problém - otvorený port v routeri

Bežné pokladnice eKasa, ale i platobné terminály, ktoré komunikujú cez socket, majú spoločnú vlastnosť, ktorá sa týka zníženej bezpečnosti. Predpokladá sa, že tieto zariadenia budú umiestnené v chránenej lokálnej sieti. Skutočnosť je často taká, že do siete majú prístup aj nepovolané osoby, ktoré môžu zariadenia v LAN tak ľahko ovládnuť.

Podobný princíp zníženej bezpečnosti, či skôr nebezpečnosti je, aj keď takéto zariadenie je vystavené do internetu. Keďže výrobcovia neaplikovali do socket komunikácie bezpečnostné pravidlá, tak sa dajú ovládať z akéhokoľvek miesta. V praxi sa to deje tak, že robot skenuje verejné IP adresy a skúma otvorené porty. Ak sa podarí zariadenie identifikovať, je možné ho podľa dostupných manuálov ovládnuť.

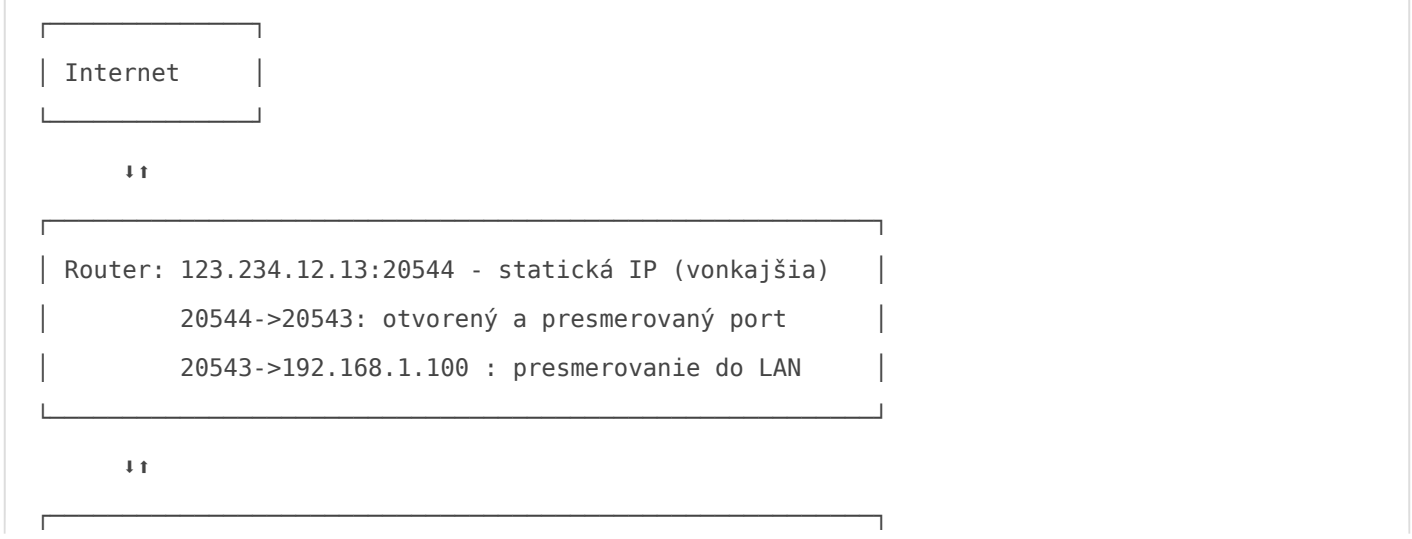
rýchlosť komunikácie cez Socket zvykne byť vyššia ako cez REST API rozhrania a preto je rozšírená napríklad v slipPrinters, komunikátoroch a podobne. Naproti tomu značne vyššia bezpečnosť je pri komunikácii cez REST API rozhranie, keďže sa jedná o modernejší spôsob komunikácie, kde sa počíta s rôznymi overeniami.

> Preto odporúčame využiť zariadenia s nechránenou Socket komunikáciou len v zabezpečenej lokálnej sieti (LAN)

> Priama nezabezpečená komunikácia nech je len testovacia, či dočasná !

Komunikácia z WAN cez socket

Komunikácia postrádajúca overenie



```
| KASA: 192.168.1.100:20543 - IP (vnútorná)                |
|        - socket komunikácia cez port 20543               |
|        - príklad: ⬇<ENQ>  ►      ⬆<ACK>                  |
|                   (Enquiry)   (Acknowledgent)            |
└──────────────────────────────────────────────────────────┘
```

Stalo sa, že v minulosti sme riešili zablokované zariadenie eFT5000. Zablokovalo sa kvôli tomu že niekto poslal cez otvorený port škodlivý kód. eFT5000, ako iné zariadenia, nemá akékoľvek zabezpečenie socket komunikácie, teda žiadna verifikácia, token či iné, len sa komunikuje cez otvorený port, obdobne bez ochrany ako FiskalPro či POI s PRSK05 a iné. Samotné zariadenie musí preto byť úplne ošetrené voči cudzím kódom a ak nieje, môže sa poškodiť. Avšak ak niekto bude posielať odkiaľkoľvek regulérne doklady, budú bez problémov prijaté a spracované. Jediné riešenie je lokálny soft, ktorý bude cez API preberať požiadavky a vracať statusy. API musí byť na serveri. Tým pádom naša pôvodná knižnica Ekasa.php stráca význam, lebo ona komunikuje cez IP socket, alebo aj nie, ak je server v LAN...

Čo sa týka servisného linku https://ekasa-tester-gecora.restapi.sk/ekasaanyfile... tak ho neodporúčame zdieľať. Pomocou neho môže zariadenie plne ovládať aj záškodník...

Komunikácia cez REST API

Komunikácia s overovaním v REST API rozhraní neprenesie na zariadenie cudzí kód (napríklad XSS - Cross-Site Scripting). Komunikuje sa pomocou HTTP protokolu, teda je to obdobné, ako prehliadanie web stránok, avšak jedná sa o dáta ktoré majú vlastnú štruktúru a ich odosielanie a prijímanie je šifrované a zviazané s viacerými formami zabezpečenia prístupu (Password, Bearer, Token). Taktiež samotné prijímané dáta môžu byť ošetrené (napríklad Escapovanie HTML, Sanitizáciou scriptov, Validáciou a FIltrami a inými novými formami).

WEB : GeSys , WordPress, **hoci kto**	⇐	← Gesys : skenovanie odpovedí
↓		↑
WEB : REST API → overenie → zápis úlohy		**WEB** : REST API → overenie → zápis odpovede
↓		↑
LAN : program strážiaci úlohy		**LAN** : program strážiaci úlohy odošle odpoveď
→ **spracovanie úlohy (pre POS, POI)**	⇒	**odpoveď**

Revision #9
Created 2025-07-29 08:26:22 UTC by Attila Jančik
Updated 2025-08-11 07:31:18 UTC by Attila Jančik