ConSecur
[security and consulting]

BAIT Anforderungen an die operative IT-Sicherheit mit ConSecur erfüllen!

ZIELE/MASSNAHMEN

+ BAIT Anforderungen an die operative IT-Sicherheit im Finanzsektor erfüllen
+ Informationssicherheit mit SIEM/ Cyber Defense Center effektiv stärken
+ Transparenz und Planungssicherheit gewinnen

BANKAUFSICHTLICHE ANFORDERUNGEN AN DIE IT

Im November 2017 wurden erstmals die „Bankaufsichtlichen Anforderungen an die IT" (BAIT) veröffentlicht. Sie konkretisierten die Vorgaben der Mindestanforderungen an das Risikomanagement (MaRisk). Nachdem die BAIT zuletzt im September 2018 aktualisiert und um das neue Themengebiet „Kritische Infrastrukturen" ergänzt wurden, gab es im Oktober 2020 ein umfangreiches Update (Konsultation). Drei neue Themenbereiche wurden aufgenommen und bestehende Bereiche inhaltlich erweitert. Naturkatastrophen und Pandemien, aber auch Digitalisierung und Cyberkrimininalität müssen im IT-Risikomanagement verstärkt berücksichtigt werden. Im Rundschreiben vom 16.08.2021 stellt die BaFin nun klare Anforderungen an Kredit- und Finanzdienstleistungsinstitute mit Blick auf den Einsatz von Informationstechnik und Cybersicherheit.

KONKRETE MARISK/BAIT FORDERUNGEN AN DIE OPERATIVE IT-SICHERHEIT

Das Kapitel 5 „Operative Informationssicherheit" adressiert die Operationalisierung der Vorgaben der Informationssicherheit und grenzt sich hierdurch klar vom weiterhin bestehenden Kapitel „IT-Betrieb" ab. Folglich stellt dieses Kapitel Anforderungen an die Bewertung von sicherheitsrelevanten Ereignissen.

Kredit- und Finanzdienstleistungsinstitute sind somit gezwungen eine Lösung aus Menschen, Technologie und Prozesse zu implementieren, die in der Lage sind Inhalte aus Logdateien regelbasiert, zentral und zeitnah auszuwerten. Damit einhergehend ist die implizite Forderung zur Etablierung eines „Cyber Defense Center (SOC)", in dem das Monitoring der Systeme zentral gesteuert wird.

JETZT HANDELN!

PROOF OF CONCEPT (POC) ALS EINSTIEG

Sie suchen einen Einstieg um ein angemessenes Portfolio an Regeln zur Identifizierung sicherheitsrelevanter Ereignisse zu definieren und möchten unsere Services für Ihr Unternehmen testen? ConSecur empfiehlt schnellstmöglich einen PoC, um Entscheidungs- und Budgetrisiken zu reduzieren.

SIEM PILOTIERUNG INNERHALB VON 15 TAGEN

Innerhalb von 15 Tagen stellen wir Ihnen ein Cyber Defense Center inkl. SIEM Tool als Proof of Concept zur Verfügung, deren Anforderung wir zuvor gemeinsam definieren.

Wir setzten uns im Rahmen des PoCs bei Ihnen vor Ort mit zu überwachenden individuellen Use Cases (Risikoszenarien) auseinander und zeigen den Funktionsumfang des SIEM-Tools, anhand konkreter Ereignisse aus den angebundenen Logquellen.

Sie werden in dem Proof of Concept sehen und erleben können, wie unsere Security-Analysten Ihre IT-Infrastruktur auf Sicherheitsvofälle hin untersucht und aktives Security Incident Management betreibt.

Gemeinsam bilden wir mit Ihrer IT-Abteilung eine schlagkräftige Allianz um Sicherheitsbedrohungen zu erkennen und rechtzeitig Gegenmaßnahmen einzuleiten. Dieses Zusammenwirken von Mensch und Technik demonstrieren wir Ihnen gerne persönlich.

KONTAKTIEREN SIE UNS !

ConSecur
[security and consulting]

BAIT Anforderungen an die operative IT-Sicherheit mit ConSecur erfüllen!

ZIELE/MASSNAHMEN

+ BAIT Anforderungen an die operative IT-Sicherheit im Finanzsektor erfüllen
+ Informationssicherheit mit SIEM/ Cyber Defense Center effektiv stärken
+ Transparenz und Planungssicherheit gewinnen

Das Managed Service Spektrum eines Cyber Defense Centers umfasst die Überwachung und Analyse der aktuellen Bedrohungslage und ein breites Spektrum an Sicherheitsdienstleistungen. Nachfolgend ein Überblick über die Leistungen in unseren beiden Cyber Defense Center/ Security Operation Center:

CONSECUR – IHR PARTNER WENN ES UM IT-SICHERHEIT GEHT

ConSecur ist einer der führenden Spezialisten, wenn es darum geht, Cyber-Angriffe und IT-Sicherheitsvorfälle zu entdecken und schnellstmöglich abzuwehren. In unserem Cyber Defense Center analysieren IT-Sicherheitspexperten alle Systeme und Ereignisse in Echtzeit (auf Wunsch 24/7).

Managed SIEM durch ConSecur bedeutet, dass unser gesamtes Team hinter Ihrem Unternehmen steht. Wir entwickeln einen maßgeschneiderten Einsatzplan, stimmen Teams und Einsatzleiter aufeinander ab und halten Ihr SIEM durch kontinuirliche Überwachung und Prüfung auf dem höchsten Stand.

Namhafte Kunden aus dem Bankenumfeld vertrauen auf die Managed Services von ConSecur.
Mehr erfahren Sie im OLB-Referenzbericht „Managed SIEM mit IBM QRadar für die Oldenburgische Landesbank“!

LERNEN WIR UNS KENNEN!

KONTAKT:
ConSecur GmbH
Nödiker Straße 118
49716 Meppen

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