REDGUARD
SECURING YOUR ASSETS

DIGITALISIERUNG UND CYBER-SECURITY

bellicon ist führender Hersteller von hochwertigen Minitrampolinen und vertreibt diese weltweit. Neu wird eine Videoplattform namens *bellicon Home* angeboten. Dort bringen Workout-Videos von virtuellen Trainern die Abonnenten ins Schwitzen. Die Plattform wächst stark und bietet grosses Potenzial für bellicon. Die Lösung wurde durch einen externen Entwicklungsdienstleister entwickelt. bellicon hat früh erkannt, dass Themen wie Verfügbarkeit und Schutz der Daten für den Erfolg der Plattform zentral sind.

bellicon
bounce soft, feel good

Um die Sicherheit der Online-Plattform zu garantieren, wurde Redguard beauftragt einen Penetration Test und ein Source Code Review dieser durchzuführen.

Die bellicon Home GmbH (bellicon) ist ein KMU aus Luzern mit grossem Potenzial. Sie produzieren hochwertige Minitrampoline – für Zuhause oder am Arbeitsplatz, für Fitness, Ausdauer und Gesundheit. Die Digitalisierung ist für bellicon ein wichtiges Thema. Darum betreiben sie eine Trainings-Plattform: Abonnenten können auf «bellicon Home» Trainingsvideos schauen, sich vom virtuellen Trainer coachen lassen und individuelle Fitnesspläne erstellen. Der Abo-Service ist ein komplett neues und vielversprechendes Geschäftsfeld für bellicon.

Neue Geschäftsfelder, neue Cyber-Risiken

bellicon wird immer mehr von der Produkt- zur Dienstleistungsfirma. Die Plattform hat bereits eine grosse Benutzerbasis, weshalb Informationssicherheit immer wichtiger wird: Der bezahlte Service muss rund um die Uhr verfügbar sein und der Schutz der Benutzerdaten wie Name, Gewicht und Trainingsplan ist zentral. Gemäss Alexander van't Wout, CEO von bellicon, ist die Plattform auch strategisch wichtig für die Firma. Deshalb ist es für ihn wichtig, das Thema Security frühzeitig zu adressieren.

Video-Plattform unter der Lupe

Welche Schwachstellen hat die Video-Plattform? bellicon wollte Klarheit und hat darum von Redguard einen Penetration Test sowie einen Source Code Review durchführen lassen. Nachdem sich die Security Tester von Redguard einen Überblick über die Plattform verschafft hatten, wurde nach Schwachstellen in den verschiedenen Bereichen gesucht. Dies deckte Benutzerbereiche wie Login-Masken, Registration, Trainings- und Profileinstellungen, aber auch für den Kunden unsichtbare Bereiche wie Admin-Panels und externe Schnittstellen ab. Anschliessend konnte mit diesem Wissen sicherheitsrelevante Bereiche im Source Code effizienter identifiziert und entsprechenden geprüft werden.

4-Augen Penetration Test

Im Kick-off-Meeting zwischen bellicon und Redguard wurde der Umfang für den Penetration Test definiert. Anschliessend haben zwei Security Tester den Penetration Test remote von Redguard's Räumlichkeiten durchgeführt. Penetration Tests werden bei Redguard jeweils von mindestens zwei Security

Testern durchgeführt. Das Vier-Augenprinzip stellt sicher, dass nichts vergessen geht und das Fachwissen mehrerer Security Tester optimal kombiniert werden kann.

Detaillierte Einschätzung der Risiken

Die Resultate aus den Tests wurden in einem Report aufgenommen. Jedes Risiko wird dabei basierend auf dessen Eintrittswahrscheinlichkeit und Schadensausmass eingestuft und zwar spezifisch auf den Business-Case von bellicon bezogen. Redguard gibt zudem basierend auf eigenen Erfahrungen eine Einschätzung ab, wie viel Aufwand mit der Behebung der Schwachstelle verbunden ist, um eine optimale Priorisierung zu ermöglichen. Die im Report gesammelten Inhalte wurden kurz darauf in einer Präsentation beim Kunden vor Ort im Detail erläutert und besprochen.

Massnahmen mit hohem Security-Plus

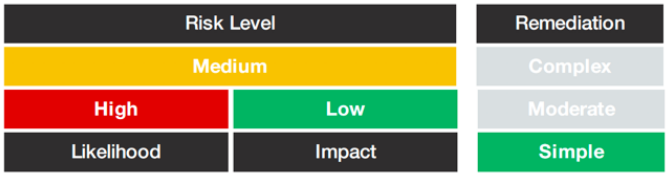
Die Erkenntnisse aus dem Penetration Test und Code Review zeigen, welche Schwachstellen am kritischsten sind und mit welchen Massnahmen bellicon das grösste Security-Plus erreichen kann. Mit dem Report als Basis kann bellicon die Informationssicherheit mit ihrem externen Entwicklungsdienstleister gezielt anpacken.
“Der Rundum-Check der Plattform durch die Redguard war für uns sehr wertvoll und hat sich definitiv gelohnt. Die gewonnene Klarheit und Gewissheit lässt mich ruhiger schlafen”, erzählt Alexander van’t Wout.

Richtiger Umgang mit Risiken

bellicon ist ein Paradebeispiel dafür, dass sich die frühzeitige Investition in Informationssicherheit für KMU lohnt. Informationssicherheit wird im Rahmen der Digitalisierung für Unternehmen vermehrt zum geschäftskritischen Faktor. Das Bewusstsein für vorhandene Cyber-Risiken ist essenziell – so kann das neue Geschäftsfeld erfolgreich und zugleich sicher aufgebaut werden.

„Der Rundum-Check der Plattform durch die Redguard war für uns sehr wertvoll und hat sich definitiv gelohnt.”

Alexander van’t Wout, CEO
bellicon Home GmbH



Der Report zeigt eine Einschätzung zu den einzelnen Schwachstellen, sowie der geschätzte Aufwand für deren Behebung.

Unsere Penetration Tests

Profitieren Sie vom technisch fundierten Wissen der Redguard-Sicherheitsspezialisten. Ein Penetration Test ist eine technische Sicherheitsüberprüfung, mit dem Ziel, Schwachstellen in einem definierten Scope (Netzwerksegmente, Server, Applikationen) zu identifizieren. Damit werden offensichtliche wie auch verborgene Schwachstellen in Systemen frühzeitig erkannt und beurteilt. Der daraus hervorgehende Bericht beinhaltet neben Informationen zu Risiken und Schwachstellen auch passende Gegenmassnahmen, um diese zu adressieren.

Unsere Penetration Tests bieten wir in folgenden Bereichen an:

Web Applikationen
Wir helfen Ihnen, Schwachstellen, in Web-basierten Applikationenzu identifizieren und gezielt zu beheben. Dazu führen wir aktive Tests aus Sicht eines Angreifers durch.

Netzwerke
Daten sind stetig in Bewegung und werden zwischen verschiedenen Systemen ausgetauscht. Ein stabiles und sicheres Netzwerk ermöglicht diesen Austausch. Wir prüfen, ob nur Berechtigte an sensible Verbindungen und Daten herankommen.

Mobile Apps
Wir prüfen die Sicherheit der einzelnen Apps und der dazugehörigen Backends. Unsere Tests umfassen die sowohl OWASP Mobile Top 10 sowie zusätzliche anwendungsspezifische Risiken.

Container Security
Wir helfen Ihnen, Container-Technologien wie Docker und Kubernetes sicher einzusetzen und überprüfen die entsprechende Umsetzung.

IoT & Hardware
Wir unterstützen Sie bei der Absicherung und Prüfung von IoT, und zwar vom Konzept bis zur Sicherheitsprüfung der Hardware-Komponenten, von der Update-Strategie bis zur JTAG-Schnittstelle.

Erstelldatum 02/2020, RG-C0