Tatjana Brozat

4. Kommunaler IT-Sicherheitskongress 2017

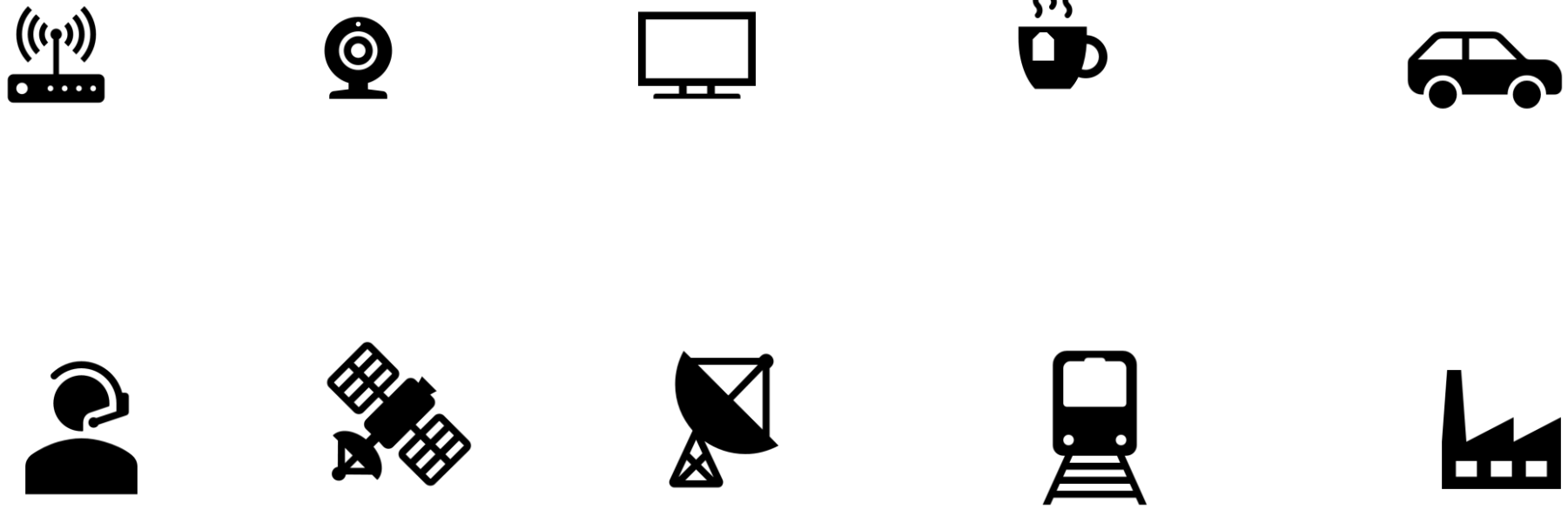
„Umsetzung der Leitlinie für Informationssicherheit des IT-Planungsrats in Kommunalverwaltungen“

„Internet der Dinge“
Gefährdungen in neuen Dimensionen

4. Kommunaler IT-Sicherheitskongress 2017

Themenkomplex

Bei ***IoT*** handelt es sich um vernetze Objekte mit eigener dezentraler Intelligenz. Sie tauschen Informationen aus und bewegen sich autonom in ihrer Umgebung.

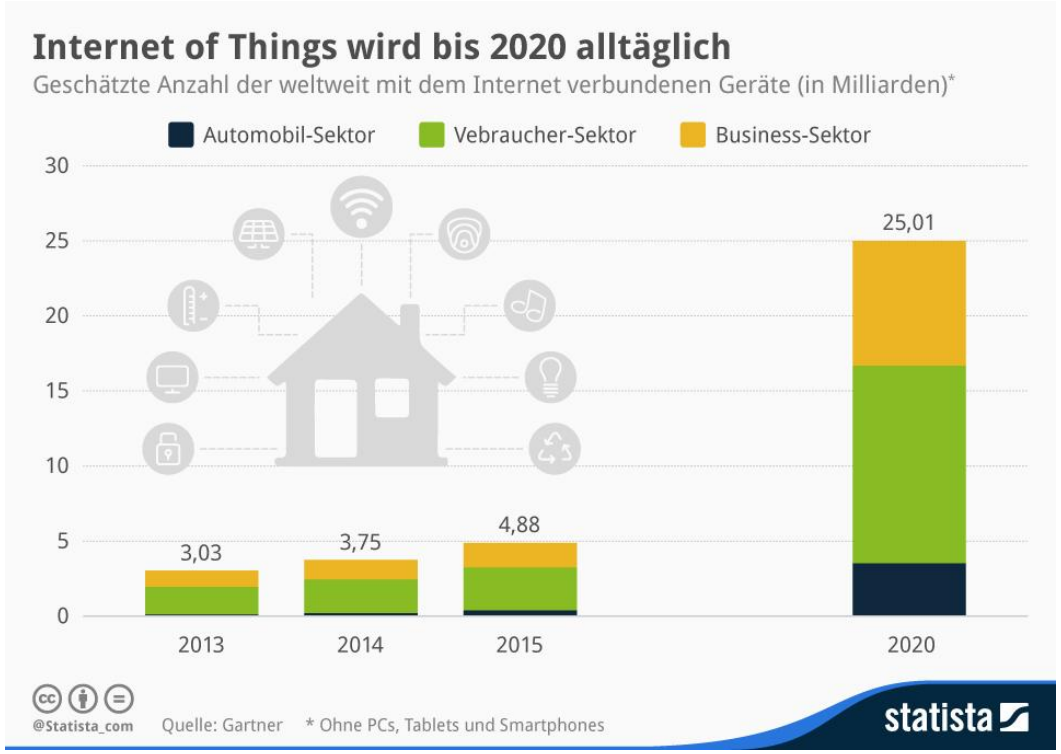


Internet der Dinge – Wachstum

Bereits heute befinden sich laut einer Studie ca. **8 Milliarden** IoT-Geräte in Betrieb

Die Unternehmensberatung Gartner geht in einer Studie davon aus, dass bis 2020 etwa 26 Milliarden Objekte im Internet der Dinge vernetzt sein werden.
http://www.gartner.com/newsroom/id/3598917

Das Marktforschungs- und Beratungsunternehmen International Data Corporation (IDC) schätzt, dass 2020 etwa 32 Milliarden Objekte mit dem Internet verbunden sein und diese dann zehn Prozent der weltweiten Daten produzieren werden.
http://www.idc.com/getdoc.jsp?containerId=prUS42209117



Quelle der Grafik - https://de.statista.com/infografik/2937/mit-dem-internet-of-things-verbundenen-geraete/

Chancen und Risiken der Digitalisierung

Smartphone, Auto, Kühlschrank oder Fitnessband

Intelligente Helfer sind bereits heute für Millionen Nutzer alltäglich und praktisch. Die allumfassende Vernetzung der Geräte birgt jedoch auch Risiken!

Geschirrspüler lässt sich über Web angreifen

IoT BrickerBot geht soweit anfällige Geräte unbrauchbar zu machen.

IoT-Wurm Hajime kapert 300.000 Geräte

Smart-TVs offenbar mit Ransomware infiziert

Kaffeemaschinen werden zu Zombies

Ein DDoS-Angriff (Distributed Denial of Service) auf die von der Infrastruktur-Firma Dyn verwaltete DNS-Infrastruktur legte am Freitag unzählige Internet-Dienste lahm

Ursache

Digitalisierung mit Sicherheitslücken und Schwachstellen:

- **technische Dokumente sind auf öffentlich zugänglichen Webservern verfügbar**
- **ungepatchte und veraltete Softwarekomponenten**
- **unsichere Web Interfaces**
- **leicht zugängliche Firmware**

- **fehlerhafte Credentials – sofern gefordert**
- **ungenügende Authentifizierungsmethoden – sofern vorhanden**
- **ungeeignete Transportverschlüsselung – sofern implementiert**
- **Zertifikate werden über alle Produktinstanzen wiederverwendet – sofern PKI vorhanden**
- …

Angriffsvektoren und Techniken

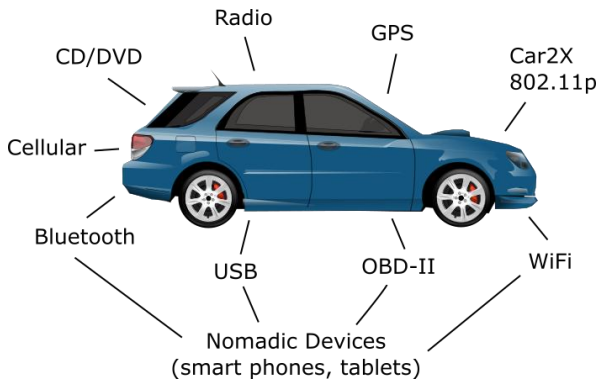
- Februar 2017
  - Die neueste Entwicklung bei Metasploit ermöglicht über eine Hardware-Bridge-API Zugriff auf die physische Welt um Zugriff auf eingebettete Hardware wie den CAN-Bus industrieller Steuerungssysteme zu bekommen.

- Wie funktioniert die Hardware-Bridge-API?
  - Anstatt auf Ethernet zuzugreifen, nutzt die Hardware-Bridge-API eine Kombination aus drahtloser Kommunikation und direkter Hardware-Manipulation.

Problemstellungen

- Die Entitäten kommunizieren über unterschiedliche Schnittstellen und Protokolle
  - dabei kann ein Objekt unter Umständen mehrere Schnittstellen besitzen und mehrere Kommunikationskanäle nutzen
- Kryptografische Verfahren kommen nur selten zum Einsatz
  - welche Verfahren kommen zum Einsatz?
- Die Identität einer Entität ist meist nicht nachweis- oder verifizierbar
  - wer verifiziert eine Identität, wer ist die Vertrauensstellung?

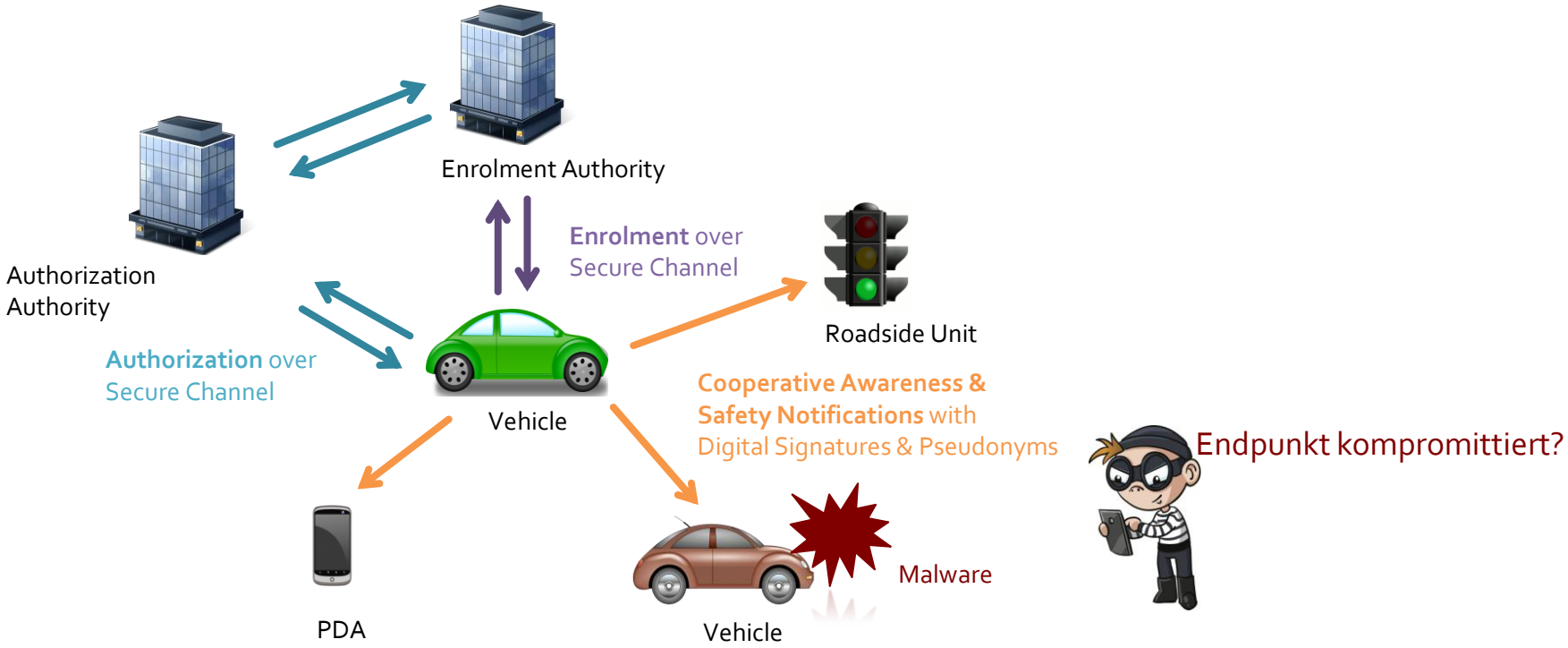
Beispiel Kommunikationssysteme



Subbus	Ereignisgesteuert	Zeitgesteuert	Multimedia	Drahtlos
• LIN • K-Line • I2C	• CAN • VAN • PLC	• FlexRay • TTP • TTCAN	• MOST • D2B • GigaStar	• Bluetooth • GSM • WLAN

Beispiel von Kommunikations- und Bussystemen in Fahrzeugen

Endpunktsicherheit?



Mit freundlicher Untersützung von Frau Dr. Sybille Fröschle
Project: Interdisciplinary Research Center on Critical Systems Engineering for Socio-Technical Systems (CSE)

Sektor Transport & Verkehr

Das Bundesamt für Sicherheit in der Informationstechnik hat **26 Angriffsziele im maritimen Transportwesen** identifiziert:

- Kranelektrik
- Nautische Entscheidungsunterstützung
- Steuerung für Bugstrahlruder
- Schiffdatenschreiber
- …

Transport und Verkehr

Luftfahrt	Schifffahrt	Schienenverkehr	Straßenverkehr
•Flughafenbetrieb •Personen- und Frachtflugbetrieb •Luftfahrtkontroll- und Sicherheitsbetrieb	•Hafen- und Wasserstraßenbetrieb •Personen- und Frachtschifffahrtsbetrieb •Schifffahrtskontroll- und Sicherheitsbetrieb	•Schienennetzbetrieb, Bahnhofsbetrieb •Personen- und Frachtschienenbetrieb •Schienenverkehrsbetrieb	•Straßenbetrieb •Personen- und Lastkraftfahrzeugbetrieb •Straßenverkehrskontroll- und Sicherheitsbetrieb

Risiken begrenzen

- Risiken für die Institution nachhaltig begrenzen mit dem Ziel der Schadensvermeidung bzw. –minimierung.

Wie können vernetzte und autonome Systeme sicher entwickelt und betrieben werden?

Durch geeignete Planung und Evaluation der Sicherheitsziele

Vertraulichkeit
[confidentiality]

Zugriff auf Informationen
nur durch Berechtigte

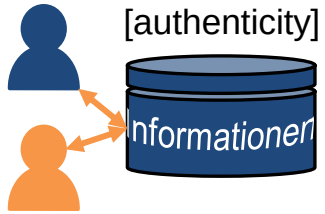
Verfügbarkeit
[availability]

Zugriff auf Informationen
im vereinbarten Rahmen

Integrität
[integrity]

Richtigkeit,
Vollständigkeit von
Informationen

Authentizität
[authenticity]



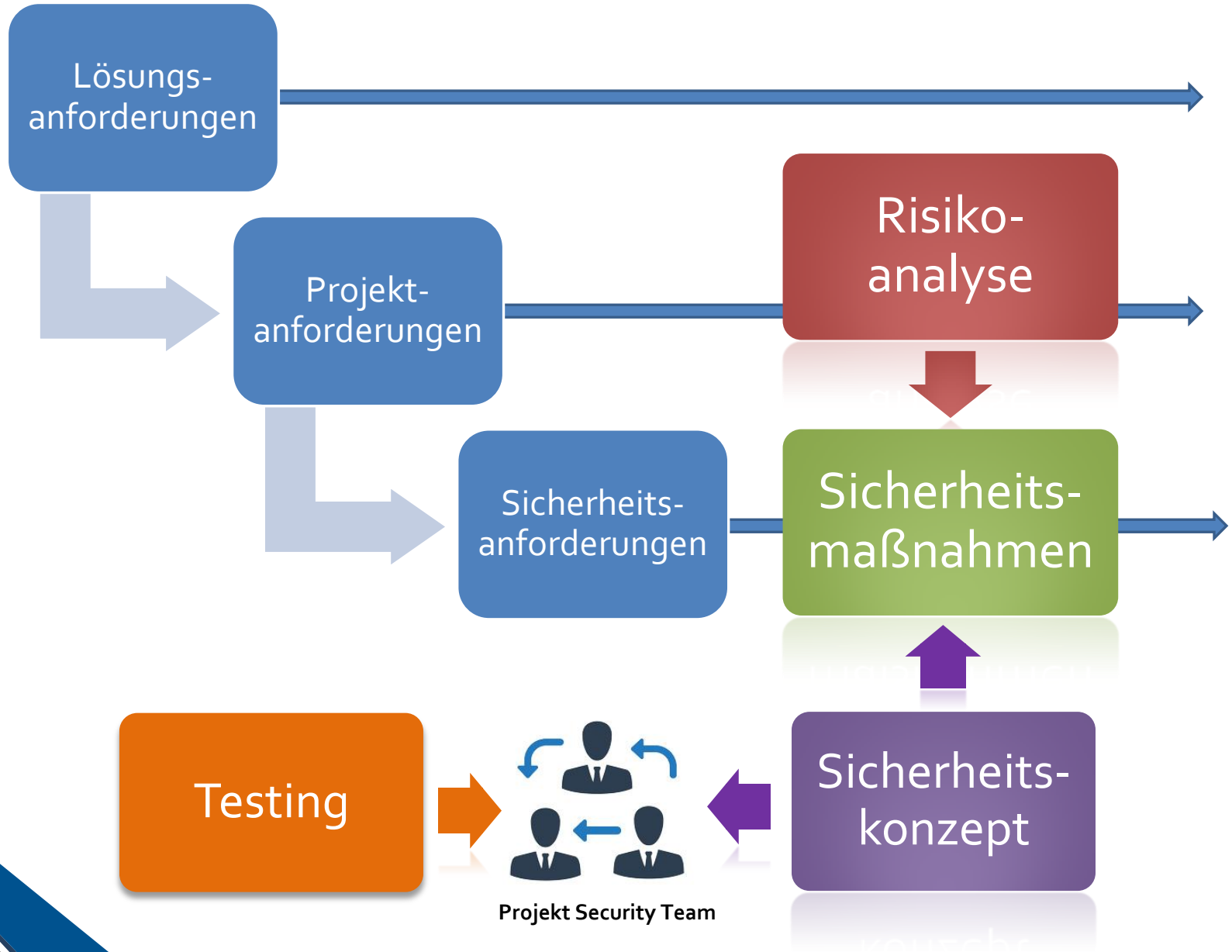
Echtheit, Zuverlässigkeit
und Glaubwürdigkeit

Empfehlungen des BSI

Im Zuge des Angriffs auf den Dyn Dienstleister im Oktober 2016 hat das BSI in einer Pressemeldung folgende Sicherheitsempfehlungen für **Hersteller** benannt:

- Voreingestellte Zugangsdaten und Passwörter für alle Zugriffsmöglichkeiten auf die Geräte, zum Beispiel via HTTP, TELNET oder SSH, müssen durch den Nutzer geändert werden können.
- Sind die voreingestellten Passwörter nicht für jedes Gerät individualisiert, so ist bei der Inbetriebnahme ein Passwortwechsel zu erzwingen.
- Nicht zwingend benötigte Dienste müssen durch den Benutzer deaktiviert werden können.
- Die eingehende und ausgehende Kommunikation des IoT-Geräts sollte nur mittels kryptografisch geschützter Protokolle wie TLS erfolgen.
- Ein IoT-Gerät sollte nicht automatisiert über Universal Plug and Play (UPnP) eine unsichere Konfiguration im Router herstellen, etwa Verbindungen zu unsicheren Diensten erlauben.
- Hersteller müssen regelmäßig, schnell und über einen hinreichenden Nutzungszeitraum hinweg Sicherheitsupdates für die Geräte zur Verfügung stellen. Die Übertragung und Installation sollte dabei mittels kryptografischer Verfahren geschützt werden.
- Die Firmware des IoT-Geräts ist hinreichend zu härten, um beispielsweise das unkontrollierte Nachladen von Inhalten aus dem Internet zu verhindern.

Anforderungsspezifikation bei der Produktentwicklung



Fachabteilung

- Definition der Lösungsanforderungen und Priorisierung der Risiken

Projektteam

- Definition der Projektanforderungen und Priorisierung der Risiken

Security Management

- Definition der Sicherheitsanforderungen und Freigabe

Empfehlungen für die öffentliche Verwaltung

Sensibilisierung aller beteiligten Parteien

- Aufbau von Security Incident Event Monitoring und Intrusion Detection Systemen
- Planung und Durchführung von Penetrationstest an Netzübergängen
- Spezifikation von Sicherheitsanforderungen bei Ausschreibungen
- Regelungen für die Genehmigung und Freigabe innerhalb der Einrichtung

Tatjana Brozat

x-net training & solutions

Ritterlandweg 18 in 13409 Berlin

brozat@x-net-solutions.de

https://www.x-net-solutions.de

Telefon: +49 | (0)30 | 740 72 682

Berater und Auditor für Informationssicherheit und IT-Sicherheit

Schwerpunkte

BSI IT-Grundschutz & ISO 27k

Risikomanagement, kryptografische Verfahren, Network Security