Datenschutz im Internet der Dinge

Risiken und Regulierungen

Michael Wittchen
Konrad Miosga

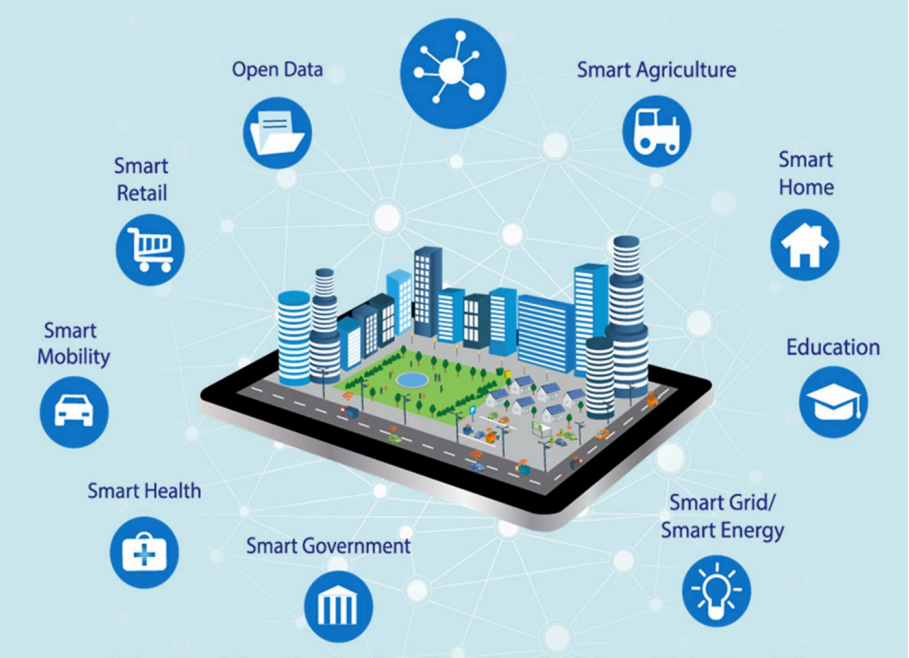
Hochschule Zittau/Görlitz

Agenda

- Einführung: Was ist das Internet der Dinge (IoT)?
- Was ist alles im IoT versteckt?
- Sicherheit & Datenschutz, Schwachstellen und Angriffspunkte
- Best Practices zur Absicherung von IoT-Systemen
- Regulierung und rechtliche Grundlagen
- Fallstudie: Sicherheitsvorfälle durch unzureichend gesicherte Geräte
- Vorstellung spezieller IoT-Suchmaschinen
- Fazit & Ausblick
- Quellen & Weiterführende Informationen

Einführung: Was ist das Internet der Dinge (IoT)?

- Vernetzung physischer Geräte über das Internet
- Geräte kommunizieren und tauschen Daten autonom aus
- Ziel: Komfort, Effizienz, Automatisierung



Zentrale Eigenschaft: Jedes Gerät ist ein „Mini-Computer“ – mit Datenzugang, Speicher und Netzwerkverbindung.

Beispiele für IoT-Geräte?

- Smarthome:
  - Automatisierte Rollläden, Heizung, Türsteuerung
  - Sprachassistenten, Smart-TVs, Kühlschränke
- Wearables & Smart Toys:
  - Sammeln Gesundheits- und Bewegungsdaten
- Smart City:
  - Sensoren zur Verkehrssteuerung, Straßenbeleuchtung
  - Öffentliche WLAN-Hotspots, Überwachungskameras
- Industrie 4.0:
  - Vernetzte Maschinen, Produktionsüberwachung

Typische Schwachstellen und Angriffspunkte

- Große Datenmengen → hohe Angriffsfläche
- Fehlende oder schwache Verschlüsselung
- Standardpasswörter & ungesicherte Authentifizierung → Botnetze (z. B. Mirai)
- Physischer Zugriff → Manipulation
- Keine Netzwerksegmentierung → Schadsoftware breitet sich im Heimnetz aus
- Cloud-Abhängigkeit – Daten oft außerhalb der EU
- Fehlende Updates und veraltete Firmware → offene Sicherheitslücken

Folge: Geräte können übernommen, Daten ausgespäht oder Netzwerke kompromittiert werden.

Best Practices zur Absicherung von IoT-Systemen

Vor dem Kauf prüfen:
- Hersteller bietet regelmäßige Sicherheitsupdates
- Unterstützt verschlüsselte Kommunikation (TLS)

Einrichtung:
- Standardpasswörter ändern
- Starke, individuelle Passwörter verwenden
- Zwei-Faktor-Authentisierung aktivieren

Betrieb:
- Automatische Updates aktivieren
- Geräte in separatem WLAN betreiben
- UPnP deaktivieren, Firewall aktivieren
- Nur notwendige Internetverbindungen zulassen

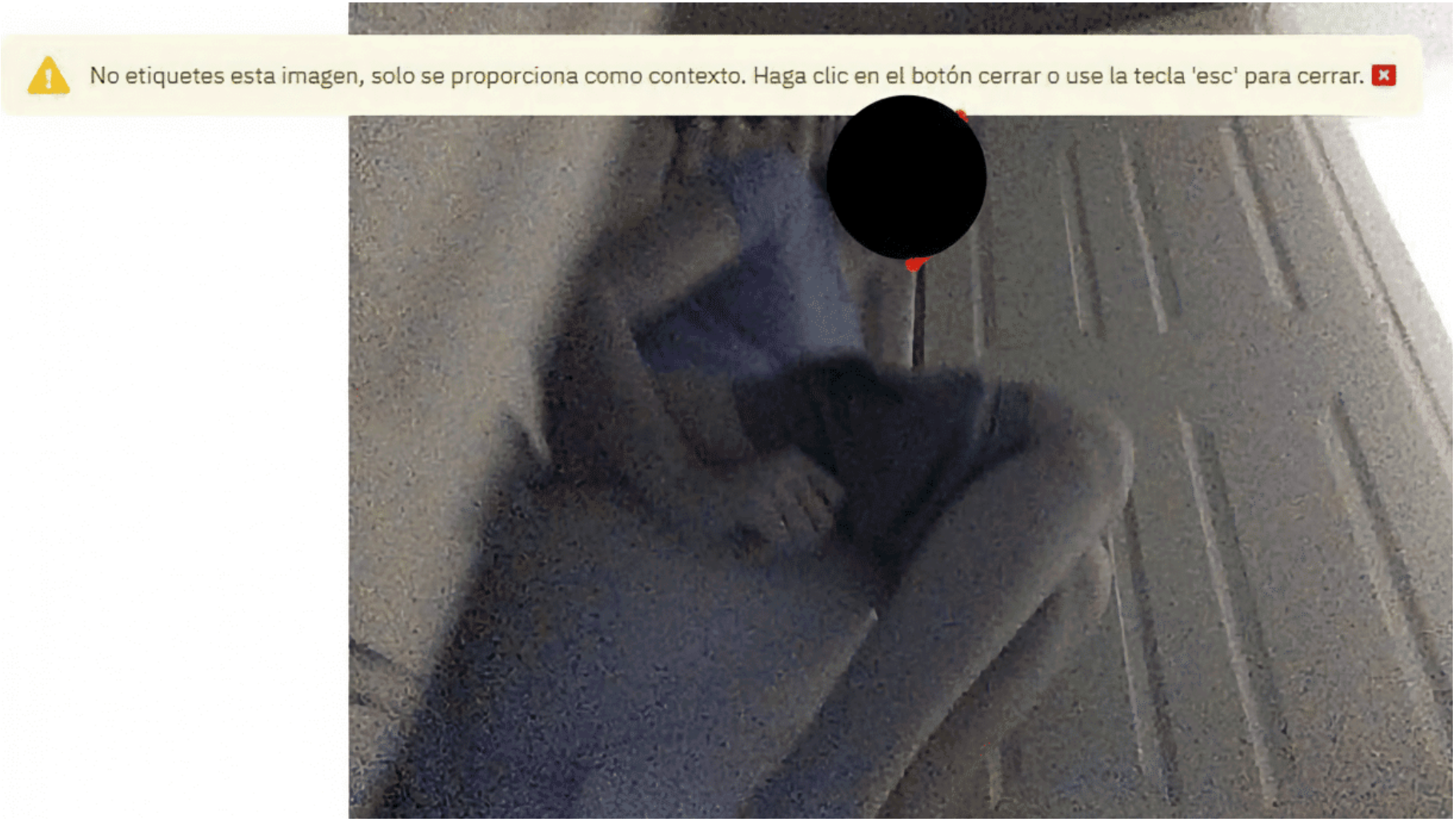
Regulierung und rechtliche Grundlagen

- **DSGVO (Datenschutz-Grundverordnung):**
  - Datenschutz durch Technikgestaltung („Privacy by Design“)
  - Rechte auf Auskunft, Löschung, Datenübertragbarkeit
- **Cyber Resilience Act (EU):**
  - Verpflichtung zu Sicherheitsstandards und Updatepflicht
- **BSI (Bundesamt für Sicherheit in der Informationstechnik):**
  - Kampagne „Einfach • Cybersicher“
  - Empfehlungen für Verbraucher & Unternehmen

Fallstudie: Datenschutzrisiken bei smarten Staubsaugern (Roomba)

- **Vorfall (2022):**
  - Testgeräte von Roomba machten Fotos während der Reinigung
  - Bilder wurden an externe Datenannotationsfirmen weitergeleitet
  - Einige Aufnahmen (u. a. von Personen in privaten Räumen) landeten über Subunternehmer in sozialen Medien (z. B. Facebook)
- **Ursache:**
  - Verwendung von Geräten in Beta-Programmen mit erweiterten Datenerfassungsrechten
  - Fehlende Kontrolle über Weitergabe durch Drittanbieter
- **Lehre:**
  - Smarte Geräte können unerwartet sensible Daten sammeln
  - Datenschutzprüfungen und Rechteverwaltung sind entscheidend vor Nutzung oder Testteilnahme

Roomba Datenschutzvorfall



[1]

Mirai-Botnet


THE WALL STREET JOURNAL.

Cyberattack Knocks Out Access to Websites

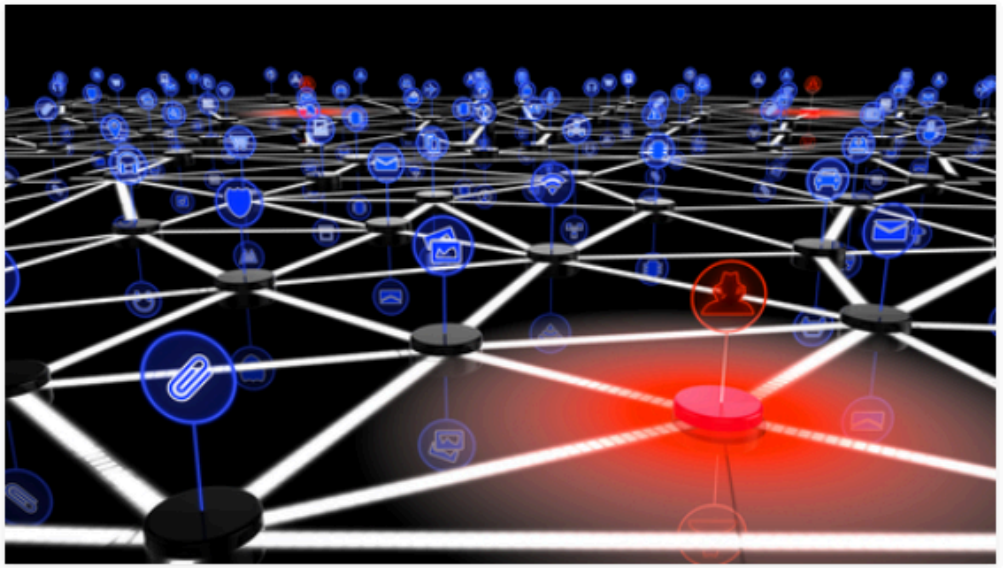
[2]

Mirai-Botnet

KrebsOnSecurity Hit With Record DDoS

September 21, 2016 122 Comments

On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not succeed thanks to the hard work of the engineers at **Akamai**, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever witnessed.



[3]

Mirai-Botnet

DDoS on Dyn Impacts Twitter, Spotify, Reddit

October 21, 2016 175 Comments

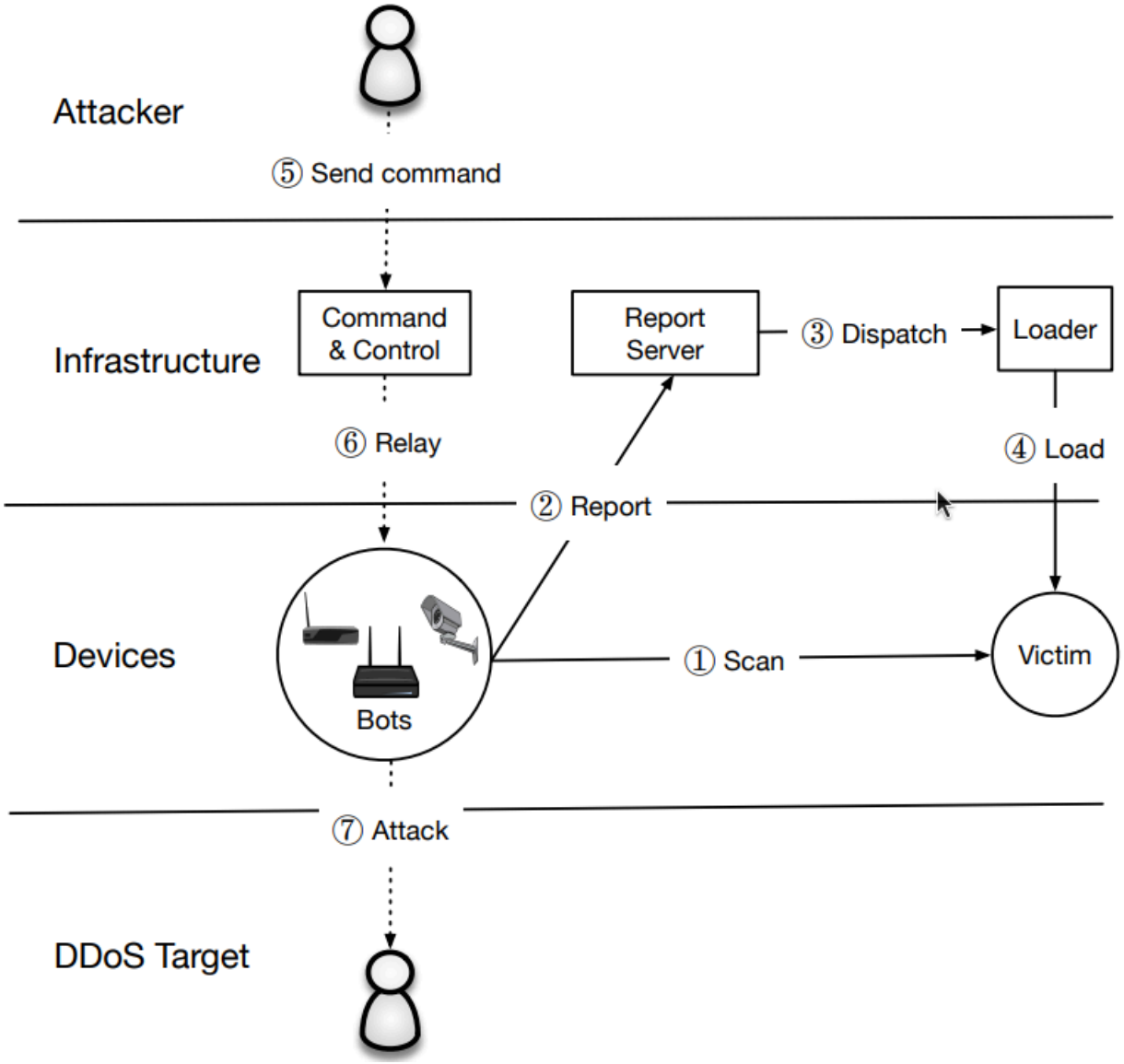
Criminals this morning massively attacked Dyn, a company that provides core Internet services for Twitter, SoundCloud, Spotify, Reddit and a host of other sites, causing outages and slowness for many of Dyn's customers.

Twitter is experiencing problems, as seen through the social media platform Hootsuite.

In a statement, Dyn said that this morning, October 21, Dyn received a global **distributed denial of service** (DDoS) attack on its DNS infrastructure on the east coast starting at around 7:10 a.m. ET (11:10 UTC).

[4]

Mirai-Botnet



[2]

Mirai-Botnet

Krebs on Security

- Am 20. September 2016 wurde die Webseite von Krebs on Security massiv angegriffen
- Der Angriff erreichte Spitzenwerte von etwa 620 Gbps
- Laut den Forschern von F5 Labs und anderen waren mehrere hunderttausend IoT-Geräte beteiligt, vermutlich mit Standard-Zugangsdaten und offenen Telnet-/SSH-Ports.

Mirai-Botnet

OHV (französischer Hosting- und Cloudprovider)

- Kurz nach dem Krebs-Angriff (Ende September 2016) wurde der französische Hosting- und Cloud-Provider OVH Opfer eines massiven DDoS-Angriffs mit Beteiligung des Mirai-Botnetzes.
- In Berichten wird von über 1 Tbps (oder deutlich näher an 1.5 Tbps) Schadtraffic gesprochen, ausgeführt von über 145.607 IoT-Geräten laut OVH CTO.
- Ursprüngliches Ziel war offenbar ein Minecraft-Gaming-Server, der bei OVH gehostet war – die Attacke traf dann aber das Hosting-Netz von OVH sehr breit.

Mirai-Botnet

Dyn

- Am 21. Oktober 2016 wurde der US-DNS Provider Dyn (die Infrastruktur vieler großer Websites bereitstellt) durch massiven DDoS in mehreren Wellen angegriffen.
- Laut Dyn wurden mehrere Millionen IP-Adressen beobachtet, die beteiligt waren.
- Der Angriffsverkehr war an manchen Stellen gemeldet mit Spitzenwerten im Bereich von hunderten Gbps bis über 1 Tbps (je nach Schätzung).
- Der Angriff führte dazu, dass populäre Websites wie Twitter, GitHub, Netflix, Reddit, Airbnb und viele andere beeinträchtigt wurden.

Vorstellung spezieller IoT-Suchmaschinen

- **Shodan.io:**
  - Suchmaschine für mit dem Internet verbundene Geräte
  - Zeigt öffentlich erreichbare IoT-Geräte (z. B. Kameras)
- **Censys.io:**
  - Scannt Geräte weltweit nach offenen Ports und Zertifikaten

Nützlich für Sicherheitsforschung, aber Risiko bei ungesicherten Geräten!

Fazit & Ausblick

- IoT bringt Komfort, Effizienz und neue Geschäftsmodelle
- Datenschutz & Sicherheit bleiben zentrale Herausforderungen
- Gemeinsame Verantwortung von Nutzern, Herstellern & Gesetzgebern

Zukunft:

- Mehr Regulierung & sichere Standards
- KI-basierte Überwachung von Netzwerken
- Bewusster Umgang der Verbraucher mit IoT-Geräten

Weiterführende Informationen

- BSI (https://www.bsi.bund.de)
- EU Cyber Resilience Act
- Shodan.io / Censys.io
- Newsletter „Einfach • Cybersicher“
- Fachliteratur zu IoT-Security & Datenschutzrecht

Quellen

[1] E. Guo, “Roomba: Wie private Fotos eines Staubsauger-Roboters auf Facebook landen können.” [Online]. Available: https://www.heise.de/hintergrund/Roomba-Wie-private-Fotos-eines-Staubsauger-Roboters-auf-Facebook-landen-koennen-7457283.html

[2] M. Antonakakis *et al.*, “Understanding the Mirai Botnet,” in *26th USENIX Security Symposium (USENIX Security 17)*, Vancouver, BC: USENIX Association, Aug. 2017, pp. 1093–1110. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[3] B. Krebs, “KrebsOnSecurity Hit With Record DDoS.” [Online]. Available: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

[4] B. Krebs, “DDoS on Dyn Impacts Twitter, Spotify, Reddit.” [Online]. Available: https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/


KNURR
Wir wissen jetzt, wie die Schadsoftware in unsere Fabrik gelangt ist. Das Einfallstor war diese smarte Kaffeemaschine.
CLOUD-SCIENCE.DE