Erfolgsgeschichten

#schaffenwir

© CyberDanube

MEHR CYBER-SICHERHEIT FÜR INDUSTRIEUNTERNEHMEN

Wie ein Wiener Unternehmen durch gezielte Cyberattacken potentielle Schwachstellen aufdeckt

Mario-Valentin Trompeter & Thomas Weber, CyberDanube (CD Security Technologies GmbH)

Industrieunternehmen sind immer wieder Opfer von Cyberattacken. Ihr Ziel ist es, Daten zu stehlen, die Kontrolle über Geräte zu übernehmen oder das gesamte Netzwerk eines Unternehmens zu gefährden. Das Wiener Unternehmen CyberDanube deckt Schwachstellen auf und minimiert das Risiko vor potentiellen Angriffen.

Damit sich Unternehmen bestmöglich vor Cyberattacken schützen können, führen wir sogenannte Penetrationstests durch. Dabei agieren wir wie reale Angreifer und führen gezielte Cyberangriffe in einem kontrollierten Szenario durch. Unser Ziel ist es, Schwachstellen im System aufzudecken, dir wir anschließend gemeinsam mit dem Betreiber und Hersteller analysieren. Durch geeignete Maßnahmen werden diese Sicherheitslücken systematisch

geschlossen, um die Sicherheit nachhaltig zu verbessern. Gemeinsam haben wir 2022 CyberDanube gegründet, das mittlerweile ein Team aus sechs Expert:innen umfasst.

Mit CyberDanube haben wir uns von Beginn an auf das Industrieumfeld und die Sicherheit im Bereich Industrie 4.0 spezialisiert. Wir testen vor allem Betreiber von kritischer Infrastruktur im Energiesektor und in der Automobilindustrie. Mithilfe von Penetrationstests prüfen wir die Sicherheit von IoT, IIoT und Embedded-Geräten. Dazu gehören beispielsweise Industriesteuerungen, Smart Meter und Drohnen.

„Gezielte Cyberattacken zu testen, ist der beste Schutz vor echten Angriffen."

Im Zuge dieser Penetrationstests erfolgt eine Bewertung der Risiken zu den jeweiligen Cyberattacken. Diese Erkenntnisse geben Aufschluss darüber, was ein Angreifer innerhalb eines begrenzten Zeitrahmens erreichen könnte. All unsere Test- und Angriffsszenarien sind individuell und können in Zusammenarbeit mit unseren Kund:innen so angepasst werden, dass eine gründliche Überprüfung samt umsetzbarer Strategie zur Sicherung ihrer Systeme und Infrastruktur gewährleistet werden kann.

IT-Sicherheit ist ein sehr sensibles Thema. Deshalb sind wir auf Qualität, Servicenähe und Vertrauen unserer Kund:innen bedacht. Auch deshalb testen wir soweit möglich auf „Digital Twins". Das bedeutet, dass wir eine digitale Kopie von (IoT)-Komponenten erstellen, unsere Tests auf diesen durchführen und die tatsächlichen operativen Komponenten samt Umgebung des jeweiligen Unternehmens wenig bis nicht beeinflusst werden.

Die Entwicklung unserer SaaS-Lösung MEDUSA – Scalable Firmware Runtime ist ein echter Meilenstein, der die Qualität und Ergebnisse der Zusammenarbeit mit unseren Kund:innen weiter erhöht hat. Das ist in dieser Form einzigartig und führt zu sehr tiefgreifenden Ergebnissen.

Wir arbeiten sehr eng mit Partnern in kritischer Infrastruktur zusammen und sind in zahlreichen Forschungsprojekten involviert, in denen wir intensiv an der Steigerung der Cybersicherheit arbeiten. Als eine der wenigen CVE Numbering Authorities in Österreich sind wir außerdem dazu befugt, internationale Schwachstellennummern zu vergeben. Das bedeutet, dass wir sogenannte Zero-Day-Schwachstellen – d.h. Schwachstellen im System und in Produkten, von denen selbst der Hersteller bis dato nicht in Kenntnis ist – identifizieren und geregelt veröffentlichen dürfen. https://cyberdanube.com

Online seit 07.02.2025 (Aktualisiert: 07.02.2025)