BTC

Verpflichtende Anomalieerkennung bei KRITIS-Unternehmen

Informationen und Umsetzungshinweise

Agenda

- Die gesetzliche Grundlage im Fokus
- Umsetzung im Unternehmen
- Mögliche unterstützende Leistungen Dritter
- Tipps für die Auswahl unterstützender Dienstleister
- Zusammenfassung

BTC auf einen Blick

BTC Business Technology Consulting AG

2000

Geschäftsfelder

- Consulting
- Systemadministration
- Applikations- & Systemmanagement
- Softwareprodukte

Partner

aws · esri Partner Network Gold · Microsoft · SAP · ORACLE

UMSATZ

247

Mio. €

Stand: 12/2021

>2.100

Stand: 12/2021

Branchenkompetenz

- Energie und
- Telekommunikation
- Industrie
- Dienstleister
- Öffentlicher Sektor

Verpflichtende Anomalieerkennung bei KRITIS-Unternehmen

Vorgaben des Gesetzgebers

BTC

„Die Verpflichtung, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung

Richtlinie zur Sicherheit in der Informationstechnik Kritischer Infrastrukturen

BTC

Spezifizierte Anforderungen des Gesetzgebers aus dem IT-Sicherheitsgesetz

Einsatz von Systemen zur Angriffserkennung nunmehr gesetzliche Vorgabe

Das **BSIG § 8a** beschreibt notwendige **Maßnahmen** von **Betreibern Kritischer Infrastrukturen** zur **Etablierung von Systemen zur Angriffserkennung**

Grundsatz: **Verpflichtung** zum **Einsatz technischer und organisatorischer Maßnahmen** zur **Angriffserkennung**

Merkmale aus dem laufenden Betrieb müssen **kontinuierlich** und **automatisch erfasst** und **ausgewertet** werden

Ziel: **Fortwährende Identifikation** und **Vermeidung von Bedrohungen** sowie **Etablierung geeigneter Maßnahmen** zur **Abwehr eingetretener Störungen**

Erfüllung der Vorgaben müssen **alle zwei Jahre nachgewiesen** werden, durch Audits, Prüfungen und/oder Zertifizierungen

Das **BSI** kann die **Vorlage von Dokumentationen** verlangen, zum Zweck der Überprüfung das **Betreten der Geschäfts- und Betriebsräume** während der üblichen Betriebszeiten einfordern.

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.
(1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Absatz 1 Satz 2 und 3 gilt entsprechend.
(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach den Absätzen 1 und 1a vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach den Absätzen 1 und 1a zu gewährleisten. Die Feststellung erfolgt

1. im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,
2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes.

(3) Betreiber Kritischer Infrastrukturen haben die Erfüllung der Anforderungen nach den Absätzen 1 und 1a spätestens zwei Jahre nach dem in Absatz 1 genannten Zeitpunkt und anschließend alle zwei Jahre dem Bundesamt nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.
(4) Das Bundesamt kann beim Betreiber Kritischer Infrastrukturen die Einhaltung der Anforderungen nach den Absätzen 1 und 1a überprüfen; es kann sich bei der Durchführung der Überprüfung eines qualifizierten unabhängigen Dritten bedienen. Der Betreiber Kritischer Infrastrukturen hat dem Bundesamt und den in dessen Auftrag handelnden Personen zum Zweck der Überprüfung das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Für die Überprüfung erhebt das Bundesamt Gebühren und Auslagen bei dem jeweiligen Betreiber Kritischer Infrastrukturen nur, sofern das Bundesamt auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen nach den Absätzen 1 und 1a begründeten.
(5) Das Bundesamt kann zur Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen nach Absatz 3 Anforderungen an die Art und Weise der Durchführung, an die hierüber auszustellenden Nachweise sowie fachliche und organisatorische Anforderungen an die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen.

BTC

Spezifizierte Anforderungen des Gesetzgebers aus dem IT-Sicherheitsgesetz

Die Orientierungshilfe des BSI unterstützt bei der Umsetzung

Wichtige Aspekte aus der Orientierungshilfe:

- **Protokollierung, Detektion** und **Reaktion**
- Berücksichtigt werden müssen **OT und IT**
- **Muss, Soll und Kann-Regeln** für Protokollierung, Detektion und Reaktion sind beschrieben und können **Ausgangsbasis** für eine **Etablierung im Unternehmen und / oder** auch für die **Formulierung von Ausschreibungen** zur Unterstützung durch Dritte genutzt werden
- Der **Umsetzungsgrad** wird anhand eines **Umsetzungsgradmodells** ermittelt
- **Nachweisformulare** unterstützen bei der **Darlegung der Umsetzungen**

Weitere Informationen zur Orientierungshilfe:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.html

Verpflichtende Anomalieerkennung bei KRITIS-Unternehmen

Bewertung unterstützender Leistungen Dritter

End2End-Kundenperspektive – auch Ihre Sicht?

Internet

ISP

Bereitstellung Internet Standortvernetzung

- Physikalische Sicherheit RZ
- DDoS Schutz
- Managed Firewall / IDS / IPS
- NOC

IT-Services IT-Provider

Security Compliance und in der Bereitstellung von IT-Services

- Security Compliance
- Informationssicherheit für Backend-Applikationen
- Client Security

SOC BTC / BITS

Angriffserkennung, -alarmierung, -auswertung

- Log-Management
- Security Information & Event Management
- Analysis & Incident Response
- Threat & Vulnerability Management

Ganzheitlicher Ansatz

Sicherheit in der Bereitstellung von IT-Betriebsleistungen (mit Kontext Internetanbindung)

BTC

Leistungen eines SOC sind auslagerungsfähig

Kein Verantwortungsübergang – Unterstützung jedoch möglich

Die Verantwortung für die Umsetzung der gesetzlichen Vorgaben kann nicht delegiert werden, gleichwohl können operative IT-Sicherheitsleitungen von Dienstleistern erbracht werden

Mögliche Auslagerungsszenarien

Anomalieerkennung

- **Logmanagement** etablieren
- **Threat & Vulnerability-Management** etablieren
- Realisierung eines **Security Information and Event Management (SIEM)**
- **Analysis & Incident Respons-Fähigkeiten** aufbauen

Etablierung eines SOC

- Vergegenwärtigung der **eigenen Umsetzungsmöglichkeiten** der Etablierung eines **Security Operation Centers (SOC)**
- **Make or Buy**: Entscheidung, welche operative IT-Sicherheits-leistung **selbst erbracht** werden können und **welche nicht**

Verpflichtende Anomalieerkennung bei KRITIS-Unternehmen

Ansätze der BTC zur Unterstützung von KRITIS-relevanten Unternehmen

BTC

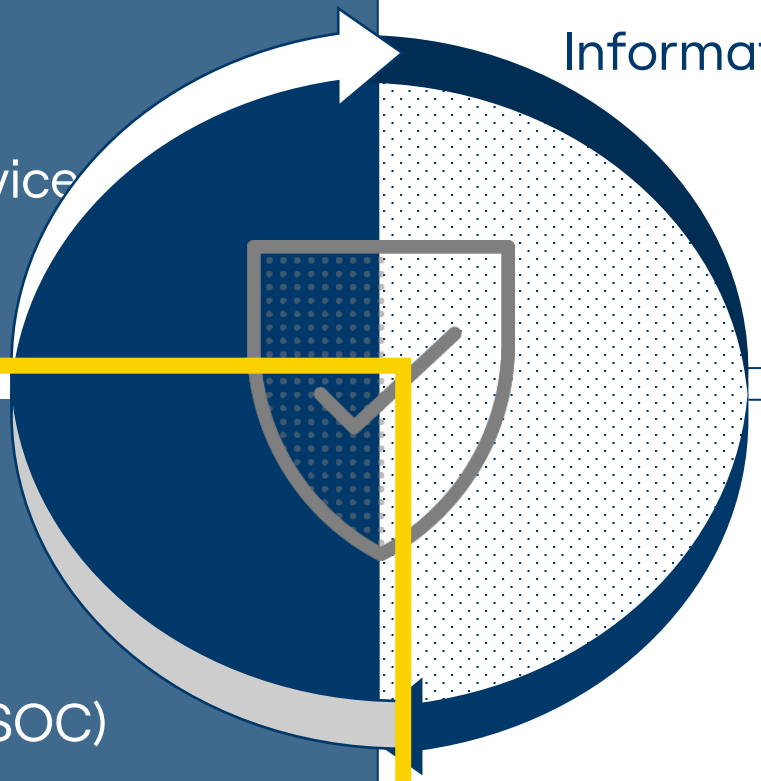
Portfolio Cyber Security

Security Assessments

Penetrationstests
Schwachstellenanalysen
Webapplication Security Service
SAP-Security

Security Consulting

Informationssicherheitsmanagement
Risikoanalysen
Datenschutz
Cloud Security
Security Awareness



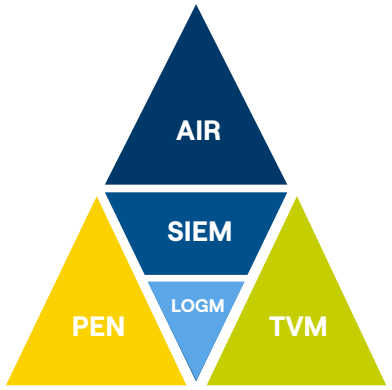
Security Operations (SecOps)

Managed Security Services
Vulnerability Management
Event Management
Security Operations Center (SOC)

Security Audit

ISMS Audits
Cyber-Sicherheits-Check
Cloud-Security-Check

BTC SOC: Service Module



LOGM (Log Management)

- Gewährleistet Zentralisierung sicherheitsrelevanter Logs und schützt diese vor Veränderungen
- Ermöglicht Aufklärung von Sicherheitsvorfällen & Beweissicherung
- Bildet die Basis für SIEM

SIEM (Security Information & Event Mgt.)

- Einrichtung SIEM Ruleset zur Angriffserkennung auf Basis der Daten und Alarmierung bei Sicherheitsvorfällen
- Verarbeitung aktueller und fortlaufend aktualisierter Bedrohungsinformationen
- Stellt ganzheitliche und zentrale Sicht auf die Bedrohungssituation dar

TVM (Threat & Vulnerability Mgt.)

- Kontinuierliche Überwachung der Infrastruktur auf Schwachstellen
- Bietet eine Gesamtübersicht über die vorhandenen Schwachstellen
- Priorisierung von Schwachstellen und Erkennung von Bedrohungen

PEN (Penetrationtests)

- Durchführung von individuellen Penetrationstests durch unsere zertifizierten Sicherheitsexperten („Ethical Hacker“)
- Webapplikationen, Mobile Apps, Client, Active Directory, Netzwerk oder OT-Systeme

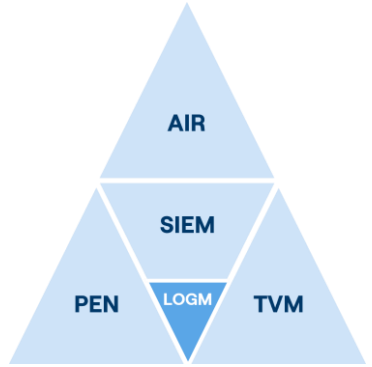
AIR (Analysis & Incident Response)

- Bewertung, Analyse und Überwachung der SIEM Alarmierungen auf Basis von definierten Use Cases (24/7)
- Einleitung abgestimmter Incident Response Verfahren, sowie Mitigations- und Behebungsmaßnahmen
- Rechtzeitige Erkennung von Sicherheitsvorfällen und Information relevanter Stakeholder
- Einleitung qualifizierter Maßnahmen zur Schadensbegrenzung

BTC SOC Service: Modul LOGM – Log Management

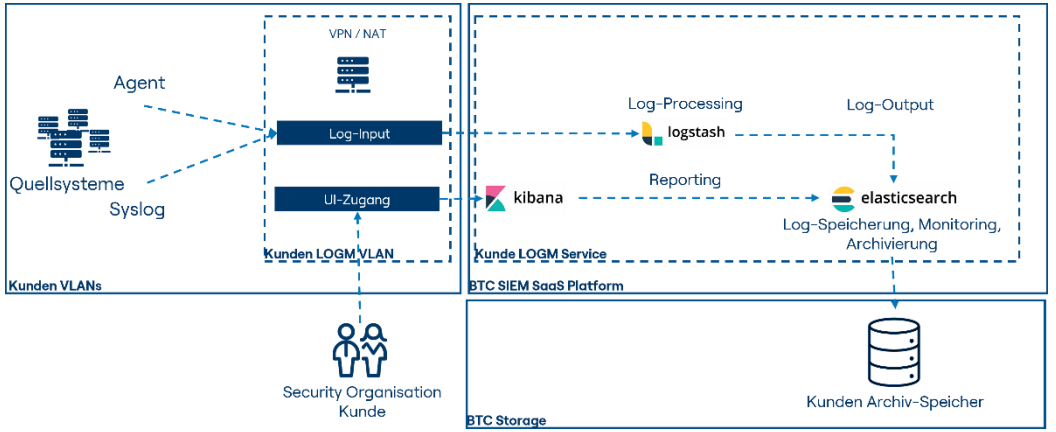
Leistungen

- Aufbau und Betrieb einer Logmanagement Umgebung auf Basis von Elastic
- Bereitstellung von Log-Inputs zur Übertragung der Logfiles
- Anbindung der gewünschten Logquellen (optional)
- Aufbereitung der Logeinträge (Normalisierung, Anreicherung, Pseudonymisierung)
- Speicherung / Archivierung der Logeinträge nach Vorgaben des Kunden
- Bereitstellung eines Webzugriffs auf die Logdaten, inkl. User & Berechtigungsmanagement
- Erstellung von Dashboards / Reports (optional)



Mehrwerte

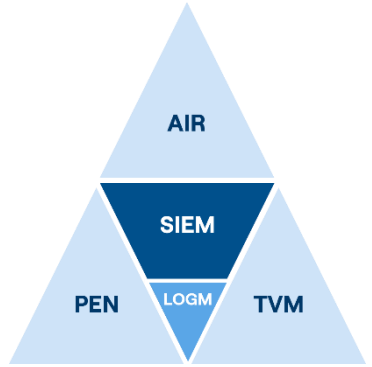
- Performante, sichere und hochverfügbare Lösung auf allen Ebenen
- Leichte Skalierbarkeit in Abhängigkeit zu den notwendigen Ressourcen
- Schnelle Bereitstellungsmöglichkeit aufgrund der genutzten Technologie
- Verbrauchs- und mengenbasiertes Verrechnungsmodell (je GB / Monat)
- Möglichkeit eines zentralen Log-Managements über Cloud- und RZ-Infrastruktur hinweg
- längerfristige Archivierung der Logdaten innerhalb der BTC Archivsysteme



BTC SOC Service: Modul SIEM

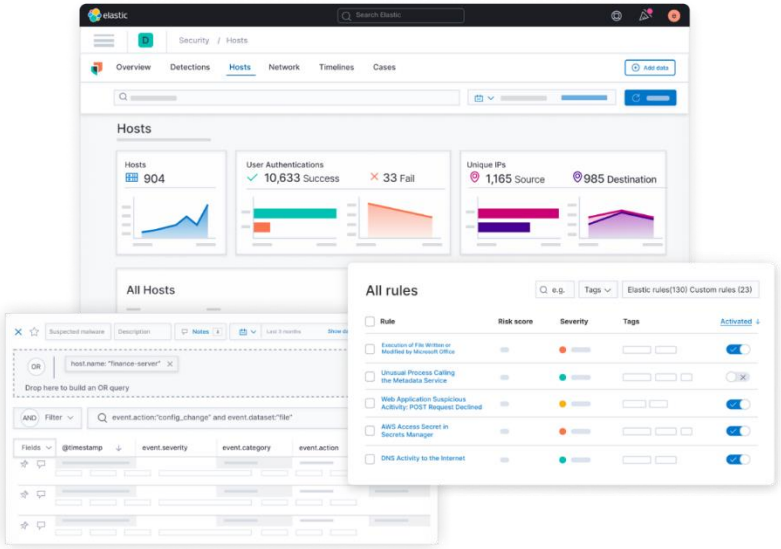
Leistungen

- Aufbau und Betrieb einer SIEM Umgebung auf Basis von Elastic
- Alle Leistungen aus LOGM
- Einrichtung SIEM Ruleset zur Angriffserkennung auf Basis der Daten und Alarmierung bei Sicherheitsvorfällen
- Echtzeit-Analyse auf Anomalien
- Machine-Learning basierte Erkennung von Sicherheitsvorfällen (optional)
- Korrelation von Ereignissen unterschiedlicher Herkunft
- Automatische Alarmierung von Sicherheitsvorfällen
- Fortlaufende Optimierung der Regeln und Heuristiken



Mehrwerte

- Schaffung einer ganzheitlichen Sicht auf die IT-Sicherheit
- Rechtzeitige Erkennung von Cyberangriffen
- Schnelle und detaillierte Analyse von Sicherheitsvorfällen
- Schnelle Einsteuerung in die Prozesse zur Vorfallsbehandlung
- Schaffung von kundenübergreifenden Synergie-Effekten bezüglich Angriffsdetektion und Bedrohungsinformationen
- Umfangreiches regelmäßig aktualisiertes Ruleset zur Detektion



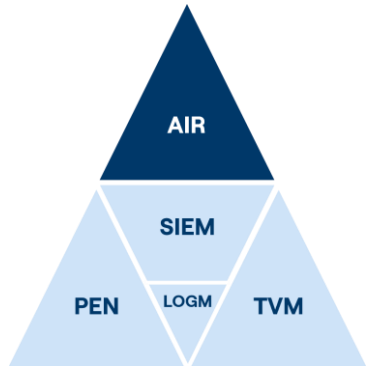
BTC SOC Service: Modul AIR

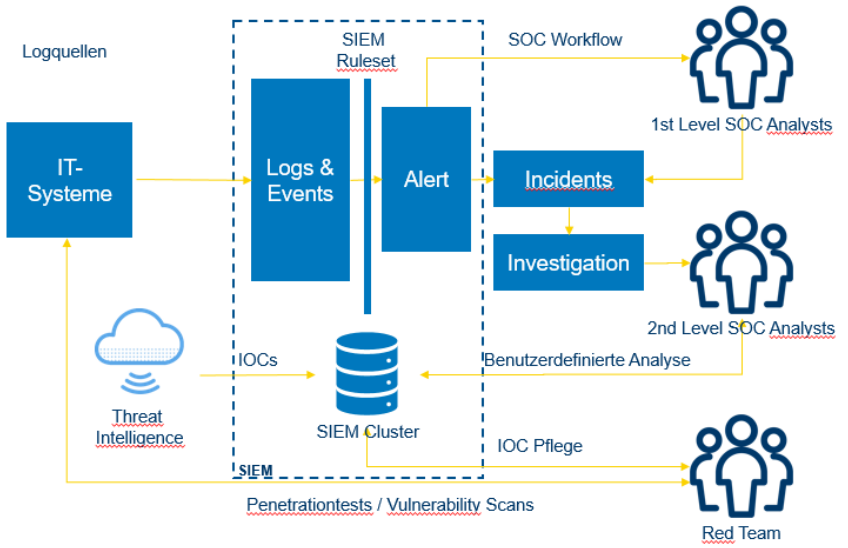
Leistungen

- Betrieb eines Security Operation Centers bestehend aus Sicherheitsexperten
- Definition der umzusetzenden Use Cases inklusive Anforderungen
- Fortlaufende Bewertung, Analyse und Überwachung von Sicherheitsereignissen und –vorfällen auf Basis von definierten Use Cases (24/7)
- Einleitung von abgestimmten Incident-Response-Verfahren, sowie Mitigations- und Behebungsmaßnahmen
- Kontinuierliche Optimierung der Use Cases
- Durchführung von Lessons Learned Meetings nach Abschluss eines Vorfalls zur Identifizierung von Verbesserungsmaßnahmen

Mehrwerte

- Reduzierung der Erkennungszeit von Sicherheitsvorfällen
- Qualifizierte Ableitung von Maßnahmen zur Milderung und Beseitigung eines Sicherheitsvorfalls
- Identifizierung des Umfangs eines Sicherheitsvorfalls und des eingetretenen Schadens
- Optimierung der Angriffserkennung durch kontinuierliche Auswertung von Bedrohungsinformationen, sodass auch aktuelle Taktiken der Angreifer nicht unerkannt bleiben
- Rechtzeitige Information relevanter Stakeholder





Verpflichtende Anomalieerkennung bei KRITIS-Unternehmen

Ansätze der BTC zur Unterstützung von KRITIS-relevanten Unternehmen

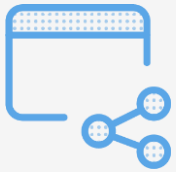
BTC

Anforderungen an SOC / SIEM-Leistungen

Tipps für die Auswahl ihres Dienstleisters

1. Vergegenwärtigung der eigenen Situation im Unternehmen

- **Ist-Analyse:** Wo steht ihr Unternehmen heute in der Operativen IT-Sicherheit?
- **Abgleich mit der Gesetzeslage:** Welche Maßnahmen müssen umgesetzt werden
- **Delta-Analyse:** Was kann / muss selbst realisiert werden, was kann / sollte ausgelagert werden



2. Eignung eines potentiellen Dienstleisters prüfen

- **Generelle Anbietereignung** checken: Gesellschafterstruktur, Bonität, Portfolio
- **Erfahrung bewerten**: Bei welchen Unternehmen erbringt bereits heute der Dienstleister Operative IT-Sicherheitsleitungen?
- **Einzelanalyse**: Abgleich der Einzelleistungen des Anbieters mit dem individuellen Bedarf des Auftraggebers (KRITIS-Unternehmen)

BTC

Christian Bruns
BTC AG
Themenmanager Cyber Security
Tel 0441 / 3612-1129
christian.bruns@btc-ag.com

Norbert Rosebrock
BTC AG
Themenmanager Managed Service Provider
Tel 0441 / 36192-1900
norbert.rosebrock@btc-it-services.com