CONSECUR SUPPORTS THE STATE BANK
BADEN-WÜRTTEMBERG STRATEGICALLY AND OPERATIONALLY

Resilience against cyber attacks – IT security for LBBW

ConSecur
[security and consulting]

Resilience against cyber attacks – IT security for LBBW

Year after year, the increasing frequency of cyber attacks threatens the IT security of banks. Landesbank Baden-Württemberg (LBBW) demonstrates its resilience to cyber threats in regular audits conducted by the European Central Bank's (ECB) banking supervision and its internal audit department.

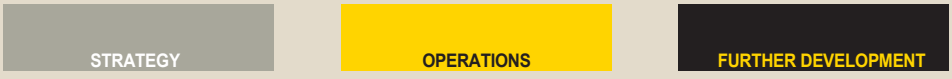
ConSecur offers a broad portfolio of high-quality IT security solutions and the expertise of IT security specialists. The result is IT security of the highest standard.

The ConSecur concept, which has evolved over the years, is constantly improving in quality through further expansion stages, for example by connecting additional log sources, expanding detection capabilities and controlling the use of privileged internal users.

CONSECUR'S SERVICES AT LBBW

IT security for Landesbank Baden-Württemberg

ConSecur provides strategic and operational support to Landesbank Baden-Württemberg. IT security consultants advise LBBW on the further development of its security strategy, assist with the selection of new specialists, and support the preparation and execution of tenders in the field of IT security. Furthermore, LBBW employs ConSecur's IT specialists for the day-to-day operation of its SIEM.



Since the start of the partnership, the scope of ConSecur GmbH's services has grown steadily to its current level. LBBW is constantly enhancing the level of security – which is based on an efficient team of external and internal specialists as well as high-performance technology – through further upgrades.

STRATEGY

Use cases for SIEM – automated alerts for suspicious activity in the IT infrastructure

Landesbank Baden-Württemberg has been using a Security Information and Event Management (SIEM) system since 2013. It was during this phase that the collaboration between LBBW and ConSecur GmbH began, with the bank commissioning the company to develop use cases for the SIEM.

Through its best-practice approach, ConSecur has laid the foundations for the now well-established workflow involving internal and external IT specialists, who were commissioned by the bank to develop use cases for the SIEM.

Properly configured use cases significantly increase the efficiency of the SIEM. False alarms, which tie up the full attention of an IT security analyst for a certain period of time, are significantly reduced. Conversely, threats to the IT infrastructure are immediately recognised as "unusual behaviour" and automatically trigger an alert, setting a chain reaction in motion.

Distinguishing between which event is a security incident and which is legitimate access begins with IT security monitoring.

OPERATIONS

Responding to security incidents – IT security monitoring

ConSecur supports the bank in managing the security monitoring service provider and in coordinating workflows for the detection and mitigation of IT security incidents.

In this capacity, ConSecur's IT security specialists enhance the efficiency of IT security monitoring by developing further use cases and fine-tuning the existing set of rules.

OPERATIONS

A well-rehearsed chain reaction: Responding to potential security incidents

Potential security incidents trigger a chain reaction, which begins with a call to the relevant department. IT security specialists from LBBW and ConSecur are on standby around the clock to determine as quickly as possible whether the anomaly reported by the IT security monitoring system is actually a security incident or a false alarm.

In the event of a security incident, ConSecur provides support until the incident has been mitigated.

The ongoing development of IT security monitoring is a continuous process that ConSecur and LBBW are consistently pursuing. Further applications and assets of the bank are being integrated on an ongoing basis; in addition, ConSecur has developed many different new use cases over the years.

"ConSecur is our trusted partner in IT security. From consultancy and strategy to the operation and maintenance of IT security."

SVEN KONERMANN
IT SECURITY MANAGER, HEAD OF SIEM,
LANDESBANK BADEN-WÜRTTEMBERG

LBBW

OPERATIONS

Detecting IT security incidents outside known patterns

With round-the-clock IT security monitoring and a constantly growing number of use cases, LBBW has two reliable constants that enable it to identify relevant anomalies from billions of log data records using rule-based analysis.

For attackers who do not adhere to known patterns, LBBW, with the support of ConSecur and external partners, has Threat intelligence established: Experienced IT security analysts track down security incidents (threat hunting) that they have identified, for example, through changes in threshold values. Without the threat intelligence system in place, there would be a risk that these minimal changes – which could indicate that the system has been compromised (Indicators of Compromise) – would go undetected.

OPERATIONS

MITRE Attack Framework – how attackers proceed in cyber attacks

Prior to the introduction of threat intelligence, ConSecur's IT security consultants collaborated on a Mitre Attack Framework, which illustrates the methods, tactics and techniques attackers may employ in cyber attacks.

In conjunction with the bank's overall system, a so-called Threat Landscape has been created, which correlates attacker behaviour with potential targets. The Threat Landscape is a dynamic system that ConSecur continually updates with new vulnerabilities and attack patterns. For each identified attack pattern, the IT security consultants assess whether it could be integrated into the IT security monitoring system as a use case within a defined rule.

“The Threat Landscape raises awareness of which systems might be exposed to which threats.”

MATTHIAS LAU
IT SECURITY CONSULTANT, CONSECUR GMBH

APPLICATION-BASED USAGE CONTROL

Identifying internal threats: Usage monitoring of accounts with privileged permissions on an application-based basis

In addition to IT security monitoring, which protects LBBW from the effects of external cyber attacks, ConSecur has established usage monitoring for privileged accounts. The aim of this monitoring is to identify and counter potential internal threats originating from this group in good time.

User monitoring enables the tracking of security-critical actions originating from accounts with privileged rights.

ARE THESE ‘MALICIOUS ACTIONS’ THAT POSE A THREAT TO THE BANK’S IT SECURITY?

ConSecur and LBBW have analysed relevant applications. Profiles are templates for critical applications that belong to a specific criticality level.

With its process landscape and infrastructure, LBBW has laid the foundations for this control function to become an integral part of LBBW’s IT security.

FURTHER DEVELOPMENT

Finding the best external partner from among many applicants in tenders

External service providers support LBBW with operational IT security. ConSecur assists the bank with tender preparation.

LBBW took the strategic decision several years ago to organise its IT security in collaboration with external service providers and permanent in-house specialists. Before tenders are published, LBBW and ConSecur defined requirements in a preliminary analysis, specifying which tasks, for example, needed to be carried out in IT security monitoring.

ConSecur also assists with the preparation of the tender by helping to formulate the requirements precisely, so that incoming applications can match the bank's requirements profile to the letter.

"BY ENGAGING EXTERNAL SERVICE PROVIDERS, WE GAIN THE SPECIALIST EXPERTISE IN THE STAFFING CAPACITY WE NEED, AND BEYOND THAT, THE GREATEST POSSIBLE FLEXIBILITY."

FLORIAN NEU, HEAD OF IT SECURITY

FURTHER DEVELOPMENT

Attracting and developing the best talent for IT security

ConSecur supports LBBW in the professional development of its staff.

ConSecur's support begins with the professional assessment of specialists and continues with the onboarding of new employees.

The professional development of internal staff is an integral part of the bank's security strategy, which promotes the ongoing, in-depth transfer of expertise through regular training sessions. ConSecur's IT security consultants therefore train internal specialists on topics such as threat hunting.

ConSecur GmbH

As a vendor-independent consultancy and service provider, ConSecur GmbH specialises in the planning and implementation of information security measures. Our passion lies in the development, assessment and implementation of IT security concepts for businesses. In this way, we protect the information you need on a daily basis for purchasing, production, services, logistics and correspondence. ConSecur specialises in integrating information security with business processes within the organisational and IT environment. In doing so, we build upon our clients' existing business processes and technologies. We establish solution-oriented, standardised and efficient measures that enable our clients to manage their IT risks and comply with existing regulatory requirements. The aim of our work is to grant access to information only to authorised persons and to protect information from unauthorised access

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