ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Juni 2019

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Kommt die Ortung im WLAN wieder zurück?

von Dr. Johannes Dams

In Zeiten von Bluetooth Low Energy (BLE) und Smartphones wurde die „Ortung mittels WLAN“ immer stärker durch eine Ortung mit BLE-Beacons und der dazugehörigen Infrastruktur abgelöst. Dies liegt nicht zuletzt an der vergleichsweise einfachen Planung und Umsetzbarkeit der BLE-Beacon-Infrastruktur. Mit dem Aufkommen der ersten WLAN-Access-Points gemäß IEEE 802.11ax zeigt sich aber eine weitere Neuerung: „Wifi Certified Location“. Diese Zertifizierung der Wifi Alliance war bis vor kurzem noch nicht in Datenblättern der WLAN-Hardware zu finden und scheint nun langsam aber sicher immer wieder aufzutauchen. Dies sollte für uns Grund genug sein, sich dem Thema einmal zu widmen.

Wie die dahinter stehende Technik funktioniert und ob sie es dem WLAN ermöglicht, BLE in Sachen Ortung die Show zu stehlen, wollen wir in diesem Artikel näher beleuchten.

Unabhängig von der genutzten Technologie stellt die Ortung in modernen Netzen immer häufiger eine wichtige Funktion dar. Dies betrifft in unseren Planungsprojekten verschiedenste Kunden. Von der typischen Anwendung der Besucher-App in Museen oder in Messehallen, in denen eine Navigation gewünscht ist, bis zur Ortung von Geräten in der Produktion, lassen sich verschiedenste Anwendungsfälle identifizieren, die eine Lokalisierung benötigen.

weiter auf Seite 6

SecOps: Operative Informationssicherheit

von Dr. Markus Ermes und Dr. Simon Hoff

Die Grundlage für eine umfassende und nachhaltige Informationssicherheit bildet ein sogenanntes Information Security Management System (ISMS), in dem Organisation, Rollen und Verantwortlichkeiten sowie ein Richtlinienapparat für die Informationssicherheit festgelegt werden.

Hierzu gehören auch Prozesse zur Erstellung, Umsetzung und Pflege von Sicherheitskonzepten sowie zur Erkennung und Behandlung von Sicherheitsvorfällen und Schwachstellen. Ein ISMS hat also einen erheblichen operativen Anteil (Security Operations, kurz: SecOps). Typischerweise werden diese operativen Elemente der Informationssicherheit als spezieller kontinuierlicher Verbesserungsprozess (KVP, engl. Continuous Improvement Process) realisiert.

weiter auf Seite 16

Geleit

Was sagt uns das SEF-Theorem?

auf Seite 2

Standpunkt

Redundanz ist keine Versicherung!

auf Seite 14

Neues Seminar

Hybrid Cloud: RZ der neuen Generation

auf Seite 13

Aktuelles Seminar

Sommerschule Neueste Trends der IT-Infrastruktur

ab Seite 4

Geleit

Was sagt uns das SEF-Theorem?

Um die Pointe vorwegzunehmen: Das SEF-Theorem besagt, dass von den drei Zielen Security, Economy und Functionality maximal nur zwei zu haben sind. Oder anders formuliert: Sichere Nutzung von möglichst vielen Funktionen der IT ist aufwändig. Deshalb empfehle ich, dass Unternehmen, Verwaltungen und andere Organisationen zumindest einen Teil des mit IT erwirtschafteten Vorteils in IT-Sicherheit investieren, was bisher nicht ausreichend geschieht.

IT-Experten kennen Regeln, die Zielkonflikte zusammenfassen. Beliebt ist eine Dreierkombination von Zielen, mit dem Satz „take any two of the three“. Nun möchte ich eine bereits bestehende Kombination aus zwei Konsonanten und einem Vokal in der Mitte umdeuten. Einige Programmierer haben bereits das SEF-Theorem für „Structured, Extensible, and Forward Compatible“ aufgestellt. Die Bezugnahme auf diese Regel ist so selten (36 Google-Treffer), dass eventuell die von mir vorgeschlagene andere Ausschreibung des Akronyms bald die Oberhand gewinnen könnte: Security, Economy und Functionality.

Sicherheit, Wirtschaftlichkeit und Funktionalität bilden bisher einen typischen Zielkonflikt. Von diesen drei Zielen sind in einer IT-Infrastruktur nur zwei gleichzeitig erreichbar. Natürlich: diese drei Ziele sind keine binären Zustände (ja oder nein). Daher kann ich mein SEF-Theorem nicht mit Mitteln der Logik oder Mathematik beweisen, aber mit Empirie, also gestützt auf einige Jahre Erfahrung.

Wie definiere ich aber Sicherheit, Wirtschaftlichkeit und Funktionalität, um daraufhin zu behaupten, dass nur zwei von diesen drei Zielen erreichbar sind? Da es sich bei keinem dieser Ziele a priori um einen binären Zustand handelt, muss ich aus jedem Ziel quasi einen binären Zustand machen. Ich lege mich hiermit fest: Ausschlaggebend ist der Vergleich des Zustands eines einzelnen Anwenders bzw. einer einzelnen Anwenderin (nennen wir die Einheit vereinfachend „User“) mit dem Marktdurchschnitt. Wenn ein User hinsichtlich Betroffenheit von Sicherheitsvorfällen besser gestellt ist als 80% aller User im Markt, dann befindet er oder sie sich in einer sicheren IT-Infrastruktur. Gleiches bei Wirtschaftlichkeit, die erreicht wird, wenn die Kosten pro User im Vergleich zu mindestens 80% aller User im Markt niedriger sind. Und schließlich wird das Ziel Funktionalität erreicht, wenn die IT-Infrastruktur die denkbare Funktionalität weniger behindert als bei mindestens 80% aller User im

Markt. Ich habe bewusst einen bestimmten Markt (zum Beispiel einen nationalen Markt) als Bezugsgröße gewählt, damit ich mich bei der Kostenbetrachtung nicht mit solchen Problemen wie Kaufkraftdisparität verschiedener Märkte herumschlagen muss.

Zwei Beispiele aus der Praxis sollen mein SEF-Theorem belegen.

Beispiel Nummer 1: Sicherer Internetzugriff

Immer mehr Endgeräte wollen „nach Hause telefonieren“, können dies aber nicht uneingeschränkt tun, wenn sie sich in einer Umgebung befinden, aus der eine Kommunikation mit dem Internet nur über Proxies möglich ist. Der Hersteller Apple beschreibt dieses Problem für die eigenen Geräte im Support-Dokument HT203609. Die Empfehlung von Apple ist, bestimmte TCP-Ports für die Kommunikation mit dem ganzen IP-Adressbereich 17.0.0.0/8 zu erlauben, damit macOS- und iOS-Clients den Apple-Push-Benachrichtigungsdienst (APNs) nutzen können. Im besagten Apple-Artikel ist ausdrücklich erwähnt, dass APNs über Proxies nicht möglich ist.

Wenn das Beispiel Schule macht und immer mehr Hersteller von Endgeräten und Software die Öffnung von Ports für große Adressbereiche fordern, verlieren Sicherheitskomponenten wie Proxies teilweise ihren Sinn. Was tun?

Von einer Vielzahl an Möglichkeiten, mit dem Problem umzugehen, nenne ich hier nur drei:

- Die Umgehung von Proxies bleibt verboten. Das ist der Verzicht auf Funktionalität.
- Die Empfehlung von Apple und ähnliche Empfehlungen anderer Hersteller werden befolgt. In letzter Konsequenz wird das interne Netz zur Verlängerung des Internets. Das ist ein Verzicht auf Sicherheit. Auf das Argument, Perimeter-Security ist nur eine scheinbare, antworte ich mit der Frage nach der Bereitschaft, etwa die Roboter in der Fabrikhalle ins Internet zu stellen. Ist die Antwort nein, folgt daraus, dass Perimeter-Sicherheit doch keine so blöde Idee ist.
- Auf den Komponenten der Perimeter-Sicherheit werden die Regeln für neue Bedarfsfälle wie APNs konfiguriert, aber mit einer ständigen Protokollierung und Prüfung kombiniert. Zum Beispiel kann Machine Learning dazu eingesetzt werden, die Verkehrsprofile bei der Kommunikation mit dem Internet zu analysieren, um Auffälligkeiten festzustellen. Viele Daten müssen aufgezeichnet und mit komplexen Algorithmen analysiert werden. Auf Alarme muss reagiert werden. Aufgrund

Kommt die Ortung im WLAN wieder zurück?

Fortsetzung von Seite 1

Dr. Johannes Dams hat in den vergangenen Jahren zahlreiche wissenschaftliche Artikel im Bereich der theoretischen Informatik mit Bezug zu Algorithmen für Funknetzwerke veröffentlicht. Seit 2015 ist er als Berater bei der ComConsult GmbH im Competence Center Netze tätig. Der Fokus liegt hier unter anderem auf der Konzeption und Planung in den Bereichen WLAN, IPv6 und weiteren Aspekten aktiver Netzwerktechnik.

Viele der Ortungsanwendungen, die als Treiber der Technologie gesehen werden, arbeiten auf Basis von Smartphone- oder Tablet-Apps. Dies betrifft insbesondere Bereiche, in denen Besucher die Lokalisierung nutzen sollen. Klassische Beispiel-Anwendungen, die die Position des Endgeräts nutzen, gibt es eine ganze Reihe. Diese reichen von der mittlerweile üblichen Indoor-Navigation bis hin zu Anwendungen im Retail-Bereich. Auf einige Details zu derartigen Anwendungen wurde bereits in unserem Artikel zum Thema BLE-Beacons im Netzwerk Insider vom August 2018 eingegangen.

Dennoch möchte ich hier kurz auf einige exemplarische Fälle eingehen. So erlauben Navigationsanwendungen auch innerhalb von Gebäuden (also ohne GPS-Signal zur Ortung) eine Wegführung. Nützlich ist dies insbesondere da, wo der Nutzer sich nicht auskennt, oder in sich regelmäßig ändernden Umgebungen. Einem Messebesucher kann so der Weg zu dem gesuchten Ausstellerstand gewiesen werden oder einem Kunden der Weg zu einem Geschäft oder Regal mit dem gesuchten Produkt. Darüber hinaus können ortsabhängige Informationen auf dem Smartphone angezeigt werden. Einem Museumsbesucher kann somit eine individuelle digitale Tour geboten und Zusatzinformationen zu Künstlern und Werken auf dem Smartphone abhängig vom gerade betrachteten Kunstwerk angezeigt werden.

Im Retail-Bereich lässt sich sogenanntes „Proximity Marketing“ umsetzen, bei dem Werbung oder zum Standort passende Sonderangebote angezeigt werden. Aber auch die Ortung des Endgeräts selbst kann eine Rolle spielen. Das Wiederfinden eines Endgeräts im Gebäude kann im Sinne von Gerätemanagement, Asset-Tracking oder Ähnlichem durchaus hilfreich sein. Unterscheiden muss man hier Anwendungsfälle, bei denen ein Endgerät, wie ein Smartphone, seine Position bestimmen will und andere Anwendungsfälle, bei denen die Position eines Endgeräts oder Gegenstands nachverfolgt werden soll.

Immer mehr Anwendungen setzen auf eine Ortung und üblicherweise wird dafür eine entsprechende Infrastruktur benötigt. Im (fast schon) einfachsten Fall genügt eine Ortung mittels GPS (Global Positioning System). Hierbei ist die benötigte Infrastruktur in Form von Satelliten prinzipiell verfügbar. Die Ortung bei GPS ist allerdings meist auf den Außenbereich beschränkt. Im Innenbereich hingegen muss die benötigte Infrastruktur erst geschaffen werden.

Abhängig von der zugrunde liegenden Technologie bieten sich für den Innenbereich unterschiedliche Varianten an. In den letzten Jahren hat sich immer stärker der Einsatz von Bluetooth- bzw. BLE-Beacons durchgesetzt. Zuvor waren durchaus auch WLAN-basierte Ortungstechnologien üblich.

Die Ortung mittels WLAN könnte in Zukunft wieder an Relevanz gewinnen. Diesen Eindruck kann man insbesondere dann gewinnen, wenn man aktuelle Datenblätter von neuen Access-Points liest. Mittlerweile kann man hier auf das Feature „Wifi Location“ stoßen. Bei weiterer Recherche findet man so auch die entsprechende Zertifizierung der Wi-Fi Alliance (siehe [2]). Seit 2017 bietet die Wi-Fi Alliance bereits die entsprechende Zertifizierung an. Wenn nun erste große WLAN-Hersteller ebenfalls dieses Thema berücksichtigen, ist dies Grund genug für uns, Ortung im Gebäude nochmals zu betrachten und die Unterschiede und Chancen durch die neue Technologie hervorzuheben.

Im vorliegenden Artikel geben wir sowohl einen kurzen Überblick über die weiteren verfügbaren Indoor-Ortungstechnologien als auch über die technischen Aspekte der Ortung mittels Wi-Fi Location. Diese wird manchmal auch als Wi-Fi Round-Trip-Time (RTT) oder Fine Timing Measurement (FTM) bezeichnet. Wir wollen natürlich auch versuchen abzuschätzen, ob diese Technik eine Option für zukünftige Ortungsanwendungen ist.

Grundlagen verschiedener Ortungstechnologien

Es existiert eine ganze Reihe verschiedener Ortungstechnologien, die für die Lokalisierung von Endgeräten in Frage kommen. Neben den unterschiedlichen Anwendungen lassen sich auch weitere Parameter zur Unterscheidung der verschiedenen Technologien heranziehen. Aus technischer Sicht sind hier Triangulation und Trilateration zu nennen. Diese Techniken unterscheiden sich darin, ob der Winkel zwischen zu ortendem Objekt und fester Stationen oder die Entfernung zur Ortsbestimmung genutzt wird. Umgangssprachlich werden beide Varianten fälschlicherweise häufig auch als Triangulation zusammengefasst.

Für Ortungsanwendungen, beispielsweise bei Smartphones, wird meist der Winkel oder Abstand zu festen Punkten, wie den Bluetooth-Beacons, durch das Endgerät bestimmt. Zur endgültigen Positionsbestimmung auf Basis dieser Messungen muss das Endgerät die Positionen der festen Punkte kennen. Dies geschieht häufig durch eine Datenverbindung zu einem entsprechenden Server-System in der Infrastruktur. So kann das Endgerät dann auch die eigene Position ermitteln. Alternativ ermittelt das Server-System auf Basis der Daten die Position des Endgeräts.

Kommt die Ortung im WLAN wieder zurück?

Neben dem zu ortenden Endgerät sind also immer ortsfeste Stationen, wie beispielsweise Bluetooth-Beacons oder WLAN-APs, und auch entsprechende Infrastrukturkomponenten beteiligt. Nur durch diese Kombination ist eine Positionsbestimmung möglich.

Bei einer Triangulation werden die benötigten Winkel üblicherweise anhand eingehender Datenpakete durch mehrere Antennen bestimmt. Man spricht hier auch von der Bestimmung des „Angle of Arrival“. Natürlich gilt: Je genauer der bestimmte Winkel, desto genauer auch die Positionsbestimmung.

In Abbildung 1 ist ersichtlich, dass immer eine ausreichende Anzahl an ortsfesten, bekannten Stationen empfangen werden muss. Für eine flache zweidimensionale Karte sollte man mindestens drei Positionen vorsehen. Es wird auch klar, dass die genauen Positionen der bekannten Stationen für die Lokationsgenauigkeit ebenfalls entscheidend sind. Aufgrund der Messungenauigkeit und auch der möglichen Ungenauigkeit der bekannten festen Positionen ergibt sich folglich auch eine Varianz in Bezug auf die bestimmte Endgeräte-Lokation. Moderne Algorithmen ermöglichen es bei mehr empfangbaren Stationen die Lokalisierung deutlich zu verbessern.

Bei der Trilateration wird im Gegensatz zur Triangulation der Abstand zwischen Endgerät und mehreren ortsfesten Stationen gemessen. Zur Ermittlung der Entfernung kommen je nach Technologie verschiedene Verfahren zum Einsatz. Prinzipiell gilt hierbei aber auch wiederum, dass drei ortsfeste Stationen empfangen werden müssen.

Bei der Trilateration ergibt sich ebenfalls, wie in Abbildung 2 eindeutig dargestellt, dass eine genauere Messung der Entfernung auch zu einer genaueren Lokalisierung führt. Mehr empfangbare ortsfeste Stationen führen auch hier zu einer genaueren Positionsbestimmung.

Sowohl bei der Triangulation als auch bei der Trilateration gibt es eine Reihe von Implementierungen und damit auch technologische Varianten. Insbesondere die Art und Weise, wie die Entfernung oder der Winkel ermittelt werden, unterscheidet sich und führt zu unterschiedlicher Genauigkeit. Wie bereits erwähnt ist diese Genauigkeit der Messung ein entscheidender Faktor für die Genauigkeit der Lokalisierung.

Um einen kurzen Überblick über die Möglichkeiten und die Verwendung von Triangulation und Trilateration zu geben, lassen

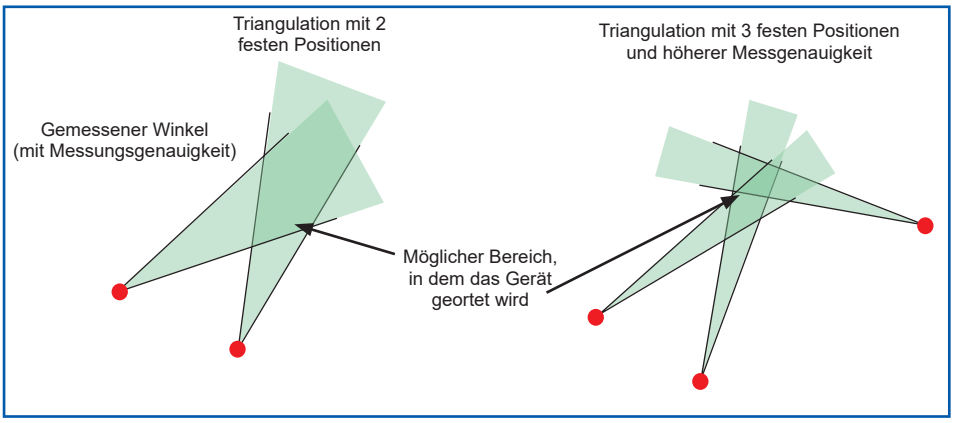

Abbildung 1: Triangulation mit unterschiedlicher Messgenauigkeit

sich ganz typische Ortungstechnologien als Beispiel heranziehen.

Die globalen Navigationssatellitensysteme „Global Positioning System“ (NAVSTAR GPS oder kurz GPS) aber auch GLOSNASS (russisch) oder Galileo (europäisch) setzen bei ihrer Ortung auf eine Form der Trilateration. Natürlich kann die Entfernung zu einem Satelliten in der Erdumlaufbahn nicht so einfach ermittelt werden. Um dies zu bewerkstelligen, senden die Satelliten Datenpakete aus, die ihre Flugbahnen und die genaue Uhrzeit enthalten. Zwischen verschiedenen Zeitpunkten und damit verschiedenen Satellitenpositionen ändert sich die Laufzeit der Signale. Hieraus berechnet der Empfänger (auch anhand seiner eigenen Uhr) die Entfernung der Satelliten und damit seine Position. Für eine Positionierung mittels GPS werden 4 Satelliten benötigt, um Ungenauigkeiten der Empfängeruhr zu bereinigen. Es gibt verschiedene Erweiterungen, wie Differential GPS, um die Genauigkeit weiter zu verbessern. Unter Idealbedingungen verspricht GPS so eine Genauigkeit unter 10 m.

Bei der Lokalisierung mittels BLE-Beacons auf Basis von Bluetooth Low Energy (BLE) wird zur Trilateration eine andere Messgrundlage eingesetzt. Wie bereits in unserem Insider-Artikel vom August 2018 beschrieben, wird hier die empfangene Signalstärke (RSSI – Received Signal Strength Indicator) des Beacon-Signals genutzt, um anhand der erwarteten Dämpfung des Signals die Entfernung zum Empfänger zu bestimmen. Klar ist, dass sich bei diesem Verfahren aufgrund der abzuschätzenden Dämpfung Fehler einschleichen. Diese ist schließlich eine sehr veränderliche Größe. Mehr dazu weiter unten in Bezug auf die bisher übliche Ortung mittels WLAN, die ein vergleichbares Verfahren einsetzt.

Neben der Bestimmung mittels RSSI für eine Trilateration ermöglicht Bluetooth bzw. BLE ab der Version 5.1 auch eine Triangulation. Der Winkel der eingehenden Beacons wird hier durch ein Anten-

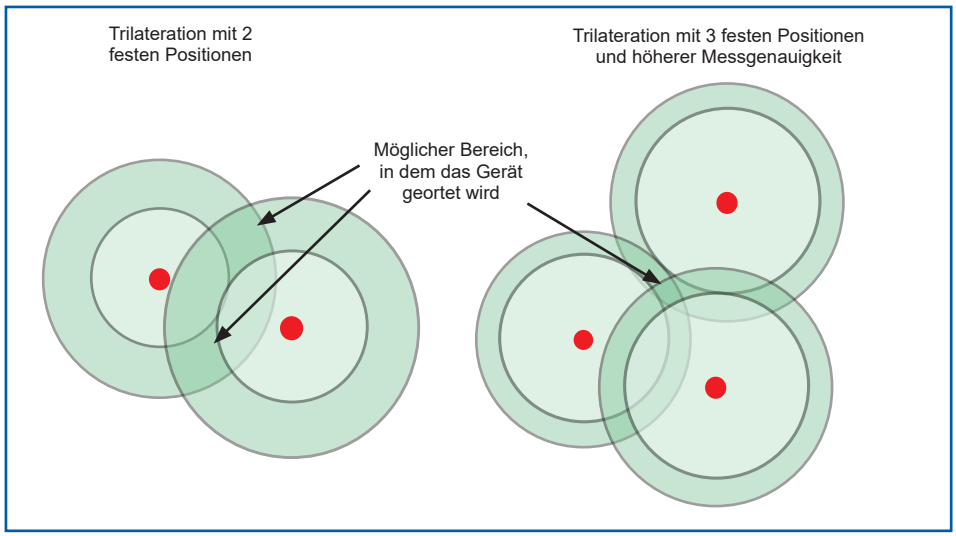

Abbildung 2: Trilateration mit unterschiedlicher Messgenauigkeit

SecOps: Operative Informations-sicherheit

Fortsetzung von Seite 1

Dr. Markus Ermes hat im Bereich der optischen Simulationen promoviert und Artikel in verschiedenen Fachzeitschriften veröffentlicht. Teil seiner Promotion waren Planung, Aufbau und Nutzung von verteilten und Höchstleistungs-Rechenclustern (HPC). Bei der ComConsult GmbH berät er Kunden im Bereich Rechenzentren, wobei seine Hauptaufgaben bei Netzwerken, Storage und Cloud-basierten Diensten liegen. Seine Kenntnisse im HPC-Bereich geben zusätzlich Einblicke in modernste Hochleistungstechnologien (CPU, Storage, Netzwerke), die in Zukunft auch im Rechenzentrum Einzug erhalten können.

Dr. Hoff ist technischer Direktor der ComConsult GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück.

Abbildung 1 illustriert einen solchen KVP anhand des Cybersecurity Framework des National Institute of Standards and Technology (NIST), das die folgenden Elemente spezifiziert [1]:

- **Identify:** Systematische Erfassung der zu schützenden IT sowie Analyse und Bewertung von Schutzbedarf und Risikolage
- **Protect:** Erarbeitung und Umsetzung von umfassenden Sicherheitsmaßnahmen

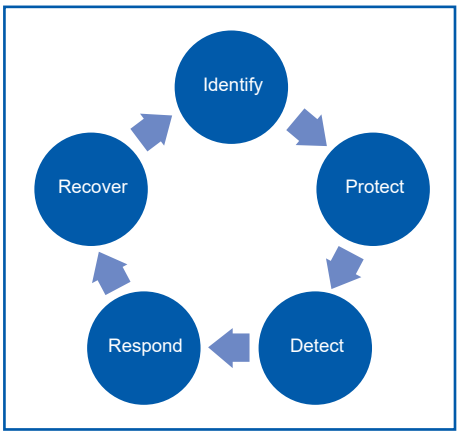

Abbildung 1: Kernelemente des NIST Cybersecurity Framework

- **Detect:** Erkennung von Schwachstellen und Sicherheitsvorfällen
- **Respond:** Aktivitäten zur Risikominimierung (und möglichst Beseitigung) von Schwachstellen und zur Schadensminimierung bei Sicherheitsvorfällen
- **Recover:** Rückkehr zum Alltag, (forensische) Analyse des Vorfalls und Lernen aus dem Vorfall

Wichtig ist dabei insbesondere der systematische Umgang mit Risiken, die sich beispielsweise aus unzureichend umgesetzten Maßnahmen oder aus Schwachstellen ergeben, die nicht schnell genug beseitigt werden können. Hierzu ist für die Informationssicherheit ein Risikomanagement erforderlich. Außerdem wird die Informationssicherheit durch Schnittstellen zu IT-Prozessen zum integralen Bestandteil der Prozesslandschaft.

Im Folgenden werden die wesentlichen Elemente der operativen Informationssicherheit genauer hinsichtlich folgender Fragestellungen betrachtet: Welche Anforderungen stellen anerkannte Standards und mit welchen Techniken können diese Anforderungen umgesetzt werden? Welche Kernprozesse sind für die operative Informationssicherheit notwendig und welche Schnittstellen zu anderen (IT-)Prozessen sind erforderlich? Welche Werkzeuge werden in der operativen Informationssicherheit eingesetzt? Wir werden uns dabei primär auf die Bereiche Detektion und Reaktion konzentrieren.

1. Relevante Standards zur Informationssicherheit

Wichtige Standards im Umfeld der Informationssicherheit, die natürlich auch die operativen Aspekte der Informationssicherheit berücksichtigen, sind ISO 27001 und ISO 27002 sowie der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI). Sehr hilfreiche Informationen liefert außerdem das bereits erwähnte “Framework for Improving Critical Infrastructure Cybersecurity” des NIST.

ISO 27001 und ISO 27002 und weitere Standards der Serie ISO 27xxx

Der Standard ISO 27001 spezifiziert Anforderungen „für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung“ eines ISMS. ISO 27001 legt hierzu auf einem vergleichsweise hohen Niveau einen umfassenden Satz von Sicherheitsmaßnahmen fest, der alle wesentlichen Bereiche der IT abdeckt (siehe Anhang A von ISO 27001):

- A.5 Informationssicherheitsrichtlinien
- A.6 Organisation der Informationssicherheit
- A.7 Personalsicherheit
- A.8 Verwaltung der Werte
- A.9 Zugangssteuerung
- A.10 Kryptographie
- A.11 Physische und umgebungsbezogene Sicherheit
- A.12 Betriebssicherheit
- A.13 Kommunikationssicherheit
- A.14 Anschaffung, Entwicklung und Instandhalten von Systemen
- A.15 Steuerung der Dienstleistungserbringung von Lieferanten
- A.16 Handhabung von Informationssicherheitsvorfällen
- A.17 Informationssicherheitsaspekte beim Business Continuity Management
- A.18 Compliance

Zu diesen Maßnahmen im Anhang A von ISO 27001 liefert der Standard ISO 27002 dann Umsetzungsempfehlungen. In den folgenden Kapiteln werden insbesondere für die Bereiche Detektion und Reaktion relevante Maßnahmen exemplarisch genauer betrachtet. Für die operative Informationssicherheit sind beispielsweise die Maßnahmen zu den Themen Betriebssicherheit (ISO 27001 A.12) und Handhabung von Informationssicherheitsvorfällen (ISO 27001 A.16) besonders wichtig.

Eine weitere Hilfestellung zur Umsetzung der Sicherheitsmaßnahmen liefern die anderen Standards der Serie ISO 27xxx. Manche dieser Standards sind eher von technischen Sicherheitsmaßnahmen geprägt, wie z.B. der Standard ISO 27033, der sich speziell mit der Absicherung von Kommunikationsnetzen beschäftigt. Andere Standards adressieren organisatorische Themen. Der Standard ISO 27035 „Information security incident management“ befasst sich beispielsweise mit der Behandlung von Sicherheitsvorfällen und beschreibt Organisation, Prozess-Schritte und notwendige Schnittstellen.

Warum ist ISO 27001 nun so wichtig? IT-Landschaften können nach ISO 27001 zertifiziert werden. Solche oder vergleichbare Zertifizierungen werden auch bei Ausschreibungen von IT-Dienstleistungen oft gefordert. Außerdem müssen kritische Infrastrukturen nach dem IT-Sicherheitsgesetz den Nachweis der nachhaltigen Umsetzung eines umfassenden ISMS erbringen, was durch eine entsprechende Zertifizierung z.B. nach ISO 27001 erleichtert wird.

BSI IT-Grundschutz

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit Erscheinen seines IT-Grundschutz-Kompendiums im Februar 2018 seinen IT-Grundschutz modernisiert[2]. Im Februar 2019 erfolgte dann ein erstes der jährlichen Updates des IT-Grundschutz-Kompendiums. Das IT-Grundschutz-Kompendium umfasst die in Abbildung 2 gezeigten System- und Prozessbausteingruppen:

- ISMS: Sicherheitsmanagement
- ORP: Organisation und Personal
- CON: Konzeption und Vorgehensweise
- OPS: Betrieb
- DER: Detektion und Reaktion
- APP: Anwendungen
- SYS: IT-Systeme
- IND: Industrielle IT
- NET: Netze und Kommunikation
- INF: Infrastruktur

Die wichtigen Bereiche Detect und Response der operativen Informationssicherheit deckt primär die Bausteingruppe *DER* Detektion und Reaktion ab und umfasst die folgenden Bausteine:

- DER.1 Detektion von sicherheitsrelevanten Ereignissen
- DER.2.1 Behandlung von Sicherheitsvorfällen
- DER.2.2 Vorsorge für die IT-Forensik
- DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle
- DER.3.1 Audits und Revisionen
- DER.3.2 Revision auf Basis des Leitfadens IS-Revision
- DER.4 Notfallmanagement

Ohne dass man hier in die Details der Bausteine eingehen muss, macht bereits die Zusammenstellung der Bausteine mehr als deutlich, dass gerade die Behandlung von Sicherheitsvorfällen ein ausgesprochen komplexes Thema ist. Während vielleicht die meisten Vorfälle mit einem überschaubaren Aufwand behandelt werden können, sind auch weitreichende Sicherheitsvorfälle zu berücksichtigen. Eine IT könnte beispielsweise Opfer eines zielgerichteten Angriffs (Advanced Persistent Threat, APT) werden, mit der Folge, dass höchst sensible Daten abfließen oder durch einen Stillstand der IT auch Unternehmensprozesse stillstehen und im Extremfall auch kritische Infrastrukturen, wie z.B. eine Stromversorgung signifikant gestört werden [3]. Ein Sicherheitsvorfall kann also durchaus auch zu einem Notfall eskalieren, und auch dies muss in den Vorgehensweisen und Prozessen zur operativen Informationssicherheit berücksichtigt werden.

2. Detect & Respond: Erkennung und Behandlung von Schwachstellen und Sicherheitsvorfällen

Für die Sicherheit der IT einer Institution ist es natürlich von entscheidender Bedeutung, dass man die eigenen Schwächen kennt, denn nur so kann zielgerichtet über eine Risikobetrachtung mit dem potentiellen Schaden umgegangen werden.

ISO 27001 fordert hier in Maßnahme A.12.6.1 „Handhabung von technischen Schwachstellen“, dass Information über technische Schwachstellen verwendeter Informationssysteme rechtzeitig eingeholt wird, die Gefährdung der Organisation durch derartige Schwachstellen bewertet wird und angemessene Maßnahmen ergriffen werden, um das dazugehörige Risiko zu behandeln.

Schwachstellenmanagement als Prozess

Kernelement ist dabei ein Prozess, der für die systematische Erfassung und Bewertung von Schwachstellen bzw. Verwundbarkeiten, die Planung von Korrekturmaßnahmen und die Kontrolle von Umsetzung und Wirksamkeit der Maßnahmen sorgt. Ein solcher Prozess zum Schwachstellenmanagement (Vulnerability Management) ähnelt dabei durchaus einem Prozess zur Behandlung von Sicherheitsvorfällen, nur handelt es sich hier um einen proaktiven Prozess, denn der Schaden ist (zunächst) noch nicht eingetreten.

Eine typische Regelung im Schwachstellenmanagement ist: Der jeweilige IT-System- oder Anwendungsverantwortliche ist für die systematische Sammlung von Informationen hinsichtlich Schwachstellen des von ihm betreuten Systems und für das Einspielen von Patches zustän-

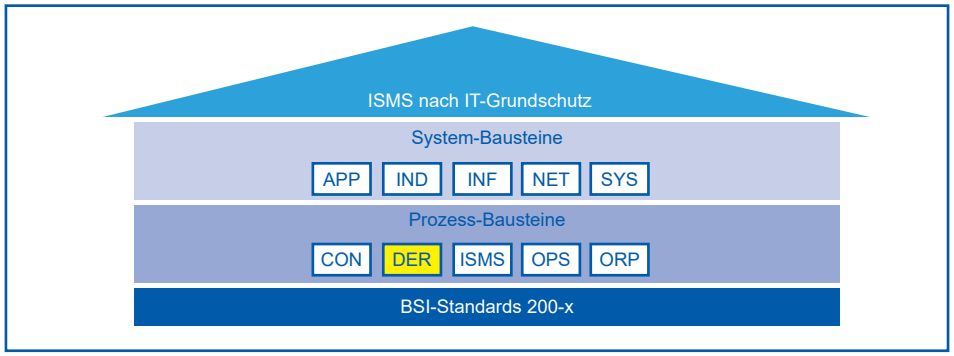

Abbildung 2: IT-Grundschutz-Kompendium des BSI