noris network

Security Information and Event Management
SIEM und was dann?

12. Februar 2021

IT-Sicherheit
Made in Germany

Agenda

noris network

Teil 1: Standortbestimmung

- **SIEM – Was ist das ?**
- **Warum ist SIEM wichtig ?**
- **Was leistet ein modernes SIEM Tool ?**
- **CERT - SOC – SIEM ?**

Teil 2: SIEM und was dann?

- **IT-Strukturanalyse**
- **Schutzbedarfsfeststellung**
- **Schwachstellenanalyse**
- **Bedrohungsmatrix**
- **Definition Use-Cases**
- **Definition Incident Response Process**

Standortbestimmung # SIEM – Was ist das?

Security Information Management (SIM)

Sammeln von LOG Dateien aus unterschiedlichsten Quellen

Security Event Management (SEM)

Korrelation der LOG Dateien anhand definierter Richtlinien

Security Information and Event Management (SIEM)

Ziel:
Anhand eines Regelwerks kontinuierlich die Standards für Sicherheit und Compliance des IT Betriebs zu verbessern

Gesetzeslage kennen

IT-Verantwortlichen und Business-Entscheidern muss klar sein, warum ein SIEM-System notwendig ist.
In Deutschland machen Gesetze und Compliance-Vorschriften ein solches System unverzichtbar.

Für Banken und Unternehmen ergeben sich die Compliance-Vorgaben auf Basis unterschiedlicher gesetzlicher Regelwerke:

- Mindestanforderungen an das Risikomanagement (MaRisk)
- BAIT (Bankaufsichtliche Anforderungen an die IT herausgegeben von der BaFin)
- KAMaRISK (Mindestanforderungen an das Risikomanagement von Kapitalgesellschaften)
- PCI-DSS (Payment Card Industry Data Security Standard)
- Datenschutzgesetze (Datenschutz-Grundverordnung, Telemediengesetz)
- ISO/IEC-Standards der 2700x-Reihe (Reihe von Standards zur Informationssicherheit)
- BSI IT Grundschutz

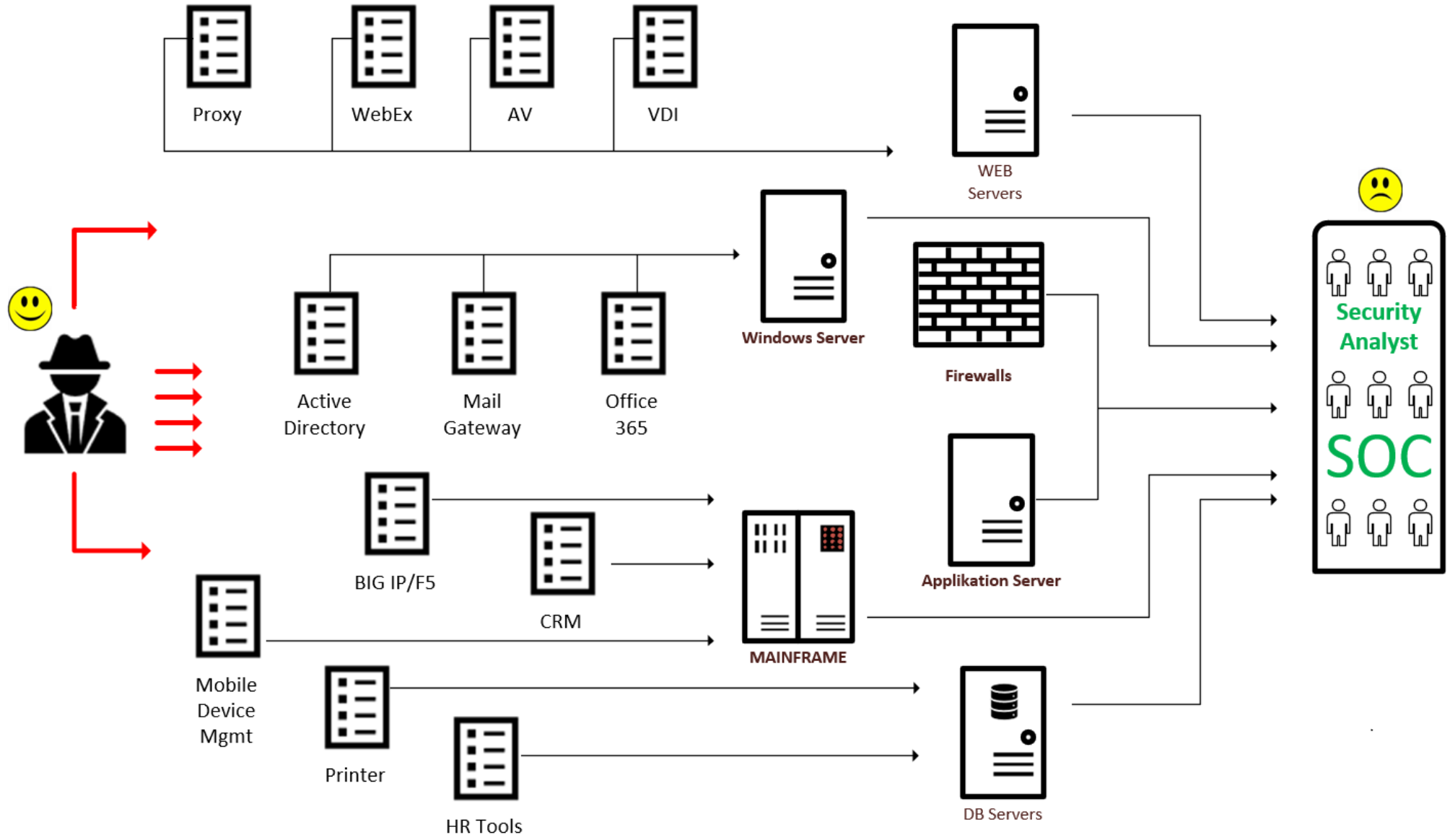
- §91 Abs. 2 AktG (Früherkennung von Risiken);
- §43 Abs. 1 GmbHG (Sorgfaltspflichten);

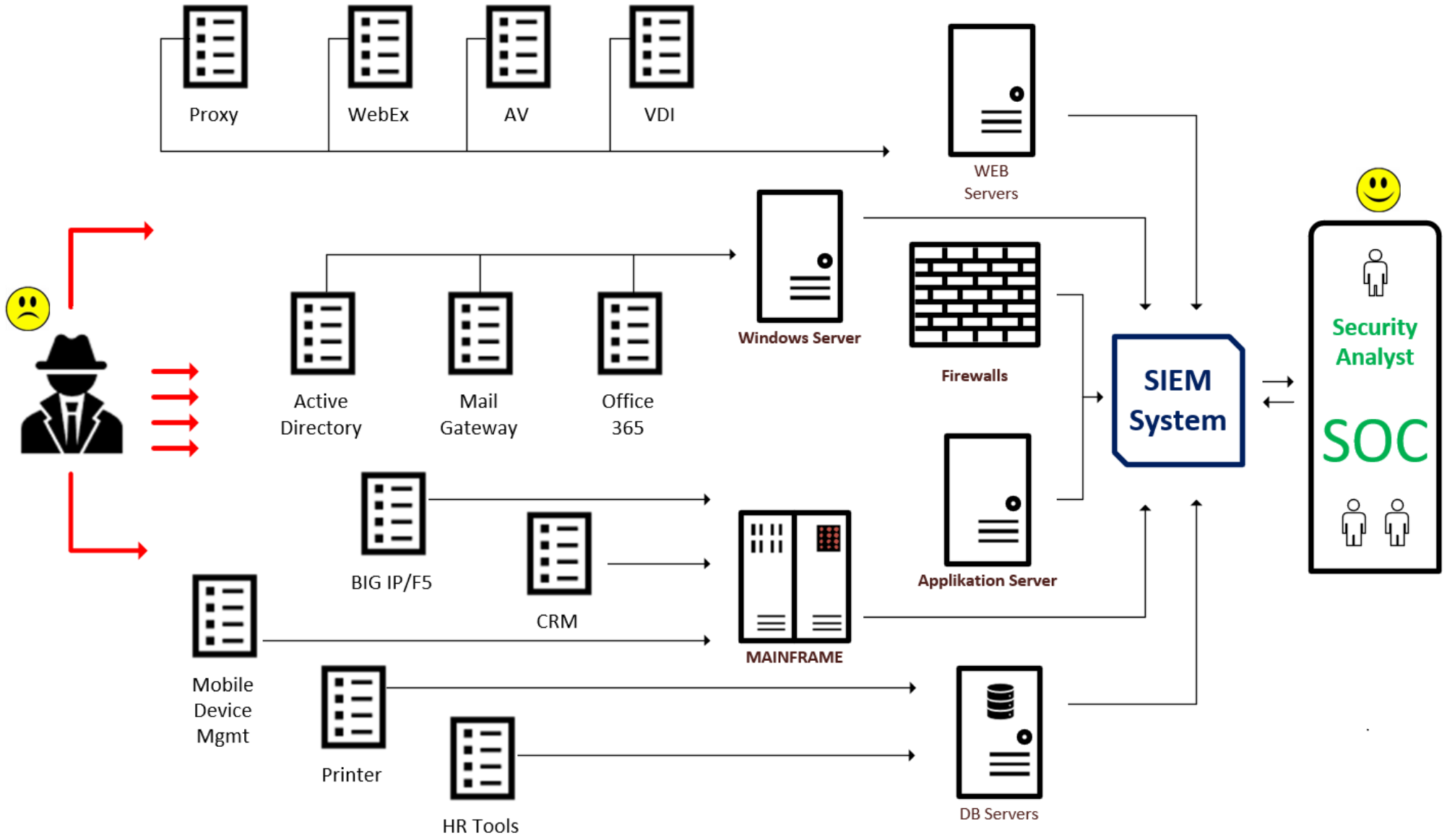
Standortbestimmung # Was leistet ein modernes SIEM Tool?

noris network

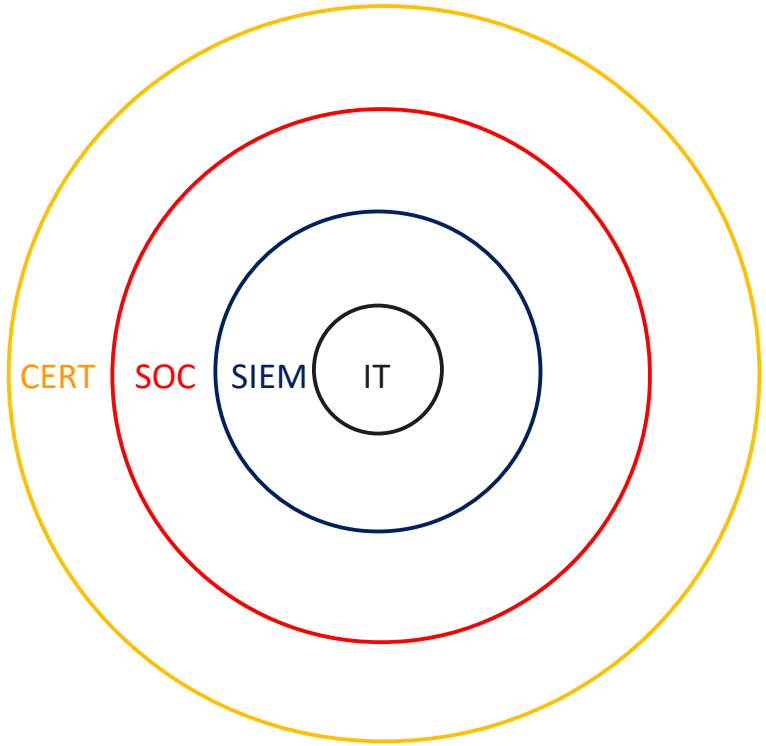
1. **Es sammelt und analysiert Daten aus unterschiedlichsten Quellen in Echtzeit**
   - Einschließlich Cloud und On Premise Protokolldaten
2. **Die Integration mit anderen (Sicherheits)-Lösungen ist möglich.**
   - Das SIEM-Produkt kann andere Sicherheitslösungen im Unternehmen veranlassen, Aktionen auszuführen, um Angriffe zu verhindern oder stoppen
3. **Es nutzt maschinelles Lernen, um durch Kontext- und Situationsbewusstsein die Effizienz zu steigern**
   - UBA (User Behavior Analytics), UEBA (User and Entity Behavioral Analytics) => Stakeholder müssen mit einbezogen werden (z.B. Betriebsrat)
4. **Es bietet verbesserte Instrumente für Untersuchungen und Reaktionen auf Vorfälle inkl. umfassender Berichtsmöglichkeiten**
   - Verbesserung der Entscheidungsfindung und Verkürzung der Reaktionszeit
   - Idealerweise mit vorgefertigten Dashboards und Berichtsvorlagen für gängige Compliance-Anforderungen
5. **Es macht Sicherheitsanalysten produktiver**
   - Bereitstellung von Anwendungsfällen (Use-Cases) durch das SIEM System
   - Verbesserte Automatisierung befreit Analysten von manuellen Aufgaben
6. **Forensische Fähigkeiten !!!**
   - Es können zusätzliche Informationen über Sicherheitsereignisse erfasst werden, die im Fall eines wirklichen Vorfalls bei der nachträglichen Betrachtung, Analyse und ggf. Strafverfolgung durch die Justiz helfen.
   - Hierzu gehört auch die Vorhaltung von revisionssicheren und manipulationsgesicherten Log- und Protokolldaten über einen längeren Zeitraum.

Standortbestimmung # Security Monitoring ohne SIEM




Proxy
WebEx
AV
VDI
WEB Servers
Windows Server
Active Directory
Mail Gateway
Office 365
Firewalls
SIEM System
Security Analyst
SOC
BIG IP/F5
CRM
MAINFRAME
Applikation Server
Mobile Device Mgmt
Printer
HR Tools
DB Servers

Standortbestimmung # CERT – SOC – SIEM



CERT (Computer Emergency Response Team)

- CERTs erfassen, beurteilen, reagieren und detektieren Sicherheitsvorfälle oder Berichte
- Sind Experten-Teams bestehend aus erfahrenen Analysten mit einer festen Zuordnungen zu einer Organisation
- Nutzen Foren und Kommunikationsnetzwerke um sich mit anderen CERTs auszutauschen und andere Betroffene zu warnen

SOC (Security Operation Center)

- Damit CERTs Ihre Hautaufgaben nachkommen können und sich möglichst mit wenigen false-positive Meldungen beschäftigen müssen, arbeiten diese Teams häufig nicht direkt mit einem SIEM-System
- Aus diesem Grund wird in größeren Organisationen eine Verarbeitungsstruktur um das eigentliche SIEM-System gebildet
- SOCs stellen diese zentralisierte Verarbeitungsstruktur dar und sind meist hierarchisch gegliedert
  - **Stufe 1** Vorsortierung der eingehenden Alarme für eine eindeutige Analyse (false positive / negative)
  - **Stufe 2** Durchführung der Analyse des Sicherheitsvorfalls und Aufbereitung der Daten für Stufe 3
  - **Stufe 3** Beurteilung von Umfang und Auswirkungen des detektierten Sicherheitsvorfalls und Einleitung weitere Maßnahmen => **Security Response Team**

Vgl. hierzu Arne Thiele: Security Information and Event Management Systems, 2019

Agenda

noris network

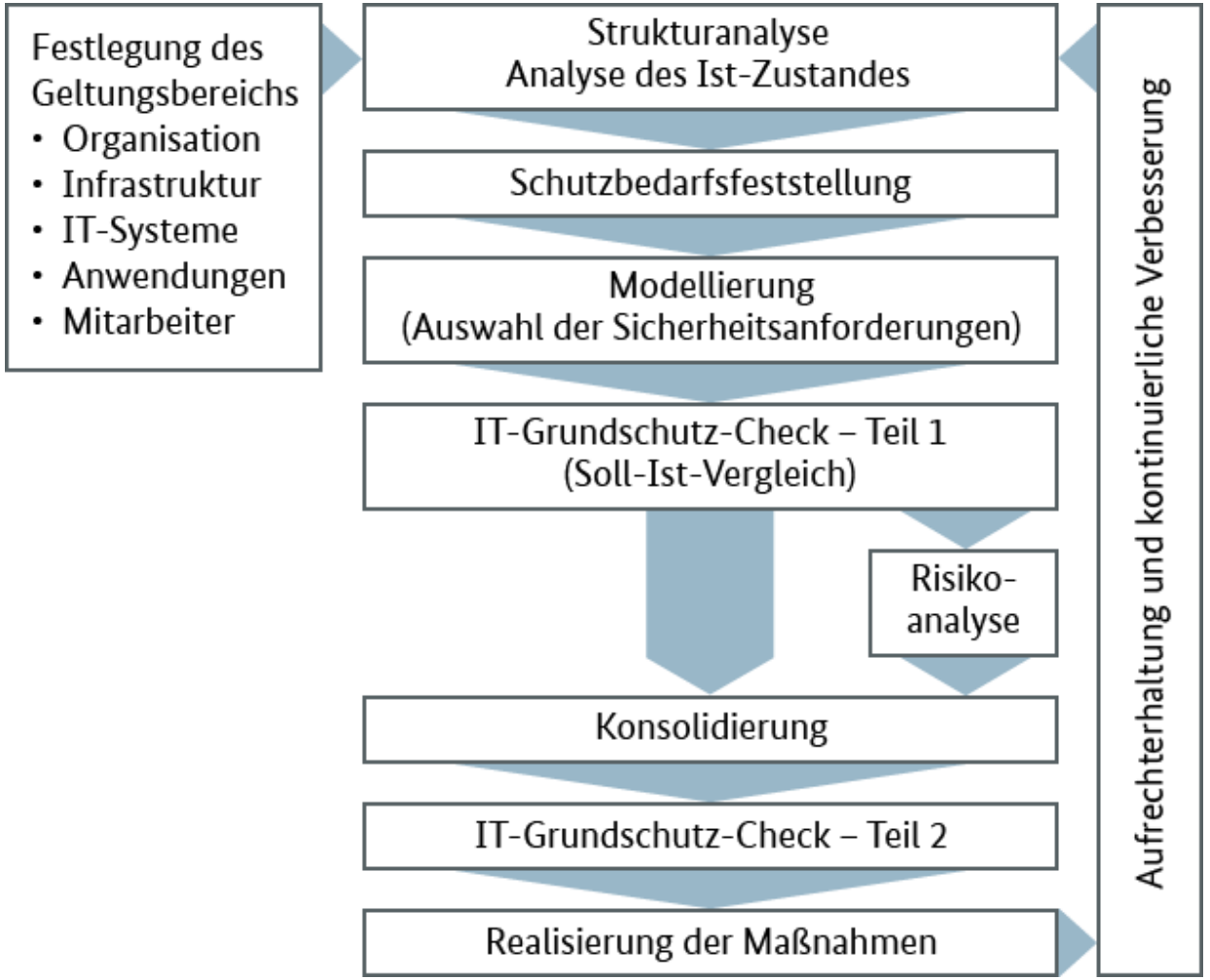
Teil 1: Standortbestimmung

- SIEM – Was ist das?
- Warum ist SIEM wichtig?
- Was leistet ein modernes SIEM Tool?
- CERT - SOC - SIEM - IDS ?

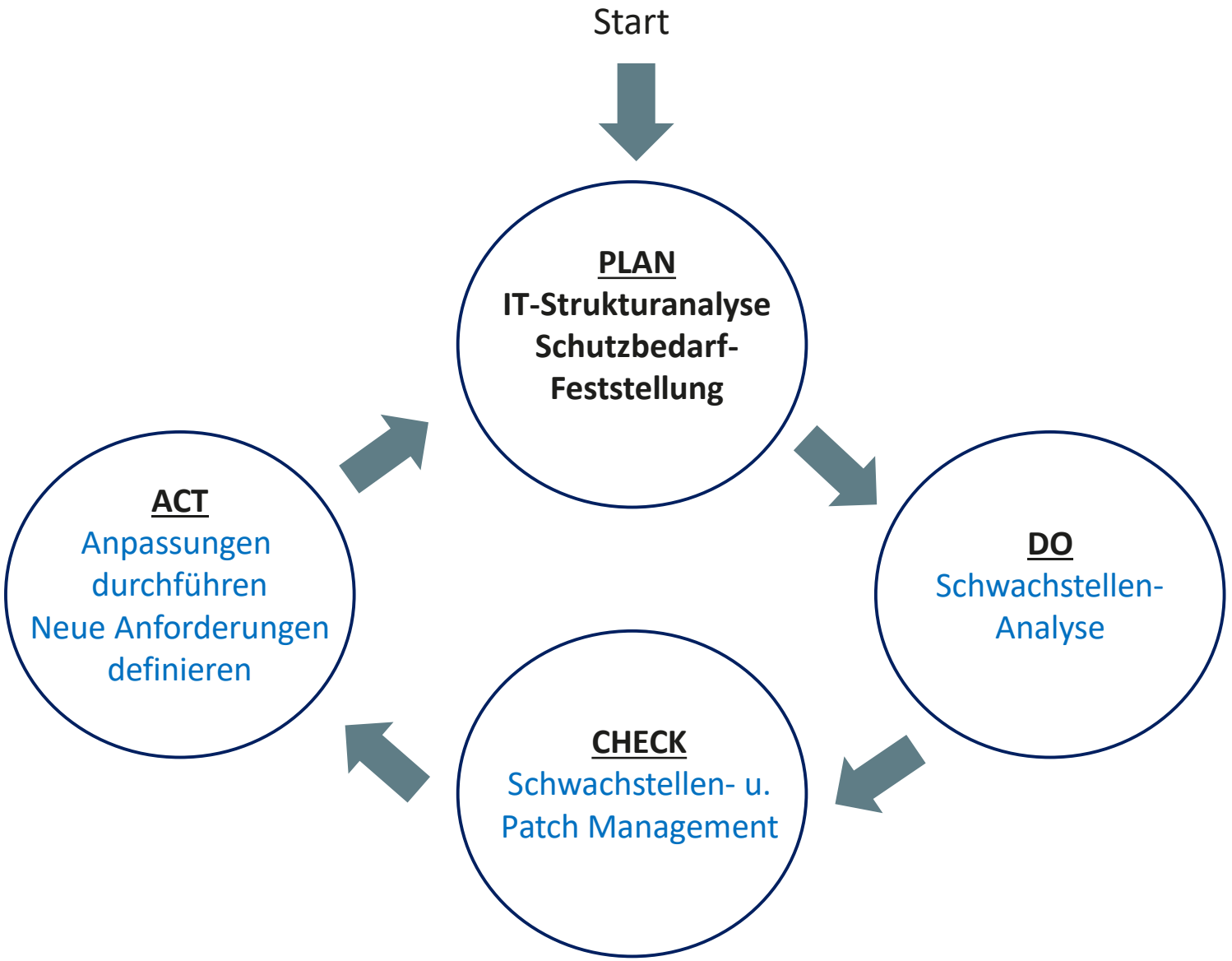
Teil 2: SIEM und was dann?

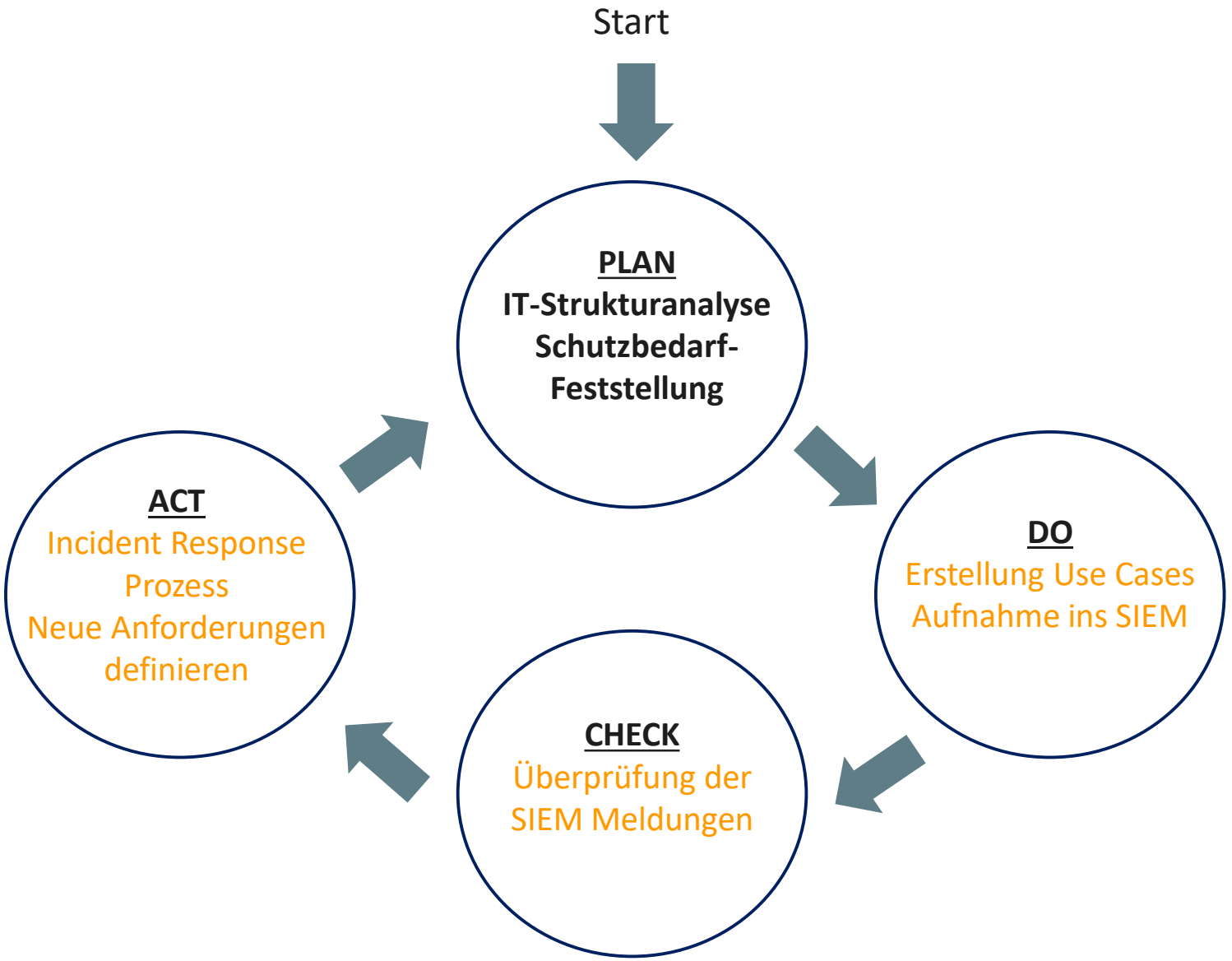
- **IT-Strukturanalyse**
- **Schutzbedarfsfeststellung**
- **Schwachstellenanalyse**
- **Bedrohungsmatrix**
- **Definition Use-Cases**
- **Definition Incident Response Process**

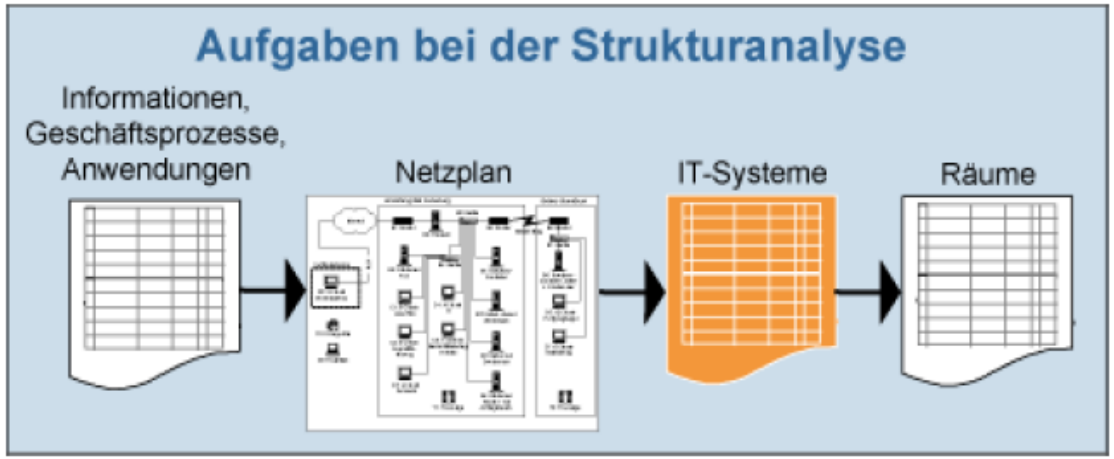
Erstellung der Sicherheitskonzeption im Informationssicherheitsmanagement

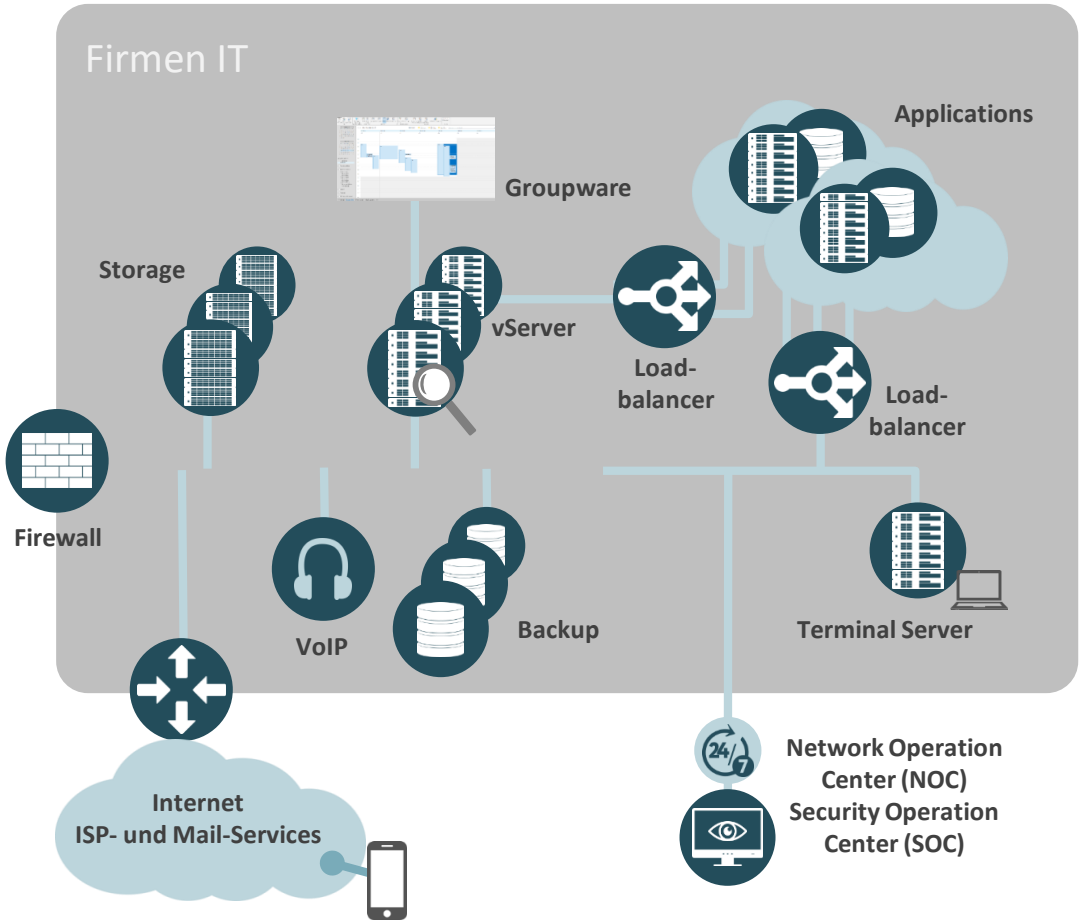


Vgl. hierzu BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise, S 36 ff


Start
PLAN
IT-Strukturanalyse
Schutzbedarf-
Feststellung
DO
Schwachstellen-
Analyse
CHECK
Schwachstellen- u.
Patch Management
ACT
Anpassungen
durchführen
Neue Anforderungen
definieren


Start
PLAN
IT-Strukturanalyse
Schutzbedarf-
Feststellung
DO
Erstellung Use Cases
Aufnahme ins SIEM
CHECK
Überprüfung der
SIEM Meldungen
ACT
Incident Response
Prozess
Neue Anforderungen
definieren



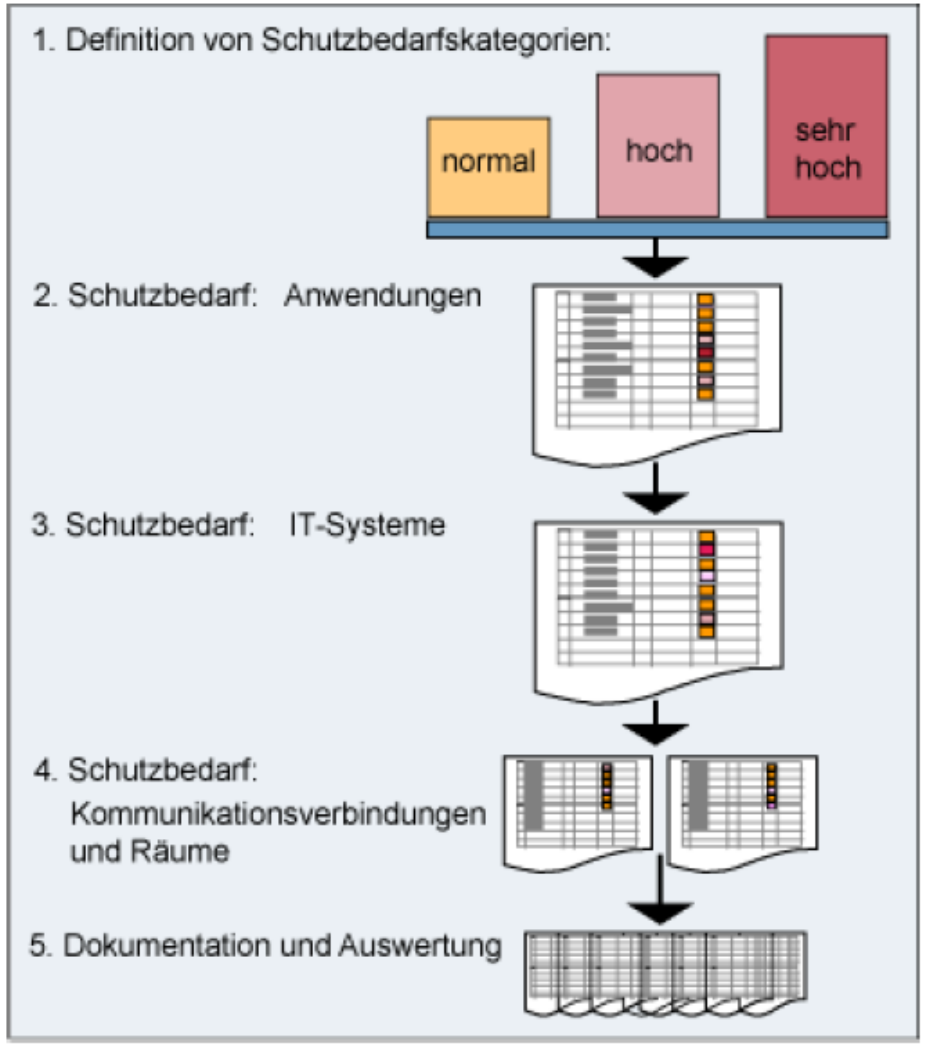


Vgl. hierzu Bundesamt für Sicherheit in der Informationstechnik (BSI): Webkurs IT-Grundschutz, S. 36 ff.

SIEM und was dann? # Welche IT Systeme und Anwendungen?

noris network

IT-System	Anwendung
Firewall (außen)	IDS, IPS, AV, Packetfilter
Firewall (innen)	Application Controll
DMZ Switch	-
Switch 1 von x	-
Core Switch	-
Domain Controller	AD, DNS, DHCP, AV
Mailserver	AV und Anti-Spam
Fileserver	AV
Anwendungsserver 1	WSUS, AV
Anwendungsserver 2	ERP
Datenbank Server	DBMS
Webserver DMZ	Apache
…	…



Schutzbedarfskategorien (nach Kritikalität)

- **normal**: Die Schadensauswirkungen sind begrenzt und überschaubar.
- **hoch**: Die Schadensauswirkungen können beträchtlich sein.
- **sehr hoch**: Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

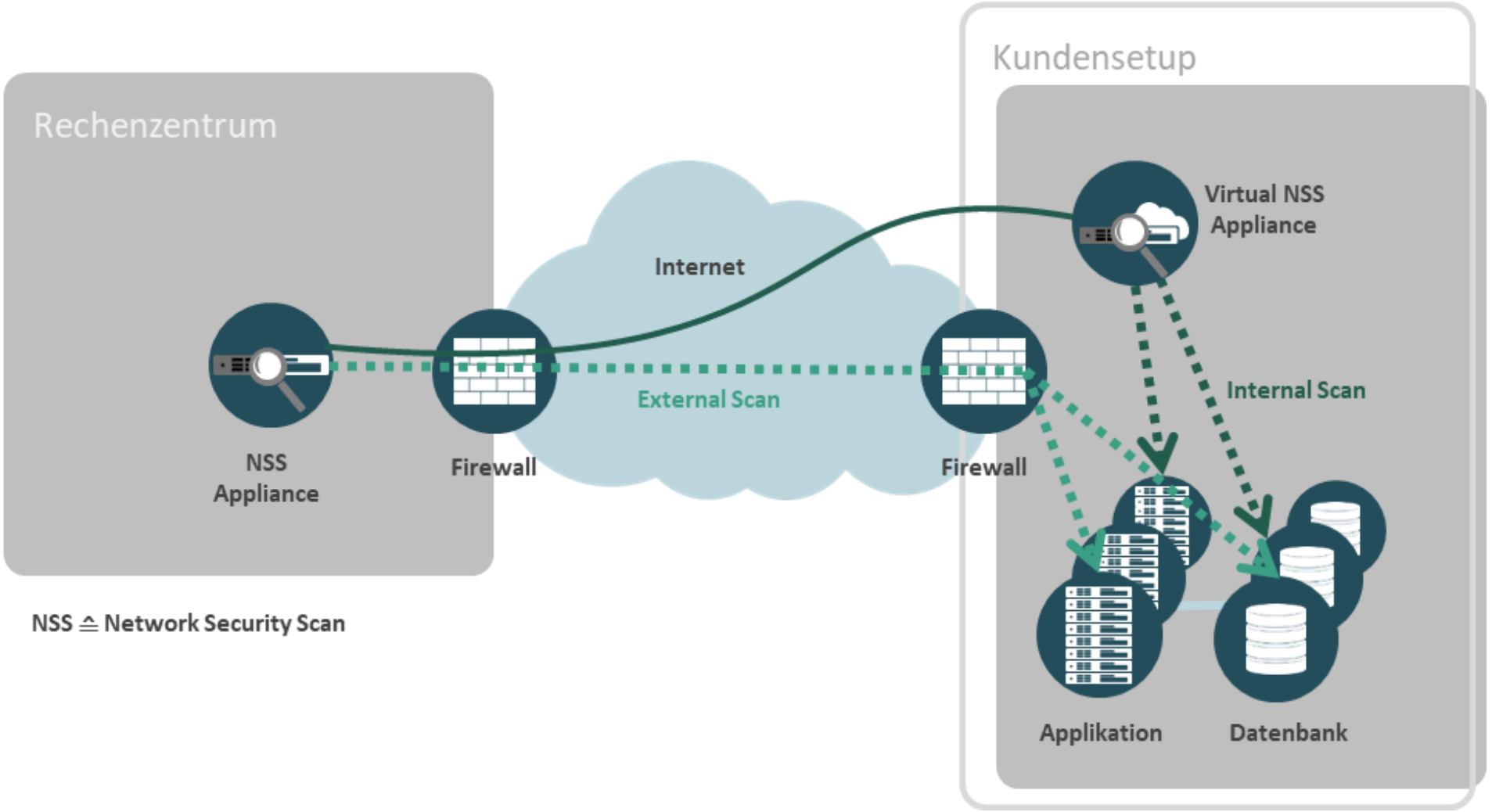
Schutzziele und Grundwerte

Bei der Schutzbedarfsfeststellung ist danach zu fragen, welcher Schaden entstehen kann, wenn die **Grundwerte** Vertraulichkeit, Integrität oder Verfügbarkeit eines Objekts verletzt werden, wenn also

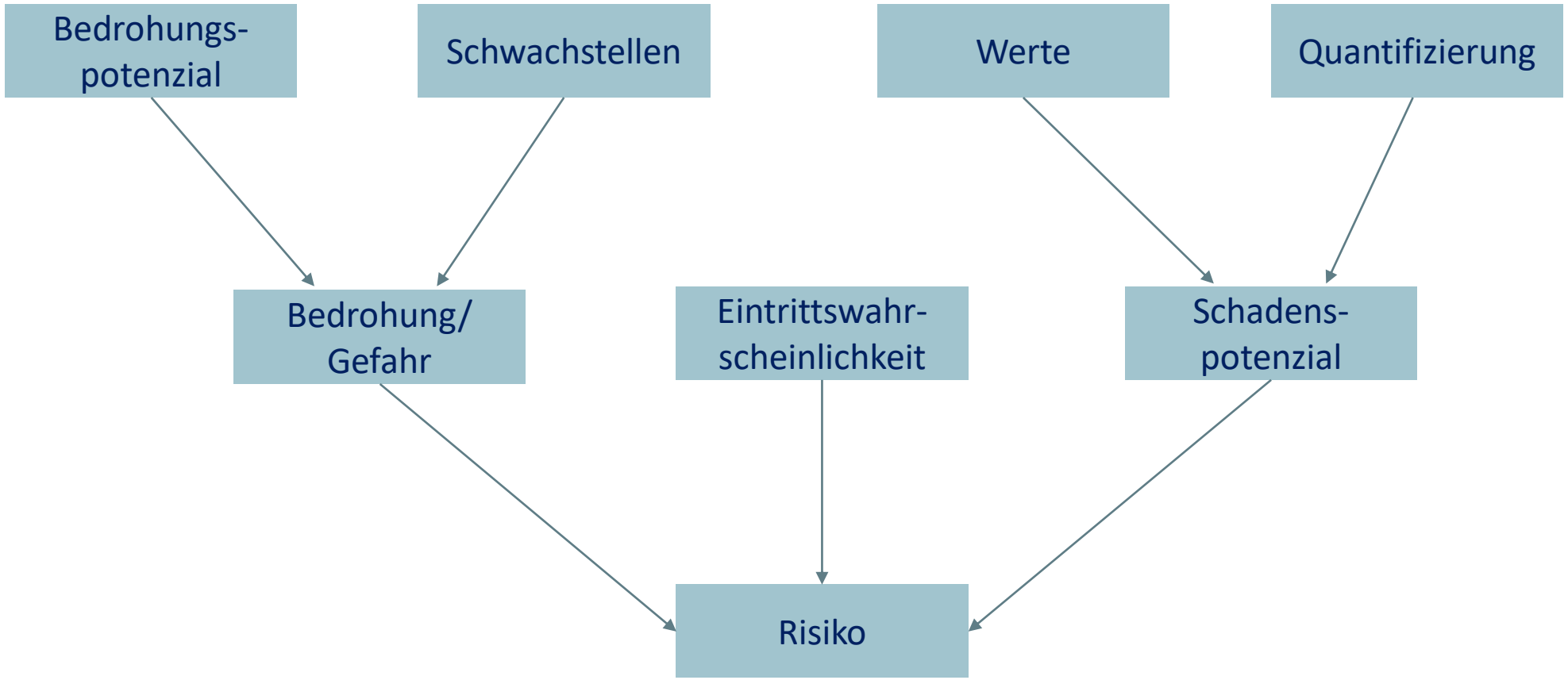
- vertrauliche Informationen unberechtigt zur Kenntnis genommen oder weitergegeben werden (Verletzung der **Vertraulichkeit**)
- die Korrektheit der Informationen und der Funktionsweise von Systemen nicht mehr gegeben ist (Verletzung der **Integrität**)
- autorisierte Benutzer am Zugriff auf Informationen und Systeme behindert werden (Verletzung der **Verfügbarkeit**).

Vgl. hierzu Bundesamt für Sicherheit in der Informationstechnik (BSI): Webkurs IT-Grundschutz, S. 42 ff.

IT-System	Anwendung	Integrität	Vertraulichkeit	Verfügbarkeit	Schutzbedarf
Firewall (außen)	IDS, IPS, AV, Packetfilter	Hoch	Hoch	Sehr hoch	Sehr hoch
Firewall (innen)	Application Controll	Hoch	Hoch	Sehr hoch	Sehr hoch
DMZ Switch	-	Hoch	Hoch	Sehr hoch	Sehr hoch
Switch 1 von x	-	Hoch	Hoch	Sehr hoch	Hoch
Core Switch	-	Hoch	Hoch	Sehr hoch	Hoch
Domain Controller	AD, DNS, DHCP, AV	Hoch	Hoch	Sehr hoch	Hoch
Mailserver	AV und Anti-Spam	Hoch	Hoch	Normal	Hoch
Fileserver	AV	Hoch	Hoch	Sehr hoch	Sehr hoch
Anwendungsserver 1	WSUS, AV	Hoch	Hoch	Sehr hoch	Normal
Anwendungsserver 2	ERP	Hoch	Hoch	Sehr hoch	Hoch
Datenbank Server	DBMS	Normal	Normal	Normal	Hoch
Webserver DMZ	Apache	Hoch	Hoch	Sehr hoch	Normal
…	…	…	…	…	



NSS ≙ Network Security Scan


Bedrohungs-
potenzial
Schwachstellen
Werte
Quantifizierung
Bedrohung/
Gefahr
Eintrittswahr-
scheinlichkeit
Schadens-
potenzial
Risiko

Risikonummer	Risikobeschreibung	Risikoklasse	Abgedeckt durch Use-Case	Use-Case-Nr.
R01	abc …	Gering	abc …	1, 2
R02	abc …	Mittel	abc …	3, 4, 5
R03	abc …	Hoch	abc …	7, 8
…				

Home Office User

- Host-Kompromittierung
- Lizenz- und Compliance-Überwachung
- Überwachung von Geräten zur VPN- und Remote-Authentifizierung

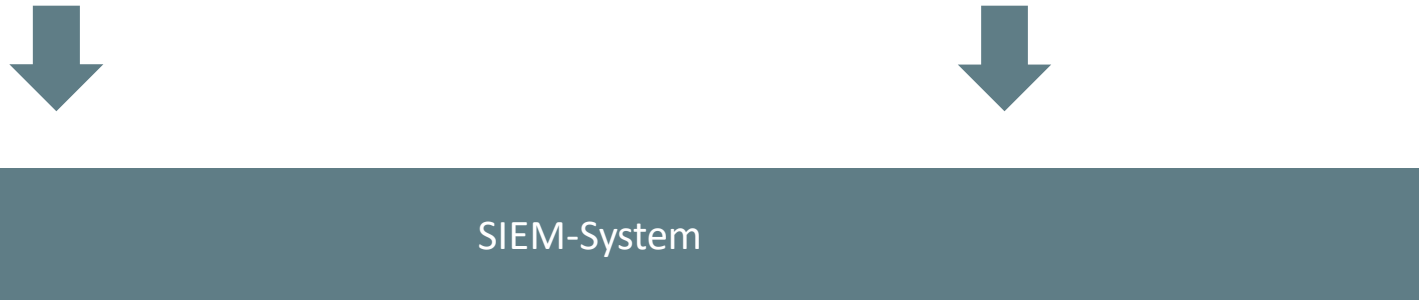
SSL VPN

- Überwachung von Insider-Bedrohungen
- Überwachung auf Phishing- und Fake Kampagnen
- Verdächtige Logins und Konten-Kompromittierung
- Sicherheitsüberwachung bei Cloud-Anwendungen

Firmen IT

Vgl. hierzu: „Die Top 10 der Anwendungsfälle im Bereich SIEM“, it-daily.net vom 28.04.2020

Nr.	Schritte	Ergebnisse
1	IT Strukturanalyse	Alle IT-Systeme und Anwendung sind erfasst
2	Schutzbedarfsfeststellung	Schutzbedarfklassen für alle IT-Systeme und Anwendungen sind festgelegt
3	Schwachstellenanalyse	Bedrohungsmatrix ist erstellt
4	Erstellung „Use Cases“	Zu Überwachende Dienste, Loginformationen, RSS-Feeds etc. sind definiert
5	Vulnerabilbity- und Patch Management	Anpassungen werden durch geführt und neue Anforderungen wurden festlegt
6	Erstellung von Playbooks	Praxisbezogene Notfallpläne für den Umgang mit definierten Security Vorfälle liegen vor



noris network

Zentrale

Nürnberg Süd:
noris network AG
Thomas-Mann-Straße 16-20
90471 Nürnberg

Telefon: +49 911 9352-0
E-Mail: anfrage@noris.de
www.noris.de
www.datacenter.de

Standorte Deutschland

München Ost:
Klausnerstr. 30
85609 Aschheim

Nürnberg Zentrum:
Deutschherrnstraße 15-19
90429 Nürnberg

München Zentrum:
Seidlstraße 3
80335 München

Hof:
Graf-Stauffenberg-Straße 6
95030 Hof

München Zentrum:
Marsstraße 26
80335 München

Berlin:
Frankfurter Allee 71-77
10247 Berlin

Standorte international

noris M.I.K.E.
Leof. Kon/nou Karamanli 170
54248 Thessaloniki
Griechenland

IT-Sicherheit
Made in Germany