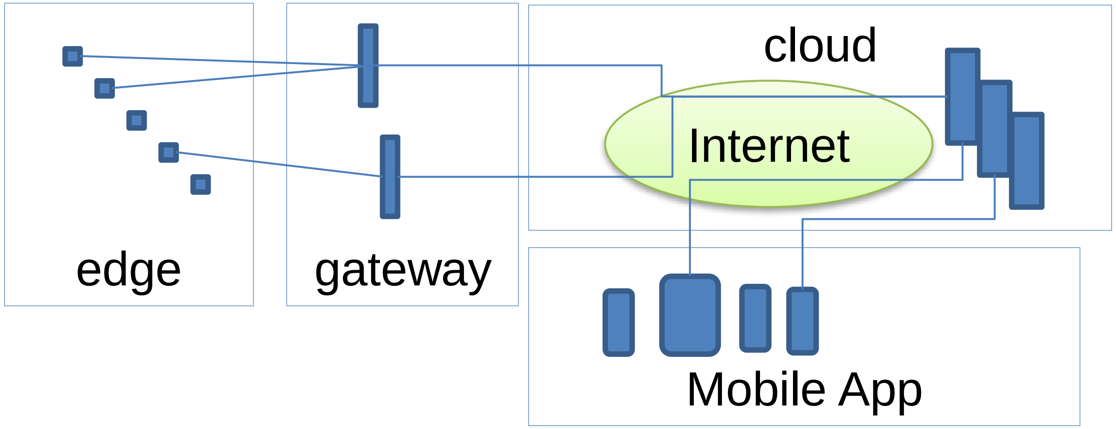
Die Dinge im Internet

IOT Security

Die OWASP-Sicht



- The **edge** code that runs on actual **IoT devices**. Often times edge components are resource constrained or operate in isolated environments.
- A **gateway** device is often used to aggregate and bridge communications from edge devices.
- The edge, or gateway, will often communicate with some sort of **cloud component**, often a web service. This component could be deployed in a company data center or a public cloud computing environment. The cloud component often supports complex user interfaces, analytics capabilities, and provide access to data aggregation back ends.
- Finally, many IoT ecosystems consist of **mobile application** components that allow users to interact with the ecosystem via smart phones or tablets.

https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

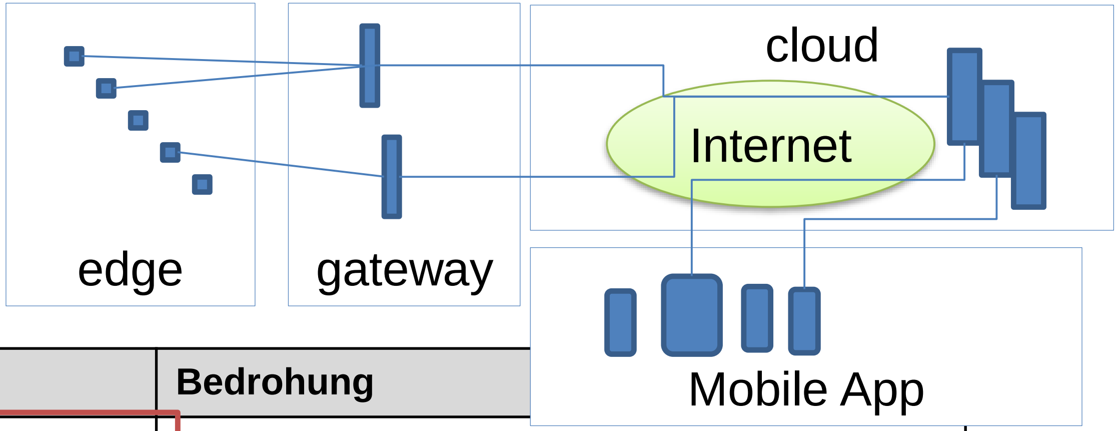
OWASP IoT Top Ten

Category	IoT Security Consideration	Recommendations
I1: Insecure Web Interface	Ensure that any web interface coding is written to prevent the use of weak passwords …	When building a web interface consider implementing lessons learned from web application security. Employ a framework that utilizes security …
I2: Insufficient Authentication/Authorization	Ensure that applications are written to require strong passwords where authentication is needed …	Refer to the OWASP Authentication Cheat Sheet
I3: Insecure Network Services	Ensure applications that use network services don't respond poorly to buffer overflow, fuzzing …	Try to utilize tested, proven, networking stacks and interfaces that handle exceptions gracefully...
I4: Lack of Transport Encryption	Ensure all applications are written to make use of encrypted communication between devices…	Utilize encrypted protocols wherever possible to protect all data in transit…
I5: Privacy Concerns	Ensure only the minimal amount of personal information is collected from consumers …	Data can present unintended privacy concerns when aggregated…
I6: Insecure Cloud Interface	Ensure all cloud interfaces are reviewed for security vulnerabilities (e.g. API interfaces and cloud-based web interfaces) …	Cloud security presents unique security considerations, as well as countermeasures. Be sure to consult your cloud provider about options for security mechanisms…
I7: Insecure Mobile Interface	Ensure that any mobile application coding is written to disallows weak passwords …	Mobile interfaces to IoT ecosystems require targeted security. Consult the OWASP Mobile …
I8: Insufficient Security Configurability	Ensure applications are written to include password security options (e.g. Enabling 20 character passwords or enabling two-factor authentication)…	Security can be a value proposition. Design should take into consideration a sliding scale of security requirements…
I9: Insecure Software/Firmware	Ensure all applications are written to include update capability and can be updated quickly …	Many IoT deployments are either brownfield and/or have an extremely long deployment cycle...
I10: Poor Physical Security	Ensure applications are written to utilize a minimal number of physical external ports (e.g. USB ports) on the device…	Plan on having IoT edge devices fall into malicious hands...

Andere Sichten

Gartner: IoT security is all about physical safety and data handling

Angriffsvektoren (cnlab)



Komponente	Zielobjekt	Bedrohung
Edge & Gateways	Daten	Vertraulichkeit
	Funktionen	Einfluss auf «Dinge»
	Credentials	Daten-Integrität
Link Edge→Gateway	Daten	Vertraulichkeit
	Funktionen	
Link Gateway→Cloud	Daten	
	Funktionen	Einfluss auf «Dinge»
Cloud	Daten	Vertraulichkeit
	Funktionen	Einfluss auf «Dinge»
Mobile App	Daten	Vertraulichkeit
	Funktionen	Einfluss auf «Dinge»
	Credentials	Vertraulichkeit, Einfluss auf «Dinge», Integrität

Links

Organisationen

- https://iotsecurityfoundation.org/
- https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
- http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/

Mobile Hersteller

- http://www.apple.com/ios/homekit/
- https://cloud.google.com/solutions/iot/
- https://developers.google.com/brillo/

Nun zum «Rundgang»

Change-38
Peter Reiser / Robert Bühler

myBeer
Rainer Stocker

Android-Geräte
Stephan Verbücheln

iOS-Geräte
Thomas Lüthi

Danke

Paul Schöbi
paul.schoebi@cnlab.ch
+41 55 214 33 33