Michal Škop's notes

Poznámky

sněmovní Podvýbor pro ochranu soukromí
21.1.2016

Finanční správa: "bezpečnost je priorita"
EET zařazeno do "kritické infrastruktura"
Studie BDO: části jsou "neaktuální"

KSČM: Odposlechy? Bude mít Policie k tomu přístup?
    ochrana bude šifrováním
    Finanční správa poskytne, pokud soud řekne

Bezpečnostní rizika?
    "jsou to ponenciální rizika"

JANUS – projekt
    dokumenty hotové do května, už dnes v pracovní verzi
dohled NBÚ
bude kompletní bezpečnostní projekt (penetrační testy, bezpečnostní audit)

vláda usnesení 889 – musí být stanovisko hlavního architekta e-governmentu

e-government: ještě to vůbec nemají, bianco šek

poslední harmonogram:
    7 měsíců po schválení, tj. teď chtějí 1.11. první fáze

v důvodové zprávě a RIA nejsou popsány rizika

EET je I ve Slovinsku od 1.1.

penetrační testy – kdo vyhraje tendr
"nevidíme v tom podstatný problém"
počítáme s tím, že na systém budou útoky
kdo pokud bude zájem

nezávislý audit nebude možný, protože "práva"
e-gov: kód nebude mít kódy??
zpřísněný bezpečnostní režim

dle finanční správy db nemá velkou hodnotu, odkud by šla poptávka
do 10 lidí v Pardubicích bude mít přístup ke všemu, kompy nemají usb porty

jednotlivé daňové subjekty: jen svoje uvidí zaměstnanec FÚ
subjekt si může vyžádat svoje data na FÚ
hlášení chipovou kartou
šifrování mezi datacentry – zatím neřešeno, obě budou v oddělených sálech
TIER3, https://en.wikipedia.org/wiki/Data_center#Data_center_tiers
videozáznam v sálech
e-gov:

Chorvatsko – nulový výpadek, nula úspěšných útoků

bude zapojena odborná veřejnost?

Příprava

EET (ochrana dat):

Špaček:
http://www.lupa.cz/clanky/videl-jsem-specifikaci-projektu-elektronicka-evidence-trzeb/

- nekonzistentní dokumentace I v otázce zabezpečení
- otázka přístupu: zabezpečení je bráno jako něco extra (samostatná položka v rozpočtu), přitom by to mělo být z principu bezpečné, ne jako „nadstavba“

Další:

- za "SSL Akcelerátorama": Dle té specifikace mají mít georeplikaci (obojí asi v Pardubicích?), takže je otázka, jak je plánované řešení zabezpečení této komunikace mezi datacentry.

Nevíme:
jak bude řešen a chráněn přístup uživatelů:

- z FÚ
- z datacentra

bude se možné dostat z jednoho účtu k celé (nebo podstatné části) databáze?
To je jednoznačně jeden ze základních „vektorů“ útoku (např. přes zcizení přístupových údajů – keyloggery, apod.)

- „closed“ software – bude možné nezávisle ověřit, že nasazený software opravdu dělá to, co MFČR říká, že dělá? (problém back doors)

- data v datacentrech mají být uložena nešifrovaná!

klientská strana:

- při porušení/ztrátě/ukradení klientského zařízení je nastavena velmi krátká doba (48 hodin) na vyřešení problému (tj. autorizační údaje bude muset mít klient někde uložené i u sebe)

- v ČR není běžná “bezpečnostní gramotnost” (Sobotka-leaks), s tím se nepočítá (je to bráno jako “problém uživatelů”)
- Jak bude realizovanej přístup podnikatelů k jejich vlastním datům (datovejm větám)? Budou se archivovat pro účely dokazování? Jak rychle se k nim dostane podnikatel? Jak často bude mít možnost přístupu? Bude to automatický, nebo bude muset žádat a bude tam správní uvážení?

Obecněji

“security through obscurity”

Národní institut standardů a technologie doporučuje nepoužívat tuto metodu pro zabezpečení serverů: “
System security should not depend on the secrecy of the implementation or its components (Zabezpečení systému nemá záviset na utajováná implementace a jeho komponent)“ (http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf).

„closed“ software – bude možné nezávisle ověřit, že nasazený software opravdu dělá to, co MFČR říká, že dělá? (problém back doors)

Nejznámější úniky dat:

finanční data:

- Birkenfeld, UBS, https://en.wikipedia.org/wiki/Bradley_Birkenfeld
- Falciani, HSBC, https://en.wikipedia.org/wiki/Lagarde_list
- Deltour/Luxleaks, PwC, EY, Deloitte and KPMG, https://en.wikipedia.org/wiki/Luxembourg_Leaks

jiná data:

- Snowden+Manning, NSA+GCHQ, https://en.wikipedia.org/wiki/Edward_Snowden#Release_of_NSA_documents
- Sobotka-leaks
- Dokument o EET (MF ČR ho zprvu “utajovalo”)

jiné významné “hacky”:

- Jeep Cherokee, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
- (zkušební) volby Washington DC, https://www.washingtonpost.com/blogs/mike-debonis/post/dc-vote-hackers-publish-their-vote-hacking-exploits/2012/03/06/gIQArbG4uR_blog.html

Zveřejněné úniky jsou malým zlomkem všech úniků, neboť naprostá většina “útočníků” (a ani správců dat) nemá zájem na tom, aby se o úniku vědělo, ba přesně naopak.