Informationssicherheit. Für die Zukunft gewappnet.

26. Oktober 2022

Nürnberg

Informationssicherheit

Der Risikobasierte Ansatz – Was wird wirklich gebraucht?

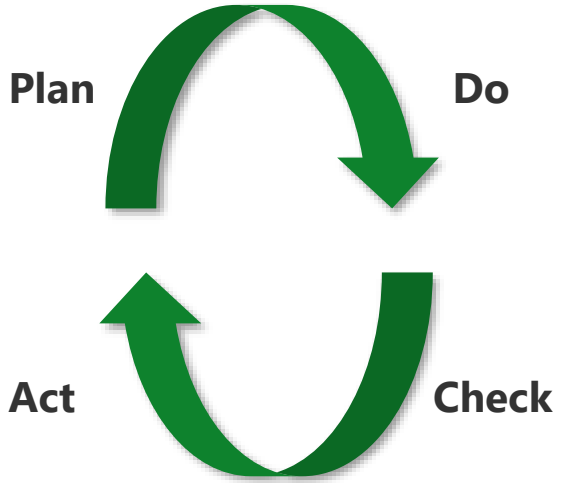
Inventar der Geschäftswerte

Bedrohung + Schwachstelle = Gefährdung

Wahrscheinlichkeit + Schaden = Risiko

Risikobewertung

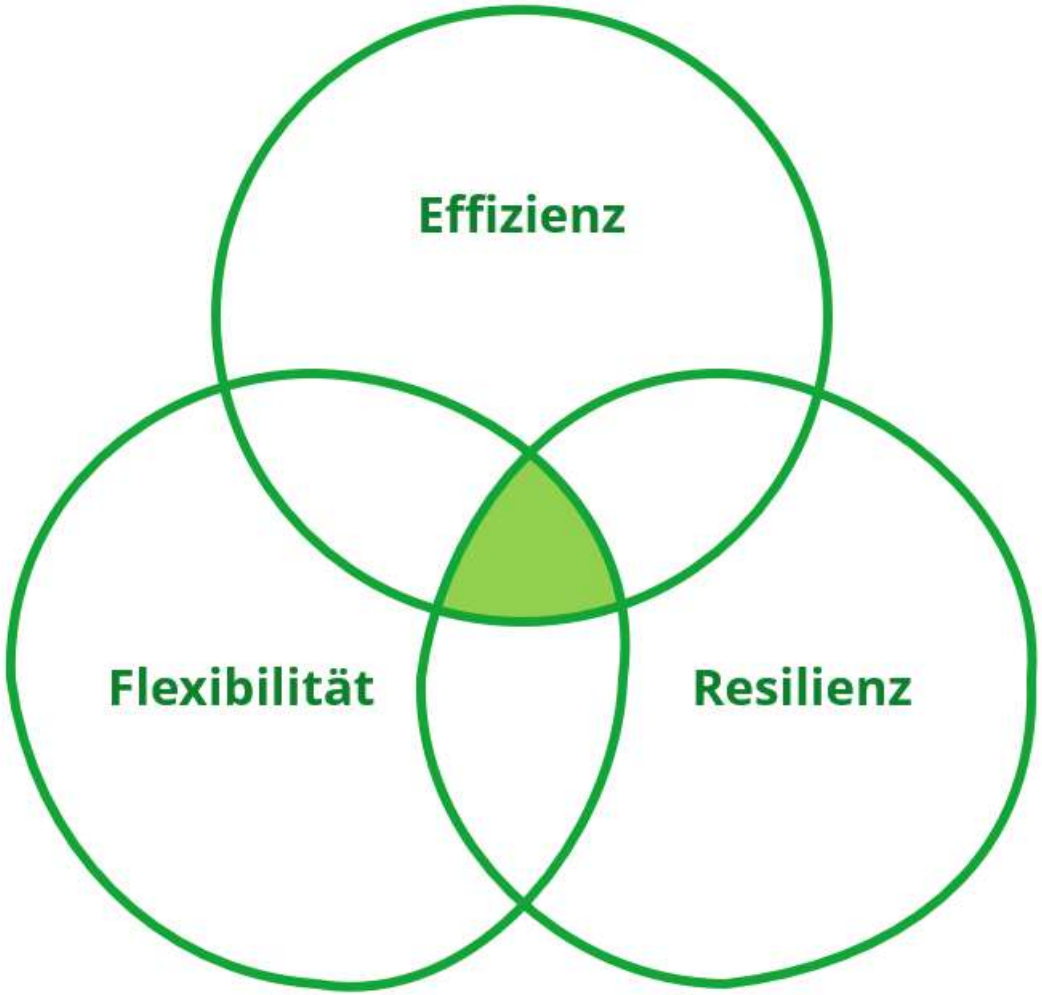
Maßnahmen
(technisch/organisatorisch)



Informationssicherheit – Strategisches Ziel

Vertraulichkeit, Verfügbarkeit und Integrität

- Werteliste, Bedrohung, Schwachstelle, Risikobewertung, Mitigation, Wirksamkeitsbewertung
- Balance zwischen Sicherheit, Flexibilität und Effizienz
- Beteiligung des ganzen Unternehmens
  - Führungskräfte
  - IT, Recht, Datenschutz, Personal, Fachbereiche, …
  - Jeder einzelne Mitarbeiter
- Auditierung? Unbedingt!
  - ISO27001
  - BSI-Grundschutz
  - Branchen: BAIT, TISAX, …



1. Phase – Initialisierung und Grundschutz

Einführung eines Informationssicherheitssystems

- Entscheidung der Geschäftsleitung zur Verbesserung der Informationssicherheit
- Verantwortlichkeit – Informationssicherheitsbeauftragter
- Konzeption und Planung
  - Sicherheitsziele
  - Leitlinien
  - Zertifizierung
- Erfassung Werte- und Geltungsbereich
  - Geschäftsprozesse
  - IT-Systeme
- Risikobasierter Ansatz und Ableitung erster TOMs

Zeitrahmen

- Drei bis sechs Monate

Ziele

- Verantwortlichkeit und Bewusstsein
- Grundlegende Richtlinien
- Erste Risikobewertung

Fehlerquellen

- Keine Chefsache
- Fehlende Ressourcen
- Unstrukturiertes Vorgehen

1. Phase – Einführung eines Informationssicherheitssystems

Typische Maßnahmen

Informationssicherheitsbeauftragter

- Zertifikation nach ISO 27001 oder BSI-Grundschutz
- Richtlinien (Benutzer, Administratoren, Entwickler, …)

Personal

- Datenschutz
- Verpflichtungen der Mitarbeiter

Informationstechnik

- Passwortrichtlinien und Mehr-Faktor-Authentifizierung
- Berechtigungskonzept (Rollentrennung, Personalisierung, Need-to-Know)
- Netz- und Systemmanagement
- Patchmanagement

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Quelle: irontechsecurity.com

2. Phase – Stabilisierung, Bewertung und IT-Sicherheit

Typische Maßnahmen

Informationssicherheitsbeauftragter

- Wirksamkeitsprüfungen der TOMs
- Behandlung von Informationssicherheitsvorfällen
- Kontinuierliche Mitarbeitersensibilisierung

Physische Sicherheit

- Zutrittsrechte und Zonenkonzepte

Informationstechnik

- Zentrales User- und Identity Access Management
- Changemanagement
- Notfallplanung
- Cloud- Sicherheit

3. Phase – Kontinuierliche Optimierung

Typische Maßnahmen

Informationssicherheitsbeauftragter

- Rezertifizierung
- Betriebliches Kontinuitätsmanagement (BCM)
- Notfallübungen

Personal

- Wissenstransfer
- On- und Offboarding Prozesse

Informationstechnik

- Schwachstellenanalyse und Pentesting
- Zero Trust
- Echtzeitüberwachung der Applikationsebenen

Red Teaming

Sicherheitsrisiko Homeoffice?

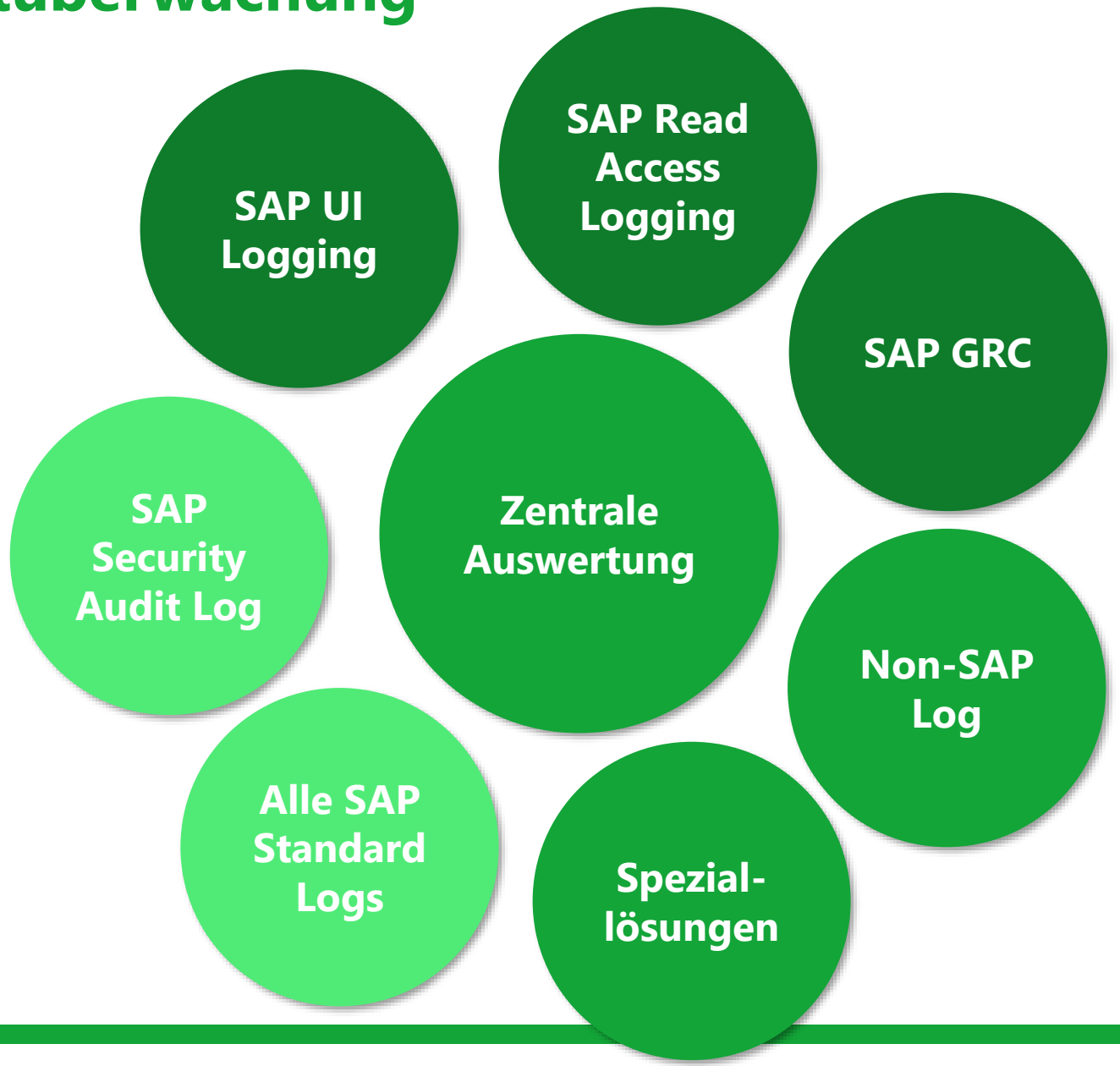
Angriffskette im Beispiel Homeoffice

Angriff auf lokalen PC (Homeoffice)	Zugang zu internen IT-Systemen	Diebstahl und Manipulation
1. Verteidigungslinie Schutzmaßnahmen des Mitarbeiters (z.B. Updates, Verhalten)	**2. Verteidigungslinie** Überwachung der Netzwerktechnik (z.B. Firewalls, SIEM-Systeme)	**3. Verteidigungslinie** Überwachung der Applikationsebene (z.B. Transaktionen, Datenzugriff)
		
Grundsätzlich sehr großer Angriffsvektor	Keine Auffälligkeiten bei System-Zugang über Mitarbeiter-PC	Alarm durch untypisches Userverhalten

SAP Forensik und Echtzeitüberwachung

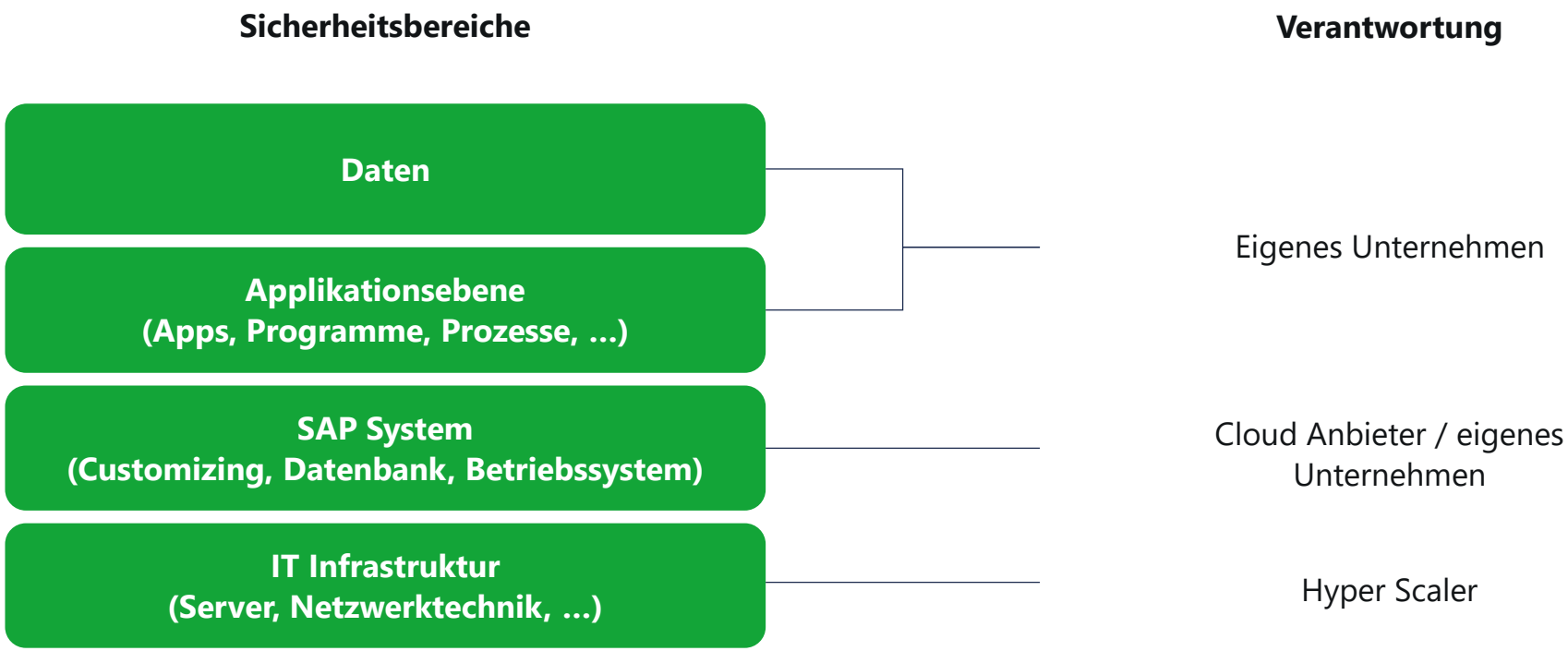
Forensik und Echtzeitanalyse einer gesamten Systemlandschaft ist ohne optimal ausgeprägtem SAP Logging und einem zentralen SIEM System nicht möglich.

- Zielführende Ausprägung des SAP Logging zur Überwachung der Applikationsebene und ein zentrales SIEM System (z.B. SAP ETD, Security Bridge, Natuvion SOPHIA)
- Angriffe und Anomalien werden ich Echtzeit erkannt



Verantwortung im Rahmen der Cloud Strategie

Die Verantwortung der Daten und der Applikationsebene bleibt im Unternehmen



Weiterführende Dokumente

Informationssicherheit

Bundesamt für Sicherheit in der Informationstechnik

- "Informationssicherheit mit System" Broschüre zur Übersicht
- BSI IT Grundschutz Kompendium

IT-Beauftragter der Bayerischen Staatsregierung

- Leitfaden-IT-Sicherheit

Natuvion

- Kundenbericht Pentesting
- Informationssicherheit in Krankenhäusern

ISO 27001

So erreichen Sie uns

Natuvion
Informationssicherheit, IT-Sicherheit und Datenschutz

Jakob Munzert
Senior Manager IT-Security Consulting
+49 151 17135718
Jakob.munzert@natuvion.com