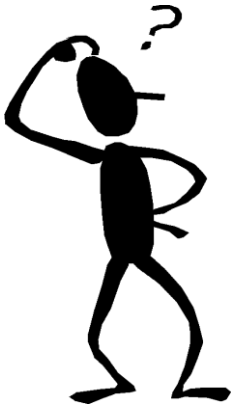
Projekty státní správy

Ing. Miroslav Ludvík, Ph.D.



Rekapitulace problémů DS

- Triviální získání přihlašovacího jména a hesla
- Možnost vystupovat za jiný subjekt. Následky .....
- Možnost zcizit někomu jeho zprávy .....
- 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

Praktická ukázka

Detailní vysvětlení principu útoku

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

- **DNES – stále se nic nezměnilo**

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.

Kroky ostatních částí státní správy

Pražská správa sociálního zabezpečení rozesílá dopisy, ve kterých píše, že jejich současný sytém, je ověřený, funkční a přiznání jim jdou přímo do systému. Dále v tomto dopise píší, 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.**

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.**

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 Korbel"
> Komu: "novy.pavel@centrum.cz"
> Datum: 22.12.2009 10:23
> Předmět: RE: Informace o Datovych schrankach
>

Dobrý den pane Nový, toto jsou jediné informace, které se mi podařilo zjistit od odělení 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 Korbel
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

Děkujeme za pozornost

www.4safety.cz