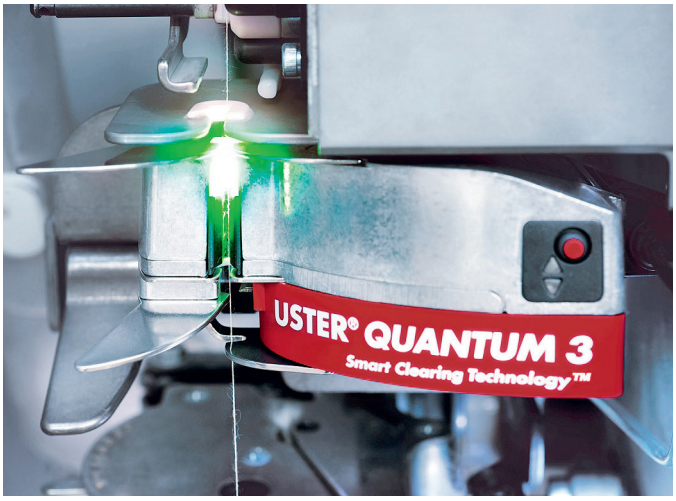
REDGUARD
SECURING YOUR ASSETS

ASSESSMENT DECKT SICHERHEITSLÜCKEN AUF

Die Uster Technologies AG ist ein internationaler Hersteller von elektronischen Mess- und Qualitätssicherungssystemen für die Textilindustrie. Unternehmenswerte wie Forschungs- und Entwicklungsdaten sind potentielle Ziele für einen möglichen Angriff von aussen, und die Uster Technologies ist bestrebt, diese Werte und Daten gegen Cyberangriffe zu schützen. Deshalb unterzog sich die Unternehmung einer 360-Grad-Betrachtung, um mögliche Schwachstellen aufzudecken.

USTER®
Think quality

Die im Jahr 2012 durch Toyota Industries übernommene Uster Technologies AG wurde im selben Jahr zur selbstständigen Tochtergesellschaft. Die Unternehmung bietet Systeme sowie Dienstleistungen an zur Qualitätssicherung bei der Herstellung und Verarbeitung von rohen Textilfasern. Uster Technologies AG beschäftigt weltweit über 650 Mitarbeitende in Europa, Asien und Amerika. Das Unternehmen legt Qualitätsstandards fest, welche als Grundlage für den globalen Handel mit Textilprodukten dienen und eingehalten werden müssen.
Die Uster Technologies stellte ihre Informationssicherheit unter die Probe – und zwar in ganzer Breite. Nicht nur ein einzelnes System wurde geprüft, sondern die gesamten Prozesse, der Datenschutz, die Datensicherheit und der physische Zugang zu den Büroräumlichkeiten. Zusammen mit der Redguard AG wurde ein umfassendes Cyber Security Assessment in



Kombination mit einer Attack Simulation durchgeführt – und die erkannten Sicherheitslücken umgehend verbessert. Diese Kombination wurde so bei der Uster Technologies bisher noch nicht durchgeführt, sie hat sich aber letzten Endes als eine gesamtheitliche Betrachtung auf den Ebenen Technologie, Organisation und Mensch bewährt.

Bewährtes Vorgehen

Gestohlene Geräte, Phishing-Attacken, unberechtigter Zugang zu Geschäftsräumlichkeiten, Sicherheitslücken in Prozessabläufen, Hardware und Software – Risiken, denen jedes Unternehmen heute gegenübersteht. Um zu definieren, welchen möglichen Bedrohungslagen sich die Uster Technologies stellen muss, wurden unterschiedliche Bedrohungsmodelle erstellt. Diese umfassende Landkarte der Bedrohungen ermöglichte eine breite Aussen- sowie Innensicht auf die gesamte Unternehmung. Redguard hat die erstelle Landkarte der Bedrohungen unter die Lupe genommen sowie evaluiert, welche Risiken sie darstellen – sowohl für den heutigen Zeitpunkt, als auch für die Zukunft. Deshalb wurden in der Standortbestimmung auch Risiken bewertet, denen Uster Technologies im Rahmen der fortschreitenden Digitalisierung in den nächsten Jahren gegenübersteht. Durch dieses Wissen kann die Uster Technologies durch eine Früherkennung mögliche Angreifer gezielt fernhalten und ihre Unternehmenswerte schützen. “Technologische Trends erfordern, dass wir stetig die Informationssicherheit überprüfen und entsprechende Massnahmen anpacken”, so Dominique Meier, Verantwortlicher für das Projekt bei Redguard. Gemeinsame Workshops und die Konfrontation mit der aktuellen Bedrohungslage sowie die möglichen Entwicklungen boten einen ersten

Gesamtüberblick über die aktuelle Situation. Alle erfassten Risiken wurden in einem weiteren Schritt in einem Beurteilungsschema zusammengetragen und bewertet. Redguard erarbeitete gemeinsam mit der Uster Technologies mögliche Risikoszenarien und Massnahmen zur Reduktion der identifizierten Risiken.

Simulierter Angriff

Aus dem ersten Teil der 360-Grad-Betrachtung ergaben sich für Uster Technologies relevante Risiken. Cyberangriffe sind Realität und können zu grossen Datenverlusten und finanziellen Einbussen führen. Deshalb wurde hier gezielt die Attack Simulation eingesetzt, um mögliche Schwachstellen direkt aufzuzeigen. Für Andreas Lötscher, Head of Group IT der Uster Technologies AG, war klar, dass eine anschliessende Durchführung der Attack Simulation notwendig war. Der Mix zwischen einem Cyber Security Assessment und der Attack Simulation sei eine ideale Wahl gewesen, sagt er. Die Redguard-Hacker versuchten somit, Zugriff zum Netzwerk von Uster Technologies zu erlangen. Eine Phishing-Attacke verleitete Mitarbeitende auf eine gehackte Website, um dort ihre persönlichen Login-Daten anzugeben. Der physische Zugriff zu den Räumlichkeiten von Uster Technologies wurde mittels Social Engineering ebenfalls getestet.

Sicherheitslücken stopfen

“Jedes Unternehmen hat Sicherheitslücken”, versichert Andreas Lötscher und fügt an: „Es ist schwierig, alle Risiken abzusichern, aber eine regelmässige Prüfung hilft die richtigen Prioritäten zu setzen. Aufgrund der von Redguard aufgedeckten Schwachstellen konnten wir Massnahmen definieren, welche die IT-Sicherheit nachhaltig erhöhen“, so Lötscher weiter.
Die Dienstleistung von Redguard bietet eine Grundlage für die Erweiterung sowie Optimierung der Cyber-Risiken. Allfällige Schwachstellen oder Lücken im bestehenden Sicherheitsmanagement auf den Ebenen Technologie, Organisation und Mensch werden sichtbar. Sämtliche Handlungsfelder und Massnahmen werden unter Berücksichtigung der Bedrohungslage ermittelt und dem Auftraggeber in Form eines Berichts abgegeben. Redguard ordnet jede Massnahme dem Cyber Security Framework von NIST zu. Für sämtliche Phasen (Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen) des Cyber Security Frameworks wird mittels Reifegradmodell der aktuelle und der gewünschte zukünftige Maturitätsgrad der Organisation bestimmt. Darin sind sämtliche für die Uster Technologies relevanten Tätergruppen, deren Angriffsvektoren und -methoden und somit die Bedrohungslage der Unternehmung bekannt. Die Spezialisten von Redguard stellen gemeinsam mit dem Auftraggeber den für die Organisation optimalen Massnahmen-Mix zusammen, damit Risiken minimal gehalten oder gar vollständig reduziert werden können.

„Unsere Bedürfnisse wurden stets respektiert und aufgenommen. Die Redguard-Mitarbeitenden konnten unsere Vorstellungen und Anliegen bestens umsetzen.”

Andreas Lötscher,
Head of Group IT bei Uster Technologies AG

Zusammenarbeit mit Redguard

Die Zusammenarbeit mit Redguard wurde seitens der Uster Technologies geschätzt und war gemäss Andreas Lötscher ein voller Erfolg: „Unsere Bedürfnisse wurden stets respektiert und aufgenommen. Die Redguard-Mitarbeitenden konnten unsere Vorstellungen und Anliegen bestens umsetzen. Aufgrund der von Redguard empfohlenen Kombination konnten essentielle Verbesserungen erzielt werden“, soweit Lötscher. Für den Head of Group IT ist klar, dass Unternehmungen ihre Risiken kennen müssen, um diese anschliessend erfolgreich eliminieren zu können. Andreas Lötscher empfiehlt eine Zusammenarbeit mit Redguard und hebt dabei vor allem deren Verständnis der Materie, das vielseitige Know-how sowie das gegenseitige Vertrauen hervor. Dank Redguard konnten die bestehenden Schutzmassnahmen weiter ausgebaut werden, was potenziellen Angreifern das Leben schwer machen wird.

Erstelldatum 03/2019, RG-C0