Zabezpečení mobilních zařízení

Mobilní zařízení, zejména tzv. chytré telefony, jsou malé počítače, které jsou často neustále připojené k Internetu. Mohou mít v sobě nainstalováno mnoho aplikací a umožňují další způsoby připojení a komunikace. Je tedy nutné se k nim chovat podobně jako ke stolním počítačům.

Co je mobilní zařízení

Mobilní zařízení je obecně zařízení, které je možné přemisťovat. Mezi mobilní zařízení patří například notebook, mobilní telefon, tablet, chytré hodinky nebo čtečka elektronických knih. Dnes nejrozšířenější mobilní zařízení je chytrý mobilní telefon, tzv. Smartphone.

Programové vybavení mobilního zařízení

Stejně jako u stolních počítačů mají i mobilní zařízení operační systém a mnoho dalších aplikací. Některé jsou již předinstalované a jiné si uživatel sám stáhne a nainstaluje z veřejných repozitářů.

Minimálně u operačního systému, aplikací s přístupem k osobním údajům nebo aplikací pro mobilní bankovnictví je nutné dbát na jejich zabezpečení a aktualizace.

U mobilních zařízení bychom neměli zapomínat na antivirová řešení, jejichž výrobci přidávají další komponenty ochrany specifické pro mobilní zařízení. Takovému řešení se říká zabezpečení koncových stanic (Endpoint Security).

Přístup k zařízení

Mobilní zařízení často přenášíme, případně ho máme stále u sebe. Je zde tedy vyšší riziko ztráty a následného zneužití neoprávněnou osobou. Mobilní zařízení bychom měli chránit některým z možných zámků obrazovky. Zařízení je zpravidla bez odemčení nepoužitelné (kromě nouzového volání).

Jako zámek obrazovky může být použit:

- **PIN** - číslo (personal identification number)
- **gesto** - předvolený specifický pohyb, který je zařízení schopno rozpoznat, pohyb prstem po dotykovém displeji, poklepání, zatřesení či jejich kombinace
- **otisk prstu** - pokud zařízení má snímač otisků
- **rozpoznání obličeje** - využívá přední kameru

Stejným způsobem můžeme bránit neoprávněnému spuštění důležitých aplikací. To mohou být aplikace pro čtení e-mailů nebo SMS, mobilní bankovnictví nebo webový prohlížeč, pokud v něm jsou uloženy přihlašovací údaje.

Ochrana dat v telefonu

V mobilním zařízení jsou často SIM karty nebo paměťové karty, které lze vyjmout a použít nebo zneužít v jiném zařízení.

SIM karta je pevně spojena s mobilním telefonním číslem. Pokud SIM kartu užívá někdo neoprávněný, může se vydávat za jejího majitele, telefonovat na jeho účet, ale také dostávat SMS například s kódy dvoufaktorové autentizace. SIM kartu ochráníme jednoduše PINem, který je třeba zadat vždy po zapnutí telefonu.

Paměťovou kartu, resp. data na ní můžeme šifrovat. Na paměťové kartě jsou zpravidla uloženy veškeré fotografie pořízené mobilním telefonem. Na fotografiích mohou být důvěrné informace. Zašifrováním zajistíme, aby bez znalosti klíče nebyla data čitelná.

Zeměpisná poloha

Mobilní telefon je schopen geolokace, čili zná svou skutečnou zeměpisnou polohu, kterou určuje tzv. triangulací. Ze známých poloh vysílačů a kvality jejich signálu, která je úměrná vzdálenosti mezi telefonem a vysílačem, je telefon schopen určit svou přibližnou polohu.

Chytřejší mobilní zařízení mají mnohem přesnější přijímač GPS (Global Positioning System). GPS je globální družicový polohový systém provozovaný Ministerstvem obrany USA. Existují i další podobné systémy, např. ruský GLONASS nebo Galileo, financovaný státy EU. Jak takový systém funguje (velmi zjednodušeně):

- Pro správnou činnost systému musí Zemi obíhat nejméně 24 GPS satelitů. V každém okamžiku jsou z jakéhokoliv (téměř) místa na Zemi viditelné alespoň 4 z nich.
- Každý satelit neustále vysílá na Zemi dvojici **velmi** přesných údajů - svoji pozici a čas.
- GPS přijímač ve smartphonu/tabletu dokáže z údajů 4 (a více) satelitů vypočítat svoji pozici na Zemi s přesností na přibližně 1-10 metrů.
- Celý navigační systém je velmi složitý a výpočty musí brát v úvahu mnoho komplikací a důsledků fyzikálních zákonů.

Dvoufázová autentizace na mobilním zařízení

Dvoufázová autentizace je proces, který zahrnuje dva různé nezávislé způsoby ověření totožnosti uživatele. První fází může být zadání hesla a druhou opsání kódu zaslaného pomocí SMS na přednastavené číslo. Případnému kyberpodvodníkovi pak nestačí pouze uhodnout nebo jinak získat heslo, ale musí získat i zařízení, kam přichází ověřovací kód.

Problém nastává, pokud je heslo vyplněno do mobilního zařízení (smartphone) a zároveň na to samé zařízení přijde i ověřovací kód druhé fáze. Pokud je zařízení odcizeno nebo napadeno, pozitivní efekt druhé fáze ověření se vytrácí.

Jsem leták ke školení IT bezpečnosti uživatelů sítě ZČU. Školení má 10 témat. Mě, ostatní letáky, brožury a prezentace najdete na https://bezpecnost.zcu.cz.

Naší almou mater je Západočeská univerzita v Plzni a na svět jsme přišly také díky podpoře Fondu rozvoje CESNET, z.s.p.o.