Security in the IoT

Protection against growing cyber threats

INSIDE M2M
SMART MACHINES

The Internet of Things (IoT) is fundamentally changing the way we live and work. Companies in all industries are using the possibilities of networked devices to optimize processes, increase efficiency and implement innovative business models. However, this new era of connectivity also brings with it new challenges - particularly in the area of cyber security.

With the increasing number of IoT devices, the attack surface for cyber criminals is growing exponentially. Traditional security solutions, which are designed to protect traditional IT infrastructures, are often not sufficient to meet the complex requirements of the IoT world. The consequences of a successful cyberattack can be devastating: Data loss, business interruption, financial damage and reputational damage.

ATTACK SCENARIOS

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

...

THE LIST IS LONG. PROTECTION IS IMPORTANT.

REAL DANGERS, CONCRETE EXAMPLES

The threat of cyber attacks is real and affects companies of all sizes. It is no longer a question of if, but when a company will become the target of an attack. In the following, we highlight the most common attack scenarios in the IoT environment and use real-life examples to show the dramatic consequences a security incident can have:

Man-in-the-Middle Attacks

Scenario: A Man-in-the-Middle attack occurs when an attacker secretly intercepts and potentially alters the communication between two parties. IoT devices that use insecure or unencrypted connections are particularly vulnerable to this type of attack.

Example: In 2014, hackers managed to take control of the control system of a blast furnace in a German steel mill, resulting in massive damage to the facility.

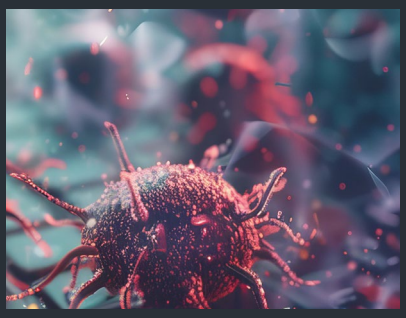
Consequences: This insidious attack method targets the communication between IoT devices and servers. The attacker intercepts the communication between the two parties and can unobtrusively capture, manipulate data, or even take control of the devices.

Device Cloning

Scenario: Cybercriminals can clone the identity of legitimate IoT devices to gain access to networks and steal data or carry out manipulations without being detected.

Example: In 2020, a vulnerability was discovered in the RFID-based access control system of HID Global, a leading provider of access control solutions. Security researchers demonstrated that attackers could intercept and clone HID Global's RFID cards with easily available hardware. These cloned cards were used to gain unauthorized access to high-security areas at Heathrow Airport in London, which raised significant security concerns.

Consequences: Unauthorized access to sensitive areas, theft of confidential information, and sabotage of critical infrastructure.

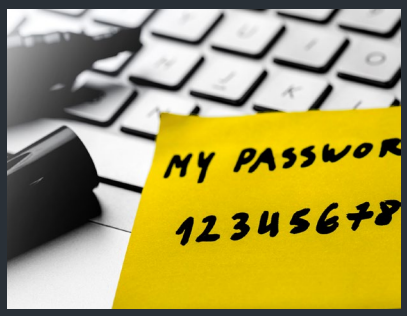


Malware Infections

Scenario: IoT devices are vulnerable to malware infections, which can be introduced through software vulnerabilities or insecure user practices. The malware can steal sensitive data, impair the device's functionality, or even use it as an entry point for further attacks on your company's network.

Example: The "WannaCry" ransomware attack in 2017 highlighted the vulnerability of inadequately protected IoT devices.

Consequences: Data loss, operational disruptions, extortion attempts.



Insecure Default Configurations

Scenario: Many IoT devices are shipped with insecure default passwords or open ports. This negligence in configuration makes it easy for attackers to take control of the devices.

Example: The website "Shodan" allows any user to search for unprotected IoT devices on the internet. These often include security-critical systems like IP cameras or industrial controls.

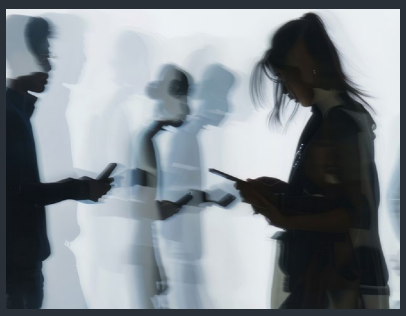
Consequences: Unauthorized access to devices and data, espionage, sabotage.

DDoS Attacks

Scenario: Imagine your company being crippled by a flood of requests from seemingly legitimate devices. Cybercriminals use compromized IoT devices like IP cameras or smart home devices to direct massive amounts of traffic to your servers or networks.

Example: In 2016, the DNS provider Dyn was the victim of a large-scale DDoS attack carried out by a botnet of compromized IoT devices. Twitter, Spotify, Reddit, and many other well-known websites were inaccessible for hours.

Consequences: Service outages, revenue losses, reputational damage.



Social Engineering

Scenario: Humans are often the weakest link in the security chain. Cybercriminals use skillful manipulative techniques to trick employees into revealing sensitive data or access credentials.

Example: Phishing emails that appear to come from a known company trick unsuspecting users into disclosing sensitive information or downloading malware.

Consequences: Data theft, financial losses, reputational damage.

M2MGATE - YOUR SECURITY GUARANTEE IN THE IOT

Secure communication

Encryption of data transmission between devices, servers and users using TLS (Transport Layer Security). Use of secure communication protocols to prevent unauthorized access to your data.

Robust device authentication

Every device that wants to connect to M2MGate goes through a multi-step authentication process. Only authorized devices with valid credentials are granted access to your network and data.

Automated updates

Centralized management and automated distribution of software and firmware updates to keep the security of your devices up to date at all times. Fast and efficient installation of updates to close security gaps in a timely manner.

Secure software development

Our development team relies on proven secure programming practices and performs regular security checks throughout the development process. This includes the use of code reviews, security analyses and automated tests to identify potential vulnerabilities at an early stage.

Personalized advice & support

Our experienced support team is on hand to answer any questions you may have about M2MGate security. We support you in the implementation and operation of your IoT infrastructure and work with you to develop a customized security concept that meets your specific requirements.

Transparency & communication

Regularly informing our customers about relevant security aspects, such as security updates, known vulnerabilities and recommended measures. Transparent communication creates trust and enables you to make informed decisions to protect your IoT infrastructure.

Proactive vulnerability management

IA two-stage security system is used in the M2MGate development process. The software is automatically checked for security risks during the build process in Harbor. Critical vulnerabilities prevent the successful completion of the build to ensure that no insecure versions are released into production.

Dependency Track is then used to continuously monitor the included software, including in-house developments and open source components. Each software version is documented by a software bill of materials (SBOM) and permanently analysed for security-relevant vulnerabilities. Identified security vulnerabilities are prioritized and rectified through targeted measures such as updates or adjustments. The entire process is continuously monitored to ensure the long-term security of the software.

M2MGATE: YOUR RELIABLE IOT PLATFORM FOR SECURE IOT SOLUTIONS

With M2MGate, you are opting for an IoT platform that sees security not as an additional feature, but as an integral component. We not only offer you a powerful and flexible solution for managing and controlling your IoT devices, but also the certainty that your data and systems are optimally protected.

Concentrate on your core business - we take care of the security of your IoT infrastructure.

HAVE WE AROUSED YOUR INTEREST?

Make an appointment today with the experts from INSIDE M2M. Together with you, we will take the first steps free of charge and without obligation at !

INSIDE M2M
SMART MACHINES

INSIDE M2M GmbH
Phone: +49 (0) 5137-90 95 0-0
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