Videotranskript

RBI

Cyber Defense Center

Thomas Heiss:
Als einer der führenden Finanzdienstleister in Österreich, Zentral- und Osteuropa, ist Datenschutz für die Raiffeisen Bank International ein hochpriorisiertes Thema. Cyberkriminalität floriert – insbesondere im Finanzdienstleistungssektor. Deshalb haben wir im Rahmen unserer Cyber Resilience Strategie ein Cyber Defense Center ins Leben gerufen.

Stephan Beer:
Accenture wurde beauftragt, die RBI beim Aufbau dieser Abteilung zu unterstützen. Mit dem Aufbau einer zentralen Monitoring Plattform, die die IT Infrastruktur in Echtzeit überwacht.

Michael Kellner
Mit Accenture haben wir einen erfahrenen Partner in diesem Bereich, mit dem wir das Konzept und die Architektur des CDC entwickeln und erfolgreich umsetzen konnten. Heute bilden verschiedene Services das CDC Ecosystem: der zentrale Punkt ist das SIEM-System, das uns ermöglicht Cyber Attacken zu erkennen und auf diese entsprechend mit Gegenmaßnahmen zu reagieren. Hierbei setzen wir auf den Marktführer Splunk. Die Analyse, der von Splunk erzeugten Tickets erfolgt 24/7 durch das Security Operations Center, einem interkontinentalen Team aus Security Analysten. Neben dem Aufbau der Splunk-Plattform, legten wir unseren Fokus auf das Anbinden sicherheitsrelevanter Datenquellen, um Logs in Echtzeit mittels spezieller Use Cases analysieren zu können. Dies benötigt eine intensive Zusammenarbeit mit den IT- und Security Abteilungen – coronabedingt zu 90% online.

Stephan Beer:
Für die Umsetzung arbeiteten wir parallel in vier Spezialisten-Teams, die im täglichen Austausch standen: Das Platform Engineering Team, zuständig für den Aufbau der Splunk Plattform, das Onboarding Team, für die Anbindung unterschiedlicher Datenquellen der jeweiligen Entitäten an Splunk verantwortlich, das Use Case Development Team, dessen Fokus auf der Identifikation von Security-relevanten Ereignissen in den Daten lag und das Service Team, zuständig für den laufenden Betrieb und die Ticket-Erst-Analyse. Cyber Security ist ein Prozess, der kontinuierliche Anpassungen erfordert. Gemeinsam ist es uns gelungen, unserem Ziel, ein zentrales Service für die RBI-Gruppe zu erarbeiten, das Daten in Echtzeit normalisiert und analysiert, einen großen Schritt näher zu kommen.

Thomas Heiss:
Das vorrangige Ziel ist es, die Mission der RBI – Gruppe und die digitale Transformation aus Cybersecurity Sicht zu unterstützen, und beim Thema Cybersicherheit ist Vertrauen vorrangig zur Gewährleistung von sicheren und modernen Bankenservices.