Bezpečnostní doporučení podrobně

1. Přihlašujte se správně a bezpečně

Přihlašování pouze základní metodou jméno/heslo je z přihlašovacích metod nejsnáze napadnutelné a zneužitelné. Množství škodlivých programů dokáže jméno a heslo odposlechnout a poslat je přes Internet mimo Váš počítač. Informační systém datových schránek (ISDS) podporuje několik bezpečnějších přístupových metod a důrazně všem uživatelům datových schránek doporučujeme používat některou z nich:

- přes Identita občana (metodu jméno/heslo lze v nastavení schránky zakázat)
- aplikace Mobilní klíč ISDS (metodu jméno/heslo lze v nastavení schránky zakázat)
- jméno/heslo/komerční přístupový certifikát;
- jméno/heslo/jednorázová hesla přes prémiové SMS

Používejte POUZE metody, které jsou popsány v nápovědě na Klientském portálu ISDS. Jiné způsoby přístupu jsou podezřelé a může jít o podvrh.

Pro přístup do ISDS je na přihlašovací obrazovce možno zvolit přihlášení přes Identita občana. Po přesměrování na Portál národního bodu pro identifikaci a autentizaci si můžete vybrat způsob autentizace, např. eObčankou, nebo jménem/heslem/SMS. Všechny nabízené metody jsou tzv. vícefaktorové, a tedy bezpečnější než přihlášení pouze jménem/heslem. Další výhodou je, že po úspěšné autentizaci a návratu do portálu ISDS se Vám zobrazí seznam všech Vašich účtů v ISDS, které jsou v ISDS vedeny k vaší osobě. Podmínkou pro používání přihlašování přes Identitu občana je, že údaje o Vás jsou vedeny v registru obyvatel ČR.

V nastavení své datové schránky si můžete pro přihlašování zaregistrovat na svém mobilním telefonu aplikaci Mobilní klíč ISDS. Tato metoda přihlašování je rovněž vícefaktorová a tedy dostatečně bezpečná. Mezi její výhody patří mimo jiné pohodlnost jejího používání a možnost přihlašování ke všem svým účtům v ISDS.

Přihlašování uživatelským jménem a heslem sice není tou nejbezpečnější metodou, přesto je obecně nejfrekventovanější. Hlavním rizikem je při něm závislost utajení uživatelského jména a odolnost hesla na chování uživatelů.

Mnohaleté zkušenosti ukazují, že statisticky významná množina uživatelů pokládá za “neprolomitelná” hesla takové řetězce, které od nich lze poměrně snadno získat (například je používají i v mnoha jiných aplikacích), případně

je lze relativně rychle uhodnout (například je vytipovat z jiných údajů o uživatelích, které jsou často veřejně dostupné či jejich okolí běžně známé).

Při prvním přístupu do ISDS dosud většina uživatelů používá uživatelské jméno a iniciační heslo, které jim bylo bezpečně doručeno. Systém přitom vynucuje změnu tohoto hesla.

Pokud se rozhodnete neměnit přístupovou metodu a ponechat si přihlašování uživatelským jménem a heslem i nadále, pak vám doporučujeme dodržovat následující pravidla:

- udržujte v tajnosti své uživatelské jméno (jeho důvěrnost je stejně důležitá jako utajení vašeho hesla!);
- nikomu dalšímu svá uživatelská jména ani svá hesla nesdělujte a nespoléhejte na vámi nekontrolovatelná ujištění, jak se o ně bude starat;
- pokud potřebujete, aby do vaší datové schránky přistupovala jiná osoba, založte jí pro tento účel další účet a nastavte práva, která můžete kontrolovat;
- volte si dostatečně dlouhá hesla (odolnost hesel proti hádání spočívá velmi významně v jejich délce, zdaleka ne jenom v jejich složitosti);
- seznamte se s požadavky kladenými na hesla používaná v ISDS (povolené znaky, minimální délka, povinné použití čísel a speciálních znaků);
- heslo do datové schránky musí být minimálně 8 a maximálně 32 znaků dlouhé, musí obsahovat minimálně jedno velké písmeno, jedno malé písmeno a jedno číslo;
- povolené znaky jsou písmena (a-z, A-Z), číslice (0-9) a speciální znaky (! # $ % & ( ) * + , - . : = ? @ [ ] _ { | } ~)
- heslo v sobě nesmí obsahovat uživatelské jméno a nesmí se v něm za sebou opakovat 3 a více stejných znaků (jako například “aaa”, “bbb” atd.);
- hesla začínající na 12345, qwert, asdfg a podobně jsou velmi snadno slovníkově uhodnutelná a proto nejsou povolena.

V současnosti uznávaná a obecně doporučovaná bezpečnostní praxe pro vytváření hesel spočívá v dodržování následujících zásad:

- volte raději dlouhá, nežli krátká hesla (ideální je volit hesla delší než 20 znaků);

- snažte se vybrat hesla pro vás dobře zapamatovatelná, která si nebudete muset nikam psát a riskovat tak jejich prozrazení;

- pokud si musíte hesla poznamenávat, můžete k tomu používat některé z osvědčených aplikací, tzv. “manažery hesel” (příliš nedoporučujeme používat automatické vyplnění jména a hesla prostředky samotného webového prohlížeče);

- dostatečně dlouhá a odolná hesla příliš často neměňte, abyste si je dokázali pamatovat (heslo o 20ti a více znacích je v systému s úrovní zabezpečení, kterou poskytuje ISDS, rozumně udržitelné i po dobu jednoho roku - ISDS vám pro takový případ poskytuje možnost vypnout standardně vynucovanou změnu hesla v nastavení datové schránky);

- nepoužívejte v heslech triviální záměny speciálních znaků a čísel za písmena, abyste si usnadnili jejich zapamatování, usnadňujete tím i jejich uhodnutí potenciálním útočníkem (jako jsou záměny “a” za “@”, “o” za “0”, “i” za “1”, “E” za “3” a podobně);

- vyhněte se také jiným, obecně známým zvyklostem, které usnadňují hádání hesel (jako je začít a skončit heslo vždy stejným speciálním znakem, číslo používat trvale s hodnotou “1”, případně zadávat posloupnosti jako “123”, “234”, vkládat číslo vždy na konec hesla atd.);

- pokud se rozhodnete pro krátké heslo (například méně než 10 znaků), nedoporučujeme vám vypínat si vynucení jeho změny - v takovém případě bude lépe si heslo po 90-ti dnech pravidelně měnit na jiné.

Zvolíte-li si přihlašování uživatelským jménem a dostatečně dlouhým a odolným heslem, které nemusíte příliš často měnit a nebudete ho mít zaznamenáno tak, aby vám mohlo být snadno zcizeno, pak lze i tuto metodu pokládat za rozumně bezpečnou a praxí ověřenou. Pokud se rozhodnete pro postup využívající dlouhé a velmi odolné heslo se současným potlačením frekvence jeho změny, pak potřebné úkony můžete po přihlášení do své datové schránky realizovat v sekci Nastavení, viz obrázek níže:

Znovu připomínáme, že i v takovém případě je doporučenou bezpečnostní praxí změnit své heslo alespoň jedenkrát ročně.

Chcete-li dosáhnout vyšší bezpečnosti přihlašování do své datové schránky, než jakou v některých ohledech představuje kombinace uživatelského jména a hesla, můžete si v ISDS registrovat komerční přístupový certifikát (který si předtím musíte pořídit u některé zakreditovaných CA) nebo použít jednorázové doplňky hesel, tj. jednorázově platné bezpečnostní kódy pro přihlášení, které vám můžeme doručovat nezávislým komunikačním kanálem přes prémiové SMS nebo pomocí bezpečnostních tokenů (ty si lze instalovat například do chytrých telefonů).

Používání komerčního přístupového certifikátu je technicky jednoduchou, byť právně více regulovanou a proto také administrativně náročnější metodou.

Používání prémiových SMS je naopak administrativně nenáročné, uživatelsky snadno nastavitelné i technicky velmi jednoduché. Postačí běžné zvládnutí mobilního telefonu. Jeho nevýhodou je zpoplatnění prémiových SMS zpráv, kterými jsou jednorázové doplňky hesel doručovány uživateli při každém novém přihlašování.

Specifickou záležitostí je přihlašování uživatelů k ISDS prostřednictvím aplikací třetích firem, které používají přístup přes webové služby (tedy poměrně běžná situace, kdy není používán klientský portál ISDS a uživatel namísto toho pracuje se svojí datovou schránkou skrze jinou aplikaci). Systém takové aplikace podporuje a poskytuje jim všechny potřebné služby, aby mohly korektně pracovat. Jejich výběr je na uživateli samotném.
Po zkušenostech s několikaletým provozem vám doporučujeme postupovat následovně:

- zvolte si aplikaci od osvědčeného dodavatele, kterého znáte nebo si jeho pověst, postavení na trhu, kvalitu služeb a solidnost můžete ověřit;

- funkčnost aplikace si v ideálním případě nejprve otestujte, pokuste se získat hodnocení od jiných uživatelů, kteří s ní pracují, a zhodnoťte také její bezpečnostní vlastnosti;

- není vhodné volit aplikace, jejichž fungování je podmíněno tím, abyste provozovateli aplikace (tedy třetí straně) sdělili své přístupové údaje (například je vložili do jeho webové stránky s tím, že on se dále bude přihlašovat “za vás”) a ztratili tak nad nimi kontrolu;

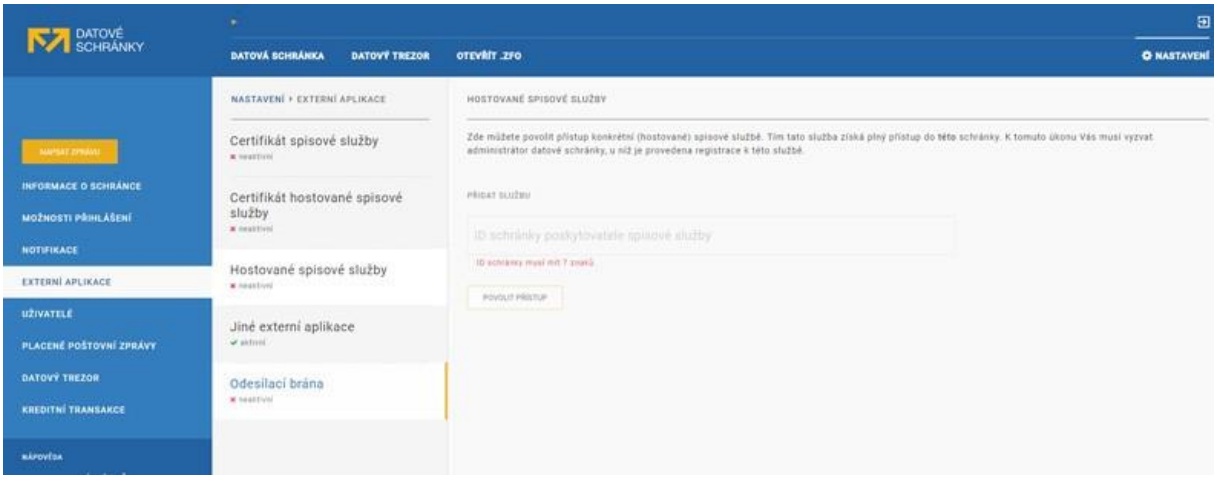
- pokud se jedná o lokálně instalované aplikace, zjistěte si alespoň, jak si můžete ověřit jejich pravost při instalaci, jak je lze aktualizovat a instalovat jejich záplaty či nové verze, zda a jak lokálně ukládají vaše přístupové údaje, zda o vás neodesílají data třetím subjektům.

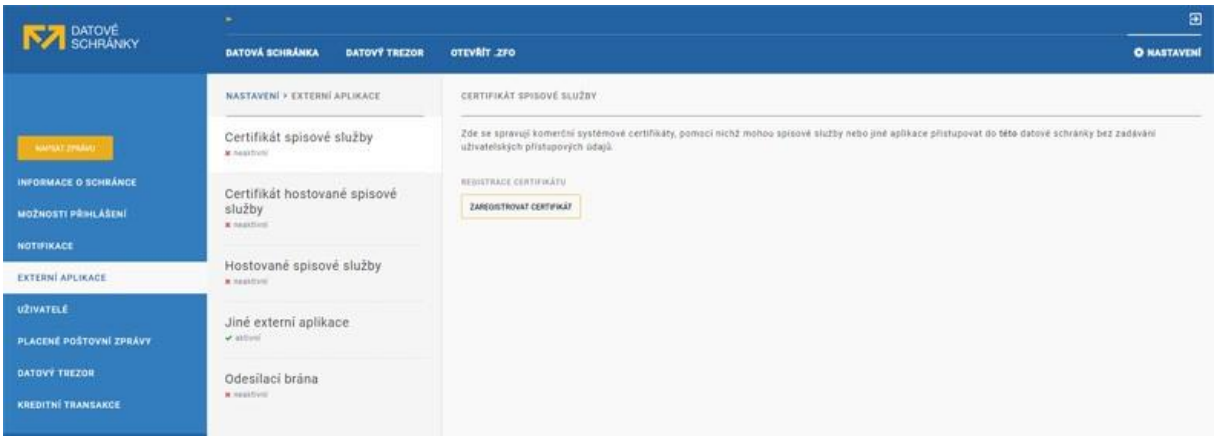
Při provozu ISDS jsme již odhalili několik aplikací, jejichž provozovatelé požadovali, aby jim uživatelé sdělovali svá uživatelská jména a hesla. Ta pak u sebe ukládali v podobě, která jim umožňovala se jimi přihlašovat, případně je i měnit. Jejich nová hesla pak tento provozovatel sděloval uživatelům ISDS nešifrovaným e-mailem. To se neshoduje s doporučenou bezpečnostní praxí.

Existují také aplikace stahující datové zprávy uživatelů ISDS, kteří s tím vědomě či nevědomě souhlasili (provozovatelé těchto aplikací uživatelům předkládají k souhlasu své vlastní podmínky, ve kterých přenášejí velkou část odpovědnosti na uživatele) a pracují s nimi nebo je ukládají na externí disky či do e-mailových systémů třetích firem, které k nim pak mohou získat přístup, a uživatelé nad nimi mohou ztratit bezpečnostní kontrolu.

Upozorňujeme proto, že výběr aplikací třetích firem pro práci s ISDS je právem, ale také odpovědností uživatele, ne odpovědností provozovatele ISDS. Jednou z nejdůležitějších povinností uživatele ve vztahu ke svým přístupovým údajům je chránit je tak, aby jich nemohlo být zneužito. Jde o povinnost, která přímo vyplývá z§ 9, odst. 2 zákona č. 300/2008 Sb. Poskytování přístupových údajů třetím osobám nebo jejich aplikacím či úložištím, která se nacházejí pod jejich kontrolou (tedy mimo kontrolu uživatele ISDS) vytváří možnost jejich zneužití.

V ISDS přitom existuje bezpečný postup, jak totéž učinit jinými, správnými prostředky. Lze ho provést pomocí sekce Nastavení klientského portálu:





Z bezpečnostních důvodů proto uživatelům ISDS doporučujeme, aby používali takové aplikace 3. stran, které výše uvedené, bezpečné udělení oprávnění k přístupu podporují a vyhýbali se těm aplikacím, které jakoukoliv formou od uživatele požadují sdělení jeho uživatelského jména a hesla třetí osobě (obvykle provozovateli externí aplikace).

2. Pozor na podvržené falešné stránky

Pokud přistupujete k datové schránce prostřednictvím klientského portálu ISDS na webové adrese https://www.mojedatovaschranka.cz,*vždy si ještě před vložením svých přístupových údajů ověřte především to, zda nejste na falešné webové stránce*, která se snaží vaše přístupové údaje podvodem vylákat.

Na toto základní doporučení si vzpomeňte zejména v takovém případě, pokud jste adresu sami nenapsali do URL řádku webového prohlížeče, ale namísto toho jste přístup k ní vyvolali kliknutím na její odkaz, na tlačítko, grafický obrázek či jakýkoliv jiný prvek umístěný mimo váš počítač (kupř. na cizí webové stránce) nebo ve zprávě (kupř. v e-mailu nebo v chatu), kterou vám kdokoliv doručil.

Doporučeným chováním je:

- používat k přístupu vždy vlastní odkaz, který jste si vytvořili tak, aby v něm byla uvedena webová adresa “https://www.mojedatovaschranka.cz”;

- pokud již takový odkaz máte vytvořen, je vhodné si zkontrolovat, zda v něm není (rovněž fungující, ale nedoporučená) webová adresa “http://www.mojedatovaschranka.cz”;

- jestliže při kontrole zjistíte, že používáte adresu ad. b) začínající na http místo https, doporučujeme vám opravit si ji na bezpečnější https podle bodu a) výše;

- správně vytvořený odkaz můžete uložit jako záložku v prohlížeči a pak ji pohodlně, opakovaně používat stále znovu.

Jakmile jste přistoupili ke klientskému portálu ISDS, je důležitým krokem vždy si ověřit jeho pravost. Pravost webové stránky klientského portálu ISDS na webové adrese https://www.mojedatovaschranka.cz si můžete ověřit velmi snadno a spolehlivě. Učiníte to kliknutím na "tlačítko" pro ověření pravosti serveru, které se nachází v adresním řádku prohlížeče. Na obrázku uvedeném níže (příklad je zpracován ve webovém prohlížeči MS Internet Explorer; v jiném webovém prohlížeči se vzhled může lišit) je v zeleném adresním řádku toto tlačítko vyznačeno modře. V závislosti na tom, kde je právě umístěn váš kurzor, může mít toto tlačítko následující vzhled:

- s nápisem "Ministerstvo vnitra [CZ] (primární varianta, objeví se po zadání správné URL adresy)

- s nápisem "Identifikoval GeoTrust" (variantu uvidíte krátce poté, jestliže jste nad tlačítko aktuálně umístili kurzor)

Zelené podbarvení adresního řádku spolu s prefixem "https://" před webovou adresou www.mojedatovaschranka.cz a s ikonou zámečku v levé části tlačítka je grafickou reprezentací pravosti serveru a signalizuje vám rovněž vytvoření šifrovaného spojení mezi vaším webovým prohlížečem a webovou stránkou klientského portálu ISDS.

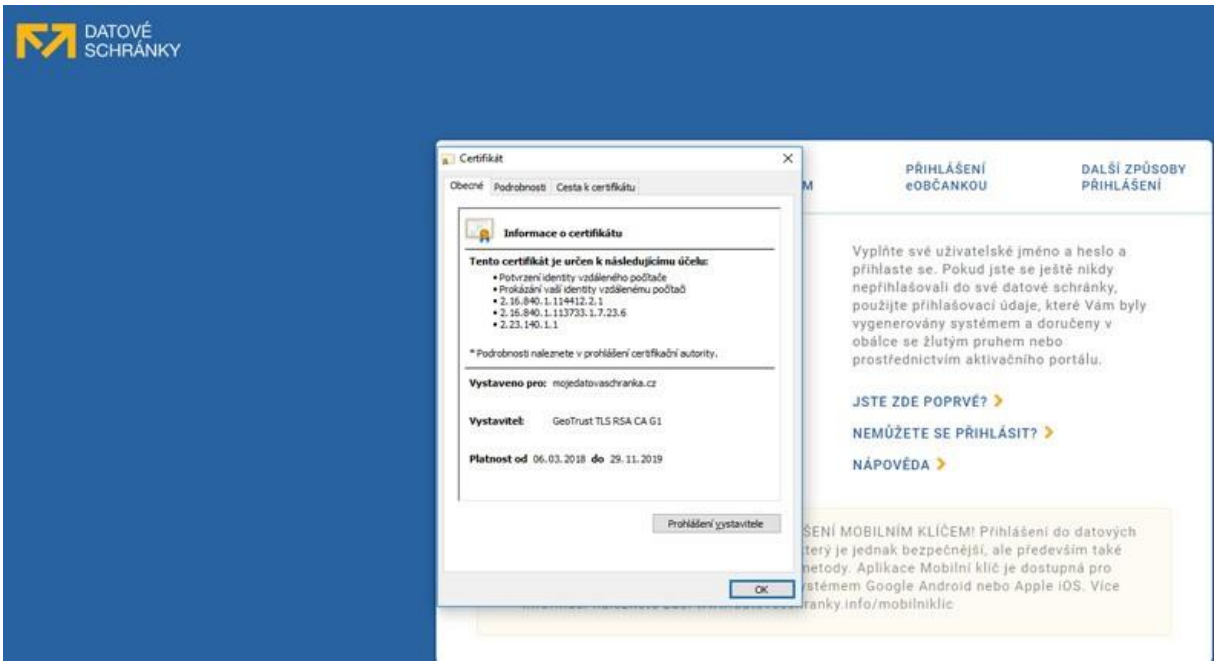
Vysokou garanci pravosti webového serveru, ke kterému se připojujete, vám v případě ISDS poskytuje EV SSL certifikát s rozšířenou validací. Grafické prvky, které jsme popsali, vám zásadně usnadňují odlišení pravého serveru od falešného (pokud by někdo falešný server vytvořil a pokusil se vás přimět k tomu, abyste do jeho falešné webové stránky zadali své přístupové údaje).

EV SSL certifikát lépe osvědčuje, že byla nezávislou autoritou důkladně ověřena reálná existence organizace, jejího sídla a také identita konkrétní osoby, které byl certifikát vydán. Současně uživateli poskytuje snadný a dobře rozpoznatelný způsob, jak se ujistit o pravosti serveru.

Po kliknutí na "ověřovací tlačítko" (v případě prohlížeče MS Internet Explorer je "tlačítko" vpravo od ikony "zámečku", tedy pod nápisem "Ministerstvo

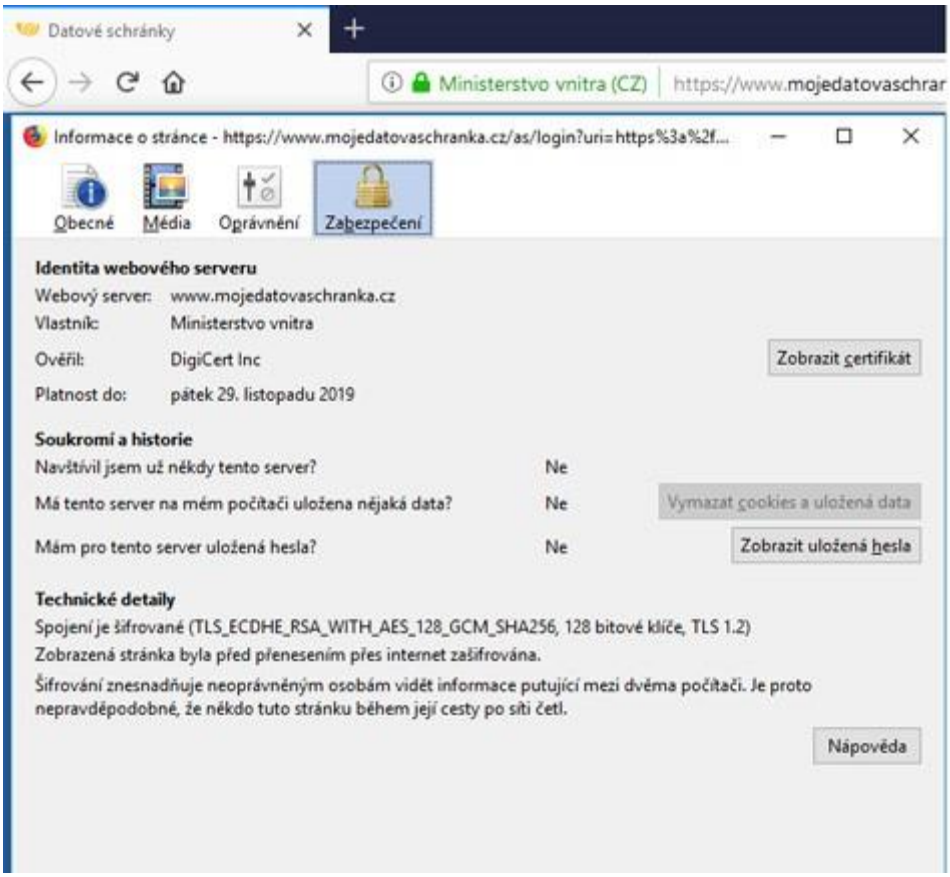
vnitra [CZ]” si lze ověřit pravost certifikátu, který stvrzuje identitu webového serveru ISDS.

Obecné údaje o EV SSL certifikátu (platné v čase zpracování tohoto dokumentu) ukazuje obrázek uvedený níže:



Abychom si lépe ukázali možné odlišnosti vzhledu v závislosti na vámi použitém webovém prohlížeči, projděme si ještě jednu ukázku téhož, tentokrát zpracovanou ve webovém prohlížeči Google Chrome.

Ověřená pravost serveru je opět zobrazována přímo v URL řádku webového prohlížeče a je výrazně podbarvena zelenou barvou. Také přímo zobrazuje i název držitele certifikátu "Ministerstvo vnitra [CZ]". Zeleně podbarvené pole v URL řádku v prohlížeči Google Chrome funguje jako "tlačítko". Tlačítkem se zelenou ikonou zámečku můžete zkontrolovat pravost webového serveru i platnost certifikátu. Po kliknutí na zeleně podbarvené tlačítko v URL řádku prohlížeče se uživateli zobrazí název držitele certifikátu "Ministerstvo vnitra“, doména pro kterou byl certifikát vydán „(mojedatovaschranka.cz)" a údaje o certifikační autoritě, která certifikát vydala (Geo Trust Extended Validation SSL CA). Současně je zobrazena informace o spojení se serverem "Vaše spojení se serverem www.mojedatovaschranka.cz" je šifrováno 256 bitovým šifrováním." Odkaz “Informace o certifikátu” zobrazí detaily. Prefix “https” je v tomto případě zobrazen vpravo od tlačítka a má zelenou barvu.



Zobrazení správné URL adresy https://www.mojedatovaschranka.cz s ověřením pravosti pomocí EV SSL certifikátu v nejvíce používaných webových prohlížečích je uvedeno níže:

- v prohlížeči MS Internet Explorer

- v prohlížeči Firefox (platforma MS Windows)

- v prohlížeči Google Chrome (platforma MS Windows)

- v prohlížeči Safari (platforma Mac OS X)

Vždy si obsah URL řádku klientského portálu ISDS pečlivě prohlížejte, zvláště pak před přihlášením do systému. Pokud by se URL řádek nezobrazoval zeleně a nevypadal obvyklým způsobem, případně se dokonce zobrazil červeně, nepřihlašujte se a informujte o tom pracoviště podpory uživatelů ISDS.

Rovněž vám doporučujeme, abyste přihlášení do ISDS neprováděli na cizí pokyn (ať už vám taková výzva byla doručena elektronickou poštou, vybízela by vás k tomu webová stránka či dokonce telefonický hovor s osobou, jejíž skutečnou identitu si nemáte jak ověřit.

Jako provozovatel ISDS vás předem ujišťujeme, že žádné naše dokumenty ani naši pracovníci vás k podobnému konání, tj. přihlášení se na pokyn, vybízet nikdy nebudou. Informační systém datových schránek s vámi vždy bude komunikovat pouze bezpečným způsobem. Nikdy vám nepošleme žádnou poštovní ani jinou zprávu, která by po vás žádala vložení vašich přihlašovacích, osobních či jiných citlivých údajů. A neuděláme to ani v případech urgentních. Jakmile takovou zprávu elektronické pošty uvidíte, věžte, že vždy pochází od podvodníka, který se za nás pokouší vydávat. Nastavíte-li si ve své schránce upozorňování na nové datové zprávy elektronickou poštou či přes SMS, nikdy vám nepošleme zprávu, která by obsahovala internetový odkaz, tlačítko nebo obrázek, na který lze kliknout. Zpráva s takovými prvky by nepocházela od nás, ale od podvodníka. Vystříhejte se příjmu takových zpráv, neplňte pokyny v nich uvedené a informujte o nich pracoviště telefonické podpory ISDS. Poté je smažte.

3. Cizí počítače používejte výjimečně a obezřetně

ISDS byl navržen tak, aby s ním jeho uživatelé mohli pracovat z celého světa. Pokud se nacházíte mimo své pracoviště nebo mimo svůj domov, můžete se proto přihlašovat i z takových míst jako jsou webové kavárny, hotely, letiště a podobně. Přitom můžete používat jak cizí počítače (tj. obecně takové, v jejichž operačním systému nemáte založen svůj vlastní účet), které v těchto objektech bývají často instalovány, tak i své vlastní přenosné notebooky, tablety, případně chytré telefony a podobná koncová zařízení vybavená webovými prohlížeči či instalovanými aplikacemi pro práci s datovou schránkou. Doporučujeme vám používat - kdykoliv je to možné - raději svůj vlastní počítač.

Při práci s datovou schránkou z cizího počítače buďte velmi opatrní. Podobně, jako byste byli opatrní např. při práci se svým internetovým bankovnictvím (pokud byste se vůbec rozhodli ho z cizího počítače použít).

Pamatujte na to, že odpovídáte za všechny právní úkony, které jsou vaším jménem z vašeho účtu v ISDS vykonány a to včetně důsledků (i možných

škod) vzniklých vám či třetím stranám, které by následně v dobré víře v jejich platnost případně rozhodovaly nebo konaly.

Jeden z možných scénářů přiměřeně opatrného chování uživatele při práci s ISDS z cizího počítače lze pro vyšší návodnost popsat kupř. takto:

- Cizí počítače, v jejichž operačním systému nemáte zřízen svůj individuální účet a jejichž aplikace proto nemáte pod žádnou kontrolou, používejte pro přístup do ISDS jen tehdy, je-li to opravdu nezbytné. Můžete-li se tomu vyhnout, raději tak nekonejte.

- Víte-li předem, že bude nezbytné, abyste svoji datovou schránku obsluhovali z cizího počítače, nastavte ještě v době, kdy do ISDS můžete přistupovat ze svého počítače k tomu účelu vhodnou přístupovou metodu. Pro tento účel můžete využít přihlašování pomocí jednorázových hesel doručovaných přes prémiové SMS nebo bezpečnostní kód. Tehdy vaše přístupové údaje nemohou zůstat zachyceny v cizím počítači.

- Přihlašujete-li se z cizího počítače do ISDS a můžete-li předtím restartovat jeho operační systém, pak je vhodné učinit alespoň toto základní, preventivní opatření, které může vypnout rezidentně běžící programy nastartované některým z uživatelů, který se systémem pracoval před vámi (obsluha internetových kaváren, hotelových recepcí aj. vám přitom může být nápomocna).

- Umíte-li to, ověřte si, zda v cizím počítači běží použitelná antivirová kontrola, případně zda jsou aktivní elementární bezpečnostní programy (například osobní firewall v MS Windows). Za šíření počítačového programu, který by mohl poškodit systém či spíše počítač některého z příjemců vaší datové zprávy, by vám mohla hrozit zákonem stanovená finanční sankce.

- Je-li to ve vašich možnostech, ověřte si další aplikace, které v tomto počítači komunikují do sítě internet a lze-li to učinit, dočasně jejich práci ukončete.

- Pokud je v cizím počítači instalováno vícero různých webových prohlížečů, vyberte si pro přístup do ISDS ten,
  který je v co nejaktuálnější verzi. Zkontrolujte si, jaké jsou do něj instalovány doplňky.

- Před přístupem do klientského portálu ISDS z cizího počítače vždy zcela ukončete práci toho webového prohlížeče, který pro přístup hodláte použít a spusťte jeho zcela novou instanci.

- Potřebujete-li si v takovém počítači připravit dokument,
  který se chystáte použít například jako přílohu datové zprávy, pak raději použijte vlastní USB disk, který k počítači připojíte a data

budete ukládat a zpracovávat na něm. Alespoň v malé míře tak zvýšíte pravděpodobnost, že vaše data skutečně odejdou s vámi.

- Nejdříve si připravte vše potřebné, abyste dobu aktivní relace se systémem zbytečně neprodlužovali. Po vykonání příprav se přihlaste do ISDS.

- Pokud máte možnost se přihlásit mobilním klíčem nebo některou metodou přes Identitu občana, volte přednostně tento způsob přihlášení.

- Máte-li možnost příjmu prémiových SMS nebo máte chytrý telefon a můžete-li to v dané situaci učinit, přihlaste se a dočasně si změňte metodu přihlašování na prémiové SMS nebo na bezpečnostní kód. Poté se odhlaste. Tím minimalizujete riziko, že někdo bude moci opakovaně použít vaše přístupové údaje. Opět, odejdou s vámi. (*Víte-li předem, že vás práce s datovou schránkou z cizího počítače čeká, můžete tento preventivní krok učinit ještě na svém pracovišti, případně z domova - viz bod b) výše.*)

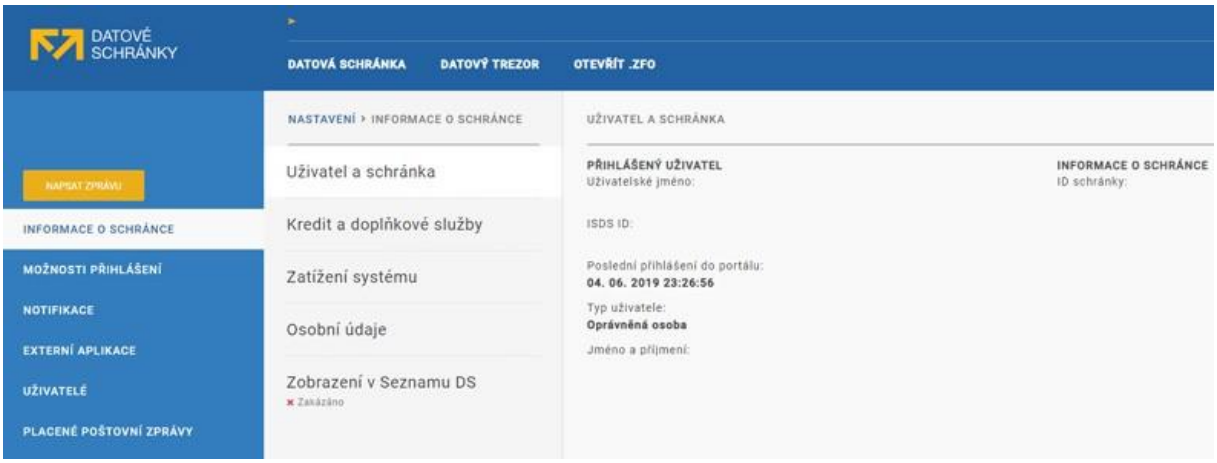
- Znovu se přihlaste za použití nastavené silnější přístupové metody a poznamenejte si čas přihlášení (to je vhodné pro každé přihlášení z cizího počítače).

- Vykonejte nezbytné úkony, které potřebujete provést. Práci si lze zpravidla rozložit a zkrátit také délku aktivní relace. Například, nejdříve jen stáhnete datové zprávy, uložíte je na svůj USB disk a odhlásíte se. Připravíte si vlastní podklady, až poté se znovu přihlásíte a odešlete odpovědi.

- Pokud dojde k pádu operačního systému nebo prohlížeče v průběhu vaší práce z cizího počítače, mějte na paměti, že prohlížeče mohou být nastaveny tak, aby lokálně uložily taková data, která lze potenciálně zneužít k obnovení vaší relace. Toto riziko odstraníte například tím, že se znovu přihlásíte (tak vynutíte otevření nové relace) a následně se korektně odhlásíte (čímž vynutíte zneplatnění nové relace).

- Práci s ISDS z cizího počítače vždy ukončete korektním odhlášením ze systému. To znamená kliknout na tlačítko “Odhlásit”. Nikdy nedělejte to, že byste práci se systémem ukončili pouze zavřením panelu v prohlížeči nebo jen zavřením webového prohlížeče.

- Později, při vhodné příležitosti, například po návratu z cesty, se “za dobré paměti” znovu přihlaste a zkontrolujte si, zda souhlasí čas vašeho posledního přihlášení s tím, který jste si naposledy vy sami poznamenali. K tomu vám poslouží následující údaj, který vám je po přihlášení vždy zobrazen:



- V případě, že čas posledního přihlášení nebude souhlasit nebo ve své datové schránce shledáte cizí zásahy, které jste sami neprovedli, kontaktujte podporu uživatelů ISDS. Můžete učinit i další preventivní kroky (například lze změnit heslo). V extrémním případě kompromitace lze zrušit váš původní účet a nechat si zřídit účet zcela nový.

4. Sdílený počítače je také riziko, avšak i zde lze s ISDS pracovat bezpečně

Počítač, který je používán pro práci s datovou schránkou, nemusí mít nutně jen jediného uživatele. Může být navzájem různými uživateli bezpečně sdílen. Na rozdíl od způsobu, jakým jsme výše definovali pojem “cizí počítač”, v tomto případě rozumíme pojmu “sdílený počítač” tak, že se jedná o systém, v jehož operačním systému má uživatel zřízen svůj vlastní uživatelský účet a ten má plně pod svojí kontrolou.

V případě sdíleného počítače uživatelé sdílejí jeden a tentýž operační systém, nikdy však nesdílejí své účty v jeho operačním systému. Pokud by uživatelé sdíleli uživatelský účet, ze kterého by se mimo jiné přihlašovali do ISDS, pak by bylo vhodné aplikovat pravidla pro práci z cizího počítače.

Pokud například pracujete s počítačem ve veřejné knihovně nebo internetové kavárně, v jehož operačním systému žádný účet zřízen nemáte, pak se jedná o cizí počítač a měli byste se podle toho chovat.

Jestliže pracujete kupříkladu s počítačem ve firmě, který společně s vámi sdílí i další uživatelé a přihlašujete se ke svému vlastnímu účtu v operačním systému tohoto počítače a tento účet je užíván pouze vámi, pak se jedná o počítač sdílený. V takovém případě jsou ve stejném počítači zřízeny navzájem oddělené účty různých uživatelů.

Klasickým příkladem sdíleného počítače by byl také domácí počítač používaný různými členy domácnosti k různým činnostem (dětmi pro školu

či zábavu, rodiči případně i pro podnikání atd.) s tím, že jednotliví uživatelé mají v jeho operačním systému své vlastní, navzájem oddělené uživatelské účty.

Jednotliví uživatelé se při používání sdíleného počítače obvykle střídají. Používání sdíleného počítače je obecně bezpečnější, než používání cizího počítače. Přináší však svá specifická rizika, která ponejvíce vyplývají z toho, že činnosti, které zde jednotliví uživatelé provádějí a způsoby, jakými se přitom chovají, se zpravidla podstatně liší. To platí i o jejich bezpečnostní povaze. Zatímco jeden uživatel se sdíleným počítačem například vykonává pracovní činnosti a chová se při nich konzervativně, jiný uživatel v něm může hrát online hry, instalovat nejrůznější neprověřené programy z neznámých zdrojů, sdílet jeho prostředky a data v něm externím aplikacím apod.

Mezi standardní riziková chování některých uživatelů sdílených počítačů mohou patřit:

- instalování neprověřených programů na základě cizích doporučení a pokynů;
- stahování dat ze serverů se sdíleným, případně i s nelegálním obsahem;
- instalace aplikací pro externí sdílení disků a adresářů, případně vzdálený přístup;
- instalace neznámých doplňků do webových prohlížečů a poštovních klientů;
- permanentní běh klientů pro připojení k sociálním sítím, chatům, konferencím;
- přehrávání potenciálně aktivních formátů (například flash) s pochybným obsahem;
- nedostatečná péče o antivirovou ochranu, případně užívání falešných antivirů atd.

Velmi důležitým doporučením proto je, abyste si pro práci se svou datovou schránkou zvolili takový počítač, kde tyto činnosti nejsou prováděny (nebo alespoň nemáte informaci o tom, že tam prováděny jsou). Existují způsoby, jak toto riziko můžete omezit a předcházet mu:

- každý uživatel sdíleného systému (počítače) by měl mít zřízen vlastní účet s omezenými právy;
- správcem by měl být pouze zkušený uživatel, schopný činnosti správy vykonávat;

- účet správce by neměl být používán pro běžná přihlášení a běžnou práci uživatele;
- správce by se měl odpovědně starat o aktualizace operačního systému či antiviru;
- hesla by měla být dostatečně silná a ve vztahu k síle se zvýšenou frekvencí měněna;
- uživatelé by neměli používat stejná hesla pro přístup do různých webových aplikací;
- uživatelé by se měli vystříhat funkcí webových aplikací jako “zůstat trvale přihlášen”
- každý uživatel by se měl při ukončení své práce odhlásit z operačního systému;
- zadání hesla by mělo být vyžadováno také po spuštění šetřiče obrazovky nebo režimu spánku počítače;
- instalované aplikace by měly být posuzovány také z hlediska jejich bezpečnosti;
- běžní uživatelé by neměli mít oprávnění vypínat a měnit funkce antiviru, firewallu aj.

Specificky pro používání datové schránky ze sdíleného počítače pak musíme zdůraznit některá pravidla, která jsou obecně vhodná, ale pro případ práce ze sdíleného počítače je uživatelům ISDS zvláště doporučujeme:

Používání sdílených počítačů zvyšuje riziko toho, že by nebezpečný software typu trojský kůň nebo spyware získal hesla nejenom toho uživatele, který ho do systému nainstaloval, ale také jiného uživatele, který v něm případně pracuje s datovou schránkou. Proto v tomto případě doporučujeme zvolit přístup přes Identitu občana, přes aplikaci Mobilní klíč, příp. přístupovou metodu využívající prémiové SMS nebo bezpečnostní klíč, aby uživatelské jméno a heslo bylo doplněno o další část přístupových údajů, dodávanou nezávislým kanálem (například přes mobilní nebo chytrý telefon), a tato kombinace byla dostatečnými údaji pro přihlášení do datové schránky.

Pokud se uživatel používající sdílený počítač přihlašuje do ISDS pomocí komerčního přístupového certifikátu, měl by ho mít instalován v nezávislém HW prostředku a měl by mít přístup k privátnímu klíči, chráněnému samostatným heslem nebo PIN kódem. Komerční přístupový certifikát by v zvláště tomto případě neměl být instalován ve vlastním softwarovém úložišti operačního systému, ve kterém existují i další, byť nezávislé uživatelské účty.

Uživatelům, kteří pracují s ISDS ze sdílených počítačů, doporučujeme, aby po ukončení práce s datovou schránkou mazali dočasně uložené soubory a data (lokální cache), které prohlížeč ukládá na pevný disk počítače. Uživatelé těchto počítačů by si měli být vědomi toho, že webové prohlížeče běžně ukládají obsah webových stránek, které častěji navštěvují. Za určitých okolností (jako například pád aplikace nebo operačního systému) mohou ale ukládat i data otevřených relací nebo dočasné soubory s obsahem příloh datových zpráv.

5. Komunikace prostřednictvím veřejné sítě je riskantní

Řada uživatelů se k síti internet připojuje bezdrátově. Je to pohodlné, mobilní a moderní. Má to však i svá rizika. Bezdrátové sítě lze z hlediska rizik rozdělit na privátní (tak můžete být připojeni kupříkladu ze svého domova či z pracoviště) a veřejné (lze se k nim připojit třeba v kavárně, v knihovně, v hotelu či na jiném veřejném místě). Jak název tohoto bodu říká, budeme se zde zabývat veřejnými sítěmi.

Jste-li k internetu připojeni prostřednictvím veřejné bezdrátové sítě (WiFi), tak je třeba si uvědomit, že veškerá vaše komunikace je pravděpodobně logována a může být tedy odposlechnuta, nebo Váš počítač může být infikován počítačovým virem, který jeho obsah může znehodnotit, zneužít, nebo jinak zkompromitovat. Nespoléhejte na bezpečnost veřejných sítí, tyto sítě bývají velmi často prostředkem pro rozsáhlé útoky na data veřejnosti. Potom její provozovatel je stejně obětí jako uživatel a případné škody nehradí.

Dokonce ani heslem chráněná, veřejná bezdrátová síť kavárny nebo hotelu nemusí poskytovat účinnou ochranu proti tomu, aby někdo další mohl kontrolovat vaši komunikaci, pokud nejsou i ostatní parametry sítě jsou správně nastaveny. Nahlížejte na takovou komunikaci podobně jako na privátní hovor, který byste konali na veřejnosti. Pokud chcete někomu sdělit něco osobního, co druzí lidé slyšet nemají, pak to na veřejnosti nahlas říkat nebudete. Neměli byste to dělat ani tehdy, když tak činíte prostřednictvím svého přenosného počítače.

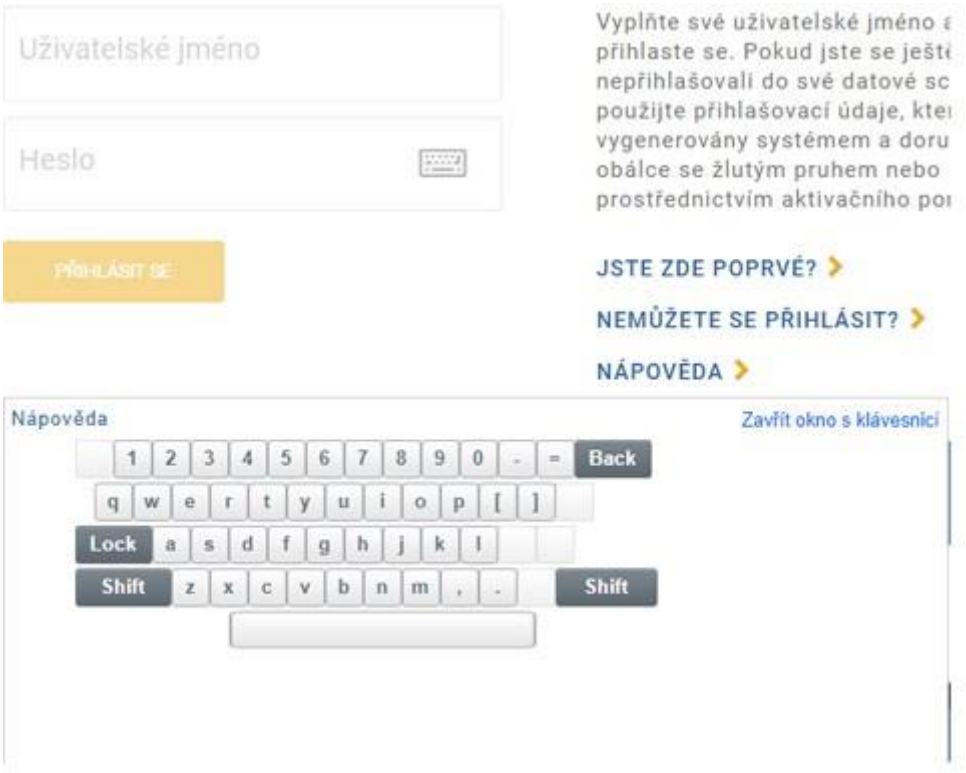
Zavolali byste v recepci hotelu na všechny “...právě teď se chystám přihlásit do své datové schránky”? Ve veřejné bezdrátové síti se tohoto můžete snadno nevědomky dopustit. Informační systém datových schránek s Vámi komunikuje šifrovaně. Toto šifrované spojení je vytvořeno mezi vaším webovým prohlížečem a systémem ISDS. Nicméně, nemusí se to vždy stát už v prvním kroku vaší komunikace se systémem ISDS. Pokud ve svém prohlížeči vložíte do URL řádku “http://www.mojedatovaschranka.cz”, bude až následně automaticky vytvořeno šifrované spojení “https://www.mojedatovaschranka.cz”. První část vaší komunikace by byla čitelná pro třetí osobu, pokud taková osoba bude veřejnou bezdrátovou síť dostatečně kontrolovat. Postačí tedy, pokud ve svém prohlížeči třeba

kliknete na záložku, která je uložena prvním z obou způsobů (tj. nešifrovaně), aniž byste si vůbec uvědomili, že jste ji právě tak kdysi dávno vytvořili.

Rovněž byste si měli dávat pozor na soukromé hotspoty. Většina chytrých telefonů dnes umí celkem snadno vytvořit hotspot, aby vypadal jako veřejná bezdrátová síť a nabídnout jej pak všem ostatním v blízkém okolí. Potenciální útočník může přijít do kavárny, spustit vlastní hotspot, nazvat ho tak, aby vás zmátl (například vedle sítě “KavarnaXYZ”, která tam běžně je, se objeví síť “KavarnaXYZ_Rychla”) a dát jí stejné přístupové heslo jako má pravá síť kavárny, aby byla kamufláž ještě dokonalejší. Existují případy, kdy se po přihlášení k takové síti objeví výzva k zadání čísla kreditní karty s tím, že rychlejší síť je placená. Stejně tak ale můžete ve vašem prohlížeči nevědomky spustit cizí program, který se bude snažit poslouchat vaši komunikaci či provádět jinou nekalou činnost.

ISDS používá EV SSL certifikát, který jsme popisovali výše (viz bod 1). Pro potenciálního útočníka by bylo velmi složité ho napodobit. Nicméně, necítíte-li se v otázce kontroly pravosti spojení dostatečně zkušení, bude lépe nepřihlašovat se skrze veřejné bezdrátové sítě, není-li to vyloženě nezbytné. Musíte-li se přesto přihlásit přes veřejnou bezdrátovou síť, pak postupujte také podle pokynů uvedených v bodě 1 výše a pečlivě si ověřte, zda komunikujete s pravým serverem. Buďte pozorní a nedělejte nic, co byste nedělali při připojení z vlastní sítě, ze zaměstnání či z domova.

Útočníci zneužívající veřejných bezdrátových sítí totiž zkoušejí i řadu dalších triků. Jedním z oblíbených je kupříkladu to, že vás hned první webová stránka načtená v prohlížeči vyzve, abyste pro zvýšení rychlosti komunikace vypnuli antivirus ve vašem počítači. Jestliže to uděláte, je následně učiněn pokus do vašeho počítače umístit trojského koně, který umí odposlechnout jméno a heslo už z vaší klávesnice a odeslat ho útočníkovi. Tomu by samotné šifrování webové komunikace nezabránilo. Pokud jste si předem nemohli nastavit přihlášení pomocí prémiové SMS nebo bezpečnostního kódu, disponuje ISDS pro tento případ grafickou klávesnicí, kterou je možné zvýšit svoji bezpečnost při zadávání hesla (viz obrázek níže).



Grafická klávesnice však neodvrací všechny možnosti, které útočník má, pokud by vás dokázal zmást natolik, že byste s ním nevědomky spolupracovali a plnili jeho pokyny. Jiným trikem bývá zneužití některého z velké škály programů pro chatování a sdílení souborů (například MP3 souborů, fotografií aj.), které jsou dnes instalovány ve velkém počtu počítačů, běží na pozadí, často nejsou správně bezpečnostně nastaveny nebo mají bezpečnostní chyby a fakt, že jsou spuštěny, si už mnozí uživatelé ani neuvědomují. I přes tyto služby lze někdy vzdáleně instalovat velmi pokročilé trojské programy. Správné je proto programy pro sdílení obsahu před prací s datovou schránkou vypnout. Vhodné je také nastavit při přístupu k veřejné bezdrátové síti aktuální umístění ve vašem osobním firewallu (například v tom, který je součástí Windows) na “veřejnou síť”, což může dočasně zablokovat další externí komunikaci, o které byste jinak ani nemuseli vědět.

Nechceme ve vás vyvolávat obavy ze všech veřejných bezdrátových sítí. Je však dobré pamatovat na to, že když jste připojeni přes takovou síť, pak nejste jen na internetu, ale jste také v lokální síti, ve které je společně s vámi připojena spousta jiných počítačů a některé z nich se mohou pokusit váš systém napadnout. Pokud cokoliv vypadá podivně, pokud se objeví nějaká varování ohledně webových certifikátů, pokud se po vás chce, abyste něco neobvyklého povolovali, abyste citlivé informace jako čísla kreditních karet, osobní údaje, jména a hesla zadávali do nezvyklých polí, je lépe z takové sítě odejít. Ačkoliv to samo o sobě nemuselo vždy něco špatného znamenat, sotva byste měli jistotu, že je vše pořádku. V životě procházíme i řadou jiných situací, ve kterých je lépe být třeba i trochu paranoidní a předejít tím potížím než se chovat příliš sebejistě a doplatit na to.

Jedná-li se kupříkladu o pracovní cestu a vy máte v jejím průběhu VPN přístup do sítě svého zaměstnavatele, odkud pak můžete přistoupit do ISDS, pak disponujete velmi dobrou variantou, jak bezpečně použít i veřejnou bezdrátovou síť. Při zachování ostatních zásad opatrného chování by vám neměla hrozit výše uvedená rizika. Kdykoliv předem víte, že se budete potřebovat přihlašovat z podobných veřejných míst a máte-li možnost si předem VPN přístup obstarat, pak je to řešení, které vám doporučujeme. Nemůžete-li použít VPN, je vhodné si v ISDS předem alespoň nastavit přístup přes přes Identitu občana, přes aplikaci Mobilní klíč, příp. metodu přihlášení pomocí prémiové SMS nebo bezpečnostního klíče, kdy je k vám část přístupových údajů doručena nezávislým komunikačním kanálem. Pokud přistupujete z vlastního počítače, což tento bod předpokládá, pak lze ke zvýšení bezpečnosti přístupu použít i komerční přístupový certifikát.

Pokud jste použili veřejnou bezdrátovou síť k přístupu do ISDS, pak je vždy dobré se po návratu z takové cesty chvíli věnovat drobnému “úklidu”. Při něm se může vyplatit:

- restartovat počítač, pokud ho po delší dobu běžně jenom uspáváte;
- aktualizovat operační systém a ujistit se, že máte všechny záplaty, které jste neměli možnost instalovat po dobu cestování;
- aktualizovat antivirové definice a provést kompletní kontrolu celého systému (lze-li, udělejte to jednou předtím než se připojíte na pracovišti nebo doma a ještě jednou poté);
- zkontrolovat nová pravidla osobního firewallu, podívat se, která povolovací pravidla vznikla v průběhu cesty a posoudit, zda je ve vašem zájmu taková pravidla ponechat či nikoliv;
- zkontrolovat si instalované doplňky prohlížeče a podívat se, zda jsou tam jen takové, kterým můžete věřit a potřebujete je, ne takové, o kterých byste nevěděli, vhodné je také smazat lokální cache z použitého webového prohlížeče;
- přihlásit se do ISDS a ověřit, zda se datum a čas posledního přihlášení shodují s tím, které jste provedli vy sami, případně si pro jistotu změnit dříve použité heslo.