IT Systems
Únor 2015
49 Kč
SPECIÁLNÍ VYDÁNÍ IT SECURITY 2015

Kdo hlídá hlídače?
Privileged Identity Management

Není to dobré a bude hůř
Jaký bude rok 2015 v oblasti bezpečnosti IT?

Ochrana citlivých dat
není jen o DLP

Uživatelé jako rizikový faktor
informačních systémů

Kde se nejčastěji chybuje
při zálohování dat?

eIDAS
Nová evropská legislativa o elektronickém podpisu

Přehled dodavatelů řešení IT bezpečnosti v ČR

Jak na bezpečnost v mobilních zařízeních?

Mgr. Jan Nožka

Nikoho zde snad už nemusíme přesvědčovat o vzrůstajícím nebezpečí úniku osobních či jiných citlivých informací z mobilních zařízení. Mobilní zařízení nemusí být ani fyzicky zcizeno, ale stačí chvilka nepozornosti při otevření neznámého odkazu a můžete rovnou řešit nepříjemné následky. Krádeže osobních dat či získání přístupů k nabourání do platebního procesu zákazníků jsou přitom většinou důsledkem selhání lidského faktoru, tedy uživatele mobilní aplikace a majitele mobilního zařízení.

Pomíjivé chápání bezpečnosti a špatné návyky uživatelů jsou hlavními příčinami kybernetických útoků na mobilní zařízení. Nejde však „pouze" o získávání informací použitelných k nabourání do soukromého bankovního účtu, za kterými stojí profesionální týmy tzv. crackerů. Doslova strategické je také shromažďování osobních informací o uživatelích, o jejich chování na síti, zájmech apod. různými provozovateli internetových služeb. Osobní data se stávají novým platidlem na internetu.

Přitom platí jednoduchá logická posloupnost. Čím více chtějí být uživatelé informačně a komunikačně mobilní, tím více se nabízí mobilních aplikací, které jejich potřebu pokryjí. Proto dnes máme aplikace pro mobilní bankovnictví, pro kontrolu záloh na energie, aplikace zajišťující přístup do firemních CRM, ERP apod. Důsledkem je, že čím více jsou uživatelé informačně a komunikačně mobilní, tím více jsou vystaveni rizikům při fyzické krádeži mobilního zařízení nebo po jeho napadení např. trojským koněm.

V telefonech jsou dnes uloženy nejen konverzace s přáteli, emaily, fotografie a obecně osobní informace, ale také v případech pracovního použití telefonu či tabletu i důvěrné firemní informace (návrhy smluvních dokumentů, investiční záměry, samotná komunikace týmu spolupracovníků apod.).

Pomineme-li narušení bezpečnosti privátních dat jedince a zaměříme se na ochranu firemních dat, resp. firemní komunikaci, je každému bezpečnostnímu technikovi jasné, že v rámci bezpečnostní politiky podniku musí počítat s několika základními faktory, které ovlivňují bezpečnost komunikace skrze mobilní zařízení.

Jednak je to neznalost uživatele, který je nejrizikovějším článkem, a vnitřní směrnice nezabrání takovému uživateli kliknout na nebezpečný odkaz. Dále je nutné počítat se zranitelností operačních systémů mobilních zařízení, se kterými mohou organizace minimálně bojovat zavedením systému MDM s možností centrální instalace záplat a aktualizací. Bezpečnost přenosu informací po síti je zejména otázkou vývojářů mobilních aplikací, stejně tak jako zabezpečení přístupu do příslušné aplikace.

Administrátoři by se měli zabývat také mobilními aplikacemi pro online komunikaci (instant messaging, chat), které jsou pro velké množství zaměstnanců neodmyslitelné i v rámci firemní komunikace. Jedná se o efektivní a vyžadovaný způsob komunikace. Pokud chce management organizace tento způsob komunikace svým zaměstnancům zprostředkovat či povolit, neměl by se spoléhat na veřejné služby. Jednak kvůli své nedostatečné nebo neznámé bezpečnosti a jednak také kvůli uložení firemní komunikace a hlavně důvěrných dokumentů na cizích serverech.

Proto OKsystem přišel s řešením šifrované mobilní komunikace BABEL Business Edition (BABEL BE), které je od začátku zamýšleno jako cross-platformní (Android, iOS, Windows 7 a 8.1) a primárně určeno pro provoz na firemní infrastruktuře. Server přitom zprostředkovává datovou komunikaci mezi mobilními zařízeními, ale neuchovává žádné klíče a neúčastní se šifrování zpráv. V případě, že odesílatel nebo příjemce nejsou připojeni on-line, zajišťuje zasílání notifikací a asynchronní doručení šifrovaných zpráv. Důležitá je vazba BABEL serveru na firemní adresář a možnost okamžitě reagovat na významná bezpečnostní rizika, jako je ztracený nebo ukradený mobil, případně odchod zaměstnance.

Výsledkem je kompletní kryptografická ochrana přenášených informací – od pořízení přímo v mobilní aplikaci BABEL, přes odeslání až po uložení u příjemce. Jednak je plně zašifrován samotný přenos dalším účastníkům, jednak je veškerá psaná komunikace, datové zprávy i SMS, pořízená fotodokumentace, audionahrávky, přílohy dokumentů, také zašifrována v rámci úložiště odesilatele i příjemce. Pořízené fotografie a audionahrávky nejsou nijak sdíleny s ostatními aplikacemi ani cloudovými úložišti. ■

Autor článku, Mgr. Jan Nožka, působí ve společnosti OKsystem.