# Penetration Test: The Remote Service Connection Put to the Test

Bosch Packaging Technology employs round 6,200 people worldwide, who develop, manufacture and install a wide range of different filling, processing and packaging technologies. In order to offer customers around the world even faster systems service, the company uses a remote service connection to the machines. Sensitive data has to be protected against possible cyber attacks. In order to do this effectively, the packaging specialist has contracted TÜV Rheinland to perform a penetration test. This gives Bosch Packaging Technology a reliable and objective appraisal of its present IT security strategy.

Coffee, vegetables or candy: Bosch Packaging Technology has a broad range of packaging solutions for the food industry. In the pharmaceutical sector, the portfolio ranges from machines for filling sterile, fluid and powder pharmaceuticals to inspection technology to tablet presses and track & trace systems.

### ATTRACTIVE TARGET FOR HACKERS

Both Bosch Packaging Technology and many of its customers are established players in the market. That makes it an attractive proposition for cyber attackers to use potential security vulnerabilities in networks, IT systems, applications or mobile devices to manipulate or steal sensitive business or customer data or even to cause a production downtime.

Many companies today are already compromised without even knowing it. The Bosch subsidiary in the field of industrial engineering didn't want to let things get that far. In order to pro-actively reduce this risk and to detect security vulnerabilities related to remote service, Bosch Packaging Technology contracted the experts from TÜV Rheinland to perform a penetration test.

### PRE EMPTING HACKERS – WITH A SIMULATED CYBER ATTACK

In a penetration test, the security analysts scrutinize the IT infrastructure from the perspective of a hacker and simulate a realistic cyber attack. The cyber security experts use a worst-case scenario to examine the maximum amount of damage that can be done by a hacker.

BOSCH
Technik fürs Leben

TÜVRheinland®
Precisely Right.

www.tuv.com/informationsecurity

After evading the initial security measures, the security analysts attempted to deliberately search for information on already compromised systems:

- Files or databases with access information,
- Log files and backups,
- Configuration and source code files which provide information about how one or another of the applications works.

By penetrating the customer's IT infrastructure, a security analyst gathers as much information as possible to understand how hackers would choose their points of attack and compromise the systems. The actual damage is not analyzed; rather it is merely demonstrated that such damage is possible.

## Greater Security by Eliminating Vulnerabilities

### REDUCED CRITICALITY

In the case of Bosch Packaging Technology, the results were positive. In terms of classification, the vulnerabilities identified were not very critical – a good indication of the effectiveness of the security strategy employed by the packaging specialist.

Nevertheless, there is still concern. Even minor security vulnerabilities can – combined with new vulnerabilities – be compounded to form a much larger problem. That is why Bosch Packaging Technology is following the recommendations of TÜV Rheinland to eliminate these potential gateways, or to reduce them to an acceptable level with practical measures corresponding to the requirements of ISO 27001 and IT basic protection as per BSI (Federal Office for Information Security).

### DETAILED DOCUMENTATION

Finally, the examination was documented in a detailed test report. This classification of the identified vulnerabilities, based on the IT security of the systems in the area of investigation using a three-level risk scale. This was supplemented by a list of recommendations for adequate protective measures. The test report also included a description of the procedures employed in the analysis and information about the reproduction of the results.

### PROFESSIONAL COLLABORATION

"The results of the penetration test and the recommendation of TÜV Rheinland are extremely valuable for us," explains Sandro Gisler, Remote Service Portal Owner at Bosch Packaging Technology.
"The collaboration was smooth and professional in both preparation and execution. We will certainly be conducting such important preventative measures in the field of cyber security regularly in the future. That is the only way we can be sure that we are not unnecessarily giving cyber criminals an attack surface and that our data and know-how have the best possible protection. That also means security for our customers."

TÜV Rheinland
Digital Transformation & Cybersecurity
service@i-sec.tuv.com

www.tuv.com/en/pentest

BOSCH
Technik fürs Leben

TÜVRheinland®
Precisely Right.