IoT with Security

Increase the security of your IoT ecosystem with security assessments and penetration tests by TÜV Rheinland.

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.

OUR SERVICE

- Securing data, brand, revenue and operations through penetration testing and source code analysis of IoT devices and ecosystems
- Penetration testing not only identifies vulnerabilities and exploits but also the effectiveness of security controls and how these controls may be bypassed or compromised to change the operation security of the IoT device and/or ecosystem
- Mature testing methodology that provides the right combination of automated and manual testing to provide efficient coverage and depth of component testing

YOUR BENEFITS

- Robust security testing portfolio that provides highly technically proficient coverage of all components involved in the IoT ecosystem to fully understand how vulnerabilities in one component can compromise another component
- Identify vulnerabilities and exploits within the IoT device and ecosystem through our flexible penetration methodology and security analysis to lower risk of exploit or breach through actionable results to allow for efficient remediation of findings
- Proactive security recommendations based on industry standards, best practices and years of security expertise for continued secure design and implementation of IoT devices and ecosystem
- High reporting quality and professional project management

OUR COMPETENCE

- With numerous experts who concentrate solely on penetration testing, we provide one of the largest German-speaking security testing services team throughout the industry. Every year, we carry out around 1,000 penetration tests and IT security analyses all over the world – and this number is growing rapidly.
- As one of the world‘s leading independent providers of cybersecurity services, we have other teams at every important location, e.g., the USA, China, India, Singapore, and Oman.

Elements of a penetration test or an IT security analysis of your IoT ecosystem

SECURITY ANALYSIS OF IOT DEVICES

IoT devices are the interface to your customers and can therefore affect the security of your customers‘ infrastructure. In our laboratory, we will carry out with you an agreed, representative setup of the IoT devices, which we will then examine for vulnerabilities. This examination is based on the OWASP IoT Top 10.

SECURITY ANALYSIS OF MOBILE APPLICATIONS

Mobile applications often form an integral part of an IoT ecosystem. The mobile devices frequently contain a large number of other more or less trusted mobile applications, which can be used as a type of springboard for an attack on your IoT ecosystem. We will evaluate the security of your mobile Android or iOS application based on the OWASP Mobile Top 10.

SECURITY ANALYSIS OF THE BACKEND

The backend is the actual brain of every IoT ecosystem, in which everything is managed, analyzed, and switched. We will examine the externally accessible interfaces for vulnerabilities, which could enable a hacker to endanger the confidentiality, integrity, or availability of your systems and data.

SECURITY ASSESSMENT OF THE BACKEND

Our experts will use structured interviews to examine aspects that we sometimes can only surmise in a penetration test, for example, hardening measures in the systems, vulnerability management, and patch management.

REPORTING

We will document and classify the detected vulnerabilities in a TÜV Rheinland test report that contains details for the technical department and is comprehensible to management. In our report, we will describe the damage a successful hacker can cause in your organization and propose countermeasures.

Simply ask us!

TÜV Rheinland i-sec GmbH
Am Grauen Stein
51105 Cologne
Tel. +49 221 806-0
cybersecurity@tuv.com

www.tuv.com/en/pentest

TÜVRheinland®
Precisely Right.