devoteam
Cyber Trust

📄 **Case Study**

IoT Device Penetration Testing: A Comprehensive Approach to Validating the Security, Resilience and Trust of Smart Products

Client
A leading business group in the retail and distribution sector, with a presence in several markets and a strong focus on digital innovation and business transformation.

The Challenge
The client had just launched a next-generation kitchen robot on the market, equipped with Wi-Fi connectivity and mobile app integration. **Despite the strong investment in innovation, there was a critical concern: how could they ensure that this device, part of families' everyday lives, would not become a gateway for cyberattacks?**

Among the risks identified were:

- The possibility of **unauthorised remote control** of the appliance, which could be used maliciously and endanger the user.
- **Exposure** of users' personal and usage data.
- Potential use of the device as an access point to **compromise home networks**.

The client needed to independently and thoroughly validate the resilience of their product before making it widely available.

The Solution
Our team of IoT Penetration Testing (Pentesting) specialists carried out a comprehensive assessment, which included:

- **Hardware and Firmware analysis** to detect embedded vulnerabilities.
- **Reverse engineering and Source Code Review** to understand the device's internal workings.
- **Testing of the Wi-Fi communication** between the robot and the mobile application, including sniffing, brute-force attacks and protocol exploitation.
- **Assessment of the API** and the product's associated mobile app.
- **Simulation of realistic attack scenarios**, such as attempts at remote access and lateral movement from the home network.

Throughout the entire process, a **collaborative approach** was adopted, ensuring that the client not only understood the risks but also received practical mitigation recommendations.

Making your tech journey more secure.

For more information, please visit
www.integrity.pt

IoT Device Penetration Testing: A Comprehensive Approach to Validating the Security, Resilience and Trust of Connected Products

Impact

The outcome of the project brought **peace of mind and trust** to the manufacturer:

- Identification and mitigation of critical vulnerabilities **before commercial launch**, preventing reputational incidents and high remediation costs.
- Implementation of **best practices in encryption and authentication**, strengthening the security of both the app and the device.
- Enhancement of the **brand's value proposition**, as consumers began to associate it with secure and reliable innovation.

Thanks to the work carried out, the client strengthened their competitive position and **significantly reduced the product's attack surface, ensuring a safe and successful launch**.

Related Services

- IoT Device Penetration Testing
- Mobile Application Analysis

Making your tech journey more secure.

For more information, please visit

www.integrity.pt