„Achtung, Unfall voraus“?
–
Was IT-Netze mit Verkehrsnetzen zu tun haben

Patrick Hof - RedTeam Pentesting GmbH
patrick.hof@redteam-pentesting.de
https://www.redteam-pentesting.de

itcs-Seminar „Innovationen rund um die Echtzeit“
18. März 2015 - Würzburg

RedTeam Pentesting, Daten & Fakten

- ★ Gegründet 2004
- ★ 10 Penetrationstester
- ★ Weltweite Durchführung von Penetrationstests
- ★ Spezialisierung ausschließlich auf Penetrationstests

RedTeam Pentesting, Daten & Fakten

Was ist ein Penetrationstest?

- ★ Angriff auf ein Netzwerk oder Produkt im Auftrag des Betreibers
- ★ Fragestellung: Wie weit kann ein Angreifer eindringen?
- ★ Durchgeführt aus der Angreiferperspektive, gleiche Methoden wie „die Bösen“
- ★ Individuelle Suche nach Schwachstellen durch Spezialisten

RedTeam Pentesting, Daten & Fakten

- ★ Penetrationstests unterschiedlichster Systeme und Branchen
- ★ Industrie, Banken & Versicherungen, Handel, Rechenzentrumsbetreiber, öffentliche Verwaltung. . .
- ★ Darunter auch: Verkehrsbetriebe
- ★ Wichtig: Immer die Umsetzung in der Praxis im Blick behalten

Vernetzung in Verkehrsbetrieben

Vernetzte IT: Aus den Verkehrsbetrieben nicht mehr wegzudenken

- Planung
- Disposition
- RBL/ITCS:
  - Datenerhebung / Telematik
  - Kommunikation (Sprache, Daten)
  - Standortverfolgung
  - dynamische Fahrgastinformation
- Ticketverkauf
- Abrechnung
- ...

Ein typischer Arbeitsweg

Vor Fahrtantritt: Nachschauen, wann der Bus kommt und ob er pünktlich ist, ggfs. Routenplanung über

- ★ Internet (Webseite)
- ★ Smartphone-App
- ★ Anzeigetafeln an der Bushaltestelle
- ★ Später im Bus: Fahrgastinformationssystem zeigt die nächsten Haltestellen an

Ein typischer Arbeitsweg

[N24.de, 18. Mai 2014]

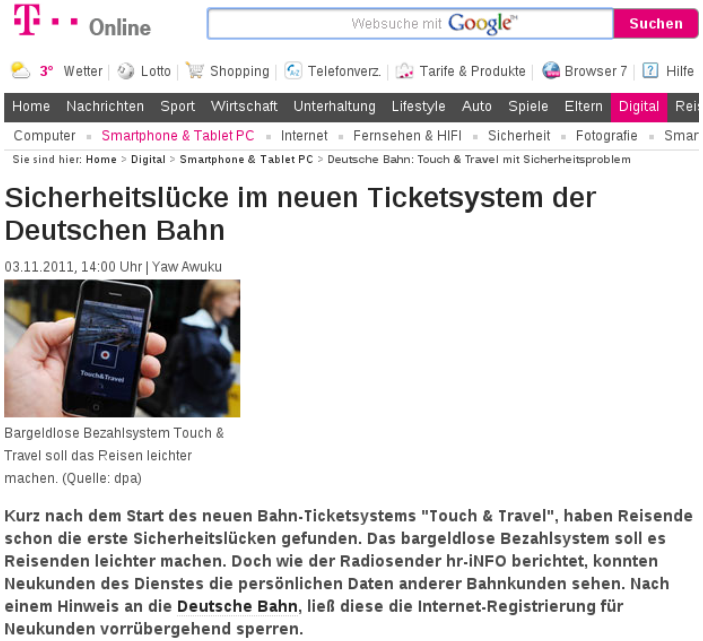
[Merkur-Online.de, 30. Januar 2009]

Ein typischer Arbeitsweg

Fahrkartenkauf:

- ★ Direkt beim Busfahrer
- ★ Fester Fahrkartenautomat an der Haltestelle
- ★ Smartphone-App
- ★ Elektronische Bezahlsysteme (SmartCard, RFID, NFC...)

Ein typischer Arbeitsweg



T-Online

Websuche mit Google — Suchen

3° Wetter | Lotto | Shopping | Telefonverz. | Tarife & Produkte | Browser 7 | Hilfe

Home Nachrichten Sport Wirtschaft Unterhaltung Lifestyle Auto Spiele Eltern Digital Rei

Computer ▪ Smartphone & Tablet PC ▪ Internet ▪ Fernsehen & HIFI ▪ Sicherheit ▪ Fotografie ▪ Smar

Sie sind hier: Home > Digital > Smartphone & Tablet PC > Deutsche Bahn: Touch & Travel mit Sicherheitsproblem

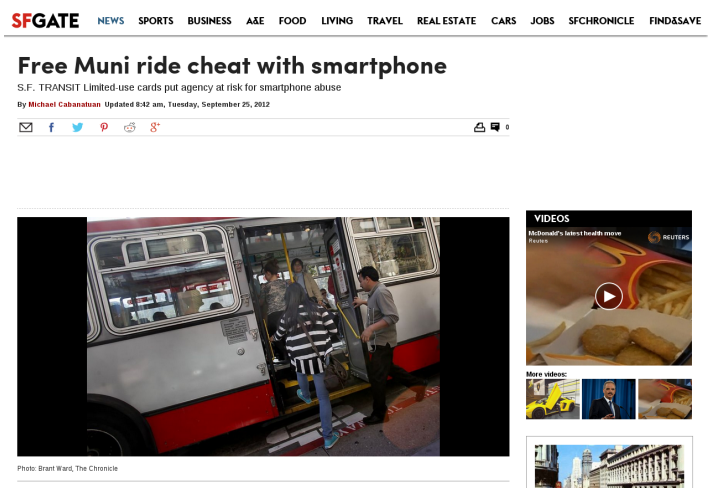
Sicherheitslücke im neuen Ticketsystem der Deutschen Bahn

03.11.2011, 14:00 Uhr | Yaw Awuku

Bargeldlose Bezahlsystem Touch & Travel soll das Reisen leichter machen. (Quelle: dpa)

Kurz nach dem Start des neuen Bahn-Ticketsystems "Touch & Travel", haben Reisende schon die erste Sicherheitslücken gefunden. Das bargeldlose Bezahlsystem soll es Reisenden leichter machen. Doch wie der Radiosender hr-iNFO berichtet, konnten Neukunden des Dienstes die persönlichen Daten anderer Bahnkunden sehen. Nach einem Hinweis an die Deutsche Bahn, ließ diese die Internet-Registrierung für Neukunden vorrübergehend sperren.

[T-Online.de, 3. November 2011]



SFGATE NEWS SPORTS BUSINESS A&E FOOD LIVING TRAVEL REAL ESTATE CARS JOBS SFCHRONICLE FIND&SAVE

Free Muni ride cheat with smartphone

S.F. TRANSIT Limited-use cards put agency at risk for smartphone abuse

By Michael Cabanatuan Updated 8:42 am, Tuesday, September 25, 2012

Photo: Brant Ward, The Chronicle

[SFGate.com, 25. September 2012]

Ein typischer Arbeitsweg

Im Bus:

- Aufkleber mit QR-Code animieren, die Smartphone-App herunterzuladen
- Busfahrer benutzt Bordinformationssystem:
  - Nächste Haltestellen
  - Verspätung
  - Fahrkartenkauf
  - Integrierte Kommunikation mit der Leitstelle (Analog-, Digitalfunk, GSM...)
  - ...

Ein typischer Arbeitsweg

14 1

24. April 2014 | 13.44 Uhr

Guerilla-Aktion vor Europawahl

QR-Code auf Wahlplakat führt zu Porno-Seite

Der Politiker Han ten Broeke twitterte dieses Bild von der Enthüllung der Wahlplakate. FOTO: Twitter / Han ten Broeke

Berlin. Eigentlich sollen sich Wähler, die sich für die Arbeit von Alexandra Thein interessieren, über den QR-Code auf ihrem Wahlplakat über die Arbeit der FDP-Politikerin informieren können. Doch Unbekannte haben die Bilder überklebt – und die Wähler landeten auf einer Porno-Seite.

[RP-Online.de, 24. April 2014]

[Great Scott Gadgets, 6. März 2015]

heise Security News Hintergrund Tools Foren

Security > News > 7-Tage-News > 2011 > KW 22 > TETRA-Digitalfunk für jedermann

01.06.2011 12:31 « Vorige | Nächste »

TETRA-Digitalfunk für jedermann

vorlesen / MP3-Download

Auf der letzten Ausgabe der Hacker-Konferenz PH-Neutral präsentierte der ausgezeichnete Open-Source-Hacker Harald Welte nicht nur die Grundlagen des Terrestrial Trunked Radio, kurz TETRA. Er zauberte auch Open Source Software aus dem Hut, mit der man den Digitalfunk empfangen, aufzeichnen und dekodieren kann.

Im Prinzip funktioniert TETRA sehr ähnlich wie der Mobilfunkstandard GSM für Handys; es unterscheidet sich allerdings dann doch so weit, dass man existierende Soft- und Hardware nicht sinnvoll wiederverwenden kann. TETRA soll in Europa eine gemeinsame Basis für den Digitalfunk von Feuerwehr, Rettungsdienst und Polizei aber auch für die Versorgung von Verkehrsflughäfen, Energieversorgungsunternehmen bis hin zu großen Verkehrsbetrieben werden.

[Heise.de, 1. Juni 2011]

Verkehrsbetriebs-IT: Probleme

Die Praxis zeigt: Auch Verkehrsbetriebe benutzen „normale“ IT

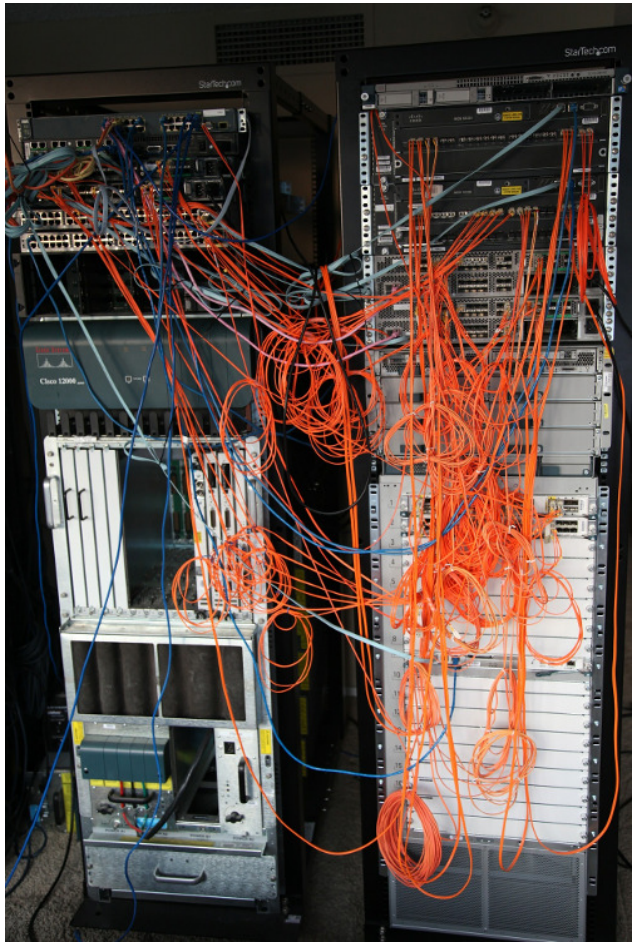
- ★ Windows-Domänen
- ★ Linux-Server
- ★ Standard-Soft- und Hardware
- ★ angepasste Software-Lösungen (oft Teile der RBL/ITCS)...

Aus Angreifersicht erstmal kein großer Unterschied zu IT-Systemen anderer Branchen

Verkehrsbetriebs-IT: Probleme

Ähnliche IT-Landschaft heißt leider auch ähnliche oder gleiche Probleme:

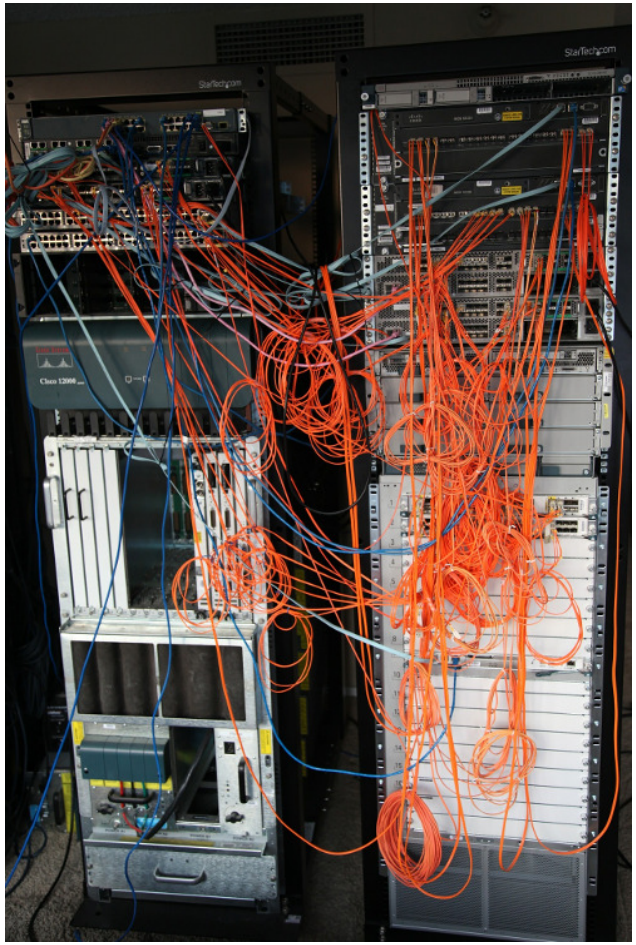
- ★ Mangelnde physische Sicherheit (z.B. einfacher Zugriff auf Schaltschränke oder Technikräume an Haltestellen)
- ★ Fehlende Separierung / nur Segmentierung von Netzen
- ★ Keine Updates, d.h. komplett veraltete Systeme mit bekannten Sicherheitslücken



Verkehrsbetriebs-IT: Probleme

Ähnliche IT-Landschaft heißt leider auch ähnliche oder gleiche Probleme:

- ★ Schwache Passwörter, Standardpasswörter
- ★ Fehlende Authentifizierung und/oder Autorisierung
- ★ Keine oder mangelhafte Verschlüsselung
- ★ Unnötige Dienste
- ★ ...



Verkehrsbetriebs-IT: Risiken

Risiken der Vernetzung bei Verkehrsbetrieben:

1. Personenschäden
2. Imageschäden
3. Finanzielle Schäden

Verkehrsbetriebs-IT: Risiken

Risiken der Vernetzung bei Verkehrsbetrieben:

1. Personenschäden
   - ★ Fernwirksysteme (z.B. Stromzufuhr von Bahngleisen, Weichenstellung...)
   - ★ (Vorrang-)Schaltungen für Ampelanlagen
   - ★ Funkgesteuerte versenkbare Poller
   - ★ Kommunikation mit der Leitstelle
2. Imageschäden
3. Finanzielle Schäden

Verkehrsbetriebs-IT: Risiken

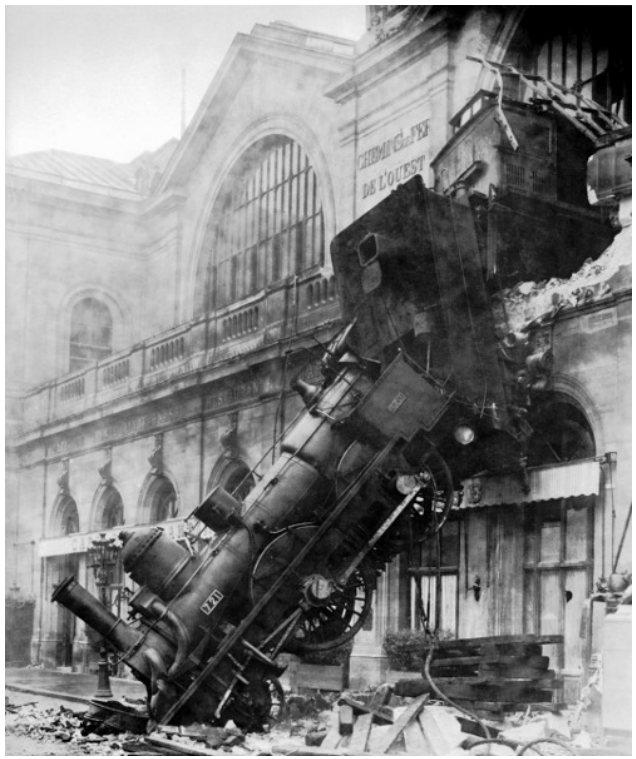
Risiken der Vernetzung bei Verkehrsbetrieben:

1. Personenschäden
2. Imageschäden
   - ★ falsche oder fehlende Fahrgastinformationen
   - ★ Unautorisierter Zugriff auf Überwachungskameras
3. Finanzielle Schäden

Verkehrsbetriebs-IT: Risiken

Risiken der Vernetzung bei Verkehrsbetrieben:

1. Personenschäden
2. Imageschäden
3. Finanzielle Schäden
   - ★ Ticketverkauf
   - ★ Ressourcenverschwendung
   - ★ Sachschäden

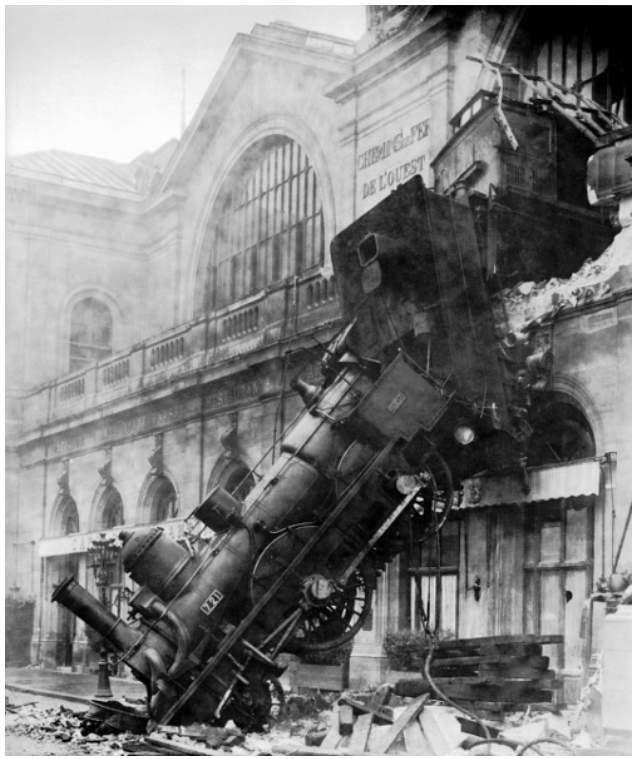


Verkehrsbetriebs-IT: Risiken

Risiken der Vernetzung bei Verkehrsbetrieben:

1. Personenschäden
2. Imageschäden
3. Finanzielle Schäden

⇒ Oft sind alle drei Kategorien betroffen.



Verkehrsbetriebs-IT: Lösungen

Verkehrsbetriebe sind längst IT-getrieben, müssen sich also dementsprechend verhalten:

- Dedizierte IT-Sicherheitsverantwortliche
- Sicherheitskonzept
  - Update-Management
  - Separierung von Netzen
  - Checkliste für Neuinstallationen
  - Regelmäßige Überprüfung der eigenen Maßnahmen
- Notfallplan („roter Ordner“)
  - Wer wird im Verdachtsfall informiert?
  - Welche Maßnahmen dürfen/müssen getroffen werden?

Die Zukunft

Schöne neue Welt?

[T-Systems Flyer, März 2011]

Die Zukunft

Schöne neue Welt?


heise Security News Hintergrund Tools Foren

Security > News > 7-Tage-News > 2014 > KW 31 > Elasticsearch-Lücke verwandelt Amazon-Cloud-Server in

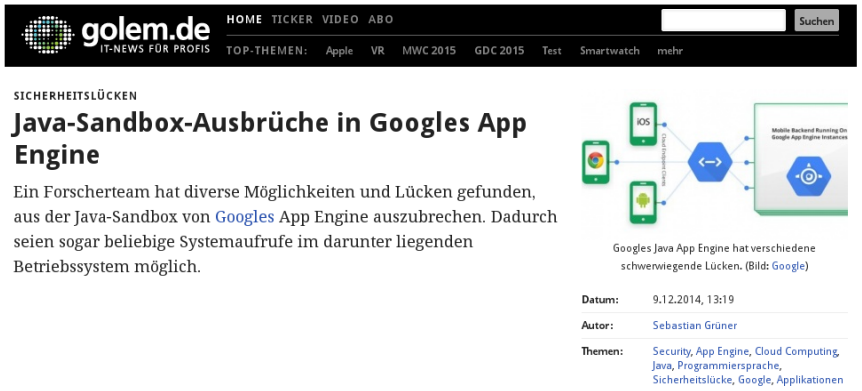
29.07.2014 16:59 « Vorige | Nächste »

Elasticsearch-Lücke verwandelt Amazon-Cloud-Server in DDoS-Zombies

vorlesen / MP3-Download

Durch eine Sicherheitslücke in einer älteren Elasticsearch-Version können Angreifer beliebigen Schadcode ausführen. Das wird momentan dazu genutzt, Server in Amazons EC2-Cloud zu kapern und für DDoS-Angriffe zu missbrauchen.

[Heise.de, 29. Juli 2014]


golem.de IT-NEWS FÜR PROFIS HOME TICKER VIDEO ABO Suchen

TOP-THEMEN: Apple VR MWC 2015 GDC 2015 Test Smartwatch mehr

SICHERHEITSLÜCKEN

Java-Sandbox-Ausbrüche in Googles App Engine

Ein Forscherteam hat diverse Möglichkeiten und Lücken gefunden, aus der Java-Sandbox von Googles App Engine auszubrechen. Dadurch seien sogar beliebige Systemaufrufe im darunter liegenden Betriebssystem möglich.

Googles Java App Engine hat verschiedene schwerwiegende Lücken. (Bild: Google)

Datum: 9.12.2014, 13:19

Autor: Sebastian Grüner

Themen: Security, App Engine, Cloud Computing, Java, Programmiersprache, Sicherheitslücke, Google, Applikationen

[Golem.de, 9. Dezember 2014]

Zeit für Ihre Fragen!

Vielen Dank für Ihre Aufmerksamkeit.

Quellenangaben

http://www.n24.de/n24/Nachrichten/Panorama/d/4764370/san-francisco-warnt-vor-godzilla-angriff.html

http://www.merkur-online.de/multimedia/zombies-schilder-64652.html

http://www.t-online.de/handy/smartphone/id_51154096/

http://www.sfgate.com/bayarea/article/Free-Muni-ride-cheat-with-smartphone-3891037.php

http://www.rp-online.de/politik/deutschland/qr-code-auf-wahlplakat-fuehrt-zu-porno-seite-aid-1.4195346

http://greatscottgadgets.com/hackrf/

http://heise.de/-1253092

http://www.t-systems.com/umn/uti/783186_1/blobBinary/Flyer_ITCS_Cloud-ps.pdf

http://heise.de/-2277689

http://www.golem.de/news/sicherheitsluecken-java-sandbox-ausbrueche-in-googles-app-engine-1412-111054.html