SONNTAG
IT Solutions

Cybersecurity – Bedrohungen und Schutzmaßnahmen

04.09.2023

MOORE

Agenda

- Kurzvorstellung & Allgemeines
- Die Top 10 der Bedrohungen
- Schutzmaßnahmen – Allgemein
- Schutzmaßnahmen gegen die Top 10 Bedrohungen
- Frühwarnsysteme

SONNTAG
IT Solutions

Kurzvorstellung & Allgemeines

Patrick Hertle

- IT-Security Expert (ISACA)
- IT-Prüfungen (Jahresabschlussprüfungen/Sonderprüfungen)
- Prüfverfahrenskompetenz nach §8a (3) BSIG
- Fachkraft für Datenschutz (Datenschutzbeauftragter)
- IT-Due Diligence
- IT-Projektmanagement
- BPMN 2.0 Prozessmodellierung
- SCRUM Master & Product Owner

Allgemeines

- Verfünffachung der Schadenssumme durch Cybercrime seit 2019 auf 202,7 Mrd.
- Massiver und anhaltender Anstieg der Phishing Angriffe während und nach der Covid-19 Pandemie
  - Identitäten sind oft genutzte Schwachstelle
- KMU rücken immer mehr in den Fokus der Angreifer
- Kritische Infrastruktur immer mehr betroffen (Krankenhäuser, Wasserversorger, etc.)

Live Cyber Threat Map

Die 5 Gesetze der Cybersicherheit

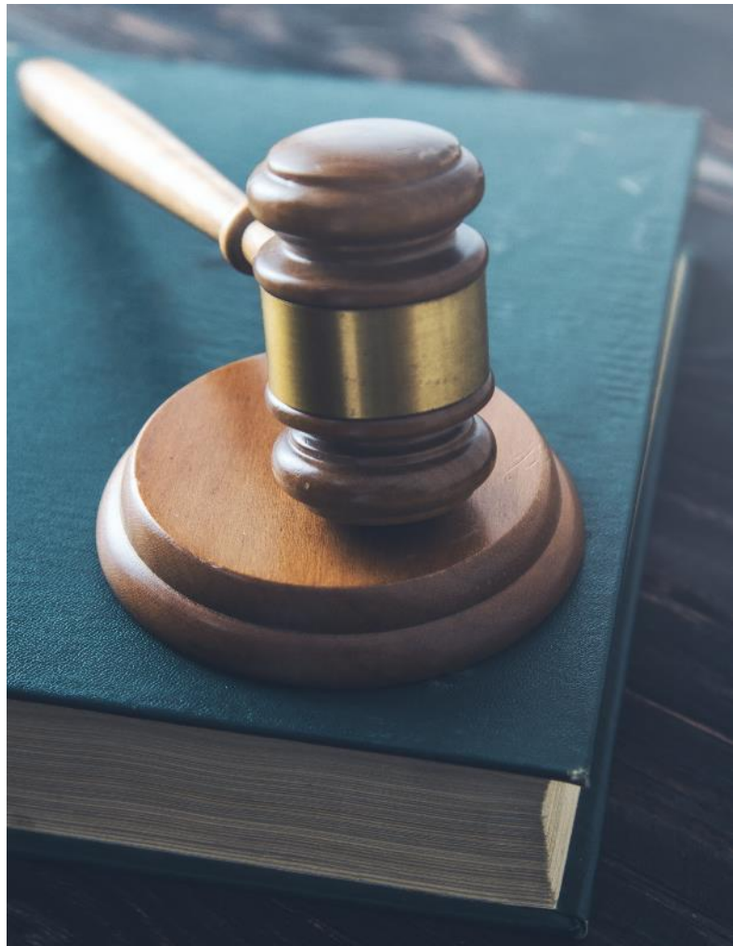
1. Wenn es eine Schwachstelle gibt, wird diese ausgenutzt

2. Alles ist in irgendeiner Form verwundbar/ausnutzbar

3. Menschen vertrauen, auch wenn sie es nicht sollten

4. Mit neuen Innovationen kommen auch neue Möglichkeiten der Ausbeutung

5. Bei Unsicherheit → auf Regel 1 zurückgreifen

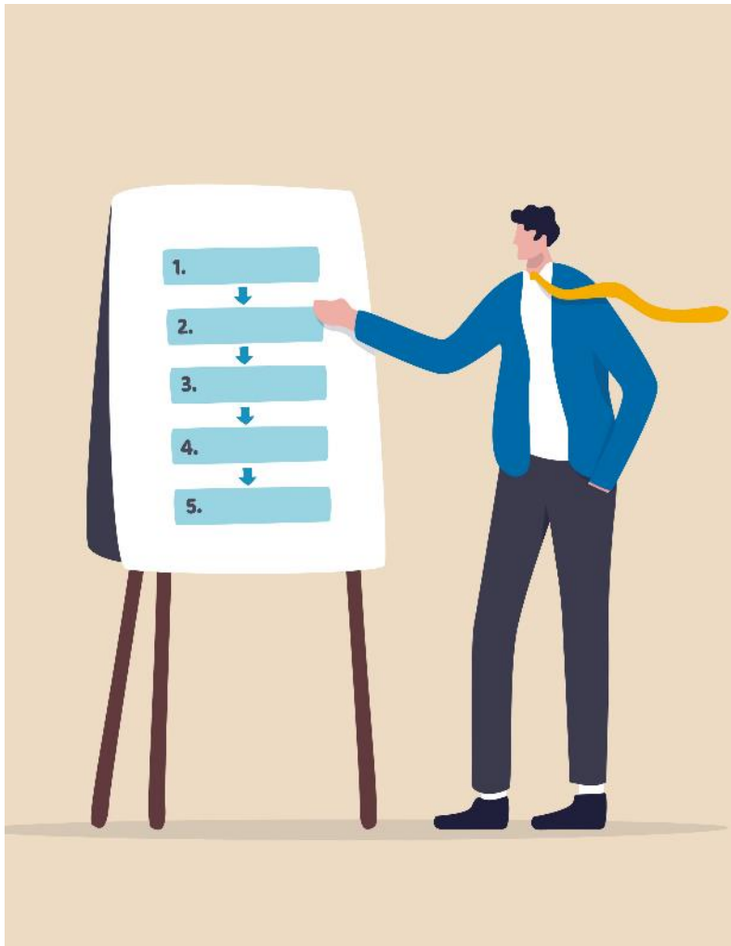


SONNTAG
IT Solutions

Die Top 10 der Bedrohungen

Top 10

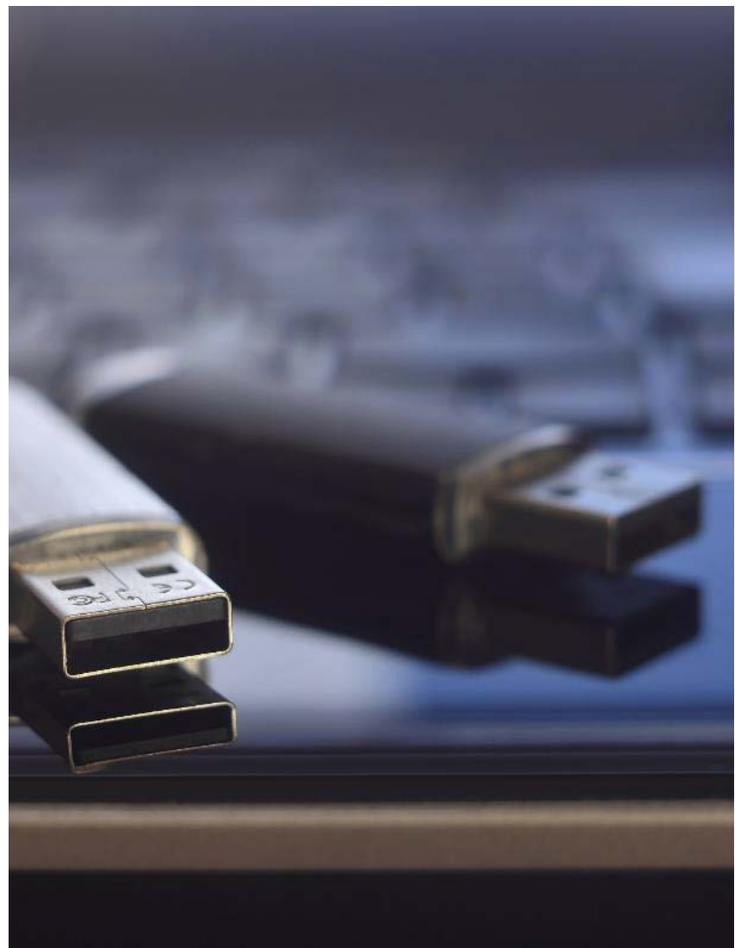
- Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme
- Infektion mit Schadsoftware über Internet und Intranet
- Menschliches Fehlverhalten und Sabotage
- Kompromittierung von Extranet und Cloud-Komponenten
- Social Engineering und Phishing
- (D)DoS Angriffe
- Internet-verbundene Steuerungskomponenten
- Einbruch über Fernwartungszugänge
- Technisches Fehlverhalten und höhere Gewalt
- Soft- und Hardwareschwachstellen in der Lieferkette



Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme

Mögliche Szenarien:

- Wechseldatenträger können im privaten Umfeld infiziert worden sein
- Wechseldatenträgermedium unbekannter Herkunft wird im Office-Netz angeschlossen
- Projektdateien oder ausführbare Anwendungen können Schadcode enthalten, der zu einer Infektion oder einem Datenabfluss führen kann.
- Diebstahl oder Verlust von mobilen Systemen mit sensiblen Informationen



Infektion mit Schadsoftware über Internet und Intranet

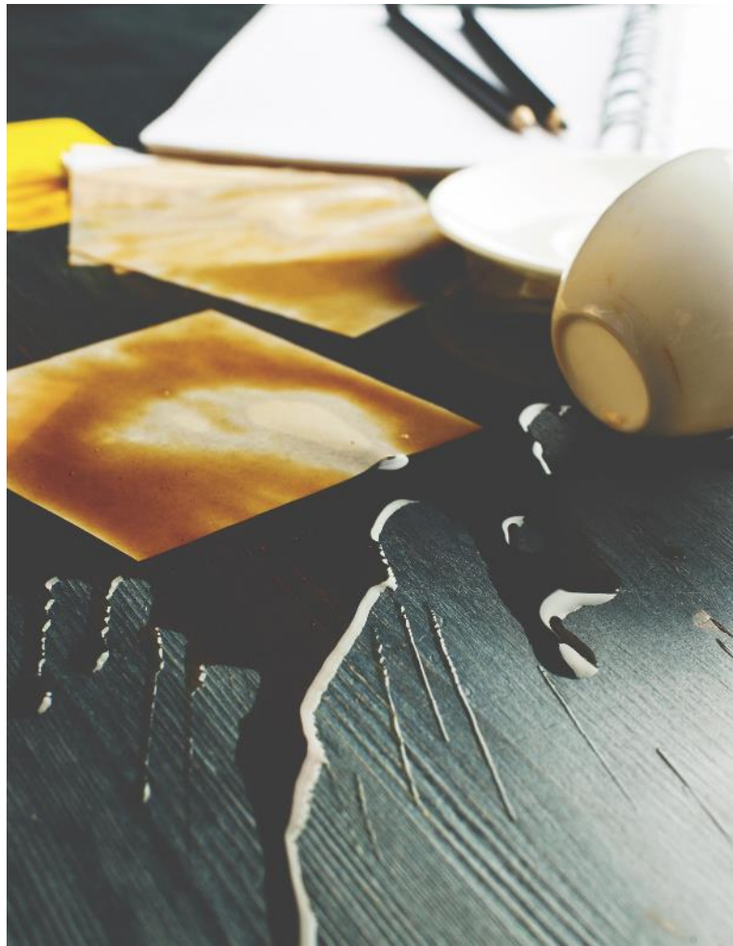
Mögliche Szenarien:

- Infektion über Kollaborations-Software (Mail Anhang, Makros in Office Dokumenten)
- Manipulation von externen Webseiten (z.B. Drive-by-Download)
- Undokumentierte oder ungeschützte Verbindungen zwischen Netzen (z.B. zwischen Unternehmensnetzen)
- Durchführung von Angriffen auf extern bereitgestellte Dienste (z.B. Webseiten)
- Installation von privater Hardware durch das Personal, die bereits infiziert ist oder Infektionswege ermöglicht

Menschliches Fehlverhalten und Sabotage

Mögliche Szenarien:

- Fehlkonfiguration sicherheitsrelevanter Komponenten
- Unkoordiniertes oder nicht vorhandenes Update- & Patchmanagement
- Seiteneffekte vorsätzlicher Handlungen (Beschädigung von Installationen, Platzierung von Abhörgeräten)
- Kompromittierung durch nicht genehmigte Hard- und Software (Schatten-IT)
- Erstellung nicht freigegebener Konfigurationen für Infrastruktur- und Sicherheitskomponenten



Kompromittierung von Extranet und Cloud-Komponenten

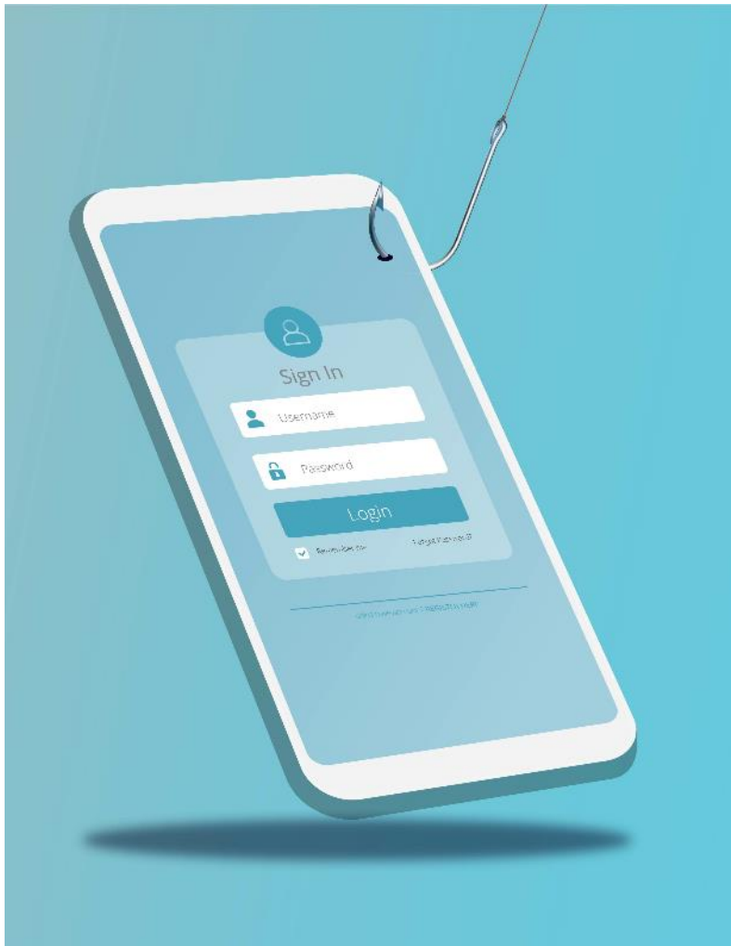
Mögliche Szenarien:

- Störung/Unterbrechung zwischen lokalem Netzwerk und ausgelagerten Komponenten (z.B. Cloud)
- Ausnutzung von Implementierungsfehlern oder unzureichenden Sicherheitsmechanismen
- Unzureichende Trennung der Mandanten eines Cloud-Anbieters kann zu einer Beeinträchtigung führen (Kollateralschaden)

Social Engineering und Phishing Angriffe

Mögliche Szenarien:

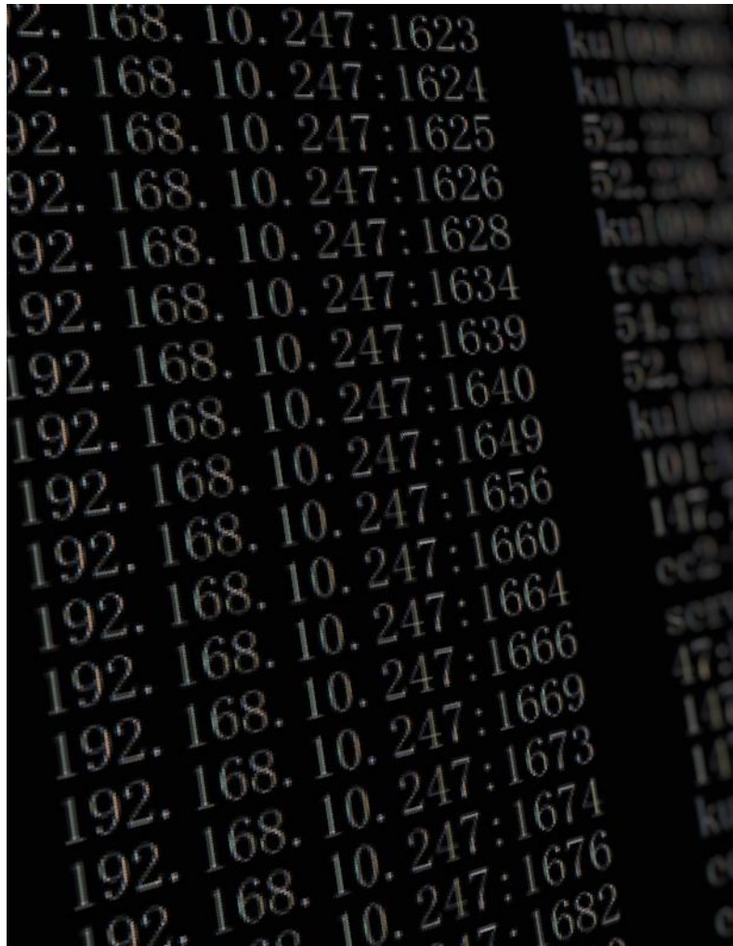
- Phishing Angriffe bei denen der Angreifer durch gefälschte Nachrichten an Zugangsdaten kommt oder Schadsoftware verteilt
- Links oder Anhänge, bei deren Öffnen Schadsoftware installiert wird
- Spear-Phishing Angriff
- Unberechtigter Zugang zu einem Gebäude durch Vorspiegelung falscher Tatsachen



(D)DoS Angriffe

Mögliche Szenarien:

- (D)DoS-Angriffe auf die Internetanbindung zentraler oder dezentraler Komponenten
- DoS-Angriffe auf Schnittstellen einzelner Komponenten
- Angriffe auf drahtlose Anbindungen oder Mobilfunknetze
- DoS-Angriffe mittels Ransomware



IoT

Mögliche Szenarien:

- Auffinden von Steuerungskomponenten durch Suchmaschinen wie Shodan
- Direkter Zugriff auf ungeschützte Komponenten oder Verwendung öffentlich verfügbarer Standardpasswörter
- Ausnutzen von Schwachstellen in den erreichbaren Diensten wie z.B. Webschnittstellen

Eindringen über Fernwartungszugänge

Mögliche Szenarien:

- Direkter Zugriff auf einen Wartungszugang mittels
  - Brute Force
  - Wiederverwendung eines zuvor aufgezeichneten Authentisierungstokens
  - Web-spezifische Angriffe auf Zugänge die zu Wartungszwecken genutzt werden
- Indirekter Angriff über die IT-Systeme des Wartungsdienstleisters
  - Trojaner welche den Zugang direkt auf dem externen Wartungsrechner ausnutzen
  - Diebstahl eines Passworts, Zertifikats oder sonstigen Tokens bzw. sonstige Beschaffung von Zugangsdaten
  - Verwendung gestohlener Hardware, auf denen ein Zugang eingerichtet ist

Technisches Fehlverhalten und höhere Gewalt

Mögliche Szenarien:

- Defekte von Komponenten die zu einem sofortigen Ausfall führen (z.B. Festplatten, Switche)
- Nicht getestete Systemupdates
- Extremwetterereignisse

Soft- und Hardwareschwachstellen in der Lieferkette

Mögliche Szenarien:

- Der Hersteller reagiert nicht auf Meldungen zu Schwachstellen und benachrichtigt Kunden nicht über Updates, Workarounds oder Patches
- Angreifer geben sich als Hersteller aus und nutzen Phishing Mails mit vermeintlichen Informationen zu Patches, um Schadcodes zu verteilen
- Es befinden sich Schwachstellen in einer externen Bibliothek, die keine Updates mehr erhält oder der Hersteller nicht mehr am Markt tätig ist

SONNTAG
IT Solutions

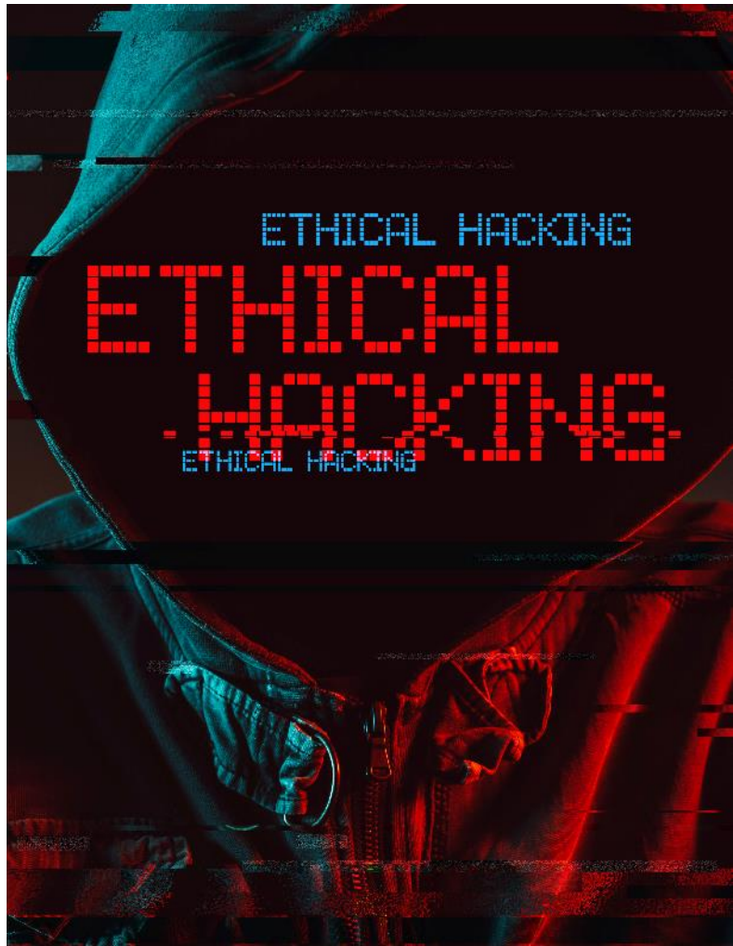
Schutzmaßnahmen - Allgemein

PEN-Testing

- Test durch (externe) Dienstleister zur Feststellung der aktuellen Sicherheit einer IT-Landschaft, Anwendung oder Organisation
- Nutzung von Methoden und Werkzeugen die Hacker verwenden
- Klassische im Vorfeld zu klärende Kriterien sind: Informationsbasis, Aggressivität, Umfang, Vorgehensweise, Technik und Ausgangspunkt
- Regelmäßige PEN-Test sind Teil eines kontinuierlichen Verbesserungsmanagements (PDCA-Zyklus)

Ziel:

- Aufdecken von Schwachstellen und Anwendungsfehlern die bisher ohne simulierten Angriff nicht erkannt worden sind
- Konkrete Handlungsempfehlungen zur Verbesserung der Sicherheit



IT-Audit

- Überprüfung der IT-Landschaft durch Einsicht ins System z.B. über Stichproben
- Einsichtnahme in (System)-Dokumentationen
- Überprüfen von IT gestützten Verfahren innerhalb eines Unternehmens (Nutzeranlage, Berechtigungsvergaben)

Ziel:

- Erfüllung von rechtlichen Pflichten
- Verbesserung der organisatorischen IT-Sicherheit
- Handlungsempfehlungen

Aufbau eines ISMS

- Umfasst Regeln, Verfahren, Methoden und Werkzeuge zur Erhöhung der Informationssicherheit
- Systematischer Schutz von wichtigen Daten und Informationen
- Schafft Klarheit über die wichtigen Assets im Unternehmen
- Notfallfahrplan für den Ernstfall
- Wichtige Normen: ISO 27001 und ISO 27002

Ziel:

- Erhöhung der Informationssicherheit durch Erfüllung der primären und sekundären Schutzziele wie z.B. Vertraulichkeit, Verfügbarkeit und Integrität

Business Continuity Management

- Entwicklung und Dokumentation von Strategien, Plänen und Maßnahmen

- Zentrale Maßnahmen des BCM:
  - Generelles Krisenmanagement
  - Business-Impact-Analyse
  - Definieren von Notfallplänen
  - Notfallübungen
  - Stetige Optimierung der Pläne und Maßnahmen

- Mögliche Szenarien für die Anwendung des BCM:
  - Personalmangel (Krankheit, Abgang)
  - Stromausfall
  - Ausfall von Hardware
  - Cyberangriff

Ziel:

- Minimierung der Unterbrechungen des IT-Betriebs in einem Unternehmen oder einer Organisation

Aufbau eines SOC

- Zentrale Sicherheitsleitstelle
- Integration, Überwachung und Analyse aller sicherheitsrelevanter IT-Systeme
- Alarmierung bei Vorfällen und Ergreifen erster Maßnahmen
- Arbeitet proaktiv

Setzt sich zusammen aus:

- SOC-Manager
- Sicherheitsingenieure
- Sicherheitsanalysten
- Threat-Hunter

Aufbau eines SOC

Vorteile:

- Schnelle Analyse, Erkennung und Abwehr von Cyber - Attacken
- Dynamische Anpassung an die aktuellen Bedrohungsszenarien
- Prävention durch proaktives Arbeiten
- Zentraler Ansprechpartner für Unternehmensführung und Management
- Erfüllung der Compliance-Pflichten dank Dokumentation aller sicherheitsrelevanter Ereignisse und Maßnahmen durch SOC

Ziel:

- Effiziente Erkennung von Bedrohungen und Schutz der IT-Infrastruktur vor Cyberangriffen

Passwortrichtlinien

- Organisatorische und technische Vorgabe wie mit Passwörtern umzugehen ist
- Unterscheidung zwischen Usern und Administratoren notwendig

Wichtige beispielhafte Aspekte für die Erstellung einer sicheren Passwortrichtlinie:

- Protokollierung von Anmeldefehlversuchen
- Sperrung des Nutzerkontos nach mehrfach fehlerhafter Anmeldung
- Komplexitätsanforderungen
- Anweisungen zur Änderung von Standardpasswörtern
- Wiederherstellung von Nutzerkonten

Passwortrichtlinien - Empfehlungen

Empfehlungen:

- Mindestens 10 Zeichen
- Groß- und Kleinbuchstaben
- Zahlen
- Sonderzeichen
- Multifaktor-Authentifizierung für alle Geräte und Konten
- Passwortlose Anmeldung (sofern technisch möglich)

Tipp: Komplizierte Passwörter mittels eines Satzes merken:

„**A**m **l**iebsten **e**sse **i**ch **P**izza **m**it **vier** **Z**utaten **u**nd **e**xtra **K**äse**!**“

Wird zu:

„AleiPm4Z+eK!“

Passwort-Manager

- Software zur zentralen, verschlüsselten und sicheren Speicherung und Verwaltung von Passwörtern
- Zugang zu Passwörtern mittels Master-Passwort
- Unterstützung bei der Passwortvergabe mittels Passwortgenerator
- Teilen von Passwörtern z.B. mit Berechtigten in einer Organisationseinheit (Hinterlegen eines Benutzerberechtigungskonzepts)

Möglichkeiten der Integration:

- Eigenständiges Programm
- Im Browser integriertes Programm (Browser Add-On)

Passwort-Manager

Nachteile eines Passwortmanagers:

- Im Worst Case Verlust aller Daten bei Vergessen des Master-Passworts
- Diebstahl aller Passwörter auf einmal bei Cyberangriff auf den Passwort-Manager
  - Einführung von Multifaktor-Authentifizierung
- Anvertrauen sensibler Daten an einen Dienstleister bei Nutzung einer cloudbasierten Lösung
  - Überprüfung der AGB und Datenschutzerklärungen

Update- und Patchmanagement

Was ist Patchen?

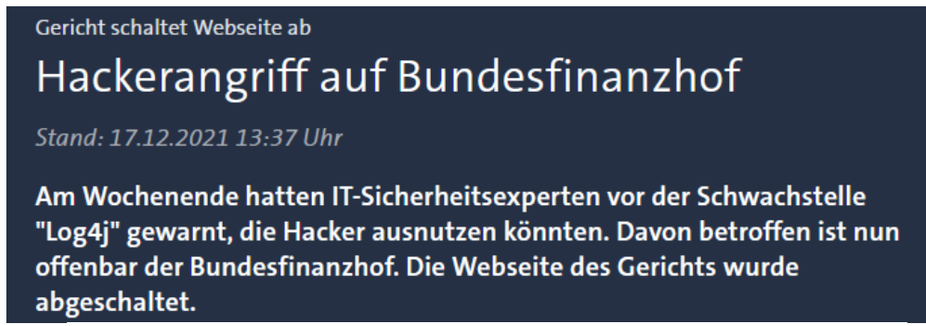
- Bedarfsorientierte Korrektur einer bestehenden Software

Welche Arten gibt es?

- Bugfix: Behebung von Fehlern im Quellcode
- Hotfix: Unaufschiebbare Behebung von Fehlern im Programm
- Update: Klassische Form der Aktualisierung. Beinhaltet Funktionserweiterungen und zum Teil Fehlerbehebungen

Was ist Update- und Patchmanagement?

- Patchmanagement ist integraler Bestandteil des System Managements
- Beschaffung, Test und Installation benötigter Updates für Applikationen, Treiber und Betriebssystemen



Update- und Patchmanagement

Warum ist Update- und Patchmanagement wichtig?

- Überblick über den Patch-Zustand aller Systeme
- Nutzung von Sicherheitslücken durch Hacker um
  - in IT-Infrastrukturen einzudringen
  - Daten zu manipulieren oder
  - auf vertrauliche Daten zuzugreifen

Die Schließung der Lücken ist essenziell!

Wichtige Hinweise:

- Minimierung der mit Patches einhergehenden Risiken
- Erstellung von Datensicherungen vor dem Patchen
- Test der Patches auf unkritischen Systemen (z.B. eigenes Testsystem)

Awareness Trainings

Warum Awareness Trainings?

- Schaffung eines Bewusstseins für Cyberrisiken innerhalb des Unternehmens
- Minderung des Risikos von erfolgreichen Cyberangriffen auf die eigene Organisation und Person

Wichtige Tipps:

- Konstantes Training
- Individuelle zielgruppenorientierte Trainingsinhalte (z.B. für Management, IT-Abteilung, normale User)
- Verwendung praktischer Elemente (Hands-on Übungen)
- Konstante Verbesserung und Anpassung des Trainings durch Feedback

SONNTAG
IT Solutions

Schutzmaßnahmen gegen die Top 10 Bedrohungen

Einschleusen von Schadsoftware über Wechseldatenträger und mobile Systeme

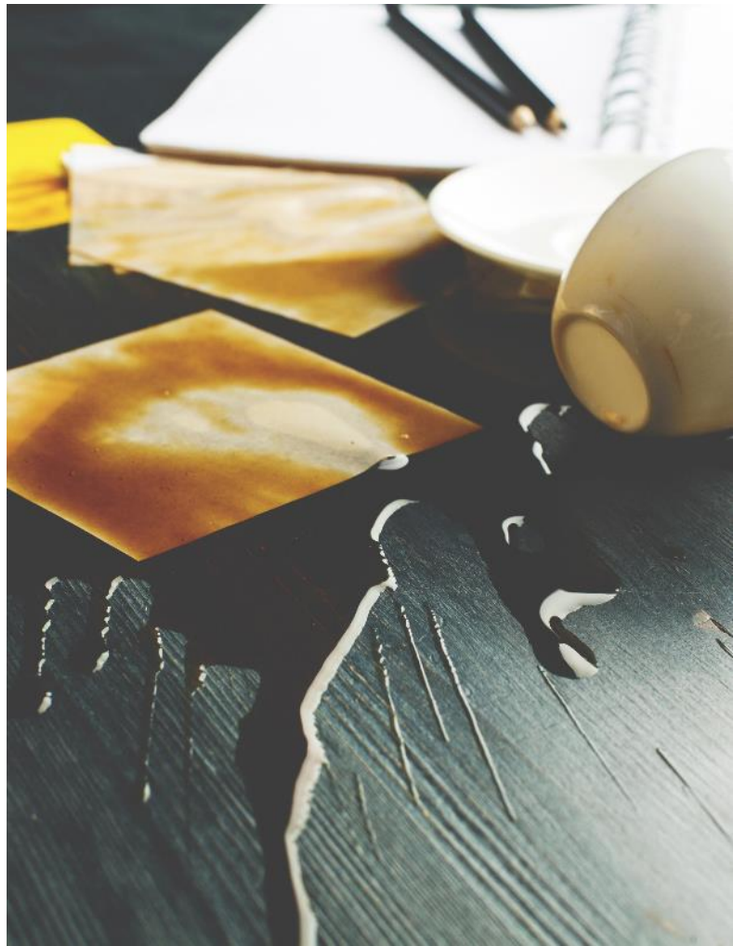
- Inventarisierung und Whitelisting von Wechseldatenträgern und Geräten
- Ausschließliche Verwendung von unternehmenseigenen Wechseldatenträgern und Geräten
- Physische Sperren gegen unbefugtes Anschließen von USB-Geräten
- Einrichtung von Quarantänenetzen
- Etablieren von organisatorischen Vorgaben (Richtlinien)

Infektion mit Schadsoftware über Internet und Intranet

- Netzwerksegmentierung durch Firewalls und VPN-Lösungen
- Abschottung nicht patchbarer Systeme
- Beschränkung der offen zugänglichen Informationen im Unternehmen (Need-to-Know-Prinzip)
- Systemhärtung

Menschliches Fehlverhalten und Sabotage

- Einführen einer automatischen Überwachung von Systemzuständen und -konfigurationen
- Deaktivieren des Internetzugangs für Systeme die diesen nicht benötigen (z.B. in der Produktion)
- Etablierung von standardisierten Prozessen für Berechtigungsvergaben (intern & extern)
- Einführung einer Endbenutzerrichtlinie

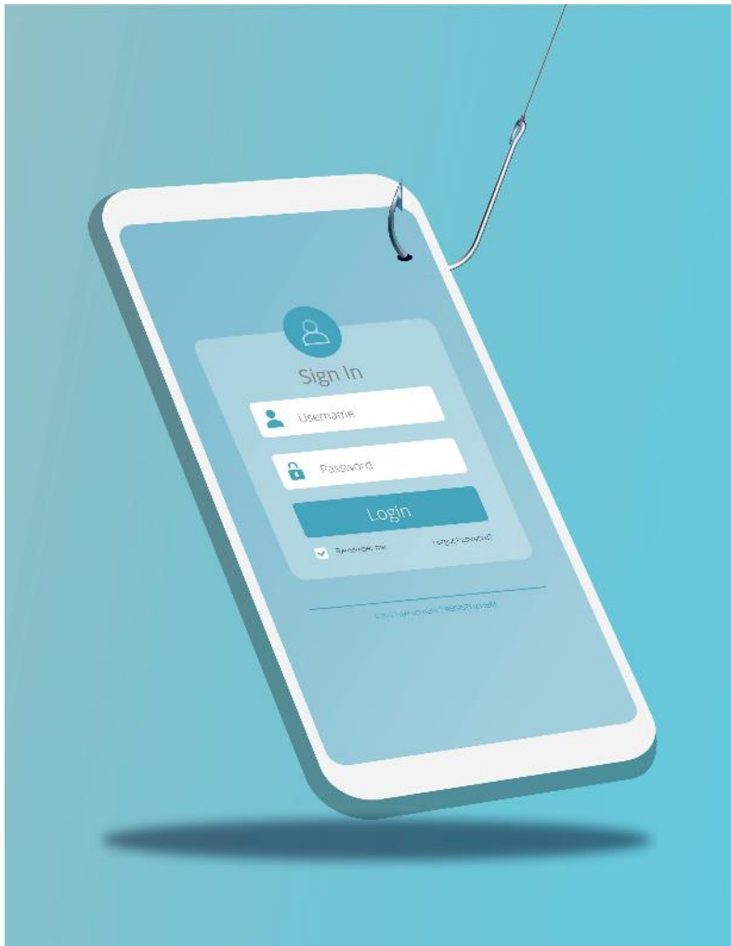


Kompromittierung von Extranet und Cloud-Komponenten

- Nutzung von zertifizierten Anbietern
- Verpflichtung der Betreiber zu einem hinreichenden Sicherheitsniveau mittels SLAs
- Betrieb einer Private Cloud
- Nutzung von kryptographischen Mechanismen zur Absicherung der Cloud Daten
- Nutzung von VPN-Lösungen

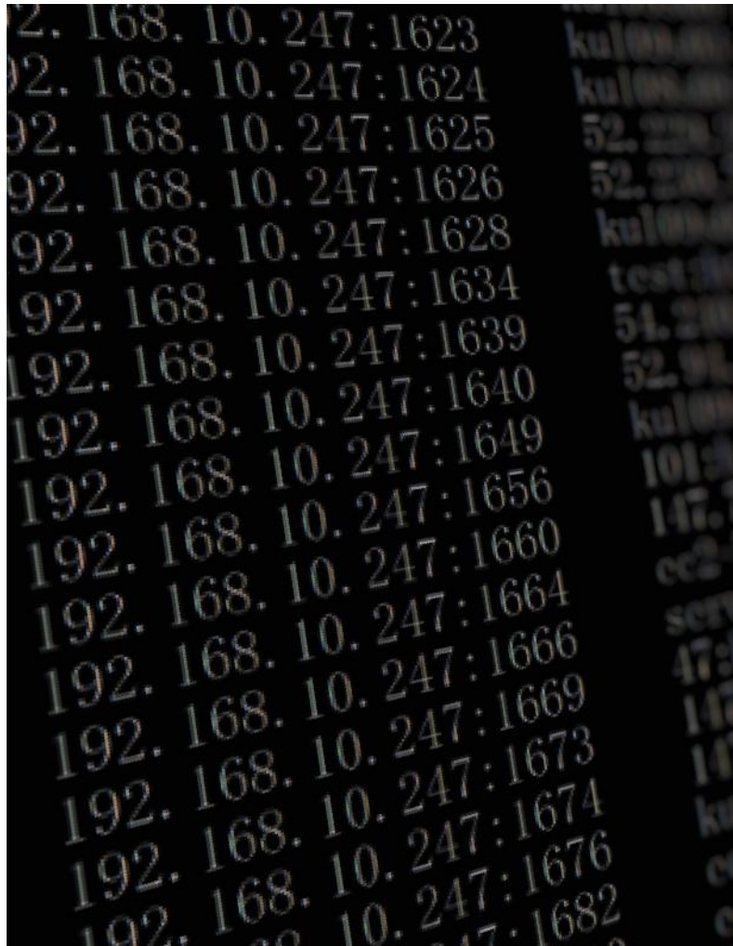
Social Engineering und Phishing Angriffe

- Awareness-Trainings
- Etablierung eines Datensicherungskonzepts
- Sichere Entsorgung von digitalen und papiergebundenen Datenträgern
- Handlungsanweisungen und Verhaltenskodex für Mitarbeiter
- Definition und Kommunikation von Alarmierungswegen bei Vorfällen
- Regelmäßige Datensicherungen



(D)DoS Angriffe

- Strikte Konfiguration und Härtung von Netzzugängen und Kommunikationskanälen
- Nutzung dedizierter kabelgebundener Verbindungen für kritische Funktionen
- Redundante Anbindung von Komponenten unter Verwendung unterschiedlicher Protokolle oder Kommunikationswege
- Verwendung von DDoS-Protection Services wie z.B. Cloudflare



IoT

- Keine direkte Verbindung von Steuerungskomponenten mit dem Internet
- Härtung der Steuerungskomponenten
- Anwenden von Defense-in-Depth Prinzipien

Eindringen über Fernwartungszugänge

- Sperren/Löschen von Standardnutzern und Passwörtern vom Hersteller
- Verschlüsselung der Übertragungswege
- Nutzung von MFA und anderen sicheren Authentisierungsverfahren
- Granulare Segmentierung der Netze zur Minimierung von lateralen Bewegungen im System
- Einrichten von Fernwartungszugriffspunkten in einer DMZ
- Personalisierung der Zugänge
- Durchführung von Audits (IT-Audit, PEN-Testing)

Technisches Fehlverhalten und höhere Gewalt

- Aufbau eines Notfallmanagements
- Vorhalten von Ersatzhardware (Redundanz)
- Regelmäßige Überprüfung der Maßnahmen hinsichtlich der Eignung und Rahmenbedingungen

Soft- und Hardwareschwachstellen in der Lieferkette

- Einführen eines Asset Managements
- Bezug von Updates und Bibliotheken nur über vertrauenswürdige Quellen
- Einführung eines Schwachstellenmanagements

SONNTAG
IT Solutions

Frühwarnsysteme

Häufige Buzzwords

- Network Detection and Response (NDR)
- Endpoint Detetction and Response (EDR)
- Intrusion Detection Systems (IDS)
- Advanced Threat Protection (ATP)
- Security Operations Center (SOC)
- Security Information and Event Management (SIEM)

Frühwarnsysteme und ihr Nutzen

- Aufzeigen der aktuellen Cyber-Sicherheitslage
- Möglichst frühe Erkennung von Angriffspotenzialen und realen Angriffen
- Nachhaltige Erhöhung der Sicherheit, Widerstandsfähigkeit und Vertrauenswürdigkeit von IT-Systemen und IT-Infrastruktur

Beispiele für Arten von Frühwarnsystemen

- BSI-Newsletter und Cyber-Sicherheitswarnungen
- Allianz für Cybersicherheit
- Threat-Monitoring-Softwarelösungen
  - z.B. SIEM-Lösungen

BSI

- Newsletter des Bundesministerium für Sicherheit in der Informationstechnik mit Infos zu
  - IT-Grundschutz
  - Cloud-Computing
  - BCM-Info Business Continuity Management
  - Mindeststandards Bund

- Aktuelle Cyber-Sicherheitswarnungen
  - Übersicht über aktuelle Cyber-Sicherheitswarnungen

Bundesamt
für Sicherheit in der
Informationstechnik

Allianz für Cybersicherheit

- Kooperative Plattform für Unternehmen, Verbände, Behörden und Organisationen
- Informationsaustausch zur aktuellen Bedrohungslage
- Austausch praxisnaher Cyber-Sicherheitsmaßnahmen
- Einfache Anmeldung zum Teilnehmer

Allianz für Cyber-Sicherheit

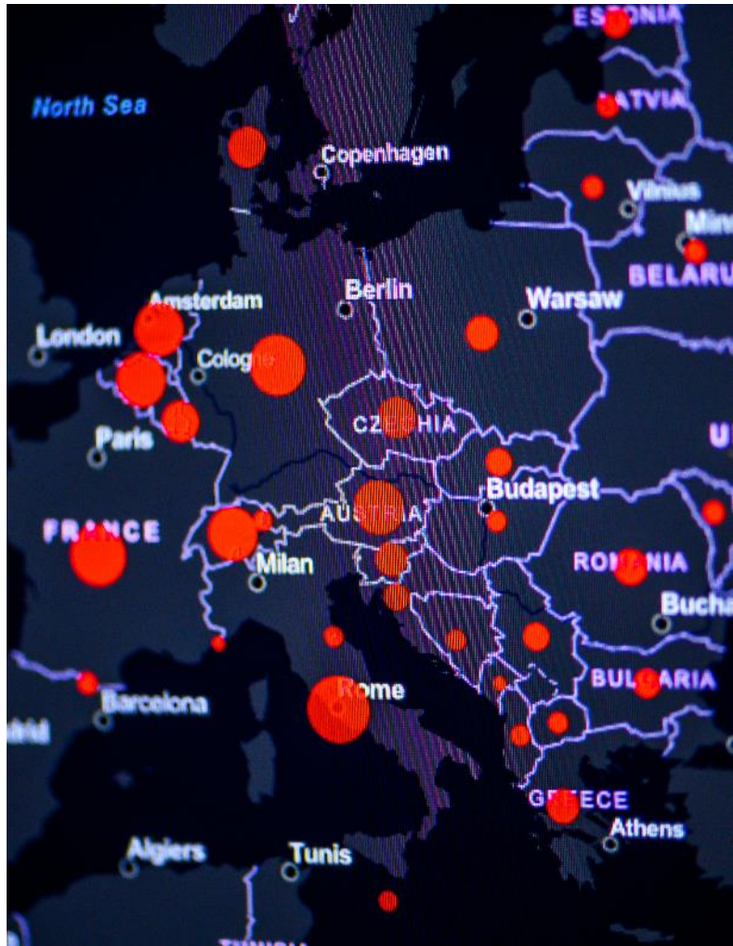
Threat-Monitoring-Softwarelösungen

- Erkennung möglicher Cyber-Gefahren durch Analyse relevanter Sicherheitsinformationen, die durch Gefahrensensoren bereitgestellt werden

- Sensoren sind IT-Systeme wie z.B. Server, Netzwerkkomponenten oder Endgeräte

- Konstante Analyse und Auswertung von Sicherheitsdaten, um Cyber Attacken und Datenschutzverletzungen zu erkennen
  - Informationen werden in einem Sicherheitsnetzwerk gesammelt und ausgewertet (z.B. alle Nutzer einer Softwarelösung)

  - Erkennen von z.B. globalen Mustern



SIEM (Security Information and Event Management)

SIEM Lösungen umfassen drei Kernkompetenzen:

- Datenerfassung
- Datenanalyse
- Reaktion auf „Events“

Aufgaben eines SIEM:

- Erfassung von Daten über das gesamte Netzwerk
- Identifizierung schädlichen Verhaltens
- Versendung von Warnungen (Alerts) an Sicherheits- und IT-Teams, um den nötigen Einblick und die erforderlichen Informationen zu geben, um entsprechend zu reagieren, ehe das Problem ernst wird (Reaktion)

Hinweis:

- Seit Anfang 2023 muss jedes KRITIS-Unternehmen ein SIEM benutzen

SIEM (Security Information and Event Management)

Vorteile eines SIEM:

- Übersichtliche Darstellung mittels Dashboards
- Genaue Erkennung von Malware
- Umfangreiche Analyse der gesamten Infrastruktur
- Fähigkeit, neue Bedrohungen zu erlernen
- Endpunkterkennung

Nachteile eines SIEM:

- Nicht jedes SIEM kann alle relevanten Datenquellen integrieren (z.B. ERP-Systeme von SAP und hybride Infrastrukturen)
- Stetig zunehmende Datenmengen lassen SIEMs an ihre Grenzen stoßen
- SIEM mit statischen Regelungen können zu einer höheren Anzahl an Fehlalarmen führen

SIEM (Security Information and Event Management)

Was sollte ein SIEM-Tool beinhalten?

- Anwenderverhaltensanalyse
- Angreiferverhaltensanalyse
- Täuschungstechnologie (z.B. Honeypots)
- File Integrity Monitoring (FIM)
- Maßnahmen zu Vorfällen
- Endpunkterkennung
- Leistungsmetriken
- Visualisierung, Reports, Dashboards

SONNTAG
IT Solutions

Zusammenfassung

Wichtige erste Schritte

- Aktualisieren aktueller Dokumentationen
- Erstellung von Richtlinien und Benutzerhandbüchern
- Einführung regelmäßiger Awareness Trainings
- Überblick über alle wichtigen Assets und kritische IT gestützte Geschäftsprozesse verschaffen
- Möglichkeiten zur Informationsbeschaffung im Bereich Cyber-Security schaffen (BIS, Allianz für Cybersicherheit)
- Absicherung der Zugriffe von außen (Fernwartungszugänge, Home Office, etc.)
- Audits durch externe Prüfer
- Einführung eines BCM
- Einführung eines ISMS

Expertise und Unterstützung im Bereich Cybersecurity durch SONNTAG

- Risikoanalyse im Hinblick auf IT- und datenschutzrechtliche Schwachstellen
- Prüfung und Anpassung von sicherheitsrelevanten Verträgen wie etwa Vereinbarungen mit externen IT-Dienstleistern, Cyber-Security-Versicherungsgebern u.ä.
- Beratung beim Schutz von Geschäftsgeheimnissen, insbesondere bei der Vertragsgestaltung unter Berücksichtigung der Vorgaben des GeschGehG sowie der (gerichtlichen) Durchsetzung von Rechtspositionen
- Unterstützung bei der Erstellung sicherheitsrelevanter Rechtstexte wie Datenschutzerklärungen, Betriebsvereinbarungen, IT-Richtlinien oder Verschwiegenheitspflichten
- Beratung bei Datenschutz- und IT-Sicherheitsverstößen, insbesondere in Folge von Cyber-Angriffen
- Kommunikation mit Aufsichts- und Strafverfolgungsbehörden
- Geltendmachung von Ansprüchen gegenüber Dienstleistern, Mitarbeitern, Versicherungen u.w.

Vielen Dank für Ihre Aufmerksamkeit!

SONNTAG IT Solutions GmbH & Co. KG

AUGSBURG | +49 821 99 98 43 23

www.sonntag-its.de

SONNTAG IT Solutions. Ein Team. Für Ihre IT Lösungen.

Patrick Hertle

IT-Berater

E-Mail: patrick.hertle@sp-it.de

Felix Hofstetter

Business Development Manager

E-Mail: felix.hofstetter@sp-it.de