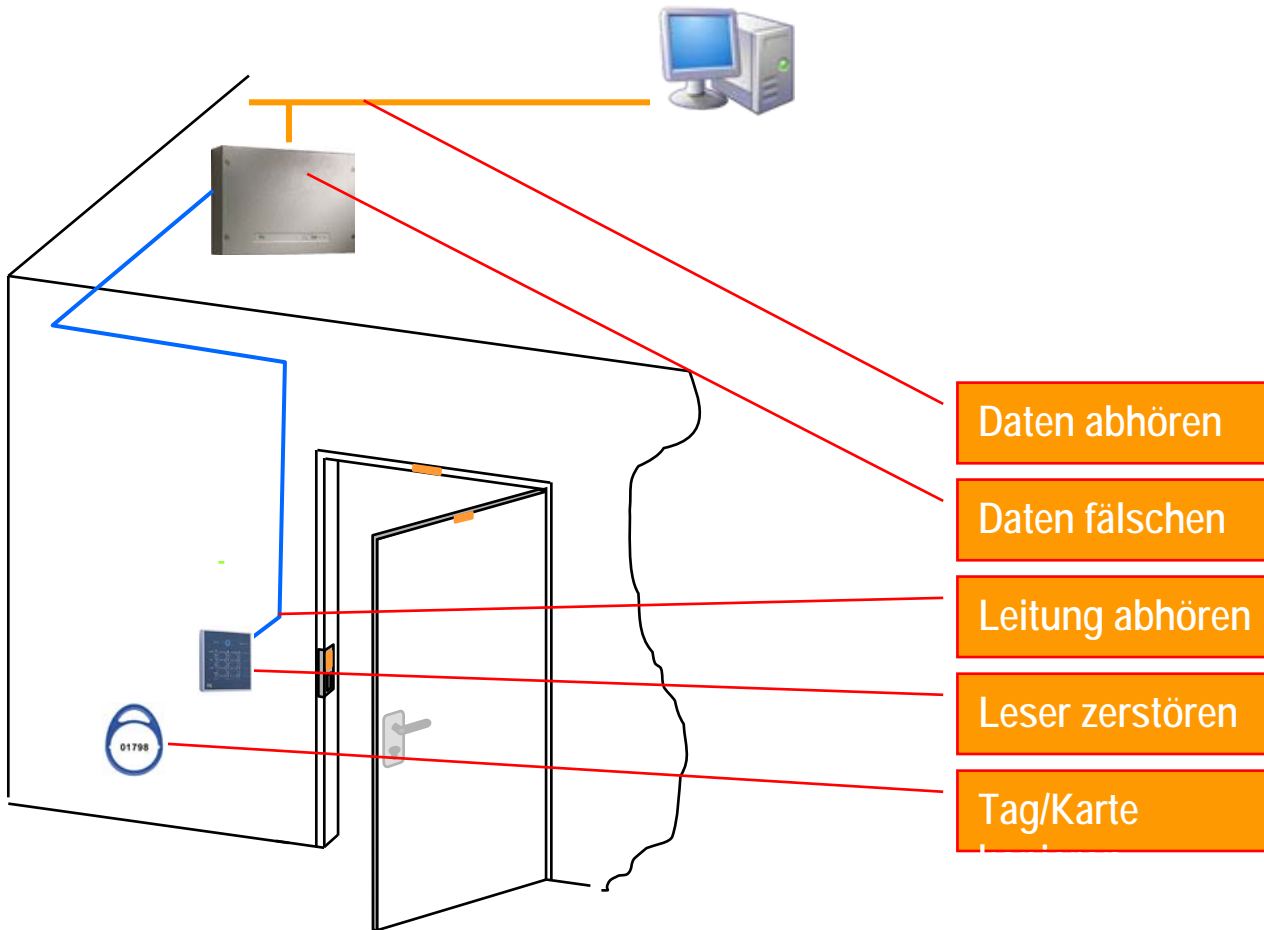




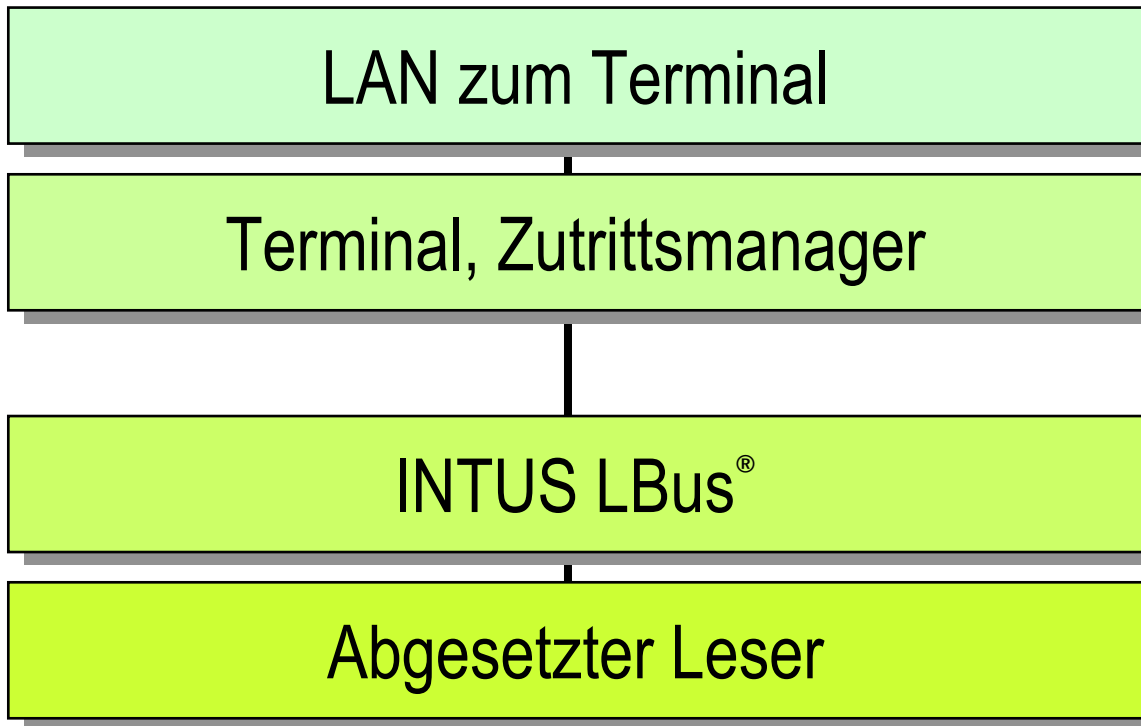
Wie sicher ist „sicher“?

Schwachpunkte bei Zutrittssystemen  
und Konzepte für höhere Sicherheit

# Trägerische Sicherheit bei Zutrittslösungen



## INTUS Systeme bieten hohe Sicherheit auf allen Ebenen



## Sicherheit on board

### LAN zum Terminal

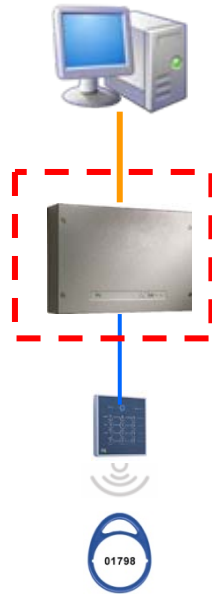
- | Daten-Verschlüsselung mit Code AES (Advanced Encryption Standard)
- | Rijndael-Algorithmus, ein Block-Algorithmus, der als besonders sicher gilt und auch bei VPN verwendet wird
- | Der Algorithmus wird im 128bit Output Feedback Mode (OFB) betrieben, um einen Datenstrom beliebiger Länge verschlüsseln zu können.
- | Bei jedem Verbindungsaufbau wird der Algorithmus aus Sicherheitsgründen neu initialisiert.



# Daten fälschen

## Terminal, Zutrittsmanager

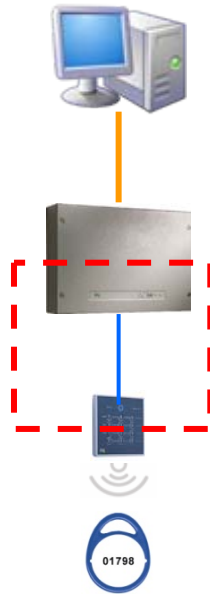
- | Offline-Fähigkeit mit Notpufferung → kein Datenverlust bei Leitungsunterbrechungen, Rechnerausfall, Netzausfall  
→ Gesicherte Übertragung bei Rückkehr des Normalzustandes
- | Embedded Firewall → verhindert Angriffe aus dem internen Firmennetz.
- | Immanenter Virus-Schutz: In TCL-Terminals kann nur 1 TCL-Programm laufen → Virus-Programm mit exe-Datei ist nicht lauffähig
- | Drei Berechtigungs-Ebenen für Setup:
  - Ebene 1 „Leser“ (z. B. für den Haustechniker)
  - Ebene 2 „LBus“ (z. B. für den Partner/Kunden)
  - Ebene 3 „Rechner“ (z. B. für Sicherheitsbeauftragte/IT-Manager)
- | Getrennte Wartungsgruppen → getrennte Verwaltung von 2 Applikationen durch 2 Abteilungen
- | Sabotagekontakt → SW-Sprungziel mit einer programmierbaren Reaktion.



## Daten abhören

### INTUS LBus<sup>®</sup>

- | LBus für den Anschluss von PCS-Peripherie
- | Übertragung mit gesichertem Übertragungs-Protokoll mit BSC (IBM)
- | Adressierung mit Checksumme, Quittungsmechanismus
- | Aktivierbare Verschlüsselung mit „RC4“ zwischen Terminal und abgesetztem Leser



## Leser zerstören und „Kurzschluss“

### Abgesetzter Leser

#### | Sabotagekontakt

| INTUS 300: Magnetkontakt

| INTUS 400: mechanischer Kontakt (Schalter)

| INTUS 500/600: optische Lichtschranke

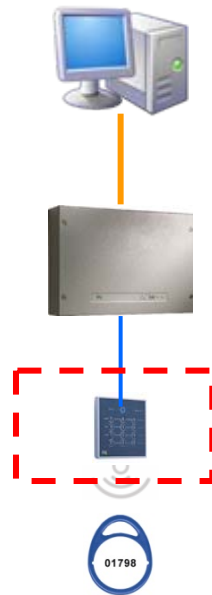
| INTUS 640H: kein Sabotagekontakt!

#### | Integriertes I/O-Modul

| → Kurzschließen des Relais

| Relais entweder aus INTUS ACM oder

| externes Relais Modul



## Solche und solche Karten...

### RFID-Medien

- | Billige Karten und Tags bieten sehr begrenzte Sicherheit
  - | Miro: Kopieren der Seriennummer „im Vorübergehen“
  - | Mit Hitag2 kann Miro emuliert werden
  - | Hitag: Schreiben auf Karte
  - | Mifare classic / Legic prime: Verschlüsselung, Kopierschutz?
- | Mifare DESFire EV1
  - | AES-128 Verschlüsselung
- | Legic advant
  - | DES/3DES Verschlüsselung, Master/Token Prinzip

