SVA INFORMATIONSSICHERHEIT

UNSER LÖSUNGSPORTFOLIO FÜR IHRE INFORMATIONSSICHERHEIT

SVA LÖSUNGSPORTFOLIO INFORMATIONSSICHERHEIT

Mit SVA Security-Experten und ausgewählten Lösungen überwachen und schützen Sie Ihre Unternehmensinformationen – im gesamten Lebenslauf.

Das Thema IT-Security ist so vielschichtig und komplex, dass es für IT-Verantwortliche immer schwieriger wird, sich zu orientieren und die richtigen Entscheidungen zu treffen. Zu den wichtigsten Aufgaben gehören die professionelle und regelmäßige Sicherheitsüberprüfung eines Unternehmens durch Sicherheitsanalysen und die Einführung geeigneter Lösungen zur Aufrechterhaltung eines angemessenen Sicherheitsniveaus.

Denn Sicherheit ist ein Prozess, ein ständiger Kreislauf von Audits und Berichten, Finden und Klassifizieren, Bewerten und Verbessern, Überwachen und Umsetzen.

Die SVA Security-Experten unterstützen Sie mit dem SVA Lösungsportfolio Informationssicherheit kostengünstig, flexibel und zukunftsorientiert im gesamten Lebenszyklus Ihrer Daten. Unser ganzheitlicher Security-Ansatz ist die optimale Voraussetzung für eine erfolgreiche Umsetzung Ihrer Security-Vorhaben.

Auf Basis ausgewählter Security-Software verschiedener Hersteller bieten wir eine kompakte Vorgehensweise und effiziente Lösungen – angefangen bei der Beratung bis hin zur Aufdeckung von Sicherheitslücken und Implementierung von Gegenmaßnahmen.

Abb.: SVA Security Lifecycle

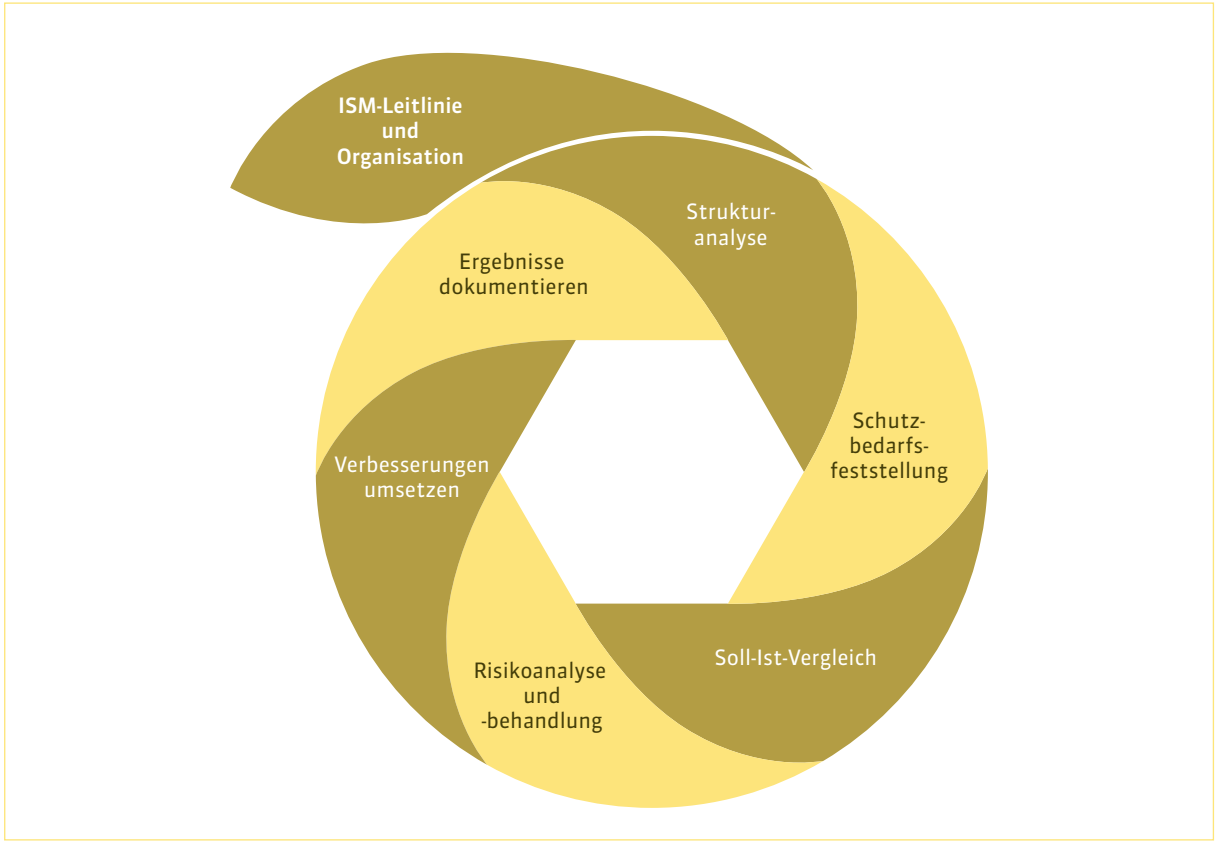

Abb.: Informationssicherheitsmanagement-System

INFORMATION SECURITY MANAGEMENT SYSTEM

Daten sind Chefsache

Der Schutz der Unternehmens-Daten und der personenbezogenen Daten von Kunden und Mitarbeitern ist existentiell für ein Unternehmen. Geschäftsprozesse sind immer stärker von IT-Services abhängig. Damit werden die Anforderungen an den IT-Betrieb oder einen IT-Dienstleister hinsichtlich der Verfügbarkeit dieser Services immer höher.

Gleichzeitig steigen auch die Anforderungen an die Vertraulichkeit und Integrität der hier verarbeiteten Daten. Kommt es hier und auch bezüglich der Datenverfügbarkeit zu Defiziten, kann das zu erheblichen finanziellen Verlusten führen und die Reputation eines Unternehmens im Markt und gegenüber den Kunden nachhaltig schädigen.

Sichern Sie sich ab und managen Sie die Anforderungen an die Informationssicherheit Ihres Unternehmens! Bringen Sie Rechtssicherheit und Standards in Ihr Unternehmen und machen Sie Ihr Informationssicherheitsmanagement (ISM) messbar.

SVA hilft Ihnen, Ihr ISM mit dem Risikomanagement und Ihrem internen Kontrollsystem zu verzahnen und ebnet gemeinsam mit Ihnen den Weg für Ihr eigenes, funktionales ISM als integralen Bestandteil Ihres unternehmensweiten Risikomanagements.

Wir beraten Sie bei Einführung eines ISM nach ISO 27001 und BSI 100-1 bis -3. Unsere langjährige Erfahrung in komplexen IT-Infrastrukturen und -Services unterstützt Sie dabei.

PERIMETER & ENDPOINT SECURITY

Firewall, Intrusion Prevention, Virtual Private Networks, Anti-Virus/Anti-Malware

In den letzten Jahren sind Unternehmens-Firewalls die Grundlage von Perimeter-Sicherheitsarchitekturen geworden. Hauptsächlich für die Steuerung des Zugriffs auf Netzwerkressourcen entwickelt, können Firewalls erfolgreich die überwiegende Mehrheit der Netzwerkangriffe verhindern, sofern Sicherheitsrichtlinien korrekt definiert und durchgesetzt wurden. Viele dieser Lösungen sind jedoch nicht in der Lage, Angriffe auf Anwendungsebene zu erkennen und zu vereiteln.

Diese Realität erkennend wurden Attacken entwickelt, um die traditionellen Zugriffsrichtlinien von Perimeter-Firewalls zu umgehen. Heutige sachkundige Angreifer haben ihre Suche nach offenen Ports auf Firewalls erweitert und attackieren nun direkt und gezielt Anwendungen.

Die Abwehr dieser aktuellen und vielfältigen Bedrohungen führt zu neuen Sicherheitslösungen, Anbietern und Hardware sowie einer zunehmenden Komplexität. Gleichzeitig hat sich durch die Mobilität der Anwender der Schutzbedarf Ihrer IT verlagert: Mitarbeiter arbeiten inner- und außerhalb des Unternehmens, wodurch die Grenzen ihrer IT-Umgebung aufgeweicht und deshalb neu betrachtet werden müssen.

Stellen Sie sich neuen Strategien bei der Sicherung Ihrer Netzwerkgrenzen, Anbindungen von Außenstellen und Partnern sowie dem Schutz der Endgeräte! Viren und Malware sind sich ständig evolvierende Bedrohungen, die nicht mehr allein durch Signaturen zu entdecken sind und daher neue Techniken und Strategien zum effektiven Schutz fordern.

SVA unterstützt Sie bei der Auswahl und Integration der für Ihre Umgebung relevanten Lösungen und berät Sie über die Möglichkeiten des erhöhten Schutzes Ihrer IT - inklusive der virtuellen Umgebungen.

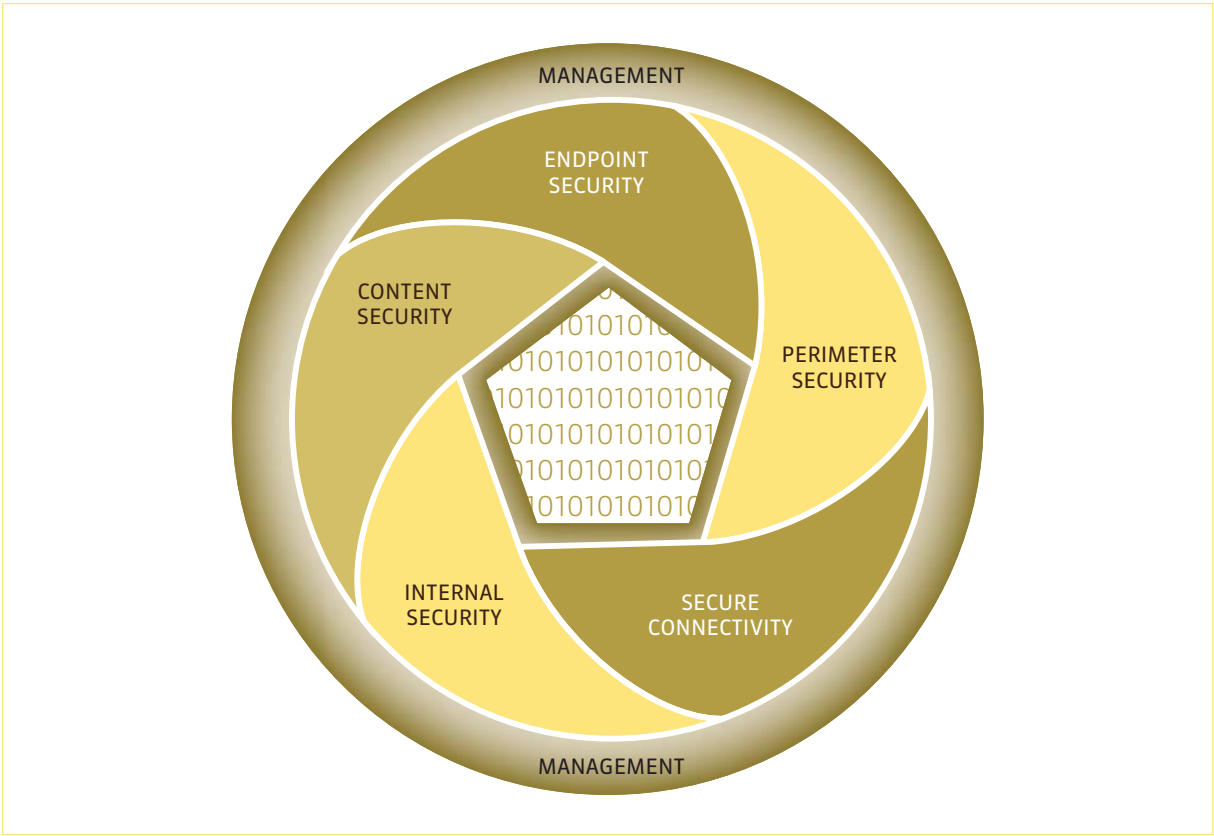

Abb.: Perimeter & Endpoint Security

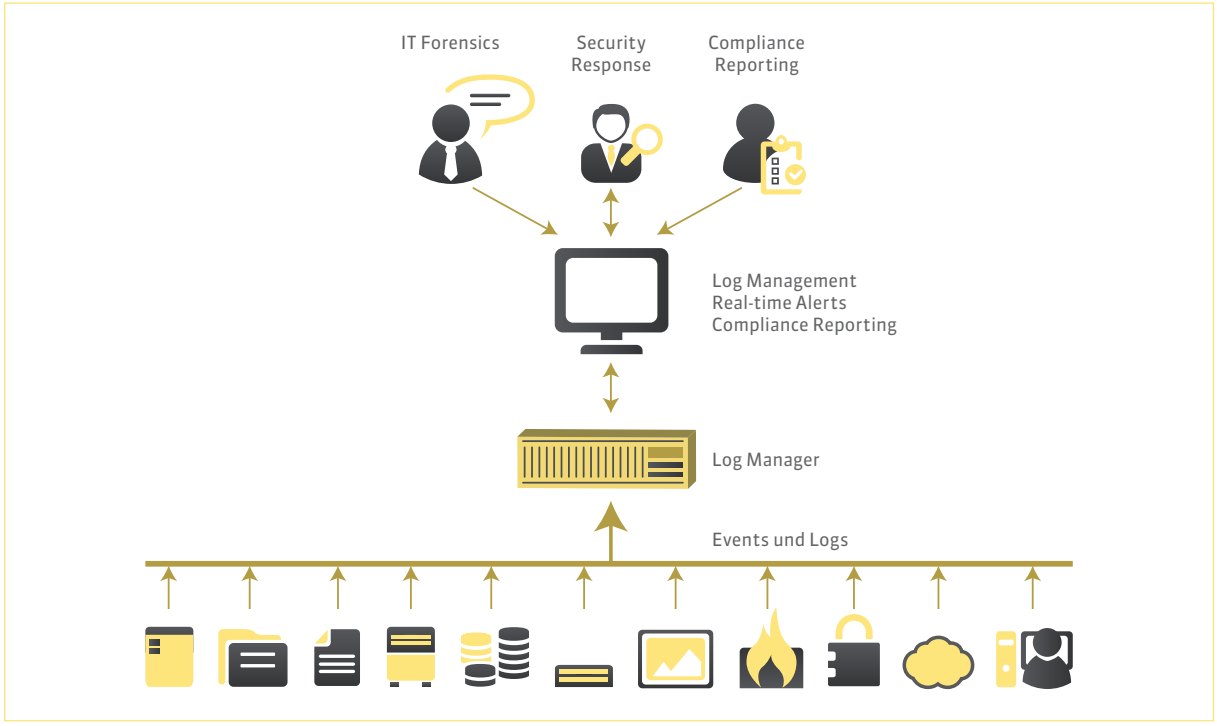

Abb.: IBM Security Intelligence QRadar

SECURITY INTELLIGENCE

Intelligentes Sicherheitsmanagement – auf Sicherheitslücken in Echtzeit reagieren mit IBM QRadar

Die heutigen komplexen Netzwerke sind nicht nur immer stärker von Internet-basierten Bedrohungen und Online-Betrug betroffen. Verstärkt treten Probleme durch die ständige Zunahme von Insider-Diebstählen auf, bei denen Mitarbeiter wertvolle Unternehmensinformationen entwenden.

Häufig ist es schwer, effiziente Schutzmaßnahmen in kurzer Zeit umzusetzen und in die Unternehmens-IT zu integrieren. Es bleibt oft wenig Zeit zum Testen und somit entstehen bei der Absicherung häufig neue Sicherheitslücken, da zentrale Fragen und Aufgaben nicht geklärt werden:

- Was sind Ihre Risiken und wo liegen die Prioritäten (Risk-Management)?
- Wie werden die Informationen Ihrer Security-Lösungen gebündelt und ausgewertet?
- Werden Angriffe erkannt? Wie können Sie darauf in Echtzeit reagieren?

IBM SECURITY INTELLIGENCE QRADAR

ist eine SIEM-Lösung (Security Information & Event Management), die isolierte Informationen konsolidiert und es somit ermöglicht, komplexe Bedrohungen effektiver zu erkennen und wirksamer zu bekämpfen. Durch Normalisierung und Korrelation der Informationen erhalten Unternehmen schnell die nötigen Erkenntnisse, um Bedrohungen identifizieren und behandeln zu können, die von anderen Sicherheitslösungen mit isolierter Sichtbarkeit nicht gefunden werden.

Mit kontextuellen, praxisrelevanten Kontrollen für die gesamte IT-Infrastruktur ermöglichen SVA und QRadar Ihrem Unternehmen die Ermittlung und Beseitigung von Bedrohungen, die bei Millionen von Ereignissen unerkannt bleiben könnten – wie etwa die vorschriftswidrige Nutzung von Anwendungen und Insider-Betrug.

SECURING BIG DATA

Datenbanksicherheit und Überwachung in Echtzeit – Herausforderungen durch Big Data beherrschen mit IBM Guardium

Je größer das in Unternehmen entstandene und gespeicherte Volumen digitaler Informationen wird, desto schwerer fällt es, sensible Informationen aufzufinden und zu klassifizieren. Dies stellt insbesondere jene Unternehmen vor große Herausforderungen, die Fusionen und Akquisitionen bewältigt haben oder IT-Umgebungen mit Altsystemen betreiben, die bereits ihre Entwickler überdauert haben. Änderungen an Anwendungs- und Datenbankstrukturen, die durch neue geschäftliche oder rechtliche Anforderungen notwendig sind, können dazu führen, dass sensible Daten nicht als solche erkannt werden und daher ungeschützt bleiben.

Datenbanken speichern große Mengen kritischer Daten – Big Data. Alles wird in Datenbanksystemen abgelegt: Von Finanzinformationen oder Intellectual Property in ERP-Systemen über Kundendaten in CRM- oder webbasierten Anwendungssystemen bis hin zu Patientendaten.

Unternehmen fällt es insbesondere schwer,

- alle Datenbankserver zu erkennen, die sensible Informationen enthalten, und zu verstehen, wie auf diese zugegriffen wird (Anwendungen der Geschäftsbereiche, Batchprozesse, Ad-hoc-Abfragen, Anwendungsentwickler, Administratoren usw.).
- Informationen abzusichern und Risiken zu bewerten, wenn die Sensibilität der gespeicherten Informationen unbekannt ist.
- die Einhaltung gesetzlicher Vorgaben zu gewährleisten, wenn nicht klar ist, welche Informationen welchen Regularien unterliegen.

Mit IBM GUARDIUM und SVA Services steht ein optimales Konzept für Big Data Security zur Verfügung:

- Echtzeit-Datenbankschutz, Monitoring & Compliance
- Echtzeit-Maßnahmen bei verdächtigen und verhaltensabhängigen DB-Zugriffen
- Compliance auditieren und validieren: Vereinfachung der Compliance-Prozesse für Basel II/III, SOX, PCI-DSS Richtlinien oder der Prozesse des Datenschutzes um Compliance-Anforderungen zu erfüllen

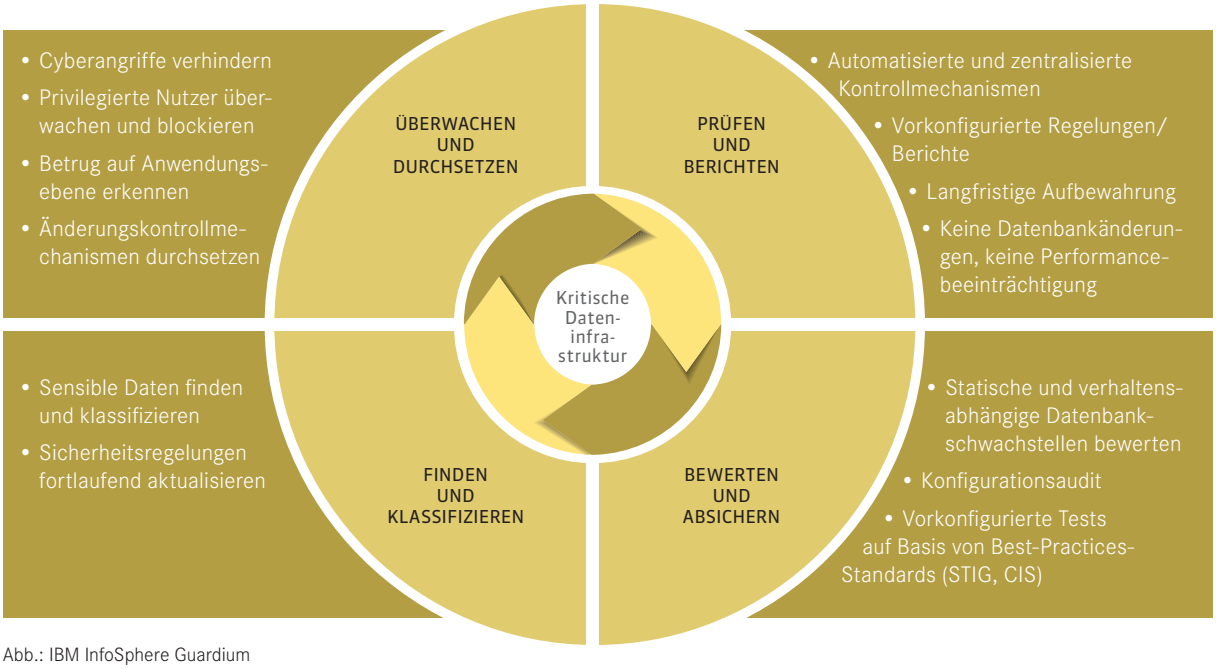

Abb.: IBM InfoSphere Guardium

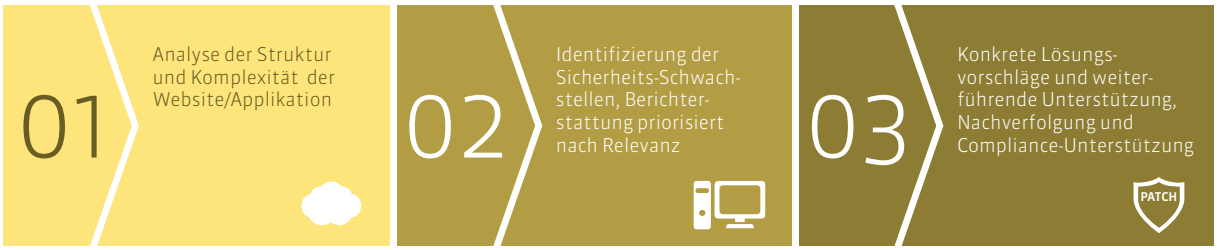

Abb.: IBM AppScan Workflow

SCHWACHSTELLENANALYSE

Automatisierte statische und dynamische Tests zur Anwendungssicherheit mit IBM AppScan

Viele Webanwendungen enthalten Schwachstellen, die durch Hacker ausgenutzt werden können. Obwohl das Bundesamt für Sicherheit in der Informationstechnologie (BSI) schon 2006 einen Maßnahmenkatalog zur Absicherung von Webanwendungen veröffentlicht hat, gestaltet sich die Umsetzung für viele Unternehmen als schwierig. Denn zum einen sind heutige Webanwendungen in der Regel komplexe und dynamische Anwendungssysteme und zum anderen entwickeln viele Unternehmen die Webanwendungen nicht selbst, sondern beauftragen dafür externe Dienstleister.

Dabei können laut einer Statistik des Web Application Security Consortium (WASC) etwa 75 % der kritischen Schwachstellen durch einen automatischen Vulnerability Scan (Blackbox-Test) erkannt und die Ursachen für Schwachstellen identifiziert werden. Wir unterstützen Sie gerne mit Hilfe eines automatischen Blackbox-Tests.

IBM SECURITY RATIONAL APPSCAN

ist das optimale Werkzeug zur Überprüfung der Sicherheit von Webanwendungen durch automatisierte Schwachstellenanalysen bzw. -Scans. Die Software liefert intelligente Empfehlungen in Form von Reports zur Analyse und Korrektur von Schwachstellen, die während des Suchlaufs (Scan) identifiziert wurden. Zusätzlich wird eine priorisierte To-Do-Liste zur Behebung der identifizierten Schwachstellen zur Verfügung gestellt.

IBM Rational AppScan wird vor allem während des Entwicklungszyklus von Webapplikationen angewandt, um Schwachstellen bereits früh im Prozess zu finden.

- Umfassende Scan-Abdeckung (geringste False-Positive Rate in der Industrie)
- Erprobte und sinnvolle Korrekturempfehlungen
- Integriert Sicherheitsüberprüfungen im Entwicklungsprozess
- Fehleranalyse als Produkt oder Service
- Reduziert Kosten für manuelle Sicherheitstests

SVA System Vertrieb Alexander GmbH | Borsigstr. 14 | 65205 Wiesbaden | +49 6122 536-0 | mail@sva.de

DIE SVA GMBH ist einer der führenden System-Integratoren Deutschlands im Bereich Datacenter-Infrastruktur und beschäftigt mehr als 320 Mitarbeiter an 13 Standorten. Das unternehmerische Ziel der SVA ist es, hochwertige IT-Produkte der jeweiligen Hersteller mit dem Projekt-Know-how, den Dienstleistungen und der Flexibilität von SVA zu verknüpfen, um so optimale Lösungen für die Kunden zu erzielen. Kernthemen des Unternehmens sind:

- Hochverfügbarkeits-Architekturen
- Datensicherung und Disaster Recovery
- Storage Area Networks
- Virtualisierungs-Lösungen im Server-, Desktop- und SAN-Umfeld
- Informationssicherheit
- IT-Service Management
- Software Consulting
- On-Site und Remote Services

SVA hat die wichtigsten Zertifizierungsstufen u. a. bei folgenden Herstellern erreicht: HDS, IBM, NetApp, VMware, Citrix, Microsoft und Hewlett-Packard.

Das SVA Security-Portfolio wird mit den Lösungen folgender Hersteller abgerundet: IBM, Check Point, Blue Coat, Trend Micro, Qualys, GRC Partner, baramundi, MobileIron und SafeNet.

Das zertifizierte „System Storage Solution Center“ der SVA in Wiesbaden bietet SVA Experten und Kunden umfassende Demonstrations-, Entwicklungs- und Schulungs-Szenarien mit allen aktuellen Hardware- und Software-Lösungen der Hersteller.

KONTAKT

Sascha Hartwich
Tel. +49 6122 536-329
Mobil: +49 151 18025704
Sascha.Hartwich@sva.de