenhol működnek a világon, vannak "fertőzöttebb" országok, területek (pl. kínai vagy orosz hackerek), Magyarországon ezt a bűncselekményt kezdetben a Budapest centrikusság jellemezte. A bárhonnan elérhető hálózatok, rendszerek miatt ez a területi koncentráció azonban fokozatosan csökken.

(2001 Pergel)

4. A kutatás

A bekövetkezett IT incidensek hatását több szempontból is meg lehet közelíteni. Egy-egy adatszivárgás miatti teljes veszteség nehezen azonosítható, hiszen a közvetlen pénzügyi veszteség, és a kiszabott bírságok mellett az üzletmenet- folytonosság fennakadása, a jogi következmények, reputációs veszteség- az ügyfelek bizalomvesztése közvetetten nem anyagi veszteség, viszont közvetve azt eredményezi.

Kutatásomban a legfontosabb szemponton keresztül arra szeretnék választ kapni, hogy a vállalatok részvényesei miképpen reagálnak az IT incidensekre, ezek nyilvánosságra kerülésére, illetve a vállalat reakcióira, kommunikációjára, intézkedéseire. A legtöbb befektető számára a legfontosabb, döntéseket meghatározó jelzőfaktora egy vállalat értékének szempontjából a piac reakciója, a részvényárfolyam mozgása. Befolyásolja-e egy-egy ilyen hír a részvényárfolyamot, ha igen, akkor pedig milyen irányban és mértékben? Ezek után pedig azt is megvizsgálom, hogy az árfolyam és a hozamok viselkedésének milyen magyarázó tényezői lehettek- például a vállalat milyen módon kommunikált a médiával és a részvényesekkel, illetve milyen intézkedéseket vezetett be stb.

Szakdolgozatom fő célja egyrészt annak bemutatása, hogy milyen lényeges az, hogy az egyes vállalatok megfelelő forrásokat fordítsanak a információ- technológiai környezetük ellenőrzésére, hiszen hatalmas pénzügyi károkat okozhat egy gondatlan lépés, főképp, ha nincsenek megfelelően kidolgozott intézkedési tervek, másrészt szeretném felhívni az olvasók figyelmét is arra, hogy a saját életünkben milyen veszélyekkel kell tudatosan számolnunk és az IT világot fokozott óvatossággal, a saját adatainkra ügyelve használnunk.

4.1. Esetek

Az elemzéshez 6 bekövetkezett, minél frissebb (2017-19-ben történt), nagy káreseményt vettem alapul.

Miért nem magyarországi eseteket vizsgálok?

A magyar esetek többségében megfigyelhető, az incidens csak bankokat érint és mivel a magyar piac világszinten kicsinek minősül, az amerikai piacon viszont nagyobb károk mutatkoznak, az eseményekről több és részletesebb hír olvasható, illetve az USA-ban könnyebben vizsgálhatók más iparágban tevékenykedő vállalatoknál bekövetkező károk is a nagyobb terület lefedésének érdekében. Ezért a tisztább vizsgálat érdekében úgy döntöttem, hogy USA- béli eseteket vizsgálok meg. Ezen kívül a Nasdaq oldalán napi lebontású idősoros historikus árfolyamok könnyű felhasználhatósága miatt is úgy találtam, hogy ezen események jobban vizsgálhatók.

Az eseteket az elemzési módszertan kifejtése után részletezem, illetve a későbbiekben még ki fogok térni a vizsgált időszakban bekövetkezett változásokat esetlegesen magyarázó, a vállalatok által hozott intézkedésekre, a publikus kommunikációjukra (amely intézkedések eredményezhettek mind javulást, mind romlást a cég részvényárfolyamára, hozamaira).

4.2. Az event study módszertan

Az event study módszertant a szakirodalom széles körben használja részvényhozamok vizsgálatára. Lényege az, hogy egy bizonyos időpont körüli eseményablakban (ld. később) kimutatható-e szignifikánsnak mondható abnormális eltérés egy előre kiszámított, elvárt hozamhoz képest. Így a vizsgálat általánosan azt a nullhipotézist fogalmazza meg, hogy a bekövetkezett eseményeknek nincs hatása a hozamok változására tehát a referencia időszak alapján számított, elvárt hozam meg fog egyezni a vizsgált, bekövetkezett esemény által érintett időszak hozamaival.

E módszer szerint a megfigyelhető árfolyamokba minden nyilvános információ beépül, így az általam vizsgált események bejelentése is befolyásolja a részvények árfolyamát (és hozamát).

Az event study módszertan eredete, szakirodalma:

Maga a módszertan és kialakulásának útja sok évtizedre tekint vissza. Legelső alkalmazása valószínűleg még 1933-ra vezethető vissza, amikor (*Dolley 1933)* írt

tanulmányt. A másik leghíresebb eseményelemzés módszerrel dolgozó kutatás 1969-ben jelent meg *(1969 Fama).*

A módszertan a 80-90-es évekre igen közkedveltté vált, ettől az évtizedtől kezdte egyre több event study elemzést tartalmazó kutatás született, illetve 1985-től kezdtek el napi lebontású árfolyamadatokat használni benne *(Brown 1985).*

Az eseményelemzés módszertanával azóta is mind magyar, mind külföldi tanulmányok dolgoztak már. Hazai tanulmány például *(Lublóy 2010)* vagy a szintén event study módszertannal dolgozó *(Szliva 2014).*

A kutatási témák sokszínűsége azt mutatja, hogy ezen módszertan jól használható bármilyen területen bekövetkező esemény hozamra tett hatásának vizsgálatára, jogi- és közgazdasági szabályozások hatásainak elemzésére, infláció alakulásának megfigyelésére, várható GDP számítására stb. Azonban azt vettem észre, hogy a szakirodalom konkrét IT támadások vizsgálatára kevéssé használta még fel az event study módszertant, nincsen sok ilyen témájú tanulmány, ezért döntöttem úgy, hogy ezt a fontos témakört megvizsgálom ilyen módon és megnézem, hogy használható-e erre is a módszertan.

A következőkben szeretném részletesen ismertetni a kiválasztott eseményeket, az eseményelemzés módszertanát, számolásának módját- illetve az itt felmerült problémákat. Ezt követve rátérek az adott események elemzésére és a kapott eredményekre, majd végül bemutatom a konklúziót, amire jutottam kutatásom kapcsán.

4.3. Az adatok

Az elemzés adatai a Nasdaq oldaláról származnak amely az USA-ban működő részvénypiac, az Amerikai Egyesült Államok második legnagyobb elektronikus részvénykereskedelmi rendszere a piaci kapitalizáció és a kereskedelmi volumen alapján. Oldalán az egyes vállalatok adatai megtalálhatóak historikusan listázva, napi szinten,

USD valutában (volumen, nyitó, záró árfolyam, legmagasabb- és legalacsonyabb napi értékek stb.).

Equifax, Inc. Common Stock (EFX) Historical Data

SELECT THE TIMEFRAME : 1M 6M YTD 1Y 5Y MAX DOWNLOAD DATA

DATE	CLOSE/LAST	VOLUME	OPEN	HIGH	LOW
12/06/2019	$138.5	319,903	$139.09	$139.48	$137.94
12/05/2019	$137.94	540,265	$136.74	$137.97	$135.785
12/04/2019	$136.42	512,760	$136.07	$138.02	$136.07
12/03/2019	$136.16	462,018	$136.85	$137.48	$135.56
12/02/2019	$138.23	480,788	$139.57	$140.085	$138.2

2. ábra Az Equifax historikus adatainak részlete a Nasdaq oldalán (Nasdaq)

1.eset: Facebook

2018 március 17-én számos lap közölt óriási port kavaró cikket arról, hogy több, mint 50 millió- későbbi adatok szerint 87 millió- amerikai állampolgár személyes adatait fel az amerikai elnökválasztás befolyásolására, a Facebook közösségi oldalról megszerezve. A megszerzett információk többek között vallási- és politikai nézetek, végzettség, kapcsolati státusz, a felhasználók ismerőseinek adatai és számos esetben chatbeszélgetések voltak.

A történet 2010-ben kezdődött, amikor a Facebook létrehozta az OpenGraph nevű felületet. Ezen a platformon keresztül a felhasználók külső alkalmazásokat használhattak, miközben az applikációk fejlesztői hozzáférést kaptak a közösségi oldalra felkerült személyes adatokhoz. Az akkor felmerülő kétségekre reagálva Zuckerberg nyilatkozatában megígérte, hogy felhasználói adatai megfelelően lesznek kezelve. Ennek ellenére 2013-ban egy marketingstratégia optimalizáló cég, a Global Science Research a Facebook platformján keresztül egy alkalmazással többmillió felhasználó adatához jutott

hozzá: a „Thisisyourdigitallife” elnevezésű app pszichológiai profilt ígért azoknak, akik adataikhoz és ismerőseikhez való hozzáférést engedélyezve kitöltötték a tesztet.

A következő évben a Facebook szigorított a szabályain annak érdekében, hogy felhasználói adatai ne kerülhessenek harmadik fél kezébe. Mivel ezt nem visszamenőlegesen érvényesítették, a Global Science Research nem törölte az összegyűjtött adatokat.

Még 2015-ben kiderült, hogy a választásokon induló egyik republikánus jelölt ezeket az összegyűjtött pszichológiai profilokat használta fel kampányához. A Facebook erre adott válaszában azt mondta, hogy előző évi szigorításai során felhívta a médiaelemző cég figyelmét arra, hogy törölje a megszerzett felhasználói adatokat és hogy a Global Science Research megerősítette, hogy ezt meg is tette. Ennek ellenére 2016-ban a cég ismét beleszólt a választásokba Donald Trumpot segítve a gyűjtött adatok alapján létrehozott irányított hirdetésekkel.

A 2018-ban kitört botrányt Christopher Wylie, a Global Science Research azóta kilépett társalapítója robbantotta ki, amikor a történtetek több nagy lapnak is megírta. A Szövetségi Kereskedelmi Bizottság (FTC) 2018 március 20.-án vizsgálatot indított arról, hogy a Facebook valóban megszegte-e a felhasználók adatvédelmére vonatkozó feltételeket, és Zuckerbergre nagy nyomás nehezedett, hogy nyilatkozzon arról, mi is történt valójában. A következő napon a Facebook alapítója egy nyilvános posztban ezt írta:

„Felelősségünk, hogy megvédjük az adatokat és ha ezt nem tudjuk megtenni, nem érdemeljük, hogy szolgáljunk. Azon dolgozunk, hogy megértsük mi történt és hogy megakadályozzunk, hogy ez megismétlődjön.” *(Guardian)*

Két héttel később pedig teljes oldalas hirdetésekben kért bocsánatot felhasználóitól több amerikai és brit újságban. Azon kívül viszont, hogy az ügyben érintett szabálysértőket kitiltotta a közösségi oldalról, további lépéseket nem tett.

3. ábra A Facebook árfolyamának alakulása a New Yorki tőzsdén a bejelentést követő napokon

(nyse)

A Facebook ellen több eljárás is indult, létrejötte óta ez volt a legsúlyosabb eset, amikor a felhasználók adatait nem megfelelően kezelték. Az ügy nemcsak az Egyesült Államokban, de a világ minden részén óriási felháborodást keltett, a közösségi oldal tőzsdei kapitalizációja a bejelentések után 61 milliárd dollárral csökkent.

2.eset: Equifax

2017 május és júliusa között nagyjából 143 millió amerikai ügyféladatot loptak el az Equifax hitelbíráló cég weboldaláról. A hackerek az Apache Struts webfejlesztő programon keresztül jutottak hozzá nevekhez, címekhez, 209 ezer ügyfél bankkártyaadataihoz, 2,4 millió jogosítványadathoz és egyéb személyes adatokhoz. Az Equifax tájékoztatása szerint Nagy Britanniában nagyjából 400 ezer, Kanadában 100 ezer ügyféladat kompromittálódott.

A cég a támadást 2017 július 29.-én észlelte és azonnal hatállyal megbízta az ügy kivizsgálásával a Mandiant kiberbiztonsági vállalatot. Az esetet szeptember 7.-én hozták csak hivatalosan nyilvánosságra arra hivatkozva, hogy a hír ne befolyásolja a már folyamatban lévő nyomozást. A társaság tájékoztatta érintett ügyfeleit és egy külön információs weboldalt hozott létre számukra, hogy ellenőrizhessék adataik kikerülésének lehetőségét. Az oldalra a vezetéknév és a társadalombiztosítási azonosító szám

megadásával lehetett belépni. A honlapon keresztül az ügyfelek számára ingyenes védelmet ajánlottak személyiséglopás ellen és lehetőséget további hitelezési kérelem befagyasztására.

4. ábra Az Equifax árfolyamának alakulása a New Yorki tőzsdén a bejelentést követő napokon

(nyse)

A média és a hatóságok kritikusan fogadták az Equifax kommunikációját, az ügyfelek nem találták elég biztonságosnak a létrehozott új weboldalt, hiszen ott további személyes adatokat kellett megadniuk. A bizalmatlanságot tovább növelte az a tény, hogy a tájékoztató oldal domainje (exuifaxsecurity2017.com) és a felülete adathalász oldalra hasonlított. Még szeptember folyamán Nick Sweeting szoftverfejlesztő be is bizonyította a weboldal sebezhetőségét azzal, hogy egy azonosan kinéző domaint hozott létre, az Equifax pedig véletlenül ezt a hamis domaint osztotta meg Twitter fiókjában és bár a bejegyzést hamarosan kitörölték, sok ügyfél kattintott rá a hamis oldalra. A vállalat ezért a hibájáért is elnézést kért.

További felháborodást okozott amikor kiderült, hogy 2017 augusztus 2.-án, nemsokkal az adatok kikerülése előtt az Equifax három vezető tisztségviselője 1,8 millió dollár értékben eladta céges részvényeit. A vállalat szóvivői nyilatkozata szerint a tranzakciók nem az incidens ismeretében történtek- azaz nem bennfentes kereskedelem történt. Ugyanebben a hónapban a cég számos vezetőjét nyugdíjaztam például két senior IT biztonsági vezetőt és Richard Smith gazdasági igazgatót is.

2017 szeptemberében két csoport peres eljárást is indítottak a vállalat ellen Kanadában és a Kanadai Szövetségi Kereskedelmi Bizottság (Federal Trade Commission) és az Adatbiztonsági Hivatal (Office of the Privacy Commissioner) vizsgálatot indított az ügyben.

3.eset: Under Armour

Az Under Armour leányvállalata a MyFitnessPal egy ingyenes okostelefonos alkalmazás. Az oldal kalóriaszámlálási lehetőséget és étrend tanácsadást kínál felhasználóinak. A vállalat 2018 március 30.-án bejelentette, hogy 25.-ei felfedezésük szerint 150 millió MyFitnessPal felhasználói fiók adatai kerültek ki az adatbázisukból. A nyilvánosságra jutott adatok főképp felhasználói nevek, jelszavak és e-mail címek voltak. Bankkártya adatok és egyéb, személyes okmányadatok nem kerültek ki.

Az Under Armour egy 1996-os alapítású, baltimore-i központú, amerikai, főképp sportruházat gyártással foglalkozó óriásvállalat, amely 2015-ben vásárolta fel 475 millió dollárért a MyFitnessPalt, amelynek bevétele a nagyságrendek szemléltetésének érdekében számszerűsítve: 2017-ben az Under Armour teljes ötmilliárd dolláros éves bevételéből 1,8 %-ot tett ki.

Márciusi bejelentésében annyit közölt, hogy a leányvállalatuk adataihoz jogosulatlan felek szereztek az előző hónapban hozzáférést, ezt azonban csak nemrég fedezték föl, illetve, hogy a vállalat azonnali intézkedéseket hozott a probléma jellegének és méretének azonosítására és az érintett felhasználók minél hamarabbi figyelmeztetésére.

5. ábra Az Under Armour árfolyamának alakulása a New Yorki tőzsdén a bejelentést követő napokon

(nyse)

A MyFitnessPal a bejelentés után négy nappal értesítette a felhasználóit az incidensről az alkalmazáson belül küldött üzenet formájában, amelyben felszólította őket az azonnali jelszóváltoztatásra, illetve javaslatokat fogalmazott meg a továbbiakban tehető biztonsági lépésekről.

A vállalat nyilatkozatában hangsúlyozta, hogy az ügyet megoldandó, a legjobb adatbiztonsági cégekkel dolgozik együtt. A bejelentést követően az Under Armour részvényeinek értéke közel 4%-ot estek a zárás utáni kereskedés alatt (ún. after- hours trading- AHT- a neve azon kereskedési módnak, amely során különböző elektronikus platformokon a tőzsde zárása után is lehet részvényekkel kereskedni, mivel a teljes részvénypiac nem áll le teljesen az éjjeli órákban, a tőzsde zárása után sem), összességében azonban nem látható nagyobb mértékű csökkenés ezen időszakban, sőt, a jövőben emelkedésnek indult.

A leányvállalat saját oldalán található részletes nyilatkozat a történtekről és a hozott intézkedésekről, amely szerint a felhasználók tájékoztatásán kívül a hatóságokkal együttműködve a továbbiakban folytatták az oldalon az esetleges gyanús tevékenységek feltérképezését, illetve fejlesztik a rendszereiket, hogy a jövőben megelőzzék az ehhez hasonló adatszivárgásokat. Ezen kívül azt is leírták, hogy a kikerült jelszavak nagyrésze egy „bycript” nevű adattitkosító matematikai módszerrel volt védve és hogy az

adatszivárgás fizetési adatokat sem érint, mert azokat a vállalat külön rendszerben dolgozza föl.

Az ügy egy évvel később, 2019 február 14.-én ismét a figyelem középpontjába került, amikor a kiszivárgott adatokat a hackerek elkezdték a feketepiacon értékesíteni, de mivel a MyFitnessPal mindenkit kötelezett a jelszava megváltoztatására, ezért a kínált adatokra nem volt nagy a kereslet, hiszen azok már nem voltak érvényesek. Ennek ellenére viszont azok számára, akik több helyen használták ugyanezen jelszavukat és máshol nem változtatták azt meg, mégis problémát okozhatott az értékesítés.

4.eset: First American Financial Corporation

A First American Financial Corporation egy amerikai székhelyű, pénzügyi szolgáltatásokat nyújtó nagyvállalat (2018-ban a teljes éves bevételük 5,7 milliárd USD volt a cég honlapján található, befektetőknek szóló összefoglalójából). *(FAF)*

2019 május 24.-én látott napvilágot a hír, hogy 2003 óta 885 millió ügyfél jelzáloghitel kérelemhez benyújtott dokumentumai kerültek nyilvánosságra a vállalat adatbázisából. Az adatlopást a KrebsOnSecurity nevű, Brian Krebs oknyomozó riporter által üzemeltetett vállalat egyik fejlesztője fedezett fel- és a nagyvállalatot azonnal értesítette. A kikerült adatok között egyaránt nyilvánosan elérhetőek voltak bankszámlaszámok, kivonatok, jelzálog- és adónyilvántartások, társadalombiztosítási számok, a banki tranzakciók nyugtái és jogosítványfotók.

Egy amerikai ingatlanfejlesztő nyilatkozata szerint bárki, aki ismert egy url linket egyetlen dokumentumhoz, a linkben egy-egy szám megváltoztatásával újabb titkos dokumentumokat érhetett el- így bárkinek az adata nyilvánosan elérhető volt, aki valaha, valamit is küldött a Fist Americannak e-mailen keresztül. A vállalat honlapja a cég elmondása szerint egy tervezési hiba folytán az adatok eléréséhez nem kért hitelesítést.

6. ábra A First American árfolyamának alakulása a New Yorki tőzsdén a bejelentést követő napokon

(nyse)

A honlapot még aznap, délután kettőkor lezárták a hiba miatt, ám egy másik internetes útvonalon keresztül (archive.org) a továbbiakban is még évekre visszamenőleg megnyithatók voltak a bizalmas dokumentumok url-jei.

A vállalat nem kommentálta sem a kikerülés okát, sem pedig a kiszivárgott dokumentumok hatalmas mennyiségét és a nyilvánossá válásuk hosszát, szóvivőjük mindössze ennyit nyilatkozott:

„A vállalat azonnali intézkedéseket tett a helyzet orvoslására és az alkalmazáshoz való külső hozzáférés lezárására. Jelenleg azt vizsgáljuk, hogy ez az eset milyen hatással van az ügyfélinformációk biztonságára. Amíg a belső felülvizsgálatunk be nem fejeződik, addig nem adhatunk további információkat."

Az eset a hatóságok figyelmét is felkeltette: rövidesen az Egyesült Államok Értékpapír- és Tőzsdebizottsága (SEC) és a New York-i Pénzügyi Szolgáltatások Minisztériumának (NYDFS) cyberbiztonsági részlege is elkezdte vizsgálni azt, hogy a vállalat törvényt sértett-e, illetve a First American ellen számos pert, illetve csoportos keresetet is indítottak.

Az First American június 18-án elmondta, hogy egy külső céggel felülvizsgáltatják a rendszernaplókat és 484 fájlt azonosítottak, amelyekhez valószínűleg engedély nélkül fértek hozzá jogosulatlan személyek. A megnevezett érintett fájlok alapján 32 személy magánjellegű adatai voltak ténylegesen érintettek- a többi dokumentum nem tartalmazott bizalmas információkat-, ezen ügyfeleket pedig értesítették és ingyenes adatmonitoring szolgáltatást ajánlottak fel számukra.

5.eset: Marriott International

A Marriott International egy amerikai tulajdonú, nemzetközi vendéglátóipari vállalat szállodaláncokkal (Magyarországon is), szórakoztatóipari franchiseokkal. 2018 november 30.-án a Mariott bejelentette, hogy a Starwood Hotel szállodalánca adatkikerülés áldozata lett.

2018. szeptember 8-án a Marriott jelzést észlelt egy belső biztonsági rendszerétől, amely azt mutatta, hogy valaki megkísérelte elérni a Starwood vendégfoglalási adatbázisát az Egyesült Államokban. A vállalat a biztonsági vezetők bevonásával elkezdte vizsgálni az esetet, amely során kiderült, hogy 2014 óta jogosulatlanul férnek hozzá a Starwood hálózathoz.

A támadást a vállalatnak végül november 19.-én sikerült azonosítania és kiderítette, hogy az adatszivárgás mindegy ötszázmillió ügyfelének személyes adatait érintette, akik szeptember 10.-e előtt foglaltak a szállodalánc brit szállodáinál. Azt is felfedezték, hogy a hackerek a jogosulatlanul elért adatokat lemásolták, titkosították és már megkezdték azok kivitelét a szálloda rendszeréből.

A támadás mintegy 31 ország lakosait érintette, amelyek közül hétmillió brit állampolgár, a többi pedig az Európai Gazdasági Térségben lakó személy. Az ötszázmillió érintett illetőből körülbelül 327 millió esetében a támadók hozzájutottak a névhez, levelezési címhez, telefonszámhoz, e-mail címhez, útlevélszámhoz, a Starwood Preferred Guest (SPG) számlainformációihoz, születési dátumhoz, az érkezési és távozási információkhoz, a szállásfoglalás dátumához. Néhány esetben a kiszivárgott adatok között bankkártyaszámok és a bankkártyák lejárati dátuma is szerepelt, azonban a fizetési

adatok a szállodalánc elmondása szerint az ún. Advanced Encryption Standard titkosítással (AES-128) voltak titkosítva. A bankkártyaadatok visszafejtéséhez szükséges kódolásról azonban nem tudták megmondani, hogy szintén hozzájutottak-e a hackerek. November 30.-án, a bejelentés napján a részvényárfolyam 6,9%-ot esett.

7. ábra A Marriott árfolyamának alakulása a New Yorki tőzsdén a bejelentést követő napokon

(nyse)

2019 július 9.-én az ICO (Information Comissioner's Office) az Egyesült Államok Értékpapír- és Tőzsdebizottságával együtt kiadott egy közleményt arról, hogy a vállalatra a GDPR törvények megszegése miatt 99 millió font (több, mint 39 milliárd Forint) bírságot szabnak ki.

Az ICO bírálata szerint a szállodalánc rendszerében a támadók már 2014 óra bent voltak. A Marriott a Starwood felvásárlásakor 2016-ban azonban nem végezte el a szükséges biztonsági vizsgálatokat, így a nem megfelelő átvilágítás miatt nem tudták a támadást felfedezni, így történhetett, hogy erre csak a rendszer feltörése után négy évvel sikerült rájönniük. A vállalat együttműködött a felügyeleti vizsgálatok folyamán és elkezdte kijavítani a megnevezett hibákat. (ICO)

6.eset: Ticketmaster

Magyarországon is sokan használják a Ticketmaster nevű online jegyvásárlási oldalt, amely 2010 óta a Live Nation Entertainmenttel összeolvadva működik. A vállalat 2018 június 23.-án fedezte fel, hogy 2017 szeptemberétől kezdődően mindegy negyvenezer felhasználó adatait (neveket, címeket, fizetési és bejelentkezési adatokat stb.) tulajdonítottak el honlapjukon keresztül nemzetközi szinten.

A cég elmondása szerint az adatlopás egy külső szolgáltatójuk, az Inbenta online chatbotján keresztül történt, amely a Ticketmaster oldalán történő foglalást és jegyvásárlást segítette. A vállalat a probléma felfedezése után az alkalmazást azonnal eltávolította- addigra azonban az adatlopás már majdnem egy éve folyt.

Inbenta elmondása szerint a chatbot a Ticketmaster megrendelési utasításai szerint lett személyre szabva, más honlapok nem használták. Elismerték, hogy a megírt Java Script kód sebezhető volt, de a chatbotot készítő vállalat azt állítja, hogy a Ticketmaster nem megfelelően használta azt, mivel a fizetési oldalon alkalmazta és mivel erről az Inbentát nem tájékoztatta, így figyelmeztetni sem tudták őket a kockázatra.

A támadók ezt a sebezhetőséget kihasználva tudták a szoftver kódját úgy módosítani, hogy a jegyeladó oldal ügyfeleinek fizetési adatait megszerezzék.

A vállalat június 27.-én e-mailben értesítette azon vásárlóit, akik a gyanú szerint érintettek lehettek az ügyben. Számukra létrehoztak egy tájékoztató oldalt, ahol 12 hónapos ingyenes biztonsági megfigyelést ajánlottak fel, amelyben a bankkártyaforgalmat vizsgálják esetleges fraud (csalás), illetve személyazonossággal való visszaélések után kutatva.

8. ábra A Live Nation árfolyamának alakulása a New Yorki tőzsdén a bejelentést követő napokon

(nyse)

Eközben a Monzo internetbank nyilatkozatából kiderült, hogy ők már 2018 április 6.-án felfedeztek gyanús tranzakciókat, amikor észrevették, hogy fraud panasszal élő ügyfeleik 70%-a a Ticketmaster oldalán használta bankkártyáját. A problémára a jegyeladó oldal figyelmét is felhívták, ám az április 19.-én visszajelzett a Monzonak, hogy a belső vizsgálat során nem találtak semmilyen bizonyítékot az esetek összefüggésére. A Monzo biztonsági okokból ennek ellenére 2018 április 19-20.-ám mintegy hatezer, vélhetően érintett ügyfelének bankkártyáját cserélte le.

Ez az eset az első szerződésszegések közé tartozik, amelyek a GDPR szabályozás alá esnek.

2019-ben a Hayes Connor ügyvédi iroda 650 ügyfelének nevében pert indított a Ticketmaster ellen. Állítása szerint ügyfeleinek adatai is kiszivárogtak a támadás folyamán, ezért összesen 5 millió angol Fontot (majdnem kétmilliárd Forintot) követelnek a vállalattól, miután a bíróságon kívüli megegyezés sikertelenül zárult.

A módszertan számolásának elmélete

A fentiekben már megfogalmaztam az elemzési módszertan kiválasztásának okait, illetve a vizsgálni kívánt eseteket, a továbbiakban pedig szeretném bemutatni azt, hogy a vizsgálatot milyen módon folyattam le.

Adatbázis:

A Nasdaq oldalán megtalálható adatokból idősoros adatbázist készítettem a fent említett vállalatokra lebontva, amely tartalmazta az esemény által érintett időszakot, illetve előtte- és utána is egy referencia, illetve egy lecsengési időszakot is.

	A	B	C	D	E	F	G	H
1		CLOSE/LAST (USD)	VOLUME (PCS)	OPEN (USD)	HIGH (USD)	LOW (USD)	Hozam	
2	2018.02.01	45,97	889,941	44,65	46,08	44,5		
3	2018.02.02	44,73	1,184,471	45,9	46	44,73	2,799552	
4	2018.02.05	43,69	1,131,274	44,28	45	43,61	-3,52941	
5	2018.02.06	43,94	1,539,976	43,45	44,04	42,71	-1,87444	
6	2018.02.07	44.22	1.130.832	44.2	44.84	43.87	1.726122	

9. ábra Saját szerkesztés- Részlet az elkészített adatbázisból

Az adatbázisom napi lebontású értékekből áll, a vizsgált időszak minden napjának (amelyen tőzsdei kereskedés folyt) nyitó, záró, adott napi legmagasabb és legalacsonyabb árfolyamát tartalmazza USD-ben, illetve a napi kereskedési volumeneket. Ezen kívül kiszámoltam az egyes napi hozamokat is, mivel az event study hozamokkal számol, nem pedig az árfolyamokkal, amelyet a későbbiek miatt itt fontos hangsúlyoznom.

$$r = \frac{\text{következő napi nyitó árfolyam (USD)}}{\text{előző napi nyitó árfolyam (USD)}} * 100 - 100\ (\%)$$

Eseményablak:

Az egyes esetekben az eseményablaknak (event- window) az adott eset hivatalos bejelentésének dátumát választom, mivel (Seiler 2005) kutatásában az objektivitás megőrzésének érdekében ezt javasolja és túl szubjektív lenne egy ettől eltérő dátumot

meghatározni, hiszen nem tudhatjuk biztonsággal megállapítani azt, hogy egy esemény kiszivárgott-e hamarabb és ha igen, erről mennyien és kik szereztek tudomást.

Valójában az eseményablakot kissé nehéz pontosan meghatározni, hiszen a hivatalos bejelentést megelőzően is megtörténhet az esemény kiszivárgása, így ez a hivatalos bejelentés előtt is befolyásolhatja már az árfolyamváltozást- emiatt a bejelentés előtti és utáni időszakot is vizsgálni kell. Az objektivitást megtartva tehát érdekében tehát az eseményablak kezdetének nagyjából a hivatalos bejelentést határoztam meg, de a kiszivárgást is figyelembe véve az eseményablak ennél pár nappal előbb kezdődik és nem csak egy napot tartalmaz, hanem egy relatív rövid, de többnapos időtartamot, amely hossza az egyes eseteknél eltér.

Fontos azonban az, hogy az eseményablak ne legyen túl hosszú, hiszen így nagyobb lenne annak az esélye, hogy ezalatt az idő alatt a szóban forgó incidensen felül, az árfolyamot szintén befolyásoló egyéb események is bekövetkezhetnek.

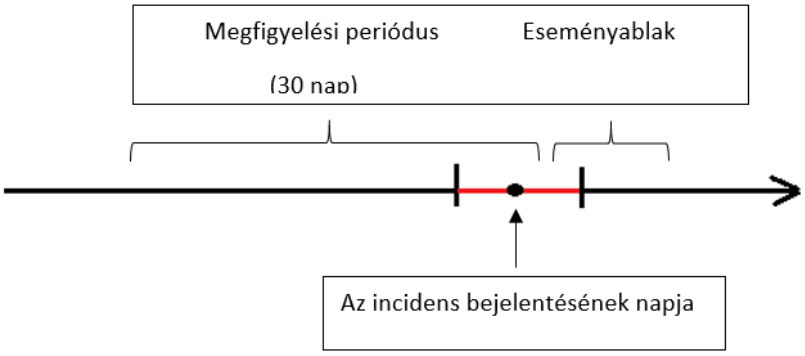
Megfigyelési periódus:

A megfigyelési periódus lényege egy olyan intervallum meghatározása, amelyben megvizsgálható, hogy az árfolyam milyen módon mozog normális időszakban (amikor még nem következett be a vizsgált esemény). Optimális esetben ebben a periódusban nem történhet másik, az adott vállalatot érintő, az árfolyamra hatást gyakorló eset, így a megfigyelési periódusban nem jelennek meg extrém elemek.

A szakirodalomban kedvelt hossz a megfigyelési periódusra 100 nap (Seiler, 2005), azonban kutatásomban ezt lerövidítettem, hiszen véleményem szerint több, mint három hónap alatt számos egyéb olyan eset történhet, amely befolyásolhatja a vállalat részvényértékének változását, így a megfigyelési periódus „tisztasága” nem lesz megfelelő. Ezen okból kifolyólag jelenlegi kutatásomban megfigyelési periódusnak az eseményablak előtti harminc napot választottam ki.

A vizsgálati periódus kiválasztása sok bizonytalansággal jár, hiszen míg egyes bekövetkező események (például két nagyvállalat összeolvadása, vagy egy törvény bevezetése) viszonylag pontosan datálható, addig egy hacker támadás ügye hónapokig, évekig húzódhat, így az árfolyamra is sok ideig lehet hatással- elég példaként említeni az

egyik vizsgált esetet, az Under Armour-t (MyFitnessPal), ahol a 2018-as nyilvánosságra kerülés után az ügy 2019-ben ismért a figyelem központjába került, amikor az addig bujkáló hackerek egy év után elkezdték az ellopott adatokat értékesíteni a feketepiacon.



10. ábra Saját szerkesztés- Az eseményablak és a megfigyelési periódus

Elvárt hozam

Az event study vizsgálat következő lépéseként kiszámolom azt az elvárt hozamot, amelyhez hasonlítani fogom esemény által befolyásolt időszak hozamát és megnézem, hogy helyes-e az a H_0 hipotézis, mely szerint a kettő között nincsen szignifikánsan kimutatható eltérés- azaz a bekövetkezett cyber incidens nem volt hatással a részvények hozamára.

Az elvárt hozam kiszámítása több módon történhet és a szakirodalomban is sok módszert javasolnak erre. Michael J. Seiler 2005-ös kutatásában (Performing Financial Studies: A Methodological Cookbook)

A legtöbb tanulmány egy bizonyos kiválasztott iparági index és a vizsgált vállalat részvényárfolyamának együttmozgását megfigyelve kalkulál elvárt hozamot az eseményablakra. Tehát egy olyan indexet kellene találni, amely megfelelő ahhoz, hogy az adott vállalatok részvényárfolyamával regressziót végezve meg tudjuk állapítani a megfigyelési periódus hozameltéréseit.

Felmerült akadály:

A következő problémába ütköztem: mivel célom éppen az volt, hogy a kiválasztott eseteim ne egy iparágba tartozzanak, hanem többféle szolgáltatást kínáló vállalatok szerepeljenek a kutatásomban (ezért vizsgálok szállodaláncot, közösségi médiumot, hitelbíráló céget, jegyértékesítő vállalatot egyaránt), emiatt nem tudok közösen használható iparági indexet sem alkalmazni, viszont egy általános index pedig hiába lenne elméletben alkalmazható mindegyik esetre, mégis, iparáganként olyan eltérések vannak, hogy ezt tenni nincsen értelme.

Ezt megoldandó, úgy döntöttem, hogy nem alkalmazok regressziót, hanem ehelyett a Nasdaq adatbázisából kigyűjtött nyitó árfolyamok alapján számolok hozamot, a fentebb már említett módon és így fogok referenciahozamokat kapni, így kerülve meg a különböző iparágakba tartozó esetek problémáját.

G3 =D3/D2*100-100

	A	B	C	D	E	F	G
1		CLOSE/LAST (USD)	VOLUME (PCS)	OPEN (USD)	HIGH (USD)	LOW (USD)	Hozam (%)
2	2017.05.01	135	946,358	135,99	136,16	134,44	
3	2017.05.02	136,48	656,953	135,09	136,48	134,75	-0,661813369
4	2017.05.03	136,08	589,189	136,2	136,73	135,88	0,821674439
5	2017.05.04	136,86	507,958	136,05	137,05	136	-0,110132159
6	2017.05.05	138,81	514,106	137,13	138,94	136,79	0,793825799
7	2017.05.08	137.23	416.243	139.18	139.5	137.04	1,494931817

11. ábra Saját szerkesztés- A hozamok számításának módja az eltérő iparágak miatt

t- próba

Az ablakbeli hozam eltérésének szignifikanciáját az elvárttól t- próba segítségével határoztam meg 95%-os szignifikanciaszinten. A fentebb említett hipotézis szerint tehát:

H_0 átlag= referencia átlag

$$t = \frac{\text{átlag- referencia}}{\frac{\sqrt{s}}{n}}$$

ahol n: az eseményablak napjainak száma

s: az eseményablak szórása

átlag: a megfigyelési időszak abnormálisnak gondolt hozamainak átlaga

A t-próbához továbbá kritikus értéket számoltam, 95%-os szignifikancia szinten, n-1 szabadságfokon.

4.4. Eredmények

A hozamok elemzését az excelben végeztem el a szintén itt összegyűjtött adatbázisom alapján. A t-próba kritikus értékének számításához T.INVERZ függvényt alkalmaztam. Az egyes esetekhez pedig a Nasdaq adatai alapján ábrát készítettem a referencia és eseményablak árfolyamairól (nyitó, legmagasabb és legalacsonyabb árfolyam USD-ben).

Facebook

A Facebook esetén a bejelentés időpontja 2018.03.17.-e volt, így az eseményablak 2018.03.14-2018.03.28-ig lett véve, annak érdekében, hogy az esetlegesen 1-2 nappal előbb kiszivárgó hírekkel is számoljak, illetve az eseményablak elég hosszú legyen, de nem olyan hosszú, hogy más befolyásoló esemény is történjen közben. Az egyhünapos referencia intervallum így 2018.02.13-2018.03.13-ig tart. Ezek alapján a hozamokkal számolva (%-os értékben):

Referenciaátlag: 0,40
Ablakra számolt átlag: -1,80
Ablakra számolt szórás: 2,02
t: -2,20
Kritikus érték: -1,81

Az eltérés láthatóan szignifikáns, mivel a t- próba abszolút értéke nagyobb a kiszámolt kritikus értéknél, ezért a H_0 hipotézist elvetjük- a H1 hipotézist fogadjuk el, amely szerint az event window hozamai 95%- os szinten szignifikánsan eltérnek a referenciaidőszak hozamaitól, tehát a vizsgált incidens befolyásolta, és oka volt az eltérésnek.

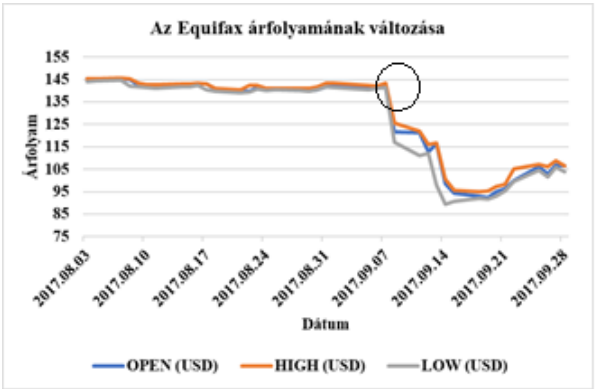
12. ábra Saját ábra- A Facebook árfolyamának változása

Az általam készített ábrán az árfolyamok változása látható, nem pedig a hozamoké- utóbbiról azért nem tartottam érdekesnek ábrát csatolni, mivel a rövid időszak azt a problémát vetette fel- amelyet később az event study módszertan kritikájában kissé kifejtek- hogy a szórás nagyon nagy, emiatt nem kaptam jól áttekinthető hozamábrát.

Equifax

Az Equifax az előbbi esethez hasonlóan szignifikáns eredményt adott, így ezt, és az árfolyamábrát csak röviden írom le:

A bejelentés időpontja 2017.09.07.-e volt, így az eseményablak 2017.09.04-09.21-ig lett véve. A referencia intervallum 2017.08.03-09.03-ig tart. Ezek alapján:



13. ábra Saját ábra- Az Equifax árfolyamának változása

Referenciaátlag: -0,100842751

Ablak átlag: -2,792051687

Ablakra szórása: 5,900749547

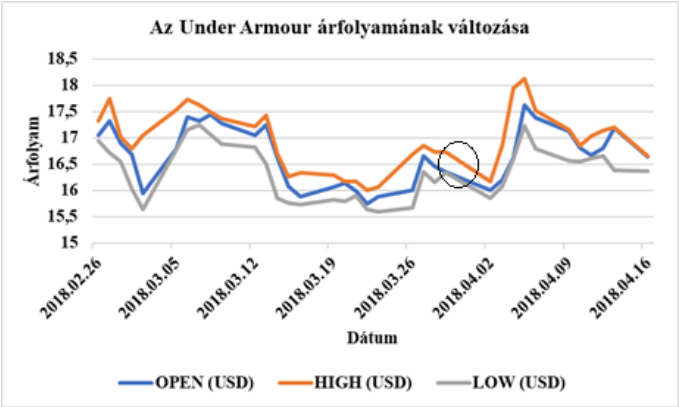
t: -2,691208936

Kritikus érték: -1,782287556

Szignifikáns

Under Armour

Az Under Armour és a további esetek nem szignifikáns eredményt adtak:



14. ábra Saját ábra- az Under Armour árfolyamának változása

Az Under Armour esetén a bejelentés időpontja 2018.03.30.-a volt, az eseményablak 2018.03.27-04.11 -ig lett véve. A referencia intervallum így 2018.02.26-03.26-ig tart. Ezek alapján:

Referenciaátlag: -0,197631279

Ablakra számolt átlag: 0,40666286

Ablakra számolt szórás: 2,723715657

t: 0,604294139

Kritikus érték: -1,812461123

Az kiszámolt értékek szerint tehát a vizsgált ablak hozama nem tér el a referencia időszak hozamától, így nem jelenthető ki, hogy a bekövetkezett incident befolyásoló hatással volt a hozamra. Mi lehet ennek az oka?

Egyrészt a H_0 hipotézis elfogadásának egyik oka az lehetett, hogy túl rövid időszakokat vizsgáltam annak érdekében, hogy más befolyásoló esemény ne következzen be, így viszont a kevés elemszám nagy szórása miatt a módszer az eltéréseket a véletlenhatásnak tudhatja be.

Másrészt érdemes figyelembe venni, hogy amint az Under Armour esettanulmányában azt leírtam, az óriásvállalatnak csupán egy kis leányvállalatánál következett be az incidens („2015-ben vásárolta fel 475 millió dollárért a MyFitnessPalt, amelynek bevétele a nagyságrendek szemléltetésének érdekében számszerűsítve: 2017-ben az Under Armour teljes ötmilliárd dolláros éves bevételéből 1,8 %-ot tett ki”- Részlet a fentebb kifejtett esettanulmányból).

A vállalat intézkedését és kommunikációját több cikk is pozitívan értékelte, amely az egyik oka lehet annak, hogy az Under Armour eseményablakában nem látható a többi esethez hasonlítható méretű részvényárfolyam csökkenés. A Forbes cikke például így fogalmaz:

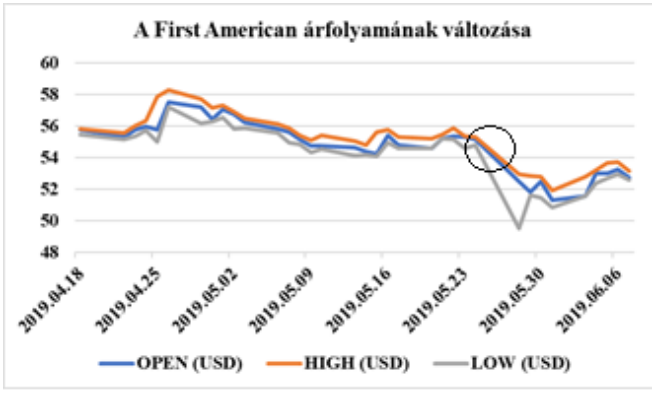
„Az Under Armour némi elismerést érdemel felhasználóinak gyors értesítése miatt, amint a problémát fölfedezték. Nem ritka, hogy egyes vállalatok hetekkel vagy hónapokkal késleltetik azt, ami elkerülhetetlen.” *(Forbes)*

A MyFitnessPal esete azt is mutatja, hogy az IT incidensek időbelisége nagyon eltér a hagyományos esetektől, hiszen az alkalmazástól ellopott adatokat a hackerek csak egy év múlva kezdték el árulni a feketepiacon. Ezért is ütközik problémába ezen terület event study módszertannal történő vizsgálata, mely egy eseményablakot határoz meg, viszont a hackertámadások, adatok kiszivárgása és eladása gyakran hónapokba, évekbe telhet, újra-és újra fellendülhet egy-egy eset híre, így az többször, eltérő időszakokban befolyásolhatja az árfolyamot, hozamot.

A további két eset szintén nem szignifikás eredményt adott annak ellenére, hogy a készített ábrán látványosan megfigyelhető az árfolyam csökkenére. Ennek okáról a későbbiekben, az event study módszertan kritikájánál fogok beszélni, így ezeket röviden írom le:

First American

A First American esetén a bejelentés időpontja 2019.05.24.-e volt, így az eseményablak 2019.05.21-05.31-ig lett véve. A referencia intervallum így 2019.04.18-05.20-ig tart.



15. ábra Saját ábra- a First American árfolyamának változása

Ezek alapján:

Referenciaátlag: -0,10005685

Ablak átlaga: -0,753070382

Ablak szórása: 2,043130078

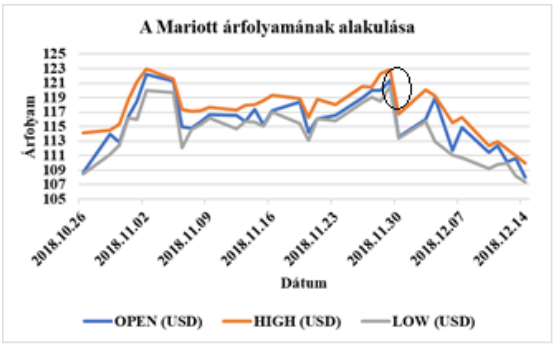
t: -0,653013532

Kritikus érték: -1,894578605

Nem szignifikáns

Marriott International

A Marriott esetén a bejelentés időpontja 2018.11.30.-a volt, így az eseményablak 2018.11.27-12.10-ig lett véve. A referencia intervallum így 2018.10.26-11.26-ig tart. Ezek alapján:



16. ábra Saját szerkesztés- A Marriott árfolyamának alakulása

Referenciaátlag: 0,479700491
Ablak átlag: -0,666037644
Ablak szórás: 3,621076303
t: -1,145738135
Kritikus érték: -1,859548038

Nem szignifikáns

Ticketmaster

A Ticketmaster esetén a bejelentés időpontja 2018.06.27.-e volt, így az eseményablak 2018.06.25-07.05-ig lett véve. A referencia intervallum így 2018.05.22-06.22-ig tart. Ezek alapján:

Referenciaátlag: 0,296877632

Ablakra számolt átlag: 0,257996635

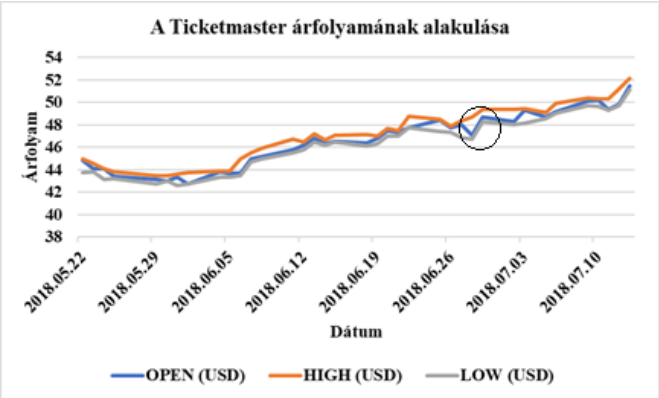
Ablakra számolt szórás: 1,963067761

t: -0,038880996

Kritikus érték: -1,894578605

Nem szignifikáns

A Ticketmaster esete az egyetlen, ahol egyrészt az event study elemzés is azt mutatja, hogy nem tér el a referencia időszak az ablaktól, másrészt pedig az árfolyam ábrámon sem mutatkozik a többi esethez hasonló, látványos törés- sőt, a csökkenés helyett egy enyhe növekedési tendencia is megfigyelhető.



17. ábra Saját szerkesztés- A Live Nation árfolyamának alakulása

A Ticketmaster esete ért legnagyobb meglepetésként. A hackertámadásról rengeteget cikkeztek, minden portálon hatalmas adatlopásról írtak és valóban, az esettanulmányom szerint is többtízezer ügyfél adatai kerültek jogosulatlan kezekbe.

Mi lehet mégis az oka annak, hogy a Ticketmaster tulajdonosa, a Live Nation gyakorlatilag meg sem érezte ezt a nagy incidenst? Lehet, hogy a „too big to fail" eset áll esetleg fenn?

Első gondolatom az volt, hogy ugyanannak a helyzetnek a fordítottja áll fönn, mint az Under Armour esete- azaz itt most nem a vizsgált vállalat hatalmas a tulajdonolt vállalathoz képest és ezért nincs nagy csökkenés, hanem a vizsgált Ticketmaster túl kicsi méretű az őt tulajdonló Live Nationhoz képest (akinek az árfolyamát vizsgáltam, mivel ez van bejegyezve a tőzsdén) és emiatt nem látszik az anyavállalatnál változás. Ám ez az elméletem nem bizonyult igaznak.

Hogy a két vállalat méretéről képet kapjak, megnéztem a 2018-as éves bevételeket: A Live Nation esetén ez 10,8 milliárd USD volt, míg a Ticketmasternél 5 milliárd dollár folyt be a bruttó tranzakciós díjkifizetésekből (ún. „fee- bearing GTV"). Egy, a vállalat növekedését elemző cikkből látható, hogy a Ticketmaster a Live Nation aranytojást tojó tyúkja, hiszen a hacker támadás ellenére is a Ticketmaster évek óta az anyavállalat legnagyobb növekedést produkáló cége, 2018-ban az előző évhez képest 14%-kal jobb eredményt ért el.

(Billboard)

Tehát véleményem szerint annak, hogy sem az ábrán, sem az event study módszertan szerint nem látható szignifikáns eltérés a vizsgált eseményablakban, az egyik oka egyszerűen az, hogy az emberek világszerte használják a Ticketmastert koncertjegyek, sportesemény- jegyek vásárlására és nincs ezen az oldalon kívül más online jegyvásárló felület, amely globálisan ennyire elterjedt lenne.

A másik ok pedig az lehet, hogy az összes általam említett cikk az Inbentát nevezi meg felelősnek, tehát egy harmadik felet, amely a meghackelhető chatbotot szolgáltatta a Ticketmaster számára, illetve az Inbenta vezérigazgatója is nyilvánosan bocsánatot kért az esetért, ezzel is magára vállalva a felelősséget.

4.5.Áttekintés

Az áttekinthetőség és összehasonlíthatóság érdekében az egyes vállalatok kapott eredményei táblázatba foglalva olvashatóak összefoglalva:

Vállalat neve	**Megfigyelési periódus**	**Eseményablak (hivatalos bejelentés dátuma)**	**Szignifikáns-e az event study szerint?**	**Bejelentés utáni részvény árfolyam változás**
Facebook	2018.02.13-03.13	2018.03.14-2018.03.28 (2018.03.17)	igen	március 14 és 27 között -31,97 USD/ részvény
Equifax	2017.08.03-09.03	2017.09.04-09.21 (2017.09.07)	igen	szeptember 7 és szeptember 18 között -48,34 USD/részvény
Under Armour	2018.02.26-03.26	2018.03.27-04.11 (2018.03.30)	nem	március 30 és április 11 között +0,39 USD/részvény
First American	2019.04.18-05.20	2019.05.21-05.31 (2019.05.24)	nem	május 25 és 31 között -3,61 USD/ részvény
Mariott	2018.10.26-11.26	2018.11.27-12.10 (2018.11.30)	nem	november 30 és december 10 között -4,22 USD/részvény
Ticketmaster	2018.05.22-06.22	2018.06.25-07.05 (2018.06.27)	nem	június 27 és július 5 között +1,31 USD/ részvény

5. Összefoglalás

Szakdolgozatom fő célja tehát egyrészt az volt, hogy átfogó képet adjak az információtechnológiai incidensek területéről. A megközelítésem több irányból történt: egyrészt utánanéztem, hogy ki és milyen szabályokat hoz a cyberbűnözés

megelőzésére mind nemzetközi, mint hazai környezetben. Ezen kívül feltérképeztem azt, hogy miért hordoznak ezek a támadások különösen nagy veszélyt magukban és hogy milyen formái léteznek.

Képet mutattam arról, hogy Magyarországon milyen statisztikákat találhatunk ebben a témában, illetve megindokoltam azt, hogy annak ellenére, hogy hazánkban is számos cyberincidens történik, miért választottam kutatásomhoz mégis külföldi esetek elemzését.

Következő lépésben megfogalmaztam azt, hogy kutatásomban mit is szeretnék pontosan megvizsgálni- azaz a kutatási kérdésemet és a H_0 hipotézist. A kutatási tervem elkészítésének folytatásaként körbejártam, hogy milyen szakirodalma van a tőzsdei árfolyam vizsgálatának, így több tanulmány elolvasása után rátaláltam az event study módszertanra.

Az elemzési módszertant körbejárva több problémába is ütköztem, amelyeket igyekeztem a leglogikusabb módon áthidalni, más megoldási alternatívákat találni.

Ezek után kiválasztottam a megvizsgálni kívánt eseményeket, ügyelve arra, hogy színes legyen a paletta és több ágazat vállalatainak eseteit nézzem. Az incidenseket a kiválasztott módszertannal megvizsgáltam, egymással összevetettem őket, illetve igyekeztem magyarázatot találni a felmerült ellentmondásokra és arra, miért nem kaptam egyes esetekben a logikusan elvárt eredményt.

A következőkben szeretnék még írni az egyik fő felmerült problémáról, amelyet tapasztaltam és megfogalmazni azt, hogy mi magyarázhatta ezt a gondot.

5.1. Eltérés a részvényárfolyam ábrája és a módszertan eredménye között, az eseményelemzés kritikája:

Az eredmények alapján észrevehettük, hogy az event study módszertan ellentmondásba ütközik azzal, amit az egyes esetek részvényárfolyam változásának ábráján láthatunk. Tehát például az First American Financial Corp esetén megfigyelhetünk egy látványos árfolyamesést az ábrán, ennek ellenére az eseményelemző módszertan eredménye szerint az incidens hatása nem szignifikáns 95%-os intervallumon.

A First American esetén megpróbáltam kétmintás t-próbával is tesztelni (Excel Adatelemzés- kétmintás t- próba nem egyenlő szórásnégyzeteknél), hátha így szignifikáns lesz az eredmény, de az alábbi táblázatban látható, hogy így sem jött ki a látványos ábra alapján várt szignifikáns válasz:

Kétmintás t-próba nem-egyenlő szórásnégyzeteknél		
	-0,12531328	*1,117626*
Várható érték	-0,09885416	-1,020313
Variancia	1,168993224	4,2035386
Megfigyelések	21	7
Feltételezett átlagos eltérés	0	
df	7	
t érték	1,137540783	
P(T<=t) egyszélű	0,146373042	
t kritikus egyszélű	1,894578605	
P(T<=t) kétszélű	0,292746085	
t kritikus kétszélű	2,364624252	

18. ábra Saját szerkesztés: A First American hozamainak vizsgálata kétmintás t-próbával

Ugyan az event study elterjedt elemzési módszer, viszont mivel csak rövid időt tudunk megvizsgálni annak érdekében, hogy más események ne következzenek be, amelyek szintén befolyásoló tényezők lehetnek, így viszont abban a problémába ütköztem, hogy a kis event window alacsony elemszáma miatt nagyon nagy a szórása. A másik probléma az, hogy hozamokkal számol, nem pedig a részvényárfolyamokkal, ami szintén oka annak, hogy hiába látványos egy részvény ábra, a hozamok statisztikája, a hozamokkal számolva azt az eredményt kapjuk, hogy nem szignifikáns az eredmény.

Ezen eredmények alapján azt a tanulságot tudom levonni, hogy gyakran érdemes nem egyetlen módszertanra hagyatkozni, hanem több vizsgálati módot is alkalmazni és átgondolni, hogy mi a logikus magyarázat arra, ha ellentmondásba ütközünk, vagy nagyon eltérő eredményt kapunk ahhoz képest, amelyre számítunk.

5.2. Jövőbeni kutatási kérdések

A szakdolgozatom írása során további kérdések merültek fel bennem, amelynek kifejtésére itt már sajnos nincs lehetőségem, viszont érdekes további kutatási téma lehet a jövőre nézve:

Az esetek vizsgálata gondolatindító volt arra, hogy vajon melyik iparág lehet a legjobban érintett az IT incidensekben? Hat eset ugyan kevés ennek kiderítésére- és ezen dolgozatban nem is ez volt a kérdés, amelyet vizsgáltam- de érdemes lehet megnézni több iparág több vállalatát és hogy mely iparágban volt átlagosan a legnagyobb árfolyamcsökkenés. Ennek pedig kideríteni az okát.

A kérdés, amely megfogalmazódott bennem, hogy ha az event study nem ad ilyen típusú vizsgálatoknál pontos képet (illetve egyes esetekben ellentmondó az eredménye pár esetnél az árfolyamcsökkenés ábrájával összehasonlítva), akkor milyen módszertan/ módszertanok léteznem még- nem csak a hozamok, hanem az árfolyamváltozás vizsgálatára is, amellyel megbízhatóbb eredményt kaphatunk?

Vállalatmenedzsment számára is hasznos, további részletezése a témámnak, ha olyan kutatás készül, amely összehasonlítja azt, hogy milyen intézkedéseket hoztak azon vállalatok, ahol az incidensek hatására kedvezően alakult az árfolyam és a hozam és hogyan kommunikáltak ott, ahol nagy romlás figyelhető meg, ebből pedig leszűrhető pár ötlet arra, hogy krízis esetén milyen intézkedéseket kifizetődő hozni a vállalatok szempontjából.

6. Irodalomjegyzék

NCSC National Security Council https://www.ncsc.gov.uk/ National Cyber Security Center- What is a Cyber crime letöltés: 2019.12.02

EC, European Commission https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en-letöltés időpontja: 2012.12.08

Raimer Böhme The Economics of Information Security and Privacy 2013 Springer (265-300.oldal)

NYSE New York Stock Exchange https://www.nyse.com

PwC Global Annual Review 2014- 40.oldal

Az internettel összefüggő adatkezelések egyes kérdéseiről szóló adatvédelmi biztosi ajánlás

Magyar Közlöny, 2011/88. szám, 2011. július 26.

TASZ Társaság a Szabadságjogokért https://tasz.hu/cikkek/elhibazott-jogalkotas-az-adatvedelmi-biztos-hivatalanak-megszuntetesevel-az-europai-unio-jogat-serti-magyarorszag letöltés: 2019.12.05

A számítógépes csalás és egyéb számítógépes bűncselekmények- KSH Statisztikai elemzések 2001 Dr. Pergel Józsefné

Dolley, , J.C. (1933), Characteristics and procedure of common stock split-ups, Harvard Business Review11, 316-326

Fama Fisher, Jensen, Roll 1969- The Adjustment of Stock Prices to New Information (International Economic Review)

Stephen J. Brown, Jerold B. Warner- Using daily stock returns: The case of event studies, 1985

Lublóy Ágnes és Tóth Eszter Közgazdasági Szemle, LVII. évf., 2010. január (37–58. o.) A közép-kelet-európai bankfúziók eredményessége című kutatása

Szliva Attila (2014) A piaci hatékonyság vizsgálata: Event study a Federal Reserve kamatdöntéseinek hatásairól a Dow Jones indexben szereplő részvényekre, 1991-1994.

Nasdaq https://www.nasdaq.com/market-activity/stocks/efx/historical
letöltés:2019.11.04

https://www.theguardian.com/technology/2018/mar/21/mark-zuckerberg-response-facebook-cambridge-analytica letöltés 2019.11.25

https://www.billboard.com/articles/business/8500554/live-nation-108-billion-2018-revenue-eighth-straight-year-growth letöltés 2019.11.25

http://investors.firstam.com/investors/overview/default.aspx letöltés 2019.11.25

Michael J. Seiler Performing Financial Studies: A Methodological Cookbook

https://www.forbes.com/sites/tonybradley/2018/03/30/security-experts-weigh-in-on-massive-data-breach-of-150-million-myfitnesspal-accounts/#36e733d63bba
2019.12.08.-i letöltött cikk

PwC Global Annual Review 2014- 40.oldal

Az internettel összefüggő adatkezelések egyes kérdéseiről szóló adatvédelmi biztosi ajánlás

FAF First American Financial Corporation http://investors.firstam.com

ICO https://ico.org.uk/

7. Képek jegyzéke

8. Melléklet

Facebook

	CLOSE/LAST (USD)	VOLUME (PCS)	OPEN (USD)	HIGH (USD)	LOW (USD)	Hozam
2018.02.14	179,52	28,852,470	173,45	179,81	173,21	
2018.02.15	179,96	20,697,440	180,50	180,50	176,84	4,064571923
2018.02.16	177,36	20,815,180	178,99	179,88	176,30	-0,836565097
2018.02.20	176,01	21,037,920	175,77	177,95	175,11	-1,798983183
2018.02.21	177,91	23,166,300	176,71	181,27	176,40	0,534789782
2018.02.22	178,99	17,766,680	178,70	180,21	177,41	1,126138872
2018.02.23	183,29	18,811,750	179,90	183,39	179,51	0,671516508
2018.02.26	184,93	17,583,030	184,58	185,66	183,22	2,601445247
2018.02.27	181,46	15,768,550	184,45	184,70	181,46	-0,070430166
2018.02.28	178,32	18,613,520	182,30	182,88	178,14	-1,165627541
2018.03.01	175,94	23,161,610	179,01	180,12	174,41	-1,804717499
2018.03.02	176,62	19,835,420	173,29	177,11	172,99	-3,195352215

2018.03.05	180,40	16,098,150	176,20	181,15	175,89	1,67926597
2018.03.06	179,78	14,868,900	181,78	182,38	179,11	3,166855846
2018.03.07	183,71	19,007,100	178,74	183,82	178,07	-1,672351194
2018.03.08	182,34	16,920,570	183,56	184,40	181,45	2,696654358
2018.03.09	185,23	18,187,880	183,91	185,51	183,21	0,190673349
2018.03.12	184,76	15,194,040	185,23	186,10	184,22	0,717742374
2018.03.13	181,88	17,873,720	185,61	185,99	181,11	0,205150354
2018.03.14	184,19	16,814,350	182,60	184,25	181,85	-1,621679866
2018.03.15	183,86	15,638,830	183,24	184,00	182,19	0,350492881
2018.03.16	185,09	23,699,600	184,49	185,33	183,41	0,682165466
2018.03.19	172,56	87,171,850	177,01	177,17	170,06	-4,054420294
2018.03.20	168,15	129,654,100	167,47	170,20	161,95	-5,389526015
2018.03.21	169,39	106,166,700	164,80	173,40	163,30	-1,5943154
2018.03.22	164,89	73,554,350	166,13	170,27	163,72	0,807038835
2018.03.23	159,39	53,478,870	165,44	167,10	159,02	-0,415337386
2018.03.26	160,06	125,971,800	160,82	161,10	149,02	-2,792553191
2018.03.27	152,22	77,468,330	156,31	162,85	150,75	-2,804377565
2018.03.28	153,03	59,803,800	151,65	155,88	150,80	-2,981255198
2018.03.29	159,79	59,266,330	155,15	161,42	154,14	2,307945928
2018.04.02	155,39	36,715,460	157,81	159,20	154,11	1,714469868
2018.04.03	156,11	42,518,400	156,55	157,39	150,81	-0,79842849
2018.04.04	155,10	49,542,320	152,03	155,56	150,51	-2,890450335
2018.04.05	159,34	41,138,460	161,56	161,58	156,65	6,271994738
2018.04.06	157,20	41,397,190	157,73	161,42	156,81	-2,370636296
2018.04.09	157,93	34,671,420	157,82	160,53	156,04	0,057059532
2018.04.10	165,04	58,051,080	157,93	165,98	157,01	0,069699658
2018.04.11	166,32	56,011,860	165,36	168,65	163,25	4,704615969
2018.04.12	163,87	38,195,140	166,98	167,45	163,10	0,979680697
2018.04.13	164,52	19,450,140	164,58	165,70	163,77	-1,43729788
2018.04.16	164,83	17,951,530	165,73	165,78	163,39	0,695710293
2018.04.17	168,66	21,986,820	165,83	169,00	165,66	0,063357973
2018.04.18	166,36	20,248,580	166,88	168,12	165,77	0,633178556
2018.04.19	168,10	21,921,120	166,20	168,33	165,20	-0,407478428
2018.04.20	166,28	18,917,050	167,79	168,43	165,81	0,9566787
2018.04.23	165,84	22,894,510	167,27	168,45	165,09	-0,309911199
2018.04.24	159,69	34,981,150	165,43	166,10	158,19	-1,100017935
2018.04.25	159,69	38,451,590	160,15	161,06	156,19	-3,194704709
2018.04.26	174,16	77,391,810	173,22	176,27	170,80	8,164475944
2018.04.27	173,59	29,773,640	176,81	177,10	172,60	2,072508948

2018.04.30	172,00	20,662,060	173,79	175,72	171,71	-1,708048187

Equifax

	CLOSE/LAST (USD)	VOLUME (PCS)	OPEN (USD)	HIGH (USD)	LOW (USD)	Hozam (%)
2017.08.03	144,94	594,068	145,46	145,46	143,95	-0,369863014
2017.08.04	145,43	404,308	145,27	145,56	144,57	-0,130620102
2017.08.07	145,47	588,741	145,36	145,63	144,61	0,061953604
2017.08.08	142,37	623,444	144,97	145,32	142,2	-0,268299395
2017.08.09	142,94	394,583	142,37	143,33	141,9	-1,793474512
2017.08.10	142,06	452,675	142,14	142,88	141,42	-0,161550889
2017.08.11	141,35	351,561	141,93	142,83	141,28	-0,147741663
2017.08.14	142,81	387,359	142,16	143,2	141,64	0,162051716
2017.08.15	142,88	467,956	142,87	143,25	141,86	0,499437254
2017.08.16	143	485,766	143,18	143,41	142,5	0,216980472
2017.08.17	140,63	373,057	142,94	143,15	140,58	-0,167621176
2017.08.18	139,89	530,586	140,9	141,002	139,73	-1,42717224
2017.08.21	139,84	388,478	140,07	140,33	139,14	-0,589070263
2017.08.22	142,22	609,388	139,81	142,36	139,46	-0,185621475
2017.08.23	140,98	281,627	141,37	142,41	140,76	1,115800014
2017.08.24	140,38	221,816	141,23	141,23	140,15	-0,099030912
2017.08.25	140,7	304,007	141,12	141,18	140,39	-0,077887134
2017.08.28	140,62	476,73	141	141,28	140,09	-0,085034014
2017.08.29	140,8	321,917	140,07	141,11	139,75	-0,659574468
2017.08.30	141,42	221,695	140,57	141,71	140,56	0,356964375
2017.08.31	142,47	425,417	141,78	143,27	141,77	0,860781105
2017.09.01	141,59	363,111	142,73	143,37	141,59	0,670052194
2017.09.05	141,1	495,148	141,42	142,49	140,57	-0,917816857
2017.09.06	141,39	452,154	141,58	142,14	141,02	0,11313817
2017.09.07	142,72	440,676	141,45	143,27	141,35	-0,091820879
2017.09.08	123,23	16,842,690	121,82	125,5	117,25	-13,8776953
2017.09.11	113,12	9,808,487	121,53	122	111,17	-0,238056148
2017.09.12	115,96	6,934,693	112,97	116,08	112,18	-7,043528347
2017.09.13	98,99	17,461,490	116,55	116,75	98,04	3,168982916
2017.09.14	96,66	34,523,070	98,69	100,75	89,59	-15,32389532

2017.09.15	92,98	16,657,480	94,4	95,69	90,72	-4,346944979
2017.09.18	94,38	10,826,720	93	95,06	92,08	-1,483050847
2017.09.19	94,87	7,839,120	92,5	95,35	91,88	-0,537634409
2017.09.20	96	7,920,697	95	97,41	93,1	2,702702703
2017.09.21	98,25	5,480,709	96,5	98,47	95,25	1,578947368
2017.09.22	105,04	12,467,840	100,1	105,2	99,8	3,730569948
2017.09.25	105,09	8,057,920	106,23	107,17	104,51	6,123876124
2017.09.26	106,05	7,550,049	102,79	106,15	101,74	-3,238256613
2017.09.27	106,44	7,598,351	107	108,99	106	4,095729157
2017.09.28	106,37	3,780,017	106,43	106,52	103,78	-0,53271028

Under Armour

	CLOSE/LAST (USD)	VOLUME (PCS)	OPEN (USD)	HIGH (USD)	LOW (USD)	Hozam
2018.02.26	17,25	4,240,341	17,05	17,33	16,94	1,669648
2018.02.27	16,75	5,157,027	17,33	17,75	16,725	1,642229
2018.02.28	16,58	6,678,938	16,9	17,02	16,545	-2,48125
2018.03.01	16,14	6,803,248	16,69	16,79	16,03	-1,2426
2018.03.02	17,02	11,580,040	15,95	17,055	15,65	-4,43379
2018.03.05	17,42	6,530,982	16,79	17,53	16,78	5,266458
2018.03.06	17,62	5,654,738	17,4	17,73	17,16	3,633115
2018.03.07	17,38	4,894,189	17,32	17,62	17,25	-0,45977
2018.03.08	17,16	5,578,871	17,45	17,49	17,06	0,750577
2018.03.09	17,05	4,323,573	17,28	17,37	16,88	-0,97421
2018.03.12	17,18	6,939,670	17,05	17,22	16,82	-1,33102
2018.03.13	16,56	8,363,739	17,25	17,435	16,5	1,173021
2018.03.14	16,08	8,547,051	16,62	16,7	15,86	-3,65217
2018.03.15	15,9	4,332,388	16,08	16,26	15,76	-3,2491
2018.03.16	16,19	6,340,601	15,88	16,345	15,74	-1,24378
2018.03.19	16,15	4,236,162	16,06	16,29	15,82	1,133501
2018.03.20	16	5,255,070	16,14	16,18	15,7899	0,498132
2018.03.21	15,95	4,637,096	15,99	16,17	15,9	-0,92937
2018.03.22	15,73	4,387,846	15,75	16,01	15,64	-1,50094
2018.03.23	15,78	5,545,041	15,88	16,07	15,6	0,825397
2018.03.26	16,67	6,012,511	16	16,69	15,67	0,755668

2018.03.27	16,44	5,191,406	16,65	16,8555	16,36	4,0625
2018.03.28	16,33	4,743,347	16,46	16,74	16,16	-1,14114
2018.03.29	16,35	6,612,656	16,36	16,74	16,34	-0,60753
2018.04.02	16,1	6,541,341	16	16,18	15,85	-2,20049
2018.04.03	16,82	5,246,531	16,2	16,85	16,075	1,25
2018.04.04	17,89	10,737,260	16,63	17,95	16,6	2,654321
2018.04.05	17,47	6,195,996	17,63	18,12	17,23	6,013229
2018.04.06	16,98	3,742,442	17,38	17,52	16,8	-1,41804
2018.04.09	16,64	5,563,175	17,12	17,15	16,57	-1,49597
2018.04.10	16,82	3,381,368	16,81	16,85	16,545	-1,81075
2018.04.11	16,74	3,770,980	16,67	17,03	16,61	-0,83284
2018.04.12	17,04	3,902,979	16,81	17,14	16,66	0,839832
2018.04.13	16,49	4,320,120	17,18	17,2	16,38	2,201071
2018.04.16	16,45	2,551,415	16,64	16,66	16,365	-3,14319

First American

	CLOSE/LAST (USD)	VOLUME (PCS)	OPEN (USD)	HIGH (USD)	LOW (USD)	Hozam
2019.04.18	55,55	417,842	55,79	55,8159	55,46	-0,1253
2019.04.22	55,41	348,98	55,32	55,57	55,18	-0,8424
2019.04.23	55,99	403,769	55,75	56,05	55,34	0,7773
2019.04.24	56,19	600,962	55,97	56,3425	55,72	0,39462
2019.04.25	57,55	731,568	55,76	57,86	55,018	-0,3752
2019.04.26	57,88	469,036	57,49	58,29	57,2	3,10258
2019.04.29	56,32	532,701	57,21	57,74	56,17	-0,487
2019.04.30	57,06	440,733	56,46	57,16	56,2901	-1,311
2019.05.01	56,62	677,716	57,03	57,29	56,56	1,00956
2019.05.02	56,19	485,489	56,73	56,92	55,81	-0,526
2019.05.03	56,19	594,578	56,25	56,47	55,89	-0,8461
2019.05.06	55,96	500,36	55,81	56,115	55,55	-0,7822
2019.05.07	55,14	416,051	55,61	55,86	54,93	-0,3584
2019.05.08	55	370,865	55,14	55,42	54,825	-0,8452
2019.05.09	54,98	351,986	54,76	55,115	54,355	-0,6892
2019.05.10	55,33	384,359	54,73	55,41	54,53	-0,0548
2019.05.13	54,32	647,227	54,64	55,07	54,11	-0,1644
2019.05.14	54,37	597,908	54,4	54,79	54,2	-0,4392
2019.05.15	55,4	481,943	54,21	55,6	54,07	-0,3493
2019.05.16	55,18	350,273	55,4	55,75	54,97	2,19517

2019.05.17	54,85	997,675	54,82	55,29	54,58	-1,0469
2019.05.20	54,96	282,039	54,58	55,23	54,58	-0,4378
2019.05.21	55,38	474,707	55,19	55,475	55,1858	1,11763
2019.05.22	55,6	281,61	55,34	55,85	55,14	0,27179
2019.05.23	54,88	406,4	55,29	55,38	54,58	-0,0904
2019.05.24	55,26	210,322	55,16	55,295	54,8	-0,2351
2019.05.28	51,8	2,465,553	52,48	52,96	49,52	-4,8586
2019.05.29	52,42	761,892	51,81	52,87	51,62	-1,2767
2019.05.30	51,79	828,357	52,51	52,79	51,46	1,35109
2019.05.31	51,65	709,258	51,3	51,95	50,85	-2,3043
2019.06.03	52,79	850,993	51,59	52,79	51,59	0,5653
2019.06.04	52,9	748,059	52,98	53,2	52,37	2,69432
2019.06.05	53,25	535,024	53,03	53,67	52,71	0,09438
2019.06.06	52,97	471,366	53,26	53,73	52,97	0,43372
2019.06.07	52,75	463,283	52,74	53,18	52,62	-0,9763

Mariott International

	CLOSE/LAST (USD)	VOLUME (PCS)	OPEN (USD)	HIGH (USD)	LOW (USD)	Hozam
2018.10.26	112,73	3,120,027	108,63	114,18	108,44	0,434541
2018.10.29	112,78	2,868,470	113,92	114,53	111,2	4,869741
2018.10.30	115,27	2,419,788	112,85	115,37	112,45	-0,93926
2018.10.31	116,89	2,437,879	116,33	118,72	116,21	3,083739
2018.11.01	121,09	2,471,128	118,485	121,23	116,02	1,852489
2018.11.02	120,93	2,797,282	122,24	122,97	119,94	3,169178
2018.11.05	120,68	2,402,128	121,3	121,53	119,71	-0,76898
2018.11.06	114,55	6,906,307	115	117,395	112,11	-5,19373
2018.11.07	116,14	2,503,054	114,82	117,15	114,635	-0,15652
2018.11.08	116,91	1,810,487	115,61	117,21	115,26	0,688033
2018.11.09	117,04	1,687,452	116,65	117,62	116,18	0,899576
2018.11.12	115,07	1,987,614	116,56	117,31	114,73	-0,07715
2018.11.13	116,55	2,381,774	115,72	117,92	115,7	-0,72066
2018.11.14	116,3	1,383,043	117,35	118	115,6	1,408572
2018.11.15	118,31	1,595,980	115,24	118,62	115,0308	-1,79804
2018.11.16	118,65	1,369,326	117,22	119,32	117,04	1,718153
2018.11.19	116,5	1,692,187	118,45	118,86	115,39	1,049309
2018.11.20	115,56	2,237,734	114,26	116,29	113,14	-3,53736
2018.11.21	117,17	1,317,537	116,1	118,74	116,09	1,610362

2018.11.23	117,26	445,155	116,51	118	115,8	0,353144
2018.11.26	119,9	1,280,633	118,99	120,51	118,28	2,128573
2018.11.27	119,97	1,539,401	120	120,4	119,07	0,848811
2018.11.28	122,19	1,497,529	119,99	122,27	118,52	-0,00833
2018.11.29	121,84	1,174,537	121,37	122,83	120,55	1,150096
2018.11.30	115,03	9,546,649	113,6	116,72	113,38	-6,40191
2018.12.03	119,53	3,620,090	116	120,09	115,69	2,112676
2018.12.04	113,5	3,097,300	119	119,23	112,92	2,586207
2018.12.06	115,32	2,910,950	111,68	115,5	111,11	-6,15126
2018.12.07	111,25	2,637,020	114,85	116,25	110,69	2,838467
2018.12.10	110,81	1,773,460	111,44	112,35	109,2	-2,96909
2018.12.11	110,03	2,613,804	112,33	112,94	109,79	0,798636
2018.12.12	110,07	2,615,777	110,19	111,895	109,9701	-1,9051
2018.12.13	108,85	2,066,551	110,57	110,975	108,24	0,344859
2018.12.14	107,66	2,241,619	108	109,98	107,37	-2,32432

Ticketmaster

	CLOSE/LAST (USD)	VOLUME (PCS)	OPEN (USD)	HIGH (USD)	LOW (USD)	Hozam
2018.05.22	44,44	2,032,062	44,81	44,95	43,78	0,246085
2018.05.23	44,06	951,977	44,07	44,6	43,84	-1,65142
2018.05.24	43,5	1,036,333	44,11	44,11	43,17	0,090765
2018.05.25	43,37	682,651	43,43	43,8	43,24	-1,5416
2018.05.29	42,91	812,603	43,14	43,49	42,71	-0,66774
2018.05.30	43,33	1,135,075	43,04	43,51	43,04	-0,2318
2018.05.31	42,63	1,462,641	43,36	43,5999	42,61	0,743494
2018.06.01	43,57	900,489	42,76	43,76	42,73	-1,38376
2018.06.04	43,52	569,644	43,82	43,879	43,34	2,478952
2018.06.05	43,66	740,01	43,67	43,89	43,33	-0,34231
2018.06.06	44,88	1,262,785	43,68	44,955	43,48	0,022899
2018.06.07	45,16	1,024,814	44,99	45,51	44,72	2,999084
2018.06.08	45,86	1,968,844	45,16	45,96	44,99	0,377862
2018.06.11	46,11	1,610,033	45,82	46,71	45,55	1,46147
2018.06.12	46,18	1,577,530	46,19	46,45	45,795	0,807508
2018.06.13	46,48	1,260,957	46,84	47,22	46,46	1,407231
2018.06.14	46,55	961,7	46,32	46,64	46,195	-1,11016
2018.06.15	46,93	1,913,035	46,54	47,09	46,455	0,474957
2018.06.18	46,97	967,182	46,43	47,13	46,12	-0,23636

2018.06.19	46,96	1,146,338	46,82	47,02	46,36	0,839974
2018.06.20	47,11	1,275,676	47,46	47,66	47,025	1,366937
2018.06.21	47,03	822,983	47,36	47,51	46,98	-0,2107
2018.06.22	48,73	2,496,659	47,78	48,75	47,78	0,886824
2018.06.25	47,77	1,312,874	48,44	48,49	47,45	1,381331
2018.06.26	47,76	753,541	47,76	47,9	47,37	-1,4038
2018.06.27	46,98	1,074,035	48,06	48,35	46,89	0,628141
2018.06.28	48,69	1,620,033	47,06	48,73	46,7247	-2,08073
2018.06.29	48,57	2,040,289	48,69	49,36	48,33	3,463663
2018.07.02	49,17	1,198,781	48,3	49,39	48,02	-0,80099
2018.07.03	48,22	502,076	49,34	49,485	48,16	2,153209
2018.07.05	49,08	995,588	48,71	49,09	48,5663	-1,27685
2018.07.06	49,69	817,114	49,19	49,96	49,05	0,985424
2018.07.09	50,04	1,181,691	50,14	50,41	49,71	1,931287
2018.07.10	49,96	850,92	50,18	50,33	49,69	0,079777
2018.07.11	49,77	964,475	49,39	50,36	49,33	-1,57433
2018.07.12	51,18	1,354,306	49,88	51,23	49,73	0,992104
2018.07.13	51,54	1,570,100	51,51	52,19	51,14	3,267843