**Sicherheit im IoT**

# Schutz vor den wachsenden Cyber-Bedrohungen



INSIDE M2M
SMART MACHINES

Das Internet der Dinge (IoT) verändert die Art und Weise, wie wir leben und arbeiten, grundlegend. Unternehmen aller Branchen nutzen die Möglichkeiten vernetzter Geräte, um Prozesse zu optimieren, die Effizienz zu steigern und innovative Geschäftsmodelle zu realisieren. Diese neue Ära der Vernetzung bringt jedoch auch neue Herausforderungen mit sich – insbesondere im Bereich der Cybersicherheit.

Mit der steigenden Anzahl von IoT-Geräten wächst die Angriffsfläche für Cyberkriminelle exponentiell. Klassische Sicherheitslösungen, die auf den Schutz traditioneller IT-Infrastrukturen ausgerichtet sind, reichen oft nicht aus, um den komplexen Anforderungen der IoT-Welt gerecht zu werden. Die Folgen eines erfolgreichen Cyberangriffs können verheerend sein: Datenverlust, Betriebsunterbrechungen, finanzielle Schäden und Reputationseinbußen.

ANGRIFFSZENARIEN

**Man-in-the-Middle Attack**
**DDoS Attack**
**Device Cloning**
**Malware Infection**
**Insecure Default Config**
**Social Engineering**

...

DIE LISTE IST LANG. SCHUTZ IST WICHTIG.

# REALE GEFAHREN, KONKRETE BEISPIELE

Die Bedrohung durch Cyberangriffe ist real und betrifft Unternehmen jeder Größe. Es geht nicht mehr darum, ob, sondern wann ein Unternehmen zum Ziel eines Angriffs wird. Im Folgenden beleuchten wir die häufigsten Angriffsszenarien im IoT-Umfeld und zeigen anhand von Realbeispielen auf, welche dramatischen Konsequenzen ein Sicherheitsvorfall haben kann:

**Man-in-the-Middle-Angriffe**

**Szenario:** Ein Man-in-the-Middle-Angriff tritt auf, wenn ein Angreifer heimlich die Kommunikation zwischen zwei Parteien abfängt und möglicherweise manipuliert. IoT-Geräte, die unsichere oder unverschlüsselte Verbindungen verwenden, sind besonders anfällig für diese Art von Angriffen.

**Beispiel:** Im Jahr 2014 gelang es Hackern, die Kontrolle über das Steuerungssystem eines Hochofens in einem deutschen Stahlwerk zu übernehmen. Die Folge waren massive Schäden an der Anlage.

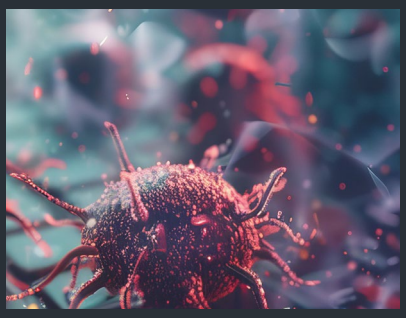
**Konsequenzen:** Diese perfide Angriffsmethode zielt auf die Kommunikation zwischen IoT-Geräten und Servern ab. Der Angreifer schaltet sich zwischen die beiden Kommunikationspartner und kann so unbemerkt Daten abfangen, manipulieren oder sogar die Kontrolle über die Geräte übernehmen.

**Geräte klonen**

**Szenario:** Cyberkriminelle können die Identität von legitimen IoT-Geräten klonen, um sich Zugang zu Netzwerken zu verschaffen und dort unerkannt Daten zu stehlen oder Manipulationen vorzunehmen.

**Beispiel:** 2020 wurde eine Schwachstelle im RFID-basierten Zugangskontrollsystem von HID Global, einem führenden Anbieter von Zugangskontrolllösungen, entdeckt. Sicherheitsforscher zeigten, dass Angreifer mit leicht verfügbarer Hardware RFID-Karten von HID Global abfangen und klonen konnten. Diese geklonten Karten wurden verwendet, um unbefugten Zugang zu Hochsicherheitsbereichen im Heathrow-Flughafen in London zu erlangen, was erhebliche Sicherheitsbedenken auslöste.

**Konsequenzen:** Unbefugter Zugang zu sensiblen Bereichen, Diebstahl von vertraulichen Informationen, Sabotage kritischer Infrastruktur.

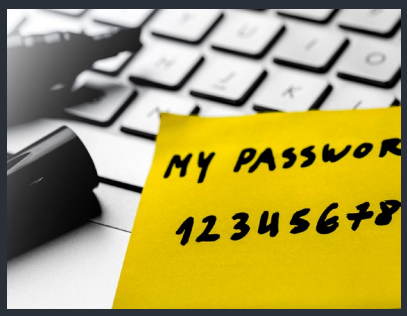


**Malware-Infektionen**

**Szenario:** IoT-Geräte sind anfällig für Malware-Infektionen, die über Sicherheitslücken in der Software oder durch unsichere Benutzerpraktiken eingeschleust werden. Die Schadsoftware kann sensible Daten stehlen, die Funktionalität des Geräts beeinträchtigen oder es sogar als Einfallstor für weitere Angriffe auf Ihr Unternehmensnetzwerk nutzen.

**Beispiel:** Der Angriff mit der Ransomware "WannaCry" im Jahr 2017 zeigte die Anfälligkeit von unzureichend geschützten IoT-Geräten.

**Konsequenzen:** Datenverlust, Betriebsunterbrechungen, Erpressungsversuche.




**Unsichere Konfigurationen**

**Szenario:** Viele IoT-Geräte werden mit unsicheren Standardpasswörtern oder offenen Ports ausgeliefert. Diese Nachlässigkeit in der Konfiguration macht es Angreifern leicht, die Kontrolle über die Geräte zu übernehmen.

**Beispiel:** Die Webseite “Shodan” ermöglicht es jedem Nutzer, nach ungeschützten IoT-Geräten im Internet zu suchen. Darunter befinden sich oft auch sicherheitskritische Systeme wie IP-Kameras oder Industriesteuerungen.

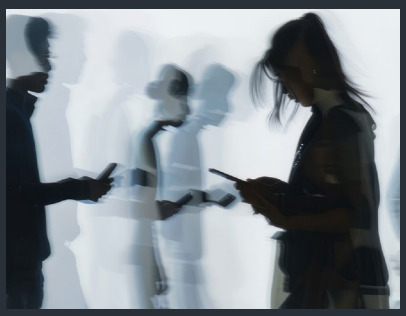
**Konsequenzen:** Unbefugter Zugriff auf Geräte und Daten, Spionage, Sabotage.

**DDoS-Angriffe**

**Szenario:** Stellen Sie sich vor, Ihr Unternehmen wird durch eine Flut von Anfragen von scheinbar legitimen Geräten lahmgelegt. Cyberkriminelle nutzen kompromittierte IoT-Geräte wie IP-Kameras oder Smart-Home-Geräte, um massenhaft Datenverkehr auf Ihre Server oder Netzwerke zu lenken.

**Beispiel:** Im Jahr 2016 wurde der DNS-Provider Dyn Opfer eines großangelegten DDoS-Angriffs, der durch ein Botnetz aus kompromittierten IoT-Geräten durchgeführt wurde. Twitter, Spotify, Reddit und viele weitere bekannte Webseiten waren stundenlang nicht erreichbar.

**Konsequenzen:** Dienstausfälle, Umsatzeinbußen, Reputationsschäden.



**Social Engineering**

**Szenario:** Der Mensch ist oft das schwächste Glied in der Sicherheitskette. Cyberkriminelle nutzen geschickt manipulative Techniken, um Mitarbeiter auszutricksen und an sensible Daten oder Zugangsdaten zu gelangen.

**Beispiel:** Phishing-E-Mails, die vermeintlich von einem bekannten Unternehmen stammen, verleiten ahnungslose Nutzer dazu, sensible Daten preiszugeben oder Schadsoftware herunterzuladen.

**Konsequenzen:** Datendiebstahl, Finanzielle Verluste, Imageschäden.

# M2MGATE –IHRE SICHERHEITS-GARANTIE IM IOT

**Sichere Kommunikation**

Verschlüsselung der Datenübertragung zwischen Geräten, Servern und Anwendern mittels TLS (Transport Layer Security). Einsatz sicherer Kommunikationsprotokolle, um unbefugten Zugriff auf Ihre Daten zu verhindern.

**Robuste Authentifizierung**

Jedes Gerät, das sich mit M2MGate verbinden möchte, durchläuft einen mehrstufigen Authentifizierungsprozess. Nur autorisierte Geräte mit gültigen Anmeldeinformationen erhalten Zugang zu Ihrem Netzwerk und Ihren Daten.

**Automatisierte Updates**

Zentrale Verwaltung und automatisierte Verteilung von Software- und Firmware-Updates, um die Sicherheit Ihrer Geräte stets auf dem neuesten Stand zu halten. Schnelle und effiziente Installation von Updates, um Sicherheitslücken zeitnah zu schließen.

**Sichere Softwareentwicklung**

Unser Entwicklungsteam setzt auf bewährte sichere Programmierpraktiken und führt während des gesamten Entwicklungsprozesses regelmäßige Sicherheitsüberprüfungen durch. Dies umfasst die Anwendung von Code-Reviews, Sicherheitsanalysen und automatisierten Tests, um potenzielle Schwachstellen frühzeitig zu identifizieren.

**Individuelle, Beratung, Support**

Unser erfahrenes Support-Team steht Ihnen bei allen Fragen rund um die Sicherheit von M2MGate zur Seite. Wir unterstützen Sie bei der Implementierung und dem Betrieb Ihrer IoT-Infrastruktur und entwickeln gemeinsam mit Ihnen ein individuelles Sicherheitskonzept, das Ihren spezifischen Anforderungen gerecht wird.

**Transparenz & Kommunikation**

Regelmäßige Information unserer Kunden über relevante Sicherheitsaspekte, wie Sicherheitsupdates, bekannte Schwachstellen und empfohlene Maßnahmen. Transparente Kommunikation schafft Vertrauen und ermöglicht es Ihnen, fundierte Entscheidungen zum Schutz Ihrer IoT-Infrastruktur zu treffen.

**Proaktives Schwachstellen-Management**

Im Entwicklungsprozess von M2MGate wird ein zweistufiges Sicherheitssystem eingesetzt. Die Software wird bereits während des Build-Prozesses in Harbor automatisch auf Sicherheitsrisiken geprüft. Kritische Schwachstellen verhindern den erfolgreichen Abschluss des Builds, um sicherzustellen, dass keine unsicheren Versionen in die Produktion gelangen.

Anschließend erfolgt mit Hilfe von Dependency-Track eine kontinuierliche Überwachung der enthaltenen Software, einschließlich Eigenentwicklungen und Open-Source-Komponenten. Jede Softwareversion wird durch eine Software Bill of Materials (SBOM) dokumentiert und permanent auf sicherheitsrelevante Schwachstellen analysiert. Identifizierte Sicherheitslücken werden priorisiert und durch gezielte Maßnahmen wie Updates oder Anpassungen behoben. Der gesamte Prozess wird fortlaufend überwacht, um die langfristige Sicherheit der Software zu gewährleisten.

# M2MGATE: IHRE ZUVERLÄSSIGE IOT-PLATTFORM FÜR SICHERE IOT-LÖSUNGEN

Mit M2MGate entscheiden Sie sich für eine IoT-Plattform, die Sicherheit nicht als zusätzliches Feature, sondern als integralen Bestandteil versteht. Wir bieten Ihnen nicht nur eine leistungsstarke und flexible Lösung für die Verwaltung und Steuerung Ihrer IoT-Geräte, sondern auch die Gewissheit, dass Ihre Daten und Systeme optimal geschützt sind.

Konzentrieren Sie sich auf Ihr Kerngeschäft – wir kümmern uns um die Sicherheit Ihrer IoT-Infrastruktur.

# HABEN WIR IHR INTERESSE GEWECKT?

**Vereinbaren Sie noch heute einen Termin mit den Fachleuten von INSIDE M2M. Gemeinsam mit Ihnen starten wir kostenfrei und unverbindlich die ersten Schritte!**



INSIDE M2M SMART MACHINES

**INSIDE M2M GmbH**
Telefon: +49 (0) 5137-90 95 0-0
E-Mail: vertrieb@inside-m2m.de

inside-m2m.de

**Garbsen**
Berenbosteler Straße 76 B
30823 Garbsen

**Bissendorf**
Gewerbepark 9-11
49143 Bissendorf

**Berlin**
Marienburger Straße 1
10405 Berlin