BLUE CONSULT.

IBM i Security

IBM i ist doch eine „sichere Festung“?

Die Aussage „IBM i ist sicher“ galt bis vor einigen Jahren als pauschal zutreffend. Oftmals wähnten sich Unternehmen bezüglich ihrer IBM i Systeme mit ihrer objektorientierten Architektur mit definierten Schnittstellen und traditionellen Anwendungen in Sicherheit. Die Zeiten haben sich gewandelt und Unternehmen stehen auch für IBM i vor neuen Anforderungen bezüglich Datenschutz und Abwehr von Cyber-Angriffen. Heute müsste man wohl eher sagen: „IBM i ist bedingt sicher“. Doch können wir die Bedingungen angesichts der Bedrohungslage dem Zufall überlassen?

Das Thema Informationssicherheit wird für IBM i Umgebungen leider häufig vernachlässigt. IBM i kann zwar ein außerordentlich hohes Maß an Datensicherheit und Integrität bieten, bringt dies aber nicht im Auslieferungszustand mit, sondern muss dafür erst entsprechend konfiguriert werden.

Durch das pandemische Ausmaß von Cyberkriminalität mit Hacking, Identitätsdiebstahl und Schadsoftware sowie durch verpflichtende Regularien wie z.B. DSGVO, NIS-2 oder PCI DSS bekommt die Sicherstellung von Informationssicherheit eine hohe Priorität. Der durch Cyber-Angriffe verursachte Schaden für die deutsche Wirtschaft im Jahr 2023 wird seitens Bitkom e.V. Branchenverband auf 206 Milliarden Euro geschätzt.

Bitkom-Präsident Ralf Wintergerst sagte: „Erstmals fühlten sich 52% der Betriebe durch Cyberangriffe in ihrer Existenz bedroht. Die deutsche Wirtschaft ist ein hoch attraktives Angriffsziel für Kriminelle und uns feindlich gesonnene Staaten“.

IBM i Systeme werden mit ihrer integrierten Datenbank oft für unternehmenskritische Anwendungen und zur Speicherung vertraulicher und sensibler Daten eingesetzt. Diese gilt es, besonders vor unbefugtem Zugriff und Manipulation zu schützen, insbesondere auch unter dem Aspekt, dass ein nicht explizit abgesichertes IBM i System insbesondere im Netzwerk grundsätzlich auch vulnerabel gegenüber internen und externen Angriffen ist.

Wie können Angriffsvektoren geschlossen und IBM i sicher gemacht werden?

Klassische Sicherheitsmechanismen für IBM i auf Anwendungsebene reichen nicht mehr aus, da wir mit der Bedrohungslage und verpflichtenden Regularien auf der einen Seite und mit der Vernetzung der Systeme, Netzwerkfreigaben und modernen Kommunikations- und Abfrageprotokollen auf der anderen Seite konfrontiert sind - von der Verschärfung der Lage durch heterogene Lösungen in Zusammenarbeit mit Windows-Systemen ganz zu schweigen.

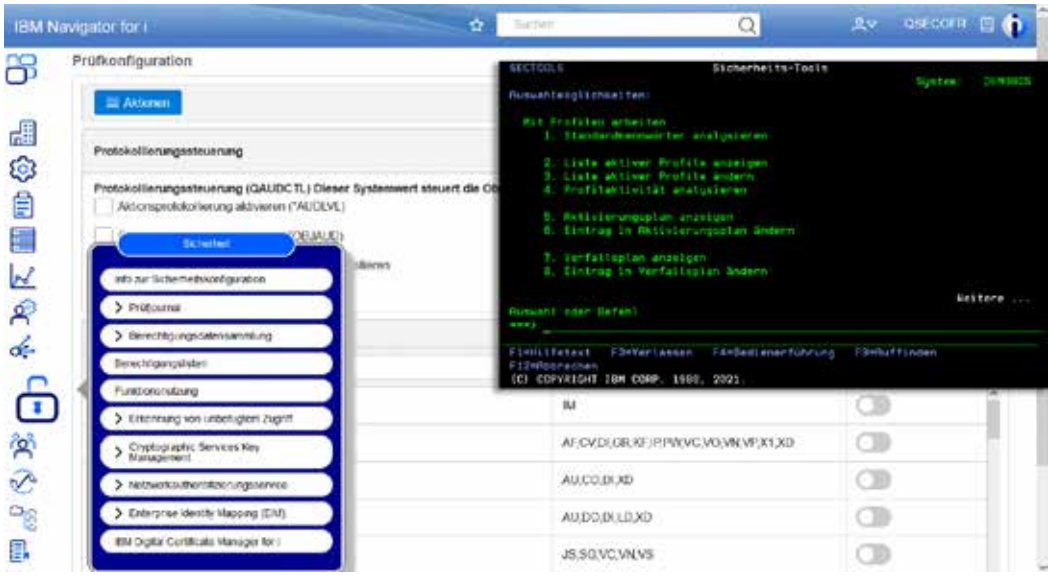
Um einen hohen Sicherheitsstandard für IBM i zu etablieren, muss folgendes gewährleistet sein:

- Einspielen von regelmäßigen Updates
- Konfiguration der umfangreichen Sicherheitsfunktionen, die IBM i bietet, wie u. a.
  - Beschränkung der Zugriffsrechte
  - Netzwerksicherheit
  - Protokollierung und Monitoring

Angebot BLUE: IBM i Security Worshop

Mit unserem Dienstleistungsangebot helfen wir Ihnen, die Informationssicherheit und den Datenschutz für Ihre IBM i Systeme signifikant zu erhöhen. Der Workshop wird an zwei Tagen durchgeführt und umfasst folgendes Leistungsspektrum:

- Aufnahme Ihrer Anforderungen und Erwartungen
- Analyse des Ist-Zustands am Beispiel eines Ihrer IBM i Systeme
- Empfehlungen zur Verbesserung der Informationssicherheit und zum Datenschutz für IBM i
- Festlegung der Priorisierung und Planung weiterer Maßnahmen und Umsetzungsschritte
- Vorstellung wichtiger IBM i Sicherheitsfunktionen und Best Practices -
  dabei behandeln wir u. a. folgende Themenfelder:
  - Zugangskontrolle
  - Berechtigungen
  - Systemintegrität
  - Protokollierung
  - Überwachung
  - Netzwerksicherheit
  - Sicherung und Wiederherstellung
  - Change Management



„Beispiel von IBM i Funktionen und Tools zur Sicherheitsverwaltung“

Ihre Benefits

- Individuelles und interaktives Workshop-Format
- Einblick in Expertenwissen zum Thema IBM i Security
- Wertvolle Informationen zur Ausarbeitung und Umsetzung einer Sicherheitsstrategie und Compliance-Anforderungen
- Identifikation möglicher Sicherheitsrisiken
- Identifikation Ihres Verbesserungspotenzials
- Erhöhung des Sicherheitsbewusstseins

Fahrplan für mehr Informationssicherheit und Datenschutz

Kontakt

Thomas Helget, BLUE Consult GmbH, Adolf-Dembach-Str. 2, 47829 Krefeld
experten@blue-consult.de, Telefon: +49 2151 6500 10

BLUE CONSULT.