Bezpečnostní zásady

Česká národní banka (ČNB) věnuje trvalou pozornost nadstandardnímu zabezpečení aplikace ABO-K internetové bankovnictví (dále jen ABO-K), proto implementovala moderní technologie pro ochranu důvěrnosti a integrity dat, dostupnosti a spolehlivosti celé aplikace.

Vedle opatření, realizovaných ČNB, je klient povinen věnovat náležitou pozornost rizikům na své straně, a to zejména rizikům vyplývajícím ze způsobu přípravy a předávání souborů s příkazy, zajištění ochrany podpisového certifikátu, klientské stanice a systémového prostředí.

Je třeba se zejména zaměřit na následující oblasti:

1. Chránit certifikáty používané pro elektronické podpisy
   a) zajistit systémovou a fyzickou ochranu soukromého klíče, který přísluší kvalifikovanému certifikátu určenému pro vytváření elektronického podpisu/elektronické značky, tj. ukládat soukromý klíč příslušející kvalifikovanému certifikátu resp. kvalifikovanému systémovému certifikátu na hardwarové úložiště (USB token, čipová karta), na kterém je soukromý klíč vygenerován při vytváření žádosti o certifikát a ze kterého nemůže být žádným způsobem exportován.
2. Vytvořit bezpečné systémové prostředí
   a) zajistit adekvátní úroveň zabezpečení klientských počítačů používaných pro ABO-K, zejména prostředky firewallů, antivirového, antispamového softwaru a dalšími prostředky pro ochranu před škodlivým softwarem, zejména viry, trojskými koni, spyware apod., dále systematickým vyhledáváním známých zranitelností a omezením přístupu klientských stanic k nebezpečnému obsahu a adresám v Internetu,
   b) zajistit pravidelné aktualizace a opravy softwaru, především operačního systému, prohlížeče webových stránek a dalších instalovaných aplikací,
   c) realizovat přihlášení disponenta k operačnímu systému pomocí standardního uživatelského účtu bez administrátorského oprávnění s dostatečně složitým heslem, resp. na základě jiného mechanismu s odpovídající nebo vyšší úrovní bezpečnosti
   d) vhodnými prostředky bránit neoprávněným osobám v užívání počítače a zejména ABO-K, např. odhlášením nebo alespoň uzamčením počítače v době nepřítomnosti disponenta
   e) pravidelně provádět bezpečnostní audit informačního systému s kontrolou zaměřenou na dodržování bezpečnostních zásad při práci s ABO-K internetové bankovnictví.
3. Zajistit vysokou úroveň zabezpečení systémů určených pro přípravu souborů s příkazy pro zpracování v ABO-K a pro zpracování výpisů z ABO-K tak, aby nebylo možné neautorizovaným způsobem manipulovat se soubory s příkazy před předáním do ABO-K a s výpisy před zpracováním v daném systému klienta.
   a) provádět elektronický podpis souborů s příkazy v zabezpečeném informačním systému klienta.

b) ověřovat pravost souboru s výpisy z účtu kontrolou elektronické značky ČNB ve svém zabezpečeném informačním systému a ukládat je pro potřeby případných reklamací. Certifikát pro ověření elektronické značky ČNB vydala certifikační autorita PostSignum České pošty:

Jedinečné jméno/Subjekt:

SERIALNUMBER = S16676,CN = Vedení účtů a platební styk (ABO),OU = Ústředí,O = Česká národní banka [IČ 48136450],C = CZ

Vystavitel:

CN = PostSignum Qualified CA 2, O = Česká pošta, s.p. [IČ 47114983], C = CZ

4. Dodržovat bezpečnostní pravidla při práci s Internetem
   a) nereagovat na výzvy k poskytnutí přihlašovacích údajů třetími osobami (spam, phishing), přihlašovací údaje jsou určeny pouze danému disponentovi a ČNB je nikdy za žádných okolností tímto způsobem nepožaduje,
   b) po přihlášení do ABO-K zkontrolovat, zda zobrazovaná stránka je stránkou serveru abok.cnb.cz.
5. Reagovat na podezření možného bezpečnostního problému zejména
   a) při nestandardním chování Internet Exploreru (dále "IE") upozornit svého správce počítače. Například na zpomalování IE, samovolné vyskakování nežádoucích oken, nemožnost spustit některé standardní funkce IE, nemožnost otevřít některé stránky, které jsou běžně dostupné atd. (obecně známé chování IE při napadení tzv. malware).
   b) při nestandardním chování aplikace ABO-K kontaktovat svého správce počítače a potom případně ČNB mailem na adrese abok@cnb.cz nebo telefonicky na číslech +420-2-2441-2531 nebo 4659.
   c) při podezření, že by mohlo dojít k neautorizovaným příkazům v ABO-K, bezodkladně zajistit zablokování přístupu do ABO-K, kontaktovat ČNB mailem nebo telefonicky (kontakty v bodě b) výše) a dohodnout další postup.
   d) při podezření, že by mohl být nebo že byl zneužit certifikát, neprodleně tento certifikát odvolat u certifikační autority, která jej vydala.