
# Náměty na zabezpečení VoIP ústředen a telefonů

Martin Dvořák

# Program

- **Intro**
- **Bezpečnostní politika**
- **Jak na to**
- **Diskuse**

# Obvyklé typy útoků

- **Roboti**
- **Útoky „zevnitř"**
- **Sociální inženýrství**

# Bezpečnostní politika

**Správci**

- byli tu, jsou a budou
- vždycky musíte někomu důvěřovat, ale dobře vybírejte komu

**Síť**

- lokální síť se jmenuje lokální, protože nemá být dostupná komukoliv

**Operační systémy**

- OS mají uživatele a jen ti mají mít přístup k systému
- uživatelé mají nastavitelná oprávnění; aby mohli dělat jen užitečné věci

# Bezpečnostní politika

**Telefony**

- telefony umí telefonovat, a mnohdy se dá nastavit kam
- kvalita telefonů se neměří délkou výčtu funkcí na letáku

**Pobočkové ústředny**

- umí vícenásobné registrace, „hovory z internetu“, volat na „účet ústředny“ a „volat zpět“
- ale taky umí omezovat volání do různých směrů

**Operátoři**

- nabízejí úvěrování klientů pomocí postpaid účtů
- při prvním úspěšném útoku proti zařízení klienta se jim vše mnohonásobně vrátí

# Jak na to :: Hesla

- používejte dlouhá hesla
- hesla musí odolat slovníkovému útoku
- nenechte uživatele volit vlastní hesla
- hesla zásadně nepřenášejte v čitelné podobě
- omezte kadenci hádání hesel hrubou silou

---

- pokud to jde, nepoužívejte hesla vůbec

# Jak na to :: Přístupy

- přístup k čemukoliv povolte vždy jen tomu, kdo ho opravdu potřebuje
- povolte přístup jen z vybraných IP adres
- omezujte práva na nezbytné minimum
- povolujte jen ty činnosti, které mají smysl
- vždy používejte šifrované kanály

---

- zaznamenávejte přístupy a činnosti, ať víte, „kdo za to může“

# Jak na to :: Služby / Opravy

- nekumulujte funkce
- startujte jen služby, které nezbytně potřebujete
- zvažte, zda můžete provozovat služby na nestandardních portech
- všechny nepoužívané porty zablokujte firewallem
- updatujte, ale s rozumem – čtěte seznamy změn/oprav
- kontrolujte, zda po updatu nedochází k spouštění nových služeb

---

- buďte konzervativní – nejnovější není vždy nejlepší

# Jak na to :: Monitoring

- sledujte své systémy; všechny a průběžně
- sledujte jen důležité parametry, ale pozorně
- používejte nezávislý monitorovací systém
- reagujte rychle a agresivně

---

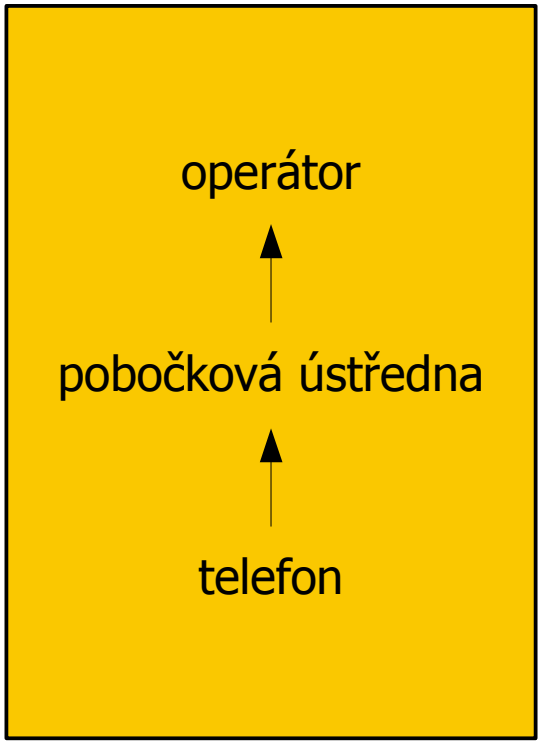
- svěřte správu odborníkům

# Shrnutí / Hierarchická kontrola

- zabezpečení konkrétního prvku vždy musí být o úroveň výš
- každý prvek zabezpečujte na co nejnižší úrovni
- dimenzujte svá zařízení adekvátně
- jediné neprolomitelné zařízení je to, které nemáte

---

- nemějte obavy, ale buďte opatrní



# Otázky / Diskuse

**Děkuji za pozornost, teď je to na vás :-)**

martin@ucag.ch