Zero Trust: Sicherheit & Isolation

Sicherheit ist in einer Fabrik sehr wichtig. Ein Gast darf nicht in das Produktionsnetzwerk gelangen. Dafür habe ich **“Zero Trust”** Prinzipien angewendet.

1. Port Security (Anschluss-Sicherheit)

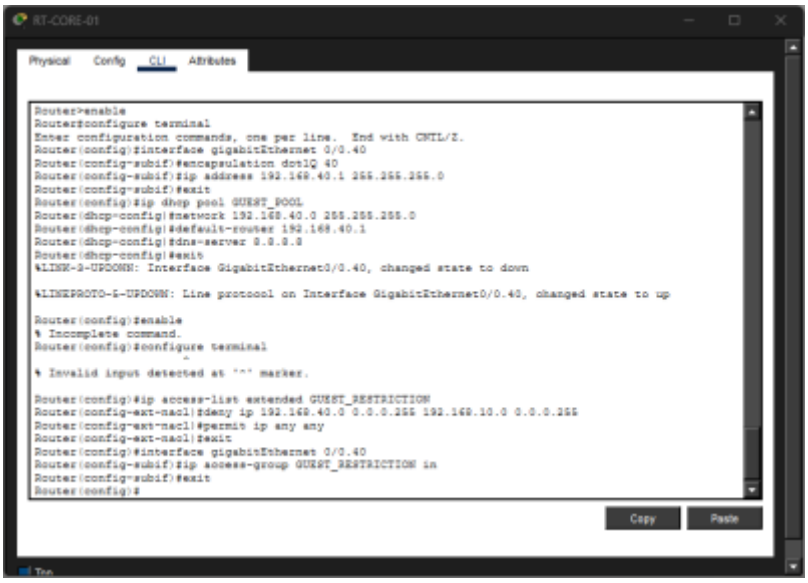
Auf dem Switch wurde die “Port Security” aktiviert:

- Der Switch merkt sich das erste Gerät, das angeschlossen wird (Sticky MAC).
- Wenn jemand ein fremdes Gerät anschließt, schaltet sich der Anschluss sofort automatisch ab (**Violation Shutdown**).

2. Access Control Lists (ACL)

Auf dem Router habe ich Firewall-Regeln (ACL) programmiert, um die Netzwerke voneinander zu trennen.

```
Router#
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)#! Create the Access List
Router(config)#ip access-list extended OT_ISOLATION
Router(config-ext-nacl)#deny ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
Router(config-ext-nacl)#permit ip any any
Router(config-ext-nacl)#exit
Router(config)#
Router(config)#! Apply it to the Office Interface
Router(config)#interface gigabitEthernet 0/0.20
Router(config-subif)#ip access-group OT_ISOLATION in
Router(config-subif)#exit
Router(config)#
```



Die Sicherheitsregeln:

- **Produktion vs. Büro:** Das Büro-Netzwerk darf **nicht** auf die Produktion zugreifen (und umgekehrt).
- **Gäste-Einschränkung:** Das Gäste-WLAN (VLAN 40) darf nur ins Internet. Es darf **niemals** in das Büro-Netz oder in die Produktion.
