Acta Informatica Pragensia
3(1), 2014, 1–7, DOI: 10.18267/j.aip.31
Online: aip.vse.cz

Sekce / Section:
Recenzované stati / Peer-reviewed papers

Analýza dopadu úniků dat na tržní hodnotu firem v období 2008 – 2012

Analysis of the Impact of Data Breaches on the Market Value of Companies in the Period 2008 – 2012

Tomáš Klíma[1], Adam Krbušek[1]

[1] Katedra systémové analýzy, Fakulta informatiky a statistiky,
Vysoká škola ekonomická v Praze
nám. W. Churchilla 4, 130 67 Praha 3

tomas.klima@vse.cz

Abstrakt: Za posledních patnáct let dochází k nárůstu počtu i závažnosti datových úniků u firem nakládajících s důvěrnými daty zákazníků a dalších osob. Cílem řady zkoumání bylo posoudit dopad takovýchto incidentů na tržní hodnotu postižených firem, nicméně všechny se zabývaly úniky před rokem 2008. Cílem tohoto příspěvku je představit výzkum, v rámci kterého byla provedena analýza dopadu úniků dat na tržní hodnotu na vzorku 27 firem postižených takovýmto incidentem mezi léty 2008 a 2012.

Klíčová slova: únik dat, tržní hodnota, analýza dopadu

Abstract: In the last fifteen years we can observe significant rise in the number and seriousness of the data breaches among the companies dealing with customer data. The aim of many analyses was to determine the impact of these breaches on market value, focusing on the breaches prior to 2008. The aim of this article is to present the findings from the analysis focused on 27 companies that suffered data breach between 2008 and 2012.

Keywords: Data breach, Market value, Impact analysis

1 Úvod

Hlavním problémem při určování výše škod utrpěných firmami v důsledku bezpečnostních incidentů je obtížnost získání potřebných dat. Pokud firma zažije bezpečnostní incident, v jehož důsledku jí uniknou osobní data klientů, tak je velice těžké odhadnout, nakolik ztratí důvěru klientů a investorů, stejně tak jako se nedá předem říci, zda se nestane terčem žalob ze strany postižených jedinců, popřípadě jak velké pokuty bude muset platit. Jelikož není možné přesně stanovit, jaké následky bude daný bezpečnostní incident na firmu mít, tak se ani nedá přesně určit, jak budou ovlivněny její tržby, konkurenceschopnost a podíl na trhu. Právě absence těchto dat určení celkové výše škod značně znesnadňuje. „Vzhledem k obtížnostem při odhalování skutečných nákladů různých bezpečnostních incidentů je dobré hledat alternativní ukazatele k přímým nákladům.“ (Yayla, Hu, 2011)
Jedním z alternativních způsobů určení výše nákladů bezpečnostních incidentů je sledování změn tržní hodnoty postižených firem. Jelikož tržní hodnota firem odráží jejich skutečnou hodnotu a je určovaná na základě všech informací a faktů, které jsou veřejně známé v daný okamžik, tak jakýkoliv incident, který firma zažije, by se měl na její tržní hodnotě projevit. Právě změna ceny akcií způsobená určitým incidentem by měla měřit jeho finanční dopad[1]. Zde se tedy pracuje s předpokladem, že velikost reakce akciového trhu na specifický incident představuje očekávanou cenu daného incidentu. (Yayla, Hu, 2011)
Na základě výše zmíněného vzniklo několik studií, které se snaží zjistit, jaký mají bezpečnostní incidenty dopad na tržní hodnotu postižených firem. Studie se samozřejmě zabývají pouze firmami, které jsou veřejně obchodované na akciové burze. V případě firem, které veřejně obchodovatelné nejsou, tuto metodu použít nelze, protože u nich neexistují potřebná data.

2 Rešerše studií

Kevin M. Gatzlaff a Kathleen A. McCullough publikovali v roce 2010 studii zabývající se dopadem bezpečnostních incidentů na tržní hodnotu postižených firem (Gatzlaff, McCullough, 2010). Pro tuto studii byl použit vzorek 77 firem, které zažily mezi lety 2004 – 2006 bezpečnostní incident. Výsledkem bylo zjištění, že bezpečnostní incidenty, v důsledku kterých firmě unikla citlivá data, mají značně negativní vliv na cenu akcií a průměrný CAR je v časovém horizontu jednoho dne -0,84%. Dále bylo zjištěno, že se průměrná cena akcií vrátí na původní hodnotu po 40 dnech a průměrná ztráta způsobená bezpečnostními incidenty je 84 milionů dolarů.
Další studie zabývající se danou problematikou byla publikována v roce 2009 (Goel, Shawky, 2009). V této studii se autoři zabývali dopadem 168 bezpečnostních incidentů, které se odehrály v období mezi lety 2004 – 2008, na cenu akcií postižených firem. Výsledkem bylo zjištění, že bezpečnostní incidenty mají negativní vliv na cenu akcií a průměrný propad ceny akcií postižených firem je 1%.
Studie (Cavusoglu et al., 2004) uvádí, že firmy v průběhu dvou dnů od oznámení bezpečnostního incidentu ztrácí v průměru 2,1% ze své tržní hodnoty. Ve studii (Campbell et al., 2003) bylo zjištěno, že pokud bezpečnostní incident zahrnuje únik citlivých/důležitých informací, nastane negativní dopad na tržní hodnotu postižené společnosti a cena jejích akcií

[1] Za úvahu též stojí využití této metody jako alternativy stanovení očekávaného dopadu incidentů za účelem analýzy a řízení rizik v podniku. Expertní odhad v těchto případech trpí značnou mírou subjektivity a využití přesnější metody by přineslo i relevantnější ohodnocení rizik.

klesne v průměru o 5,5%. Dále pak bylo zjištěno, že pokud uniknou data, která nejsou nijak významná, je dopad incidentu na cenu akcií minimální.

3 Analýza dopadu bezpečnostních incidentů na tržní hodnotu postižených firem

Studie popsané výše poukazují na to, že bezpečnostní incidenty mají negativní dopad na tržní hodnotu postižených firem. Tyto studie se nicméně liší svými výsledky, které nejsou jednotné. Výzkum popsaný dále je tedy věnován vlastní analýze dopadu bezpečnostních incidentů na tržní hodnotu postižených firem, které zaznamenaly únik dat mezi lety 2008 – 2012. Toto období bylo vybráno záměrně, jelikož na rozdíl od předchozích let, z tohoto období žádné podobné analýzy zatím neexistují. Základem analýzy pak je hypotéza říkající, že bezpečnostní incidenty mají negativní dopad na tržní hodnotu postižených firem.

3.1 Popis metody CAR

Při ověřování hypotézy byla použita stejná metoda, jakou kolektiv v čele s Katherine Campbell popsal a aplikoval ve své práci (Campbell et al., 2003). Hlavním důvodem jejího výběru byla možnost srovnat výsledky zde prezentované studie se studiemi historickými, což by v případě výběru jiné metody, nebo tvorby vlastní možné nebylo. Metoda CAR si dává za úkol určit rozdíl mezi očekávanou cenou akcií a cenou skutečnou. Jejím cílem je určení velikosti dopadu neočekávaných událostí na tržní hodnotu firem – mezi neočekávané události se dá zařadit například zveřejnění informací o úniku dat, oznámení mimořádných dividend, oznámení fúzí, apod.
Rozdíl mezi očekávanou cenou akcií a cenou skutečnou se nazývá abnormální výnos (AR). V této studii se bude pracovat s jeho souhrnnou hodnotou, nazvanou kumulativní abnormální výnos (CAR), která slouží k určení toho, jak velký dopad měla určitá událost na cenu akcií. V tomto článku je tedy použito analýzy kumulativního abnormálního výnosu k určení vlivu datových úniků (tedy neočekávané události) na tržní cenu zkoumaných firem.
Rovnice pro CAR je následující:

$$CAR_i = \sum_{t=t_1}^{t_2} AR_{it} \qquad \textbf{(1)}$$

Kde t_1 a t_2 představují časové okno události. V případě této práce bylo časové okno zvoleno v intervalu (-3;10) dní okolo data, kdy byly zveřejněny informace o incidentu.
Rovnice pro AR je následující:

$$AR_{it} = R_{it} - (\hat{\alpha}_i + \hat{\beta}_i R_{mt}) \qquad \textbf{(2)}$$

Kde R_{it} je výnos akcií i v den t a R_{mt} je výnos tržního portfolia m v den t. Pro účel této práce byl jako ukazatel pro R_{mt} použit burzovní index S&P 500. Proměnná $\hat{\alpha}_i$ pak je intercept a $\hat{\beta}_i$ je korelace výnosů jednotlivých akcií firmy i vůči burzovnímu indexu. Rovnice pro R_{it} je následující:

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it} \qquad \textbf{(3)}$$

3.2 Zdrojová data

Pro vlastní analýzu byl vybrán vzorek 27 firem, které zažily mezi lety 2008 – 2012 únik dat[2]. Tyto firmy byly vyhledány díky specializovanému serveru datalossdb.org, který shromažďuje informace o bezpečnostních incidentech vedoucích k únikům dat. Veškeré informace o bezpečnostních incidentech získané z tohoto serveru byly následně ověřeny v tisku.
Při výběru firem se postupovalo podle několika kritérií. Hlavním kritériem bylo, že každá z požadovaných firem musela zažít v daném časovém horizontu (od začátku roku 2008 do konce roku 2012) únik dat. Dále bylo důležité, aby každá z těchto firem byla v době úniku dat kótovaná na akciové burze. Posledním kritériem byla znalost přesného data, kdy se informace o úniku dat staly všeobecně známé. Toto kritérium je klíčové, jelikož pokud by přesné datum známé nebylo, tak by nebylo možné určit, jaký dopad bezpečnostní incident na cenu akcií dané firmy měl.
Jako ukazatel trhu byl zvolen burzovní index S&P 500 a časové okno okolo události, v níž je sledována cena akcií, bylo nastaveno v intervalu (-3;10) dní okolo data, kdy byly zveřejněny informace o incidentu.
Samotná data, použitá pro analýzu, byla obstarána z několika zdrojů. Jedním z nich byl již zmiňovaný server datalossdb.org, kde byly vyhledány informace o bezpečnostních incidentech. Informace o cenách akcií zkoumaných firem byly získány prostřednictvím internetového portálu Yahoo!, konkrétně jeho služby finance.yahoo.com. Prostřednictvím služby finance.yahoo.com byla obstarána data o vývoji burzovního indexu S&P 500.

3.3 Vyhodnocení výsledků

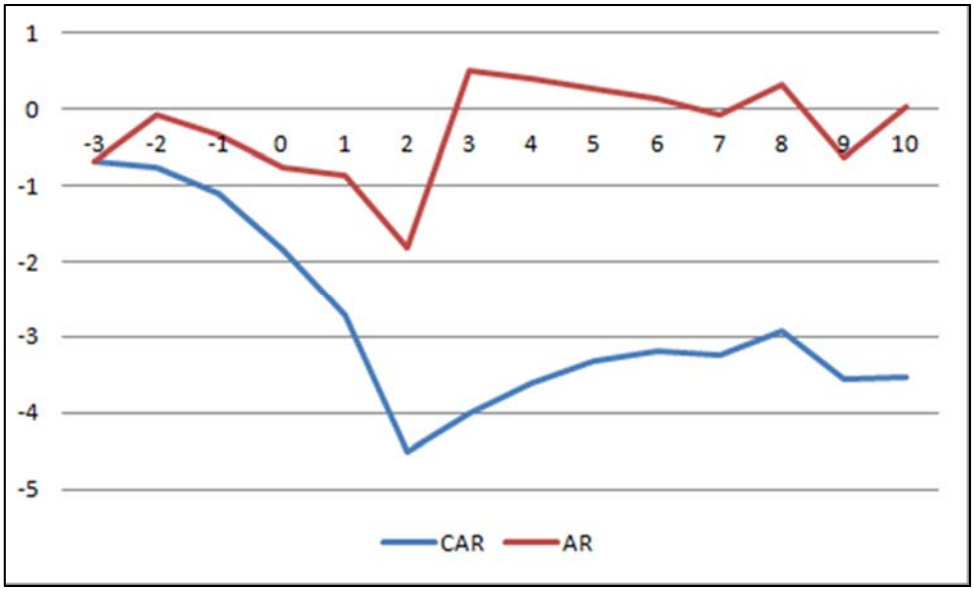
Pro vyhodnocení výsledků analýzy se testovala hypotéza říkající, že bezpečnostní incidenty mají negativní dopad na tržní hodnotu postižených firem. Tato hypotéza se testovala na analyzovaném vzorku dat pomocí t-testu na hladině pravděpodobnosti α=0,05.
Pro výpočet byl použit následující vzorec:

$$t = \frac{\bar{x} - \mu_0}{s_x'}\sqrt{n} \qquad \textbf{(4)}$$

Kde $\bar{x}$ představuje aritmetický průměr hodnot CAR, μ_0 je nulová hypotéza, s_x' je směrodatná odchylka a n představuje počet pozorování.
Pro testování hypotéz byla stanovena nulová hypotéza H_0 říkající, že bezpečnostní incidenty nemají žádný dopad na tržní hodnotu postižených firem. Jako alternativní hypotéza H_A byla zvolena námi testovaná hypotéza, říkající, že bezpečnostní incidenty mají negativní dopad na tržní hodnotu postižených firem. Potvrzení, či vyvrácení nulové hypotézy a následné přijetí, či nepřijetí hypotézy alternativní, se provedlo tak, že se t-hodnota porovnala s kritickou hodnotou t rozdělení pro stanovenou hladinu významnosti.
Pro potvrzení alternativní hypotézy H_A musí být $\mu < \mu_0$. Kritický obor je v tomto případě $W_\alpha = \{t < -t_{1-\alpha}\}$. Hodnota t rozdělení je pro hladinu významnosti α =0,05 při 27 pozorováních rovna 1,706, což znamená, že pro přijetí alternativní hypotézy H_A bylo nutné, aby byla hodnota t menší než -1,706.

[2] Ve vzorku jsou zastoupené následující firmy: GE Money, SAIC, JPMorgan Chase, Heartland Payment Systems, TeleTech Holdings, Bank of America, Citigroup, Sony, Hartford Life Insurance Company, Adobe Systems, Barnes & Noble, NVIDIA Corporation, Yahoo!, LinkedIn, DIRECTV, Global Payments, Coca-Cola, WellPoint, The Toronto-Dominion Bank, First Republic Bank, Intel Corporation, Wells Fargo & Company, Digital River, AT&T, AMR Corporation, Netflix, Wal-Mart Stores.

Na základě výsledků t-testu byla hypotéza říkající, že bezpečnostní incidenty mají na tržní hodnotu postižených firem negativní dopad, potvrzena.
Na Grafu 1 je možné vidět, jaký má zveřejnění bezpečnostních incidentů dopad na tržní hodnotu postižených firem. Průměrná hodnota CAR je u analyzovaných firem jeden den po oznámení bezpečnostního incidentu -2,71362%, po dvou dnech od oznámení bezpečnostního incidentu je -4,51908% a po třech dnech je -4,00159%. Po čtyřech a více dnech již dopad bezpečnostních incidentů na tržní hodnotu postižených firem není podle t-hodnoty průkazný. Detailní výsledky analýzy jsou v Tab. 1.
Na základě výsledků analýzy bylo zjištěno, že bezpečnostní incidenty mají značně negativní dopad na tržní hodnotu postižených firem a průměrný CAR je jeden den po zveřejnění incidentu -2,71362%.
Na základě výsledků analýzy bylo dále zjištěno, že cena akcií společnosti začíná klesat ještě před tím, než je bezpečnostní incident oficiálně oznámen – průměrný CAR je jeden den před oznámením incidentu -1,09777%. To je možné pozorovat na Grafu 1. Tento jev může být způsoben únikem informací o incidentu před jeho oficiálním oznámením, nebo například insider tradingem, kdy držitelé akcií, kteří jsou nějak spjati s postiženou firmou, využijí toho, že mají k dispozici informace o bezpečnostním incidentu dříve, než je oficiálně oznámen a začnou prodávat své akcie.



Graf 1. Výsledky analýzy CAR a AR. Zdroj: Autoři

Dny	AR	CAR	t-hodnota (CAR)
-3	-0,66891	-0,66891	-1,985082246
-2	-0,08156	-0,75047	-1,707312112
-1	-0,34729	-1,09777	-2,788519656
0	-0,75041	-1,84818	-3,012819789
1	-0,86544	-2,71362	-3,209476252
2	-1,80545	-4,51908	-2,166951351
3	0,51748	-4,00159	-1,998282172
4	0,39501	-3,60658	-1,596725899

5	0,27222	-3,33435	-1,581890825
6	0,14443	-3,18992	-1,647797533
7	-0,06175	-3,25167	-1,633667775
8	0,31434	-2,93732	-1,542929864
9	-0,61874	-3,55607	-1,745479156
10	0,03098	-3,52509	-1,790948782

Tab. 1. Výsledky analýzy. Zdroj: Autoři

3.4 Porovnání výsledků

Při vyhodnocování výsledků analýzy bylo zjištěno, že bezpečnostní incidenty mají negativní dopad na tržní hodnotu postižených firem. Pokud se tento závěr porovná s výsledky předchozích studií provedených jinými autory, je patrné, že se navzájem shodují.
Ačkoliv se studie shodují v tom, že bezpečnostní incidenty mají negativní dopad na tržní hodnotu postižených firem, výsledné hodnoty CAR jsou rozdílné. Příkladem může být studie (Goel, Shawky, 2009), jejímž výsledkem bylo zjištění, že průměrná hodnota CAR je jeden den od zveřejnění incidentu -1,03%. Na tomto příkladu je vidět, že se výsledná hodnota CAR neshoduje s výsledkem této analýzy, kdy hodnota CAR byla jeden den od zveřejnění incidentu -2,71362%.
Dalším příkladem je studie (Cavusoglu et al., 2004), která uvádí, že firmy dva dny od oznámení bezpečnostního incidentu ztrácí v průměru 2,1% ze své tržní hodnoty. Tato hodnota opět nekoresponduje s výsledkem této analýzy, kdy hodnota CAR byla dva dny od oznámení incidentu v průmětu -4,51908%.
Rozdílné hodnoty CAR této a jiných studií mohou být způsobeny odlišným obdobím, které bylo zkoumáno. Zatímco jiní autoři zkoumali období předcházející roku 2008, tato studie se zabývá obdobím mezi lety 2008 – 2012, včetně. Vzhledem k tomu, že mezi lety 2008 – 2012 probíhala světová finanční krize, která zažívala v letech 2008 a 2010 svá maxima, může být volba jiného období důvodem rozdílných hodnot CAR. Finanční krize v tomto období totiž způsobila volatilitu cen prakticky všech finančních instrumentů na trhu, což mohlo do určité míry ovlivnit reakci trhu na oznámení informací o bezpečnostním incidentu (Jo et al., 2009). Dalším možným důvodem je snížení citlivosti investorů na zprávy o datových únicích, kterých bylo v posledních letech takové množství, že je širší veřejnost, mimo ty největší případy, přestala vnímat.

4 Závěr

Analýza dopadu bezpečnostních incidentů na tržní hodnotu postižených firem byla provedena na vzorku 27 firem, které zaznamenaly únik dat mezi lety 2008 – 2012. Toto období bylo vybráno záměrně, jelikož na rozdíl od předchozích let z tohoto období žádné podobné analýzy zatím neexistují. K analýze byla použita metoda CAR (cumulative abnormal return), což je stejná metoda, jakou použili autoři předchozích studií. Základem analýzy byla hypotéza říkající, že bezpečnostní incidenty mají negativní dopad na tržní hodnotu postižených firem. Tato hypotéza se testovala na analyzovaném vzorku dat pomocí t-testu na hladině pravděpodobnosti α=0,05, přičemž byla na základě jeho výsledků potvrzena.
Na základě výsledků analýzy bylo zjištěno, že bezpečnostní incidenty mají značně negativní dopad na tržní hodnotu postižených firem a průměrný CAR je jeden den po zveřejnění incidentu -2,71362%.

Výsledky analýzy dále ukazují, že cena akcií společnosti začíná klesat ještě před tím, než je bezpečnostní incident oficiálně oznámen – průměrný CAR je jeden den před oznámením incidentu -1,09777%. Tento jev může být způsoben únikem neoficiálních informací o bezpečnostním incidentu před jeho oficiálním oznámením, nebo například insider tradingem.

Při porovnání výsledků této analýzy s výsledky předchozích studií, byla nalezena shoda – závěrem všech studií bylo zjištění, že bezpečnostní incidenty mají negativní dopad na tržní hodnotu postižených firem. Přestože se závěry studií shodují, hodnoty CAR se od sebe liší. Rozdílné hodnoty CAR této a jiných studií mohou být způsobeny odlišným obdobím, které bylo zkoumáno, vzhledem k tomu, že mezi lety 2008 – 2012 probíhala světová finanční krize.

Poděkování

Příspěvek byl zpracován jako součást výzkumného projektu IGA, VŠE v Praze: „Inovace systému řízení digitální forenzní laboratoře“ (F4/74/2014).

Seznam použitých zdrojů

Campbell, K., Gordon, L.,A., Loeb, M.P., Lei, Z. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*. 11, 431-448.

Cavusoglu, H., Mishra, B., Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce.* 9(1) 69-104.

Goel, S., Shawky, H.A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*. 46(7), 404-410.

Gatzlaff, K.M., McCullough, K.A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review.* 13(1), 61-83.

Jo, H., Lee, C., Munguia, A., Nguyen, C. (2009). Unethical misuse of derivatives and market volatility around the global financial crisis. *Journal of Academic and Business Ethics*. 12, 1-11.

Yayla, A.A., Hu, Q. (2011). The impact of information security events on the stock value of firms: the effect of contingency factors. *Journal of Information Technology*, 26(1), 60-77.