Standardy bezpečnosti IT

Existuje mnoho kategorií standardů (někdy nazývaných také *normy*), zabývajících se tvorbou bezpečných informačních systémů. Jde o standardy mezinárodní, regionální (např. evropské standardy), národní standardy, standardy státní správy některého státu, standardy určitého zájmového sdružení nebo průmyslové standardy.

Význam každého z těchto standardů zcela závisí na rozsahu jeho použití. Tento rozsah použití nemusí vždy odpovídat úmyslům tvůrců standardu (PKCS). Známe mnoho případů, kdy ambiciózní standardy upadly v zapomnění, nebo kdy původně zcela opomíjený standard získal celosvětový význam (RFC).

Zpravidla však platí, že nejširší platnost mají standardy mezinárodní a regionální. Použití národních standardů a standardů státní správy zpravidla nepřesahuje hranice státu, ve kterém byly tyto standardy vytvořeny. Výjimkou z tohoto pravidla jsou národní standardy USA (označované ANSI) a standardy státní správy USA (FIPS), které jsou někdy používány i mimo hranice USA.

Základní pojmy

Řešení, které je založeno na specifické formě vázanosti na jediného výrobce, dané nikoliv jeho monopolním postavením, ale neslučitelností jím používaného technického řešení s tím, které používají jiní výrobci se v angličtině označuje přívlastkem **proprietary**, stejně tak jako produkty, které z tohoto řešení vycházejí.

Prosadit vlastní řešení, a to ještě se ziskem, si však v dlouhodobém výhledu mohou dovolit jen ty největší firmy. Menší firmy se ve vlastním zájmu musely přizpůsobit těm řešením, které si zvolily velké firmy. Nešlo přitom ani tak o převzetí technologií či výrobních postupů (které jsou často pečlivě chráněné), jako spíše o převzetí konvencí, parametrů a protokolů, s cílem zajistit **kompatibilitu** (slučitelnost) vlastních produktů s produkty jiných výrobců. Názorným příkladem může být architektura osobních počítačů PC - zde se prakticky všichni výrobci přizpůsobili řešení, které si podle svého zvolila jediná firma - IBM.

Řešení, kterému se přizpůsobují různí výrobci a které tak představuje určitou společnou konvenci, zajišťující vzájemnou kompatibilitu produktů od různých výrobců, si již zaslouží přívlastek **standardní**, jako protipól anglického **proprietary**. Samotný obsah resp. podstata tohoto řešení se pak v širším slova smyslu označuje jako **standard.**

Standardní řešení resp. standard může vniknout tak, že se z podnětu či pod záštitou určité instituce, která je k tomu příslušná, sejde skupina odborníků a vypracuje návrh příslušného řešení. Ten je posléze kodifikován (tj. dostane formu oficiálního dokumentu příslušné instituce), a pak je prosazován do praxe. Podstatné přitom je, že zmíněné standardizační instituce obvykle nereprezentují přímo jednotlivé výrobce (i když tito se na jejich práci mohou významně podílet).

Standard, který je kodifikován, je standardem **de jure**. Jeho závaznost pro výrobce i uživatele je ovšem různá podle toho, jaký má právní statut resp. jaký je statut toho, kdo jej formálně vydává.

Například standardy, vypracované a vydávané mezinárodními standardizačními institucemi, mají často pouze formu **doporučení** a po formální stránce nejsou právně závazné.

Právní závaznost pak mívají až návrhy ve formě **norem**, které v rámci jednotlivých zemí vypracovávají k tomu oprávněné instituce, často na základě doporučení, přijatých mezinárodními organizacemi. Právní závaznost tyto normy mít však nemusí – záleží na postavení národní normotvorné instituce a konkrétní národní legislativy.

Samotní výrobci nemají možnost vydávat standardy *de jure*, neboť obvykle nemohou vydávat oficiální doporučení či dokonce normy, závazné pro jiné výrobce. Pokud jejich vlastní řešení spontánně a na dobrovolném základě přebírají i jiní výrobci, stává se toto řešení standardardem **de facto**.

Jsou ovšem i případy, kdy se vlastní ("proprietary") řešení určitého výrobce může stát "oficiálním" standardem (standardem *de jure*). Jde o taková řešení, která se ukáží být natolik životaschopná, že se nejprve stanou standardy *de facto*, a posléze je příslušné standardizační instituce převezmou jako "své" standardy - buď bez jakýchkoli změn, nebo s určitými úpravami. Příkladem může být koncepce sítí Ethernet, která původně vznikla jako vlastní řešení firmy Xerox, záhy se stala standardem *de facto*, a posléze se s drobnými úpravami stala i standardem *de jure* (standardem IEEE 802.3).

Standardy v průmyslovém světě znamenají jednu ze zásadních cest předávání znalostí, snižování nákladů a k umožnění vzájemné spolupráce a kompatibility produktů.

Jedno z možných členění

V bezpečnosti IT lze standardy členit do skupin:
-- základní standardy -- pro obecné požadavky uživatelů -- např. bezpečnostní architektura OSI, mechanismy autentizace entit atd.,
-- funkční standardy -- pro zajištění a certifikaci produktů, pro služby -- vysvětlují obecný přístup k využití základních standardů (např. požadavky k autentizaci dat, základům integrity atd.),
-- kritéria hodnocení -- pro hodnocení produktů a systémů (např. TCSEC, ITSEC, CC),
-- průmyslové standardy a postupy -- technické a procedurální standardy vyžadované specifickými skupinami uživatelů nebo společností (např. bankovní standardy),
-- výkladové dokumenty -- průvodce, slovníky pro informovanost a vzdělání (pokyny k ochraně soukromí, seznamy termínů atd.).

Poznámka:
Při příprav tohoto a následujících sedmi dokumentů jsem použil mimo vlastních článků a originálních dokumentů i materiály autorů:
Beneš, Hanáček, Pužmanová, Peterka, Pinkava, Staudek, Wallenfels

1. Úvod
2. RFC (Request For Comment)
3. Standardy PKCS (Public-Key Cryptographic Standards)
4. České technické normy a svět
5. Přehled norem v oblasti bezpečnosti informačních technologií (normy vyvíjené ISO/IEC JTC1 SC27 a ISO TC 68) zavedených do soustavy českých norem
6. Přehled mezinárodních a národních normalizačních institucí
7. Přehled některých základních kritérií hodnocení bezpečnosti IT