REDGUARD
SECURING YOUR ASSETS

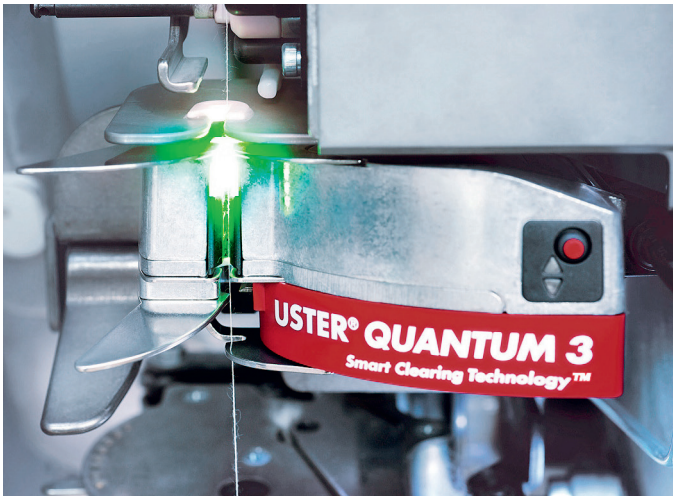
COMPREHENSIVE ASSESSMENT UNCOVERS SECURITY GAPS

Uster Technologies is the global leader in textile testing and quality control. Corporate assets such as research and development data are potential targets for a possible external attack, and Uster Technologies strives to protect these values and data against cyber-attacks. Therefore, the company underwent a 360-degree review to uncover potential vulnerabilities.

USTER®
Think quality

Uster Technologies AG, an independent subsidiary of Toyota Industries, supplies systems and services for quality control in the manufacturing and processing of raw textile fibers. Uster Technologies employs more than 650 people worldwide in Europe, Asia and America. The company defines quality standards which serve as the basis for the global trade in textile products and which must be adhered to.

Uster Technologies put its information security to the test – across the board. Not only a single system was tested, but the entire processes, data protection, data security and physical access to the office premises. Together with Redguard, a comprehensive cyber security assessment was carried out in combination with an attack simulation – and the detected security gaps were immediately improved. This was the first time that such a comprehensive assessment was conducted at Uster Technologies and it has proven its worth at the levels of technology, organization and people.



Proven procedure

Stolen devices, phishing attacks, unauthorized access to business premises, security gaps in processes, hardware and software – nowadays, every company faces these risks. In order to identify Uster Technologies' potential threats, different threat scenarios have been assessed. This comprehensive threat map allowed a broad external and internal view of the entire company. Redguard has examined the created threat map and evaluated the risks, for both now and for the future. Uster Technologies also assessed the risks it faces in the context of the ongoing digitalization process over the next few years. With this knowledge, Uster Technologies can use early detection to keep potential attackers away and protect its corporate assets. "Technological trends require us to constantly monitor information security and take appropriate measures," says Dominique Meier, responsible for the project at Redguard.

Joint workshops, the threat map as well as possible developments provided an initial overview of the current situation. In a further step, all the risks identified were compiled and evaluated in an assessment scheme. Together with Uster Technologies, Redguard developed possible risk scenarios and measures to reduce the vulnerabilities.

Simulated attack

The first part of the 360-degree analysis revealed risks relevant to Uster Technologies. Cyber-attacks are a reality and can lead to large data and financial losses. For this reason, an attack simulation was used to identify vulnerabilities. For Andreas Lötscher, Head of Group IT at Uster Technologies, it was clear that a subsequent attack simulation was necessary. The mix between a cyber security assessment and attack simulation was an ideal choice, he says. The Redguard hackers thus tried to gain access to the Uster Technologies network. A phishing attack led employees to a fake website and encouraged people to enter their personal login details. Physical access to Uster Technologies' premises was also tested using social engineering.

Closing security gaps

"Every company has security gaps," assures Andreas Lötscher, adding: "It is difficult to cover all risks, but regular checks help to set the right priorities. Thanks to the vulnerabilities Redguard discovered we were able to define measures to sustainably increase IT security," Andreas Lötscher continues.
Redguard's service provides a basis for addressing and optimizing cyber risks. Any vulnerabilities or gaps in existing security management at the technology, organization and human levels become visible. All fields of action and measures are determined, taking into account the threat situation, and are submitted to the client in the form of a report. Redguard assigns each measure to the NIST Cyber Security Framework. For all phases (identify, protect, detect, respond, recover), the current and desired maturity level of the organization is determined. This maturity model contains all the perpetrator groups relevant to Uster Technologies, their attack vectors and methods and thus the threat situation of the company. Together with Uster Technologies, Redguard's specialists put together the optimal mix of measures for the organization so that risks can be kept to a minimum or be reduced completely.

"The Redguard employees were able to put our ideas and concerns into practice in the best possible way".

Andreas Lötscher,
Head of Group IT bei Uster Technologies AG

Collaboration with Redguard

The collaboration with Redguard was appreciated by Uster Technologies and, according to Andreas Lötscher, was a complete success: "Our needs were always respected and accepted. The Redguard employees were able to implement our ideas and concerns in the best possible way. Due to the combination recommended by Redguard, essential improvements could be achieved," said Andreas Lötscher. For the Head of Group IT it is clear that companies need to know their risks in order to be able to eliminate them successfully. Andreas Lötscher recommends a cooperation with Redguard and emphasizes their understanding of the matter, their versatile know-how as well as the mutual trust. Thanks to Redguard, the existing protective measures have been further expanded, which will make life difficult for potential attackers.

Erstelldatum 03/2019, RG-C0