

9

Zabezpečení mobilních zařízení

Cyklus školení IT bezpečnosti uživatelů sítě ZČU.



Licensed under Creative Commons Attribution 4.0 International



CENTRUM INFORMATIZACE
A VÝPOČETNÍ TECHNIKY
ZÁPADOČESKÉ
UNIVERZITY
V PLZNI



fondrozvoje^{cesnet}

- Zařízení, které je možné **přemísťovat**
 - Notebook
 - Mobilní telefon
 - Tablet
 - a jiné
- Často **neustále připojené** k Internetu
- Umožňují **několik** dalších způsobů připojení a komunikace
 - NFC
 - USB
 - LTE
 - Bluetooth



- Mobilní zařízení mají **operační systém** a další aplikace stejně **jako počítače**
- Nutné dbát na zabezpečení a aktualizace operačního systému
- Nutné dbát na zabezpečení a aktualizace aplikací, které:
 - Mají přístup k **osobním údajům**
 - Slouží pro přístup do **mobilního bankovníctví**
- Neměli bychom zapomínat na **antivirová řešení**
 - Stejně jako u počítačů
 - Zabezpečení koncových stanic (Endpoint Security) s dalšími komponentami ochrany specifickými pro mobilní zařízení
 - Vyhledání polohy zařízení
 - Smazání a zablokování na dálku
 - Pořízení a odeslání fotografie z předního fotoaparátu po několika neúspěšných pokusech o odemčení
 - Kontrola výměny SIM karty

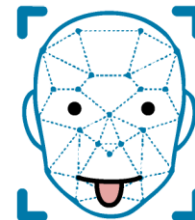
Přístup k zařízení



- **Vyšší riziko ztráty a zneužití** neoprávněnou osobou

- Chráníme zámek obrazovky

- PIN
- Gesto
- Otisk prstu
- Rozpoznání obličeje



- Stejně lze bránit i **neoprávněnému spuštění** důležitých aplikací

- E-mailový klient
- Aplikace na čtení SMS
- Mobilní bankovníctví
- Webový prohlížeč

- Mobilní zařízení často obsahuje **další karty**, které lze **vyjmout a zneužít** v jiném zařízení
 - SIM karta
 - Paměťová karta
- SIM karta je pevně spojena s **mobilním telefonním číslem**
 - Riziko zneužití identity (volání jménem majitele)
 - Volání na účet majitele
 - Obdržení SMS s kódy pro druhou fázi autentizace

Používejte PIN

- Paměťová karta obsahuje např. **fotografie** pořízené mobilním telefonem
 - Mohou obsahovat důvěrné informace

Data šifrujte

Mobilní telefon je schopen geolokace – **určení zeměpisné polohy**

- Využití triangulace
 - Ze známých poloh vysílačů mobilního signálu a jejich síly, která je úměrná vzdálenosti mezi telefonem a vysílačem, je telefon schopen určit svou polohu
 - **Poloha přibližná** – záleží na pokrytí mobilním signálem, funguje i v budovách
- Využití satelitního přijímače polohy
 - Americká GPS, evropský Galileo, ruský Glonass
 - GPS dnes nejrozšířenější
 - **Poloha velmi přesná**
- Podmínky fungování GPS
 - Zemi musí obíhat nejméně 24 GPS satelitů
 - Každý satelit neustále vysílá dvojici velmi přesných údajů – **svoji polohu a čas**
 - GPS přijímač dokáže z údajů 4 (a více) satelitů vypočítat svoji pozici na Zemi
 - Celý navigační systém je velmi složitý a výpočty musí brát v úvahu mnoho komplikací a důsledků fyzikálních zákonů

Dvoufázová autentizace na mobilu



- Při dvoufázové autentizaci je **mobilní telefon** často použit jako **druhý nezávislý** způsob ověření totožnosti
 - SMS zpráva s kódem na přednastavené telefonní číslo
 - Propojená aplikace se synchronizovanými kódy (např. Google Authenticator)
- **Není vhodné** zadávat **jméno a heslo** do stejného zařízení, které slouží jako zařízení pro druhou fázi ověření
- Efekt dvoufázové autentizace se tím vytrácí
- V případě zneužitého/napadeného mobilního zařízení útočník může získat jak přihlašovací údaje, tak ověřovací kód druhé fáze



<https://bezpecnost.zcu.cz/kapitola9>



CENTRUM INFORMATIZACE
A VÝPOČETNÍ TECHNIKY
ZÁPADOČESKÉ
UNIVERZITY
V PLZNI

fondrozvoje^{cesnet}
.....