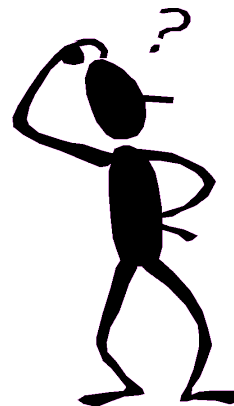


Další vývoj Datových schránek

Ing. Miroslav Ludvík, Ph.D.



Rekapitulace problémů DS

- Triviální získání přihlašovacího jména a hesla
- Tři role p. Radka Smolíka
- Nepravdivá tvrzení MVCR ústy p. Smolíka a naše vysvětlení jeho dezinformací
- Další nepravdivá tvrzení MVČR
- Další zranitelnosti Datových schránek
- Kroky dalších částí státní správy (Pražská správa sociálního zabezpečení)
- Rozpočet DS včetně využití EU fondů
- Stále nezveřejněný audit projektu DS
- Software od 602 není opensource, nikdo neví co to ve skutečnosti dělá
- Digitální podpis a daňové přiznání

Časová souslednost

- Říjen 2009 – oficiální upozornění na vážné problémy
- 1.11.2009 – právnické osoby mají datovou schránku povinně
24.11.2009 – tisková konference a praktická demonstrace útoku
- Následně vyplouvají na světlo další nepravdy šířené MVČR
17.2.2010 – Konference [Security 2010](#) a demonstrace útoku před odbornou veřejností a následná diskuse.

- **DNES – stále se nic nezměnilo, zmíněný útok stále funguje a uživatel nemá prostředky jak poznat, že se stal obětí útoku.**

Tři role p. Radka Smolíka

Jednatel společnosti eTRENDS

100% podíl této společnosti je Zuzana Smolíková

Pod hlavičkou této společnosti propaguje nezávisle Datové schránky viz březnová konference.

Telefonica O2 Czech Republic a.s.

Vedoucí projektu Datové schránky

MVČR - bezpečnostní architekt ISDS

Externí konzultant projektu Datové schránky

Není tam střet zájmů?

Tvrzení p. Smolíka (přiznání problému)

Ještě před Tiskovou konferencí poslal p. Radek Smolík pořadateli TK následující mail:

Od: "Radek Smolík" <smolikr@e-trends.cz>
Komu: "Katarína Rusnáková" <rusnakova@averia.cz>
Odeslané: Úterý, 24. Listopad 2009 9:22:18 GMT +01:00 Amsterdam / Berlín / Bern / Řím / Stockholm / Vídeň
Předmět: RE: Registrace na TK

Dobrý den,

osobně to tedy tipuji na Mirka Ludvíka a 4Safety – jak jsem psal o problému s kořenovým certifikátem, asi to bude variace na toto téma. J sice zneužitelné, ale jediné pokud uživatel sám poruší platné postupy pro ověřování kořenových certifikátů (vzato do důsledku je to spíše na jeho straně než na straně systému) a je to triviálně řešitelné. Stačí promptně vyměnit SSL certifikát za Verisign, což lze udělat kdykoliv. Pokud je to tento problém, pak je to tak trochu „mnoho povyku pro nic“. Uvidíme, počkám si na výsledek a Mirkovi se ozvu, znám ho ještě od AC a S&T.

Zdravím,
Radek

Radek Smolík
eTRENDS s.r.o.

Reakce na mail p. Radka Smolíka

- Mou osobu odhadl p. Smolík správně
- Jedná se o problém certifikátu pro konkrétní web
- Kořenový certifikát CA je jen způsob jak zařídit, aby uživatel postupoval přesně podle návodu, nedostal žádné varování a útok byl úspěšný.
- Při našem útoku, uživatel postupoval (jak jste viděli) přesně podle instruktážního videa, vydaného MVČR
- P. Radek Smolík má pravdu, že stačí vyměnit certifikát. Náklady budou cca 10.000 Kč ročně a bude po problému. Nedomníváme se, že se jedná o „mnoho povyku pro nic“. Jak jsme demonstrovali v loňském roce, je útok skutečně nebezpečný a co horší velmi jednoduchý na provedení a pro uživatele postupujícího podle oficiálního návodu neodhalitelný.
- Při našem útoku uživatel postupuje přesně podle návodu vydaného MVČR a neporuší žádné platné postupy. Tím, že uživatel prakticky nemá možnost tento útok detekovat se jedná zcela nepochybně o chybu systému, nikoli uživatele.
- Dále bych rád dodal, že p. Smolík mě asi zná, ale v době kdy jsem působil v S&T či AC jsem s p. Radkem Smolíkem nejednal a nevím odkud mě tam zná. To ale není podstatné. Za důležitější považuji fakt, že p. Smolík se mi neozval, jak slíbil organizátorům.

Naše reakce na tvrzení p. Smolíka

Bezpečnostní firma se nabourala do cizí datové schránky

<http://www.ct24.cz/domaci/73458-bezpecnostni-firma-se-nabourala-do-cizi-datove-schranky/video/2/>

Radek Smolík: Podle mého soudu si stačí pečlivě ověřit ten řetězec, který přímo vidíte ve svém počítači .

4Safety: Jak prakticky předvedla společnost 4Safety, zfalšuje-li útočník certifikát, není pro něj problém zfalšovat i tento kontrolní řetězec na webových stránkách, neboť je distribuovaný stejným kanálem, jako samotný certifikát.

Radek Smolík: Podvrhnout falešný certifikát lze pouze někomu, kdo nedodržel postup, jakým se má certifikát instalovat .

4Safety: Společnost 4Safety na tiskové konferenci předvedla útok, při kterém koncový uživatel zcela přesně následoval kroky instruktážního videa distribuovaného MVČR a přesto mu byly přihlašovací údaje odcizeny. To by se útočníkovi v případě nasazení důvěryhodného certifikátu nepodařilo.

Naše reakce na tvrzení p. Smolíka

Datové schránky nejsou podle firmy bezpečné

<http://www.financniny.cz/podnikatele/zpravy/datove-schranky-nejdou-podle-firmy-bezpecne/409155>

Radek Smolík: Uživatel by musel dvakrát ignorovat výzvu ke kontrole certifikátu.

4Safety: Dle prezentovaného videa nebyl při útoku (podvržení certifikátu) uživatel varován **ani jednou**.

Naše reakce na tvrzení p. Smolíka

Do datových schránek se dá vloupat, tvrdí odborníci

<http://www.novinky.cz/domaci/185209-do-datovych-schranek-se-da-vloupat-tvrdi-odbornici.html>

Radek Smolík: Budou-li uživatelé datových schránek opatrní, žádné riziko jim nehrozí.

4Safety: Nedůvěryhodný certifikát umožňuje správci sítě/připojení přeměřovat uživatele na falešný server datových schránek, aniž by byl jakkoli varován operačním systémem či webovým prohlížečem. Opatrnost jim v tomto ohledu nepomůže. Uživatel nemá způsob jak takovýto útok poznat!

Radek Smolík: Oni to naaranžovali do podoby, kdy už falešný certifikát pro aktivaci schránky byl instalován. Kdyby ukázali, jak přesvědčí tisícovky uživatelů, jak ho tam dostat, pak bych to bral.

4Safety: I toto bylo na tiskové konferenci vysvětleno (pan Smolík se konference neúčastnil, přesto se k ní negativně vyjadřoval). Uživatel následoval kroky instruktážního videa ministerstva, a přesto si k sobě nainstaloval podvržený certifikát sám, nikde totiž nebyl upozorněn na digitální otisk a i kdyby byl, přesto i ten byl na stránkách PostSignum podvržen.

Radek Smolík: Podvrhnout falešný certifikát lze pouze tomu, kdo nedodrží správný postup přihlašování.

4Safety: Bude-li uživatel následovat kroky instruktážního videa z dílny ministerstva (které bylo k dispozici v době, kdy se registrovalo nejvíce subjektů), pak mu útočník snadno podstrčí falešný certifikát a uživatel nemá možnost takový útok poznat, natož se mu bránit..

Další tvrzení MVČR

Změna způsobu přihlašování pro uživatele webového portálu

<http://www.datoveschranky.info/clanek/299/>

MVČR: 23.11.2009 (den před naší první tiskovou konferencí) byla aplikována „ochrana“ před útoky robotů. Na webu MVČR se píše, že se jedná o Turingův test.

4Safety: Zmíněná ochrana rozhodně nesplňuje kriteria Turingova testu, což jsme již demonstrovali. Slovo „ochrana“ je v tomto případě velmi silné, neboť na její překonání potřebuje útočník cca 20 řádků kódu. Napsání těchto 20 řádků zabralo kolegovi cca 30 min.

Konference Security 2010

Na této konferenci, která se konala 17.2.2010 v Hotelu Top byly před odbornou veřejností opět prakticky demonstrovány zmíněné bezpečnostní nedostatky projektu Datové schránky

Po naší praktické demonstraci slabin Datových schránek přišly i některé námitky, které jsou vysvětleny na následujícím slide.

Vysvětlení sporů v panelové diskusi

KPMG: Přes captchu neprojdete, uživatel nahlásí bezpečnostní incident.

4Safety: Naše společnost není za tento audit placena a tak nemůžeme reagovat na každé pseudoopatření, se kterým provozovatele přijdou. Nicméně dokud nezmění princip, tak jak jsme naznačili je z principu **nemožné** aplikaci zabezpečit, neboť zcela chybí **chain of trust**. Jediné co provozovatel dělá jsou věci, které vedou pouze k nutnosti útok lehce modifikovat. Abychom svá slova podpořili, tak jsme udělali drobnou modifikaci a uživateli to běží celé dál a nemá šanci nic poznat.

Úvahu, jaké procento uživatelů by nahlásilo incident a jaké procento by to po pěti minutách zkusilo znovu a když by to fungovalo, tak by nic neřešilo, necháváme na posluchačích.

Michal Rada: Není možné využít certifikát CA, která je v prohlížeči, neboť jsou zahraniční a to naše zákony neumožňují.

4Safety: Dle **rozhodnutí** rozhodnutí Evropské Komise ze dne 16. října 2009 mají jednotlivé členské státy povinnost uznávat kvalifikované certifikáty vydané v jiných členských státech EU. Toto rozhodnutí je závazné. Z toho plyne, že je možné využít certifikát vydaný CA v jakémkoli členském státu EU. Což potvrzuje i **text** na oficiálních stránkách Ministerstva vnitra České Republiky.

Další zranitelnosti DS

Útočník může zcela bez problémů podvrhnout uživateli falešný program, který se bude tvářit jako XML602 Filler. Uživatel tak nainstaluje z jeho pohledu software, na který ho odkázal web datových schránek. **Útočník tak může snadno získat veškerá uložená jména a hesla uložená v prohlížeči stejně tak jako celou historii. Obdobným způsobem lze získat plnou kontrolu nad počítačem, ze kterého se se oběť snaží přistupovat na server datových schránek.** Kromě získání citlivých dokumentů z tohoto počítače získává útočník základnu pro vedení dalších útoků ve vnitřní síti napadené organizace.

V celém projektu DS jsou další závažné zranitelnosti, které umožňují zneužití celého systému a tím jej činí **nevěrohodným.**

Kroky ostatních částí státní správy

Pražská správa sociálního zabezpečení rozesílá dopisy, ve kterých píše, že jejich současný systém je ověřený, funkční a přiznání jim jdou přímo do systému. Dále v tomto dopise píše, že podávání přiznání přes Datové schránky komplikuje práci a že doufá, že zůstaneme u starého funkčního a osvědčeného

Zarážející je nekonzistentnost postupu jednotlivých částí státní správy.

Audit aplikace Datové schránky

Když jsme minulý rok prakticky demonstrovali asi největší zranitelnost Datových schránek, všude se mluvilo o tom, že renomovaná společnost KPMG dělá audit této aplikace. Skutečnost, že audit buď stále nebyl dokončen, nebo jeho výsledky nebyly zveřejněny celému projektu **na věrohodnosti rozhodně nepřidává.**

Software od Software602, a.s.

Pro plnohodnotné využívání Datových schránek je nutné si nainstalovat software 602XML Filler od společnosti Software602 a. s.. Tento software není opensource a tak nemohl být prověřen bezpečnostní komunitou. Podle veřejných informací nebyl podroben ani review zdrojového kódu a tak **kromě autorů nikdo neví co zmíněný software dělá nebo nedělá.**

Pro vyváženost je nutné uvést, že software 602XML Filler od společnosti Software602 a. s. je podepsán důvěryhodnou certifikační autoritou, ale to bohužel k jeho důvěryhodnosti nestačí. Tento podpis zaručuje uživateli, že instaluje skutečně to, co si myslí, ale výš uvedený problém zůstává.

Cena projektu Datové Schránky

- > Od: "Jiří Korbek"
- > Komu: "novy.pavel@centrum.cz"
- > Datum: 22.12.2009 10:23
- > Předmět: RE: Informace o Datových schránkách
- >

Dobrý den pane Nový, toto jsou jediné informace, které se mi podařilo zjistit od oddělení provozu projektů eGovernment.

Publikovatelná čísla:

Marketingové aktivity: ČP 25 mil., MV 25 mil. (z toho většina z evropských fondů)

Provoz ISDS: paušál 15 milionů měsíčně MV -> ČP

Poplatky za zprávy jsou hrazeny z prostředků všeobecné pokladní správy. Cena za jednu přenesenou zprávu se bude snižovat podle množství přenesených zpráv.

S pozdravem,

Jiří Korbek
OTPR MV ČR

Cena datové zprávy

Cena odeslané Poštovní datové zprávy činí necelých 18 Kč včetně DPH
<http://www.cpost.cz/cz/sluzby/datove-schranky/postovni-datova-zprava-id29096/>

Další náklady vznikají uchováváním datových zpráv s uchováváním datových zpráv v datových trezorech či konverzí a uchováváním v listinné podobě.

Shrnutí celé situace

- Projekt stál a stojí nemalé peníze nás všechny
- Špatné vedení celého projektu
- Chybí nebo byla nekvalitně udělána počáteční analýza
- Systém byl spuštěn bez auditu aplikace ale i celého systému.
- Jediný, kdo může špatnou situaci zlepšit je MVČR
- MVČR není ochotno naslouchat názorům odborníků a na místo toho připomínky bagatelizuje a odmítá spolupráci



4Safety

Děkujeme za pozornost



www.4safety.cz