CONSECUR BEGLEITET DIE LANDESBANK
BADEN-WÜRTTEMBERG STRATEGISCH UND OPERATIV

Resilienz gegenüber Cyber-Attacken – IT-Sicherheit für die LBBW

ConSecur
[security and consulting]

Resilienz gegenüber Cyber-Attacken – IT-Sicherheit für die LBBW

Jahr für Jahr bedroht die steigende Frequenz von Cyberattacken die IT-Sicherheit von Banken. Die Landesbank Baden-Württemberg (LBBW) beweist ihre Resilienz gegenüber Cyber-Bedrohungen in turnusmäßigen Audits von Bankenaufsicht der Europäischen Zentralbank (EZB) und interner Revision.

ConSecur bietet ein breites Portfolio hochwertiger IT-Sicherheitslösungen und die Expertise von IT-Sicherheitsexperten. Das Ergebnis ist IT-Sicherheit auf hohem Niveau.

Das über die Jahre gewachsene ConSecur-Konzept gewinnt mit weiteren Ausbaustufen, zum Beispiel durch Anbindung zusätzlicher Log-Quellen, der Erweiterung der Detektionsmöglichkeiten sowie der Nutzungskontrolle privilegierter, interner Anwender, permanent an Qualität.

LEISTUNGEN DER CONSECUR BEI DER LBBW

IT-Sicherheit für die Landesbank Baden-Württemberg

ConSecur begleitet die Landesbank Baden-Württemberg strategisch und operativ. IT-Security-Consultants beraten die LBBW bei der Weiterentwicklung ihrer Sicherheitsstrategie, unterstützten bei der Auswahl neuer Fachkräfte sowie bei der Vorbereitung und Durchführung von Ausschreibungen im Bereich der IT-Security. Darüber hinaus setzt die LBBW IT-Fachkräfte der ConSecur für den laufenden Betrieb ihres SIEM ein.

Seit dem Beginn der Zusammenarbeit ist das Aufgabenspektrum der ConSecur GmbH beständig auf dieses heutige Niveau gewachsen. Das Sicherheitsniveau, das auf einem effizient arbeitenden Team aus externen und internen Spezialisten sowie Hochleistungstechnologie basiert, steigert die LBBW permanent mit weiteren Ausbaustufen.

STRATEGIE

Use Cases für das SIEM – automatisierte Alarme bei verdächtigen Aktivitäten in der IT-Infrastruktur

Die Landesbank Baden-Württemberg setzt seit 2013 auf ein Security Information and Eventmanagement (SIEM). In dieser Phase hat die Zusammenarbeit zwischen LBBW und der ConSecur GmbH begonnen, die von der Bank mit dem Aufbau von Use Cases für das SIEM beauftragt hat.

Mit dem Best-Practise Ansatz von ConSecur hat ConSecur die Grundlage für den heute eingespielten Workflow interner und externer IT-Spezialisten geschaffen, die von der Bank mit dem Aufbau von Use Cases für das SIEM beauftragt worden ist.

Sauber aufgesetzte Use Cases steigern die Effizienz des SIEM in hohem Maße. Fehlerhafte Alarmierungen, die die volle Aufmerksamkeit eines IT-Security.-Analysten eine gewisse Zeit binden, werden deutlich reduziert. Bedrohungen für die IT-Infrastruktur jedoch werden im Umkehrschluss unmittelbar als „ungewöhnliches Verhalten“ erkannt und lösen automatisch eine Alarmierung aus, die eine Kettenreaktion in Gang setzt.

Die Unterscheidung, welches Ereignis ein Sicherheitsvorfall ist oder ein berechtigter Zugriff, beginnt mit dem IT-Security-Monitoring.

BETRIEB

Auf Sicherheitsvorfälle reagieren – IT-Security-Monitoring

ConSecur unterstützt die Bank bei der Steuerung des Dienstleisters für Sicherheitsmonitoring sowie bei der Koordination der Workflows für Detektion & Mitigation von IT-Sicherheitsvorfällen.

In dieser Eigenschaft unterstützen IT-Security-Spezialisten der ConSecur die Effizienz des IT-Security-Monitorings mit dem Aufbau weiterer Use Cases und dem Tuning des vorhandenen Regelwerks.

BETRIEB

Eingespielte Kettenreaktion: Handeln bei potentiellen Sicherheitsvorfällen

Potentielle Sicherheitsvorfälle lösen eine Kettenreaktion aus, an deren Anfang ein Anruf bei der zuständigen Stelle steht. IT-Security-Spezialisten von LBBW und ConSecur stehen rund um die Uhr bereit schnellstmöglich aufzuklären, ob die aus dem IT-Security-Monitoring gemeldete Anomalie tatsächlich ein Sicherheitsvorfall ist oder falscher Alarm.

Im Falle eines eingetretenen Sicherheitsvorfalls unterstützt die ConSecur, bis der Sicherheitsvorfall mitigiert worden ist.

Die Weiterentwicklung des IT-Security-Monitorings ist ein permanenter Prozess, den ConSecur und LBBW konsequent verfolgen. Weitere Anwendungen und Assets der Bank werden kontinuierlich angebunden, darüber hinaus hat die ConSecur über die Jahre viele verschiedene Use Cases neu entwickelt.

„ConSecur ist unser verlässlicher Partner in der IT-Sicherheit. Von Beratung und Strategie bis zum Betrieb und zur Aufrechterhaltung von IT-Sicherheit.“

SVEN KONERMANN
IT-SECURITY MANAGER, LEITUNG SIEM
LANDESBANK BADEN-WÜRTTEMBERG

LBBW

BETRIEB

IT-Sicherheitsvorfälle außerhalb bekannter Muster aufspüren

Mit dem IT-Security-Monitoring rund um die Uhr und einer permanent wachsenden Anzahl Use Cases besitzt die LBBW zwei funktionierende Konstanten, um regelbasiert aus Milliarden Logdaten die relevante Anomalien identifizieren zu können.

Für Angreifer, die sich nicht an bekannte Muster halten, hat die LBBW mit Unterstützung ConSecurs und externer Partner die Threat Intelligence etabliert: Erfahrene IT-Security-Analysten spüren Sicherheitsvorfälle auf (Threat Hunting), denen sie zum Beispiel durch veränderte Schwellwerte auf die Spur gekommen sind. Ohne die eingeführte Threat Intelligence bestünde die Gefahr, dass diese minimalen Veränderungen, die auf eine Kompromittierung des Systems (Indicators of Compromise) hindeuten könnten, unerkannt unterm Radar blieben.

BETRIEB

Mitre Attack Framework – wie Angreifer bei Cyber-Attacken vorgehen

Vor Einführung der Threat Intelligence haben IT-Security-Consultants der ConSecur an einem Mitre Attack Framework mitgearbeitet, das aufzeigt, mit welchen Methoden, Taktiken und Techniken Angreifer bei Cyber-Attacken vorgehen können.

In Verbindung mit dem Gesamtsystem der Bank ist eine sogenannte Threat Landscape entstanden, die Angreiferverhalten und mögliche Angriffsziele korreliert. Die Threat Landscape ist ein atmendes System, das ConSecur beständig um neue Angriffsflächen und -muster ergänzt. Die IT-Security-Consultants prüfen für jedes erkannte Angriffsmuster, ob dieses in einer formulierten Regel als Use Case in das IT-Security-Monitoring integriert werden könnte.

„Die Threat Landscape sensibilisiert dafür, welche Systeme welchen Bedrohungen ausgesetzt sein könnten.“

MATTHIAS LAU
IT-SECURITY CONSULTANT CONSECUR GMBH

NUTZUNGSKONTROLLE AUF ANWENDUNGSBASIS

Interne Bedrohungen identifizieren: Nutzungskontrolle von Accounts mit privilegierten Berechtigungen auf Anwendungsbasis

Über das IT-Security-Monitoring hinaus, das die LBBW vor den Auswirkungen externer Cyber-Angriffe bewahrt, hat ConSecur die Nutzungskontrolle privilegierter Accounts etabliert. Ziel der Nutzungskontrolle ist, mögliche interne Bedrohungen aus diesem Kreis rechtzeitig identifizieren und abwehren zu können.

Über die Nutzerkontrolle können sicherheitskritische Handlungen nachvollzogen werden, die von Accounts mit privilegierten Rechten ausgegangen sind.

HANDELT ES SICH UM „DOLOSE HANDLUNGEN“, DIE EINE BEDROHUNG FÜR DIE IT-SICHERHEIT DER BANK DARSTELLEN?

Relevante Anwendungen haben ConSecur und LBBW analysiert. Steckbriefe sind Templates für kritische Anwendungen, die einer bestimmten Kritikalitätsstufe angehören.

Die LBBW hat mit der Prozesslandschaft und der Infrastruktur die Basis dafür geschaffen, dass diese Kontrollfunktion ein fester Bestandteil der IT-Sicherheit der LBBW geworden ist.

WEITERENTWICKLUNG

In Ausschreibungen aus vielen Bewerbern den besten externen Partner finden

Externe Dienstleister unterstützen die LBBW bei der operativen IT-Sicherheit. ConSecur begleitet die Bank bei der Ausschreibungsvorbereitung.

Die strategische Entscheidung, IT-Sicherheit gemeinsam mit externen Dienstleistern und festen internen Fachkräften zu organisieren, hat die LBBW vor einigen Jahren getroffen. Bevor Ausschreibungen veröffentlicht werden, haben LBBW und ConSecur in der Voranalyse Anforderungen definiert, welche Aufgaben zum Beispiel im IT-Security-Monitoring umzusetzen sind.

ConSecur unterstützt bei der Vorbereitung der Ausschreibung auch mit der exakten Formulierung der Bedürfnisse, sodass eingehende Bewerbungen auf den Punkt dem Anforderungsprofil der Bank entsprechen können.

„MIT DEM EINBEZUG AN EXTERNE DIENSTLEISTER GEWINNEN WIR FACHLICHE KOMPETENZ IN DER PERSONELLEN STÄRKE, DIE WIR BENÖTIGEN, UND DARÜBER HINAUS DIE GRÖSSTMÖGLICHE FLEXIBILITÄT.“

FLORIAN NEU, HEAD OF IT-SECURITY

WEITERENTWICKLUNG

Die besten Köpfe für IT-Sicherheit gewinnen und fortbilden

ConSecur unterstützt die LBBW bei der fachlichen Weiterbildung ihrer Mitarbeiter.

Die Unterstützung der ConSecur beginnt bei dem fachlichen Assessment von Spezialisten und findet ihre Fortsetzung mit dem Onboarding neuer Mitarbeiter.

Die fachliche Qualifizierung interner Mitarbeiter ist ein fester Bestandteil der Sicherheitsstrategie der Bank, die den permanenten, vertiefenden Know-how Transfer in regelmäßigen Schulungen fördert. IT-Security-Consultants der ConSecur schulen interne Fachkräfte deshalb zu Themen wie Threat Hunting.

ConSecur GmbH

Als herstellerunabhängiges Beratungs- und Dienstleistungsunternehmen befasst sich die ConSecur GmbH mit der Planung und Umsetzung von Maßnahmen zur Informationssicherheit. Unsere Leidenschaft ist die Entwicklung, Bewertung und Realisierung von IT-Sicherheitskonzepten für Unternehmen. So beschützen wir die Information, die Sie täglich für Einkauf, Produktion, Dienstleistung, Logistik und Korrespondenz benötigen. ConSecur hat sich darauf spezialisiert Informationssicherheit an die Geschäftsprozesse im organisatorischen und informationstechnischen Umfeld anzubinden. Hierbei setzen wir auf die bestehenden unternehmerischen Prozesse und eingesetzten Technologien unserer Kunden auf. Wir etablieren lösungsorientierte, standardisierte und effiziente Maßnahmen, die unsere Kunden in die Lage versetzen, ihre informationstechnischen Risiken zu beherrschen und bestehenden regulatorischen Vorgaben zu genügen. Ziel unserer Arbeit ist es, nur berechtigten Personen den Zugriff auf Informationen zu gewähren und Informationen vor Übergriffen Unbefugter zu schützen

ConSecur – next level information security

ConSecur
[security and consulting]

ConSecur GmbH
Nödiker Straße 118
49716 Meppen

TEL.: +49 5931 9224-0
info@ConSecur.de
www.ConSecur.de