PROFI.info

ADVANCED CYBER DEFENSE CENTER – EINE KOOPERATION VON PROFI AG UND KPMG

UMFASSENDE INFORMATIONSSICHERHEIT

PROFI
Innovative IT-Lösungen

ACDC: SIEM UND COMPLIANCE, WO SIE ES BENÖTIGEN

Nachdem das Thema Informationssicherheit lange Zeit ein Schattendasein geführt hat, ist es inzwischen ein fester Bestandteil jeder Unternehmensagenda.

Doch neben der erhöhten Wahrnehmung hat Informationssicherheit in den letzten Jahren weitere Entwicklungen vollzogen:

UMFASSENDER ANSATZ

War Informationssicherheit früher auf IT-Systeme und deren technischen Schutz durch isolierte Maßnahmen wie Firewalls, AV-Systeme etc. beschränkt, so wurde dieser Ansatz inzwischen durch die Top-Down-Herangehensweise eingeholt. Erst nachdem ein Unternehmen festgestellt hat, welche Werte es vor welchen Gefährdungen schützen muss, kann über sinnvolle Maßnahmen – technischer wie organisatorischer Natur – entschieden werden.

COMPLIANCE

Die Anforderungen an Informationssicherheit resultieren nicht nur aus der unternehmensinternen Risikobetrachtung, sondern immer mehr aus externen Forderungen. Diese kommen üblicherweise von relevanten Kunden oder aber dem Gesetzgeber selbst in Form des Informationssicherheitsgesetzes.

Diese Entwicklungen stellen Unternehmen früher oder später vor die Herausforderung, dass ihre IT-Systeme keine ausreichenden Möglichkeiten zur Detektion von Anomalien und unerwünschten Vorgängen bieten. Hierfür wurden SIEM-Systeme entwickelt, in denen Logmeldungen und Netzwerkkommunikation unterschiedlicher Systeme normalisiert, korreliert und gegebenenfalls alarmiert werden.

Die Implementierung eines SIEM-Systems stellt eine besondere Herausforderung dar:

- **Welche Daten und Vorgänge haben den größten Schutzbedarf?**
- **Welche Use Cases und Alarme bringen mir realen Mehrwert?**
- **Welche Quelldaten sind tatsächlich relevant?**
- **Die Pflege des Systems erfordert oft völlig neue Skills im Unternehmen.**
- **Der Betrieb muss 24/7 gewährleistet sein**

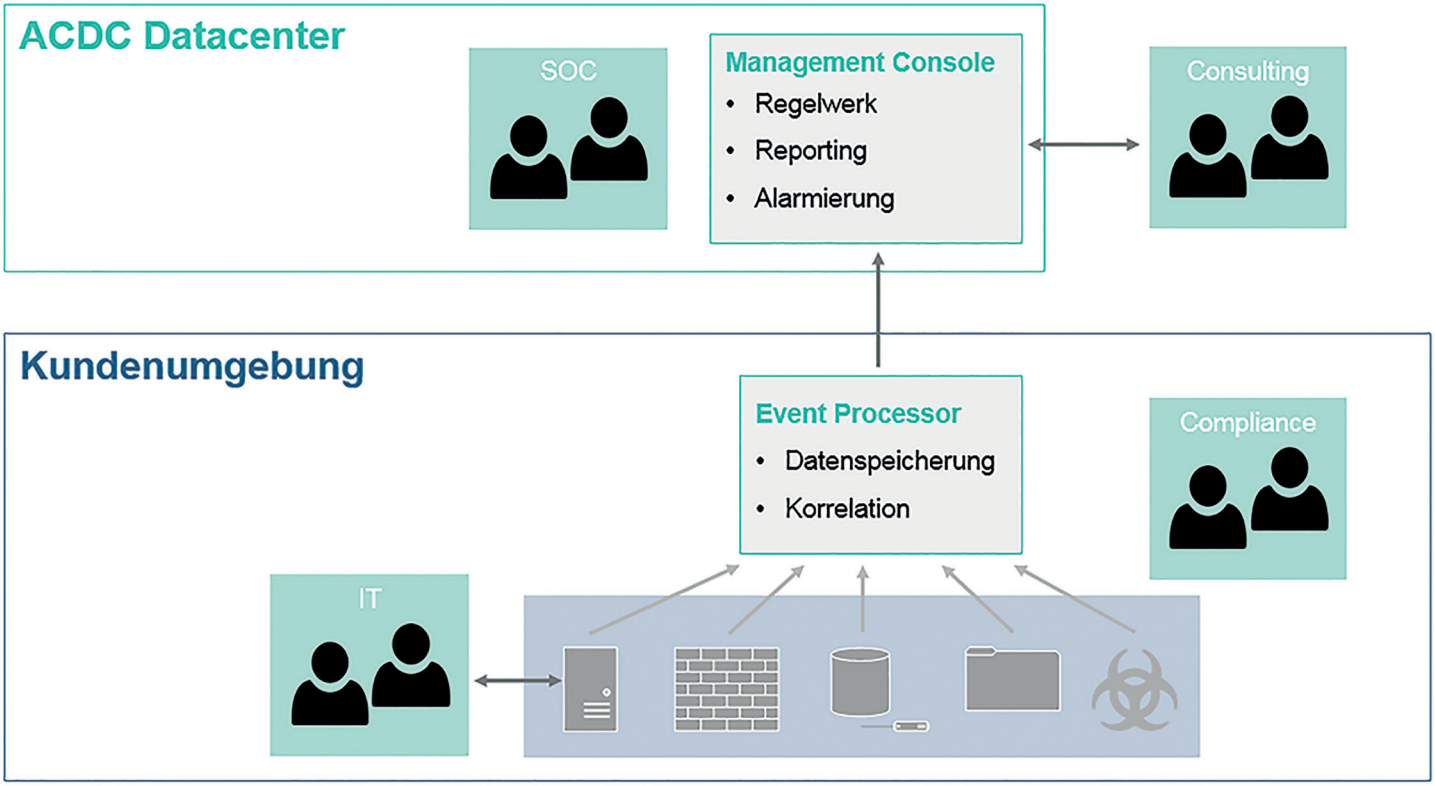
Die ACDC-Lösung

(Advanced Cyber Defense Center) geht einen anderen Weg als die klassischen SIEM-Lösungen. Die Idee hinter ACDC ist, dass nicht alle anbindbaren Systeme auch tatsächlich angebunden werden sollten, sondern dass die Grundlage immer die Definition der wichtigen Use Cases ist. Dazu werden beim Kunden durch KPMG-Berater entsprechende Assessments durchgeführt, um die für den Kunden wichtigen Systeme und Daten zu identifizieren und entsprechende Use Cases zu entwickeln.

Daraus resultieren die benötigten Logs, relevante Regeln sowie individuelle Alarmierungsketten. Die Use Cases werden dann in eine Managed SIEM-Umgebung überführt, die 24/7 im PROFI-eigenen SOC (Security Operation Center) betrieben wird.

Der Kunde erhält schließlich genau das, was er tatsächlich braucht, um Compliance-Anforderungen zu erfüllen: Eine Alarmierung im Falle einer Regelverletzung, ohne selbst eine ganze SIEM-Infrastruktur betreiben zu müssen.

UMFASSENDE IT-SECURITY MIT DER ACDC-LÖSUNG



Die beim Kunden definierten Use Cases werden in die Managed SIEM-Umgebung des Advanced Cyber Defense Centers überführt und im Security Operations Center betrieben.

Haben wir Ihr Interesse geweckt?

Dann sprechen Sie mich direkt an:

Marcus Pfeiffer,
Geschäftsfeldleiter Managed Services
+49 6151 8290-7534
m.pfeiffer@profi-ag.de

PROFI
Innovative IT-Lösungen

DIE PROFI ENGINEERING SYSTEMS AG

Wir sind ein mittelständisches, inhabergeführtes und finanzkräftiges IT-Lösungshaus mit Hauptsitz in Darmstadt. Innovationskraft und Kundenorientierung sind wesentliche Säulen unserer Unternehmensstrategie. Seit über 30 Jahren unterstützen wir unsere Kunden mit individuellen hochwertigen Lösungen zur Optimierung von IT- Prozessen und Systemlandschaften.

Wir begleiten Ihr Unternehmen bei der digitalen Transformation – von der Strategie über die Umsetzung bis zum Betrieb. Unsere erfahrenen Berater und Architekten beschäftigen sich seit vielen Jahren intensiv mit der Digitalisierung aller Geschäftsabläufe und Unternehmensbereiche im Kontext von bimodaler IT (traditionelle und agile IT-Prozesse), Industrie 4.0, Security, Cloud, Big Data, mobilen Lösungen, Social Media und SAP.

Wir übernehmen für Sie Projektmanagement und Implementierung, einschließlich dem Betrieb Ihrer Systeme und Plattformen. Unser Anspruch ist höchste Kompetenz, Zuverlässigkeit und Qualität, mit messbarem Erfolg und direktem Beitrag zur Wertschöpfung und Wettbewerbsfähigkeit unserer Kunden.

Wir beschäftigen rund 380 Mitarbeiterinnen und Mitarbeiter bundesweit an 15 Standorten. Seit vielen Jahren gehören wir zu Deutschlands erfolgreichsten Systemhäusern und pflegen langjährige Partnerschaften mit allen führenden IT-Herstellern.

Unsere IT-Lösungen für Ihren Erfolg

- **Strategie- & Prozessberatung**
- **Industrie 4.0**
- **Big Data & Analytics**
- **Mobile**
- **Cloud-Lösungen**
- **Security & Netzwerke**
- **SAP-Lösungen**
- **Infrastruktur-Lösungen**
- **Business-Lösungen**
- **Managed Services**

PROFI Engineering Systems AG
Otto-Röhm-Straße 18
64293 Darmstadt
Telefon: +49 6151 8290-0
Telefax: +49 6151 8290-7610
E-Mail: profi@profi-ag.de
www.profi-ag.de

UNSERE PARTNER

Gemeinsam mit unseren zertifizierten Partnern entwickeln wir für Sie die optimale Lösung.

IBM Platinum Business Partner
SAP Partner
DELL EMC PARTNER PLATINUM
FUJITSU SELECT Circle
Microsoft Partner Gold Server Platform, Silver Messaging, Gold Management and Virtualization
2015 Business Partner Gold Lenovo
NUTANIX
NetApp Gold Partner
CISCO Premier Partner
veeam GOLD propartner
vmware PARTNER PREMIER SOLUTION PROVIDER
DARZ Daten sind wertvoller als Geld

03 / 2017

PROFI Innovative IT-Lösungen