Datové schránky, zase špatně

Vložil/a cm3l1k1 [1], 11 Květen, 2010 - 09:08

- Encryption [2]
- Recenze [3]
- Security [4]

Dnes mi přišlo na e-mail oznámení týkající se nové zprávy v mé datové schránce. Nutno podotknout, že musím mít dvě datové schránky. Jednu jakožto má osoba a druhou jakožtá já-podnikající osoba. Neptejte se proč, nikdo to neví/nechápe. Když e-mail přišel, byl jsem nucen se přihlásit do obou účtů, protože v těle emailu se nepíše, zda zpráva patří vám nebo vám-podnikateli. A to byl jen začátek...

Jako vždy se jednalo právě o tu druhou schránku... V případě druhé schránky po mě už asi po desáté (z deseti přístupů) požadovali změnu hesla.

To je značně nepochopený smysl bezpečné obměny hesla, když si při každém přístupu musí uživatel měnit heslo... Minimálně 8 znaků dlouhé, obsahující různorodé znaky (přitom spousta z nich je zakázána a tudíž nepoužitelná). Věřte tomu, že zrovna tato hesla budou mít naštvaní uživatelé napsaná na papírku u počítače nebo v osobním diáři.

A změnit si ho musíte. Jinak se vám účet po dalších pěti přihlášeních uzamkne.

A co že mi to tak důležitého píšou?

Že se přechází (a teď dejte pozor) na **šifrovací algoritmus SHA-2**. Bože, jak se může o naši bezpečnost při styku se státními institucemi/orgány starat někdo, kdo napíše, že SHA-2 je šifrovací algoritmus??

Certifikát certifikační autority začal používat hashovací algoritmus SHA-2... Teď jsme tedy moderní a bezpeční...

A perlička na konec

PDF dokument, informující o této změně, je podepsán Ing. Jindřichem Kolářem z MVČR, ale certifikátem podepsaným I.CA, který není používaný v systému datových schránek (používá se PostSignum CA), a tím pádem je považován za nedůvěryhodný!!
Takže první věc, která na mě vybafla při otevření PDF, bylo upozornění, že v dokumentu je problém s ověřením podpisu :o)

S takovým přístupem se kvapně přibližujeme velkému problému. Již nyní se neoficiálně mluví o SQL Injections v systému datových schránek. Je tedy opravdu na místě začít se bát zneužití své identity.

Ne kvůli virům, malwaru, facebooku etc., ale kvůli datovým schránkám.

Přikládám odkaz na výše zmíněnou zprávu o "šifrovacím algoritmu", včetně PDF dokumentu.

http://www.datoveschranky.info/clanek/351/ [5]
Prechod_SHA_2.pdf [6]

URL článku:
https://security-portal.cz/clanky/datov%C3%A9-schr%C3%A1nky-zase-%C5%A1patn%C4%9B

Odkazy:
[1] https://security-portal.cz/users/cm3l1k1
[2] https://security-portal.cz/category/tagy/encryption
[3] https://security-portal.cz/category/tagy/recenze
[4] https://security-portal.cz/category/tagy/security
[5] http://www.datoveschranky.info/clanek/351/
[6] https://security-portal.cz/sites/default/files/Prechod_SHA_2.pdf