FALLSTUDIE

IBM i-Schutz vor Ransomware und Viren bei einem Versicherungsunternehmen

(Die Fallstudie wurde auf Kundenwunsch anonymisiert)

RAZ-LEE

Kundenprofil

Branche	Versicherungen
Region	Amerika
Umgebung	IBM i — 2 LPARs zur zur Unterstützung von Policenverwaltung und Schadenbearbeitung
Sicherheitsziel	Schutz vor Ransomware und Malware
Assessment Type	Interne Sicherheitsbewertung und Härtung der Cybersecurity

Ausgangssituation

Die IBM i-Umgebung des Unternehmens unterstützt geschäftskritische Versicherungsprozesse und verarbeitet sensible Kundendaten. Dadurch stellt sie ein attraktives Ziel für Ransomware- und Malware-Angriffe dar.

Nachdem mehrere Unternehmen der Versicherungsbranche von Ransomware-Vorfällen betroffen waren, identifizierte das Unternehmen wesentliche Sicherheitsrisiken innerhalb seiner IBM i-Infrastruktur.

Schutz vor Ransomware

Dem Unternehmen fehlte eine speziell für IBM i entwickelte Lösung, die:

- ungewöhnliche Dateiverschlüsselungsaktivitäten erkennt
- massenhafte Dateiänderungen in Echtzeit identifiziert
- Administratoren frühzeitig warnt, bevor Geschäftsprozesse beeinträchtigt werden
- verdächtige Jobs oder Benutzer automatisch stoppt

Das Security-Team benötigte eine sofortige Transparenz über potenziell schädliche Aktivitäten in Produktivbibliotheken und gemeinsam genutzten Geschäftsdaten.

Malware- und Virenschutz

Die bestehende Sicherheitsarchitektur verfügte nicht über einen nativen Virenschutz für das IBM i Integrated File System (IFS) und für ausgetauschte Dateien. Gesucht wurde eine Lösung mit:

- kontinuierlicher Malware-Erkennung
- Erkennung infizierter Dateien beim Eingang ins System
- Schutz vor schädlichen Uploads und Dateiübertragungen
- reduziertem Risiko einer Malware-Ausbreitung über verbundene Systeme hinweg

Operative Anforderungen

Die Lösung sollte:

- schnell implementierbar sein, ohne Änderungen an bestehenden Anwendungen
- nativ auf IBM i laufen
- die Performance produktiver Systeme nur minimal beeinflussen
- sich in bestehende Sicherheits- und Monitoring-Prozesse integrieren lassen

Implementierte Lösung

Raz-Lee implementierte die folgenden iSecurity-Module in der IBM i-Umgebung:

iSecurity Anti-Ransomware (AR)

Zur Erkennung und automatischen Abwehr von Ransomware-Aktivitäten in Echtzeit wurde iSecurity Anti-Ransomware eingeführt. Funktionen:

- Kontinuierliche Überwachung von Dateiaktivitäten und Verschlüsselungsvorgängen
- Erkennung ungewöhnlicher Dateiänderungen und Massenverschlüsselungen
- Automatische Gegenmaßnahmen durch das Stoppen verdächtiger Prozesse und Benutzer
- Sofortige Alarmierung der Sicherheitsverantwortlichen
- Schutz von Produktivbibliotheken und geschäftskritischen Daten

Durch die Implementierung konnte das Unternehmen potenzielle Ransomware-Aktivitäten erkennen und stoppen, bevor es zu Betriebsunterbrechungen kam.

iSecurity Antivirus (AV)

Zusätzlich wurde iSecurity Antivirus als nativer Malware- und Virenschutz für IBM i eingeführt. Funktionen:

- Echtzeitprüfung von Dateien im IFS
- Erkennung und Quarantäne infizierter Dateien
- Schutz vor schädlichen Dateiübertragungen und Uploads
- Geplante sowie bedarfsgesteuerte Scans inklusive aktueller Virensignaturen

Die Lösung erhöht die Sicherheit beim Datenaustausch zwischen IBM i und externen Systemen und reduziert das Risiko einer Malware-Infektion deutlich.

Ergebnisse

- Verbesserter Schutz vor Ransomware-Angriffen auf IBM i-Systeme
- Echtzeit-Transparenz über verdächtige Verschlüsselungs- und Dateiaktivitäten
- Reduziertes Risiko der Verbreitung von Malware über übertragene Dateien
- Schnellere Reaktion auf Sicherheitsvorfälle durch automatische Erkennung und Alarmierung
- Implementierung ohne Änderungen an bestehenden Anwendungen
- Minimale Auswirkungen auf Systemleistung und Geschäftsprozesse
- Deutliche Stärkung der Cybersecurity auf IBM i bei gleichzeitig hoher Betriebsstabilität für geschäftskritische Versicherungsanwendungen

Kundenfeedback

„Ransomware gehört mittlerweile zu unseren größten Sicherheitsrisiken. Raz-Lee hat uns eine native IBM i-Lösung bereitgestellt, die verdächtige Aktivitäten unmittelbar erkennt und gleichzeitig wirksam vor Malware schützt. Die Implementierung verlief schnell, effizient und ließ sich nahtlos in unsere bestehenden Betriebsabläufe integrieren.“

— IT Security Manager (sinngemäß wiedergegeben)