Michael **LANG** · Hans **LÖHR**

IT-Sicherheit

Technologien und Best Practices für die Umsetzung im Unternehmen

HANSER

Lang/Löhr (Hrsg.)

IT-Sicherheit

IT-Sicherheit

Technologien und Best Practices für die Umsetzung im Unternehmen

Herausgegeben von

Michael Lang und Hans Löhr

Mit Beiträgen von

Daniel Angermeier, Martin Braun, Hans Höfken, Thomas Jansen, Stefan Karg, Nicolai Kuntze, Hagen Lauer, Thomas Lohre, Markus Nauroth, Jutta Pertenaïs, Norbert Pohlmann, Andreas Reisch, Marko Schuba, Christoph Skornia, Fabian Topp, Marcel Winandy

HANSER

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über *http://dnb.d-nb.de* abrufbar.

Lektorat: Sylvia Hasselbach
Copy editing: Sandra Gottmann, Wasserburg
Umschlagdesign: Marc Müller-Bremer, *www.rebranding.de*, München
Umschlagrealisation: Max Kostopoulos
Titelmotiv: © stock.adobe.com/blackboard
Satz: Manuela Treindl, Fürth
Druck und Bindung: Eberl & Koesel, Altusried
Ausstattung patentrechtlich geschützt. Kösel FD 351, Patent-Nr. 0748702
Printed in Germany

Print-ISBN: 978-3-446-47223-5
E-Book-ISBN: 978-3-446-47347-8
E-Pub-ISBN: 978-3-446-47511-3

Inhalt

Vorwort

Informationen sind die wertvollsten Güter für Unternehmen. Die zur Informationsverarbeitung eingesetzten IT-Systeme sind heutzutage zentraler Bestandteil jedes Unternehmens und bilden die Grundlage für nahezu alle Geschäftsprozesse. Ohne sie funktioniert fast nichts mehr.

Kommt es zu Störungen in der IT, kann dies im schlimmsten Fall das komplette Unternehmen zum Stillstand bringen und existenzbedrohend sein. Gleiches gilt, wenn Informationen des Unternehmens oder dessen Kunden verloren gehen, gestohlen werden, manipuliert werden oder nicht mehr verarbeitet werden können.

Daher ist es für Unternehmen existenziell bedeutend, die Sicherheit der Informationen, Systeme und Produkte zu gewährleisten. Dies trifft heute mehr denn je zu, denn mit zunehmender Vernetzung wächst auch die Angriffsfläche: Jedes vernetzte Gerät ist ein potenzielles Einfallstor für Gefährdungen, und das erhöht das Risiko zusätzlich.

Doch wie können Sie Ihr Unternehmen vor diesen Gefährdungen schützen und Sicherheit gewährleisten?

Die Antwort auf diese Frage – und viele hilfreiche Impulse und Best Practices zur Umsetzung – erhalten Sie in diesem Buch.

Wir freuen uns, dass dazu 16 ausgewiesene Experten/Expertinnen als Autoren/Autorinnen an diesem Buch mitgewirkt haben, um Ihnen die relevanten Aspekte zur IT-Sicherheit von Unternehmen zu beschreiben.

Wir wünschen Ihnen viel Spaß beim Lesen des Buches und viel Erfolg beim Umsetzen der dabei gewonnenen Erkenntnisse!

Ihre Herausgeber

Michael Lang und Hans Löhr

1 IT-Sicherheit konsequent und effizient umsetzen

Norbert Pohlmann

In diesem Beitrag erfahren Sie,

- welche Chancen und Risiken die fortschreitende Digitalisierung mit sich bringt,
- welche Angriffsvektoren heute für erfolgreiche Angriffe genutzt werden,
- welche IT-Sicherheitsstrategien helfen, Risiken zu reduzieren und mit verbleibenden Risiken umzugehen, und
- welche IT-Sicherheitsmechanismen gegen welche Angriffe wirken.

1.1 Einleitung

Wir befinden uns gerade in einer digitalen Transformation, die mit einer radikalen Umgestaltung unseres Alltags und unserer Arbeitswelt sowie aller Geschäftsmodelle und Verwaltungsprozesse einhergeht. Wirtschaftskraft und Wohlstand sowie die Leistungsfähigkeit unserer modernen Gesellschaft werden durch den gelungenen digitalen Wandel bestimmt.

1.1.1 Chancen durch die Digitalisierung

Die Digitalisierung eröffnet über alle Branchen und Unternehmensgrößen hinweg enorme Wachstumschancen und führt zu immer besseren Prozessen, die die Effizienz steigern und Kosten reduzieren. Die Digitalisierung beschleunigt auf allen Ebenen, und der Wertschöpfungsanteil der IT in allen Produkten und Lösungen wird immer größer (Pohlmann 2020) (siehe Bild 1.1, obere Kurve).

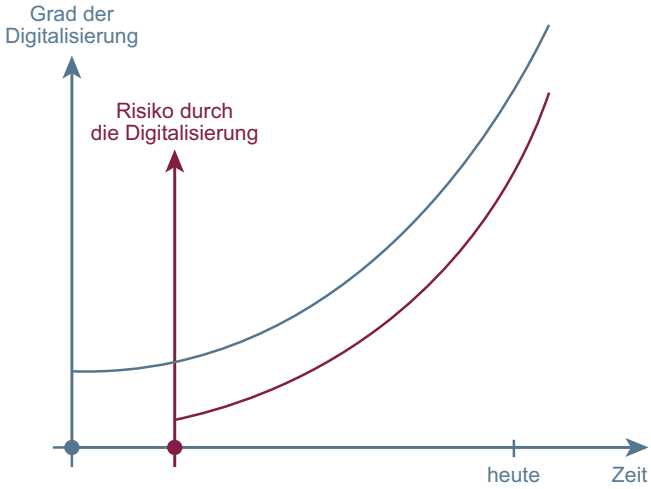

Bild 1.1 Entwicklung der Digitalisierung und des korrespondierenden Risikos

Mögliche Erfolgsfaktoren der Digitalisierung sind vielfältig:

- Mit 5G- und Glasfasernetzen erhöhen sich Kommunikationsgeschwindigkeit und -qualität, wodurch neue Anwendungen möglich werden.
- Smarte Endgeräte wie Smartwatches, Smartphones, PADs oder IoT-Geräte bringen viele neue sinnvolle Anwendungen mit sich.
- Zunehmend leistungsfähige zentrale IT-Systeme wie Cloud-Systeme, Edge-Computing oder Hyperscaler schaffen Innovationen mit großen Potenzialen.
- Da immer mehr Daten zur Verfügung stehen, ist die Verwendung von KI (ML ...) ein weiterer Treiber von neuen Geschäftsmodellen (Pohlmann 2019a).
- Moderne Benutzerschnittstellen, wie Sprache und Gestik, vereinfachen die Bedienung der smarten Endgeräte.
- Die Optimierung von Prozessen schafft ein enormes Rationalisierungspotenzial, das es zu heben gilt, um wettbewerbsfähig zu bleiben und Wachstumschancen zu nutzen.
- Neue Optionen wie Videokonferenzen und Cloud-Anwendungen ermöglichen, im Homeoffice zu arbeiten und damit die Personenmobilität zu reduzieren sowie letztendlich die Umwelt zu schonen.

1.1.2 Risiken durch die Digitalisierung

Wir müssen aber auch feststellen, dass seit Beginn der IT – sowie jetzt mit der zunehmenden Digitalisierung – die IT-Sicherheitsprobleme jedes Jahr größer werden und auf absehbare Zeit definitiv nicht abnehmen. Eine wichtige Erkenntnis ist, dass die heutigen IT-Architekturen unserer Endgeräte, Server, Netzkomponenten und zentralen IT-Dienstleistungen nicht sicher genug konzipiert und aufgebaut sind, um den Angriffen intelligenter Hacker erfolgreich entgegenzuwirken. Die Vielzahl der lokalen und zentralen Anwendungen, die unterschied-

lichen Zugänge zum Internet, die Masse der IT-Systeme und IT-Infrastrukturen sowie die zunehmenden Abhängigkeiten innerhalb der Supply Chain machen die Komplexität der IT immer größer und damit auch die Anfälligkeit für bösartige Angriffe. Täglich können wir den Medien entnehmen, wie sich kriminelle Hacker die unzureichende Qualität der Software zunutze machen, indem sie Malware installieren und damit Passwörter sowie Identitäten stehlen, Endgeräte ausspionieren oder die IT-Systeme verschlüsseln, um Lösegeld für die notwendigen Schlüssel zur Entsperrung zu erpressen. Aufgrund der generierten Datenmengen werden die Angriffsziele mit fortschreitender Digitalisierung kontinuierlich lukrativer.

Die Robustheit und Resilienz unserer IT-Systeme sind nicht hinreichend, und der Level an IT-Sicherheit entspricht nicht dem „Stand der Technik“. Mit dem höheren Grad an Digitalisierung steigt momentan das Risiko eines Schadensfalls (siehe Bild 1.1, untere Kurve). Daraus ergibt sich in der Konsequenz, dass durch Diebstahl, Spionage und Sabotage der deutschen Wirtschaft jährlich ein Gesamtschaden von mehr als 220 Milliarden Euro entsteht.

1.1.3 IT-Sicherheitsbedürfnisse als Grundwerte der IT-Sicherheit

IT-Sicherheitsbedürfnisse sind Grundwerte der IT-Sicherheit, die mithilfe von IT-Sicherheitsmechanismen befriedigt werden können. IT-Sicherheitsbedürfnisse werden auch als IT-Sicherheitsziele bezeichnet.

- **Gewährleistung der Vertraulichkeit**
  Vertraulichkeit ist wichtig, damit keine unautorisierten Personen oder Organisationen in der Lage sind, übertragene oder gespeicherte Informationen zu lesen.
- **Gewährleistung der Authentifikation**
  Mithilfe des IT-Sicherheitsmechanismus Authentifikation wird verifiziert, wer der Partner bei der Kommunikation oder Transaktion ist beziehungsweise welcher Nutzer auf Betriebsmittel und Informationen zugreift.
- **Gewährleistung der Authentizität**
  Mithilfe des IT-Sicherheitsmechanismus Authentizität wird verifiziert, dass Informationen oder Identitäten echt sind.
- **Gewährleistung der Integrität**
  Beim IT-Sicherheitsbedürfnis „Gewährleistung der Integrität“ wird überprüft, ob Informationen, die übertragen werden oder gespeichert sind, unverändert, das heißt original, sind.
- **Gewährleistung der Verbindlichkeit**
  Das IT-Sicherheitsbedürfnis „Gewährleistung der Verbindlichkeit“ sorgt für die Gewissheit, dass die Prozesse und die damit verbundenen Aktionen auch verbindlich sind.
- **Gewährleistung der Verfügbarkeit**
  Dieses IT-Sicherheitsbedürfnis sorgt für die Gewissheit, dass die Informationen und Dienste auch zur Verfügung stehen.
- **Gewährleistung der Anonymisierung**/Pseudonymisierung
  Mit diesem IT-Sicherheitsbedürfnis wird gewährleistet, dass eine Person nicht oder nicht unmittelbar identifiziert werden kann.

1.2 Beispiele von aktuellen Angriffsvektoren

Im Folgenden werden exemplarisch relevante Beispiele von Angriffsvektoren mit den entsprechenden Angriffstechniken und Angriffswegen dargestellt.

1. **Malware-Infiltration über manipulierte Webseiten**
   Als Erstes wird mit einem gezielten Hacking-Angriff auf den Webserver die Platzierung von Angriffssoftware zur Durchführung eines Drive-by-Downloads unter Nutzung einer vorhandenen Schwachstelle auf dem Webserver umgesetzt. Um einen Nutzer (Opfer) zum Besuch der manipulierten Webseite zu motivieren, kann beispielsweise ein Phishing-/Social-Engineering-Angriff durchgeführt werden. Beim Zugriff auf die manipulierten Webseiten werden dann beim Drive-by-Download Sicherheitslücken des Browsers oder des Betriebssystems des Opfer-IT-Systems des Nutzers ausgenutzt, um Malware zu installieren. Mit der generalisierten installierten Malware kann dann der Angreifer spezielle Schadfunktionen nutzen, um das gekaperte IT-System gemäß seinem Ziel zu manipulieren.

2. **Malware-Infiltration über schadhafte E-Mail-Anhänge**
   Mithilfe von sozialen und Berufsnetzwerken werden die Vorlieben eines potenziellen Opfers analysiert. Mit diesen Kenntnissen wird dem Opfer eine persönliche Nachricht gesendet, die perfekt dazu verleitet, auf den Anhang der E-Mail zu klicken. Durch das Klicken wird ein Prozess ausgelöst, der ermöglicht, über vorhandene Schwachstellen eine Malware zu installieren. Damit ist die Übernahme der Kontrolle über das betroffene Opfer-IT-System umgesetzt. Anschließend nutzt der Angreifer entsprechende Schadfunktionen, um seine Ziele auf dem Opfer-IT-System umzusetzen.

3. **Mehrstufiger Angriff auf die IT-Infrastruktur von Unternehmen**
   Ein Angreifer verschafft sich einen ersten Zugang auf ein IT-System in einem Unternehmen, wie in den Beispielen 1 und 2 beschrieben. Dann sorgt der Angreifer mit der Schaffung einer individualisierten Malware dafür, dass er den Zugang etabliert, um sich im IT-System frei bewegen zu können und seine Spuren zu verwischen. Anschließend verschafft sich der Angreifer mit zusätzlichen Angriffstechniken mehr Administrationsrechte. Damit kann er die Kontrolle über weitere IT-Systeme bekommen und lateral in große Teile des Netzwerks gelangen. So sammelt der Angreifer umfangreiches Wissen über vorhandene Schwachstellen, Funktionen oder Werte auf den IT-Systemen des Unternehmens und kann darüber eine Strategie für den eigentlichen Angriff entwickeln und erfolgreich umsetzen. Diese Vorgehensweise wird auch als Advanced Persistent Threat (APT) bezeichnet.

4. **Man-in-the-Middle-Angriff (MITM)**
   Bei der Man-in-the-Middle-Angriffsmethode schleust sich ein Angreifer aktiv, aber heimlich – physisch oder logisch – in die Kommunikation zwischen mindestens zwei Kommunikationspartnern mit dem Ziel, Daten lesen oder manipulieren zu können. Die Kommunikationspartner bemerken diesen Eingriff nicht und gehen davon aus, dass sie direkt und vertraulich miteinander kommunizieren, da sich der Angreifer bei beiden Kommunikationspartnern jeweils als das wahrgenommene Gegenüber ausgibt. Durch einen Man-in-the-Middle-Angriff ist es möglich, Passwörter oder weitere wichtige Daten mitzulesen, Kommunikationsverbindungen zum Beispiel nach einer Authentifikation zu übernehmen oder Daten zu manipulieren.

5. **Angriff mithilfe eines Software-Updates (Supply-Chain-Angriff)**
   Bei einem Supply-Chain-Angriff oder Lieferketten-Angriff ist die prinzipielle Idee, dass ein vertrauenswürdiger Dienst (Software), der seit längerer Zeit bei einer Organisation/einem Unternehmen in Einsatz ist, irgendwann für einen Angriff verwendet wird. Als Angriffsvektor missbraucht der Angreifer ein legitimiertes Software-Update, das der vertrauenswürdige Softwarehersteller (Supplier) zur Verfügung stellt. Für die Durchführung dringt der Angreifer zuerst in das IT-System des vertrauenswürdigen Softwareherstellers ein und infiltriert ein Software-Update mit Malware. Voraussetzung für den eigentlichen Angriff ist, dass dieser Vorgang unbemerkt bleibt, daher muss er an einer bestimmten Prozessstelle umgesetzt werden. Nur so lässt sich sicherstellen, dass das manipulierte Software-Update offiziell als Hersteller-Update digital signiert wird, wodurch es mit einem autorisierten Code versehen ist und dadurch vom Kunden akzeptiert und eingespielt werden kann. Darauf basierend ist es dem Angreifer möglich, bei mehreren Tausend Organisationen gleichzeitig das Software-Update des Herstellers zu nutzen, um die eigentlichen Angriffe umzusetzen. Beispiele dieser Angriffsmethode sind: Kaseya und SolarWinds.
6. **Angriff auf die Verfügbarkeit von IT-Systemen (DDoS-Angriff, Distributed Denial of Service)**
   Der Angreifer nutzt die Schwachstelle aus, dass IT-Systeme nur begrenzte Ressourcen (Bandbreite, CPU, RAM ...) haben. Für den Angriff wird das IT-System gezielt mit einer großen Last spezieller Anfragen überflutet, dadurch überlastet und letztendlich lahmgelegt. Dies wird in der Regel unter Einsatz von Botnetzen, bei denen die Bots die Schadfunktion DDoS aktiviert haben, und weiteren Verstärkungsmechanismen wie Reflection und Amplification erfolgreich umgesetzt. Die Motivation der Angreifer ist vielfältig: Entweder soll ein IT-System für eine definierte Zeit lahmgelegt werden, um beispielsweise einen Wettbewerber zu behindern, oder es steckt eine erpresserische Absicht dahinter, um von dem angegriffenen Unternehmen eine bestimmte Summe verlangen zu können, damit der DDoS-Angriff gestoppt oder gar nicht erst durchgeführt wird.
7. **Missbräuchliche Ausnutzung einer Business-Beziehung mit einem High-Level-Phishing-Angriff**
   Ein Angreifer erlangt mithilfe eines Malware-Keyloggers den Zugang zu einem E-Mail-Konto im Unternehmen. In der Vorbereitungsphase analysiert der Angreifer kontinuierlich die E-Mails des angegriffenen Mitarbeiters dahingehend, welche Informationen für einen Angriff verwendbar sind. Das kann zum Beispiel eine hohe Rechnung an einen langfristigen Kunden sein. Sobald diese über das E-Mail-Konto versendet wird, beginnt der Angriff. Im ersten Schritt wird dafür diese E-Mail zusammen mit allen alten Inhalten kopiert, im zweiten Schritt dann in der PDF-Rechnung die Kontonummer verändert. Nach einer sehr kurzen Zeitspanne erfolgt dann der Versand dieser E-Mail zusammen mit einer E-Mail, in der der Angreifer nachfragt, ob die Rechnung bereits beglichen wurde. Der Zeitpunkt muss so gewählt sein, dass es sehr unwahrscheinlich ist, dass eine Bezahlung bereits stattgefunden hat. Denn nur so ist es möglich, das angegriffene Unternehmen dazu aufzufordern, die Rechnung an eine neue Kontonummer zu überweisen, zum Beispiel mit der Begründung, dies sei aufgrund aktueller Sicherheitsvorkehrungen notwendig geworden. Wichtig ist, dass diese E-Mail seitens des Angreifers von einem anderen E-Mail-Konto versendet wird, damit der Mitarbeiter – dessen E-Mail-Account kompromittiert wurde – den Vorgang nicht mitbekommt. Trotzdem ist bei dieser E-Mail der eigentliche Mitarbeiter als Absender angegeben (Mail-Spoofing). Als Return-Pfad

im E-Mail-Header ist jedoch eine andere E-Mail-Adresse angegeben, damit, falls der Empfänger eine Nachfrage hat, diese nicht bei dem Mitarbeiter des (angegriffenen) Unternehmens ankommt, denn in diesem Szenario ist es zwingend notwendig, dass der Angreifer diese (eventuelle) E-Mail erhält, damit er entsprechend reagieren kann. Dass der Empfänger glaubt, die E-Mail kommt von der altbekannten Kundenbeziehung, lässt sich dadurch erreichen, indem die Absenderadresse dieselbe ist und Fragmente älterer E-Mails integriert sind. Durch diese umfangreiche Vorarbeit ist sichergestellt, dass das angegriffene Unternehmen den geforderten Betrag auf das neue Konto überweist. Aufgrund längerer Zahlungsziele, zum Beispiel von sechs Wochen, fällt den beteiligten Unternehmen nicht rechtzeitig auf, dass sie einem Phishing-Angriff ausgesetzt waren. Daher ist die Verfolgung des Vorfalls sehr schwer bis unmöglich.

8. **Nutzung von homografischen Domänen für einen Angriff**
   Eine Ergänzung zum Angriffsvektor 7 im Business-Bereich ist, dass der Angreifer eine ähnliche Domäne, eine sogenannte homografische Domäne, eines Unternehmens registriert, um diese für einen Angriff zu nutzen. Dies ist möglich, da die homografische Domäne Zeichen enthält, die den Buchstaben der originalen Domäne ähnlich sind, etwa die Ziffer 0, die dem Buchstaben O ähnelt, oder die Buchstaben l (kleines L) und I (großes i). Beispiel für eine homografische Domäne: internet-sicherheit.de – im Original mit einem i am Anfang –, manipuliert mit einem kleingeschriebenen L, also lnternet-sicherheit.de.

   Der Angreifer kann diese Domäne für einen E-Mail-Dienst nutzen, um sich so fälschlicherweise als das eigentliche Unternehmen auszugeben, da der Empfänger die Täuschung mit hoher Wahrscheinlichkeit nicht bemerkt. Dadurch ist es dem Angreifer möglich, mit einer beliebigen falschen E-Mail-Adresse eine Kommunikationsbeziehung mit einem Mitarbeiter eines beliebigen Kunden von dem anvisierten Unternehmen aufzubauen, denn Kommunikationsinhalte sowie die richtigen Kommunikationspartner lassen sich leicht und strukturiert über Webseiten, Social-Media-Kanäle sowie Businessnetzwerke ermitteln. So ist es möglich, einen hohen Schaden anzurichten, beispielsweise bezüglich der Reputation: Aufkündigung von Verträgen oder Veränderung von Konditionen zuungunsten des Unternehmens.

9. **Die Geschichte eines erfolgreichen APT-Angriffs**
   Ein Steuerberater erhält per E-Mail die Mitteilung, dass über einen längeren Zeitraum eine Kopie seiner kompletten Mandantenkartei angefertigt wurde. In der gleichen E-Mail fordert der Angreifer den Steuerberater auf, 100.000 Euro zu zahlen, da er ansonsten den gesamten Datenbestand veröffentlichen würde. Zum Beweis, dass der Steuerberater nicht kontinuierlich zahlen müsse, übersendet der Angreifer, als Zeichen seiner Vertrauenswürdigkeit, eine Referenzliste. In dieser waren die Kontaktdaten derjenigen Steuerbüros aufgeführt, die aufgrund der Zahlung tatsächlich eine Veröffentlichung dauerhaft abgewendet haben. Interessant ist in diesem Fall auch die Frage bezüglich der Höhe des geforderten Betrags – also warum nicht 50.000 oder 250.000 Euro? Die Erklärung dafür lieferten im Weiteren die Experten, die der Steuerberater zu Hilfe holte. Diese fanden heraus, dass der Angreifer sich tief in die IT des Steuerberaters eingenistet hatte. Das ließ den Schluss zu, dass es sich nicht um Freizeit-Hacker handelte, sondern ein Profi mit einem langfristigen „Geschäftsmodell“ am Werk war, der die Lösegeldzahlung als einmalige und deshalb für die Opfer lohnenswerte Investition sieht. Zur Ermittlung der Summe hatte der Angreifer jahrelang jede digitale Bewegung beobachtet, geduldig die betriebswirtschaftliche Entwicklung des Steuerbüros verfolgt und dann zugeschlagen als das Geschäft für ihn einträglich, aber gleichzeitig für den Steuerberater wirtschaftlich verkraftbar war.

1.3 IT-Sicherheitsstrategien

Durch die steigende Digitalisierung wird das Risiko eines Schadens immer größer (siehe Bild 1.2, rote Kurve), weil dadurch nicht nur die Angriffsziele kontinuierlich lukrativer werden, sondern auch die Angriffsfläche zunehmend größer wird. Um diese Situation im Sinne der Unternehmen zu verbessern, werden grundsätzliche IT-Sicherheitsstrategien benötigt, die die IT-Sicherheitsrisiken strategisch reduzieren (siehe Bild 1.2, gestrichelte Kurve).

- **IT-Sicherheitsstrategien zur Reduzierung der Risiken**
  Die IT-Sicherheitsstrategien „Vermeiden von Angriffen“ und „Entgegenwirken von Angriffen“ helfen, den Level an verbleibenden Risiken so weit wie möglich zu verringern und zu halten. Die verbleibenden Risiken beschreiben die noch vorhandene Eintrittswahrscheinlichkeit eines Schadens, der trotz durchgeführter IT-Sicherheitsmaßnahmen zur Reduzierung der Risiken in Unternehmen auftreten kann, weil es keine hundertprozentige IT-Sicherheit gibt.
- **IT-Sicherheitsstrategien, um mit verbleibenden Risiken umzugehen**
  Da mit dem Einsatz der IT-Sicherheitsstrategien zur Reduzierung der Risiken keine hundertprozentige IT-Sicherheit erzielt werden kann, müssen weitere IT-Sicherheitsstrategien für die verbleibenden Risiken angewendet werden. Hier helfen die zwei IT-Sicherheitsstrategien „Erkennen von Angriffen“ und „Reagieren auf Angriffe“.

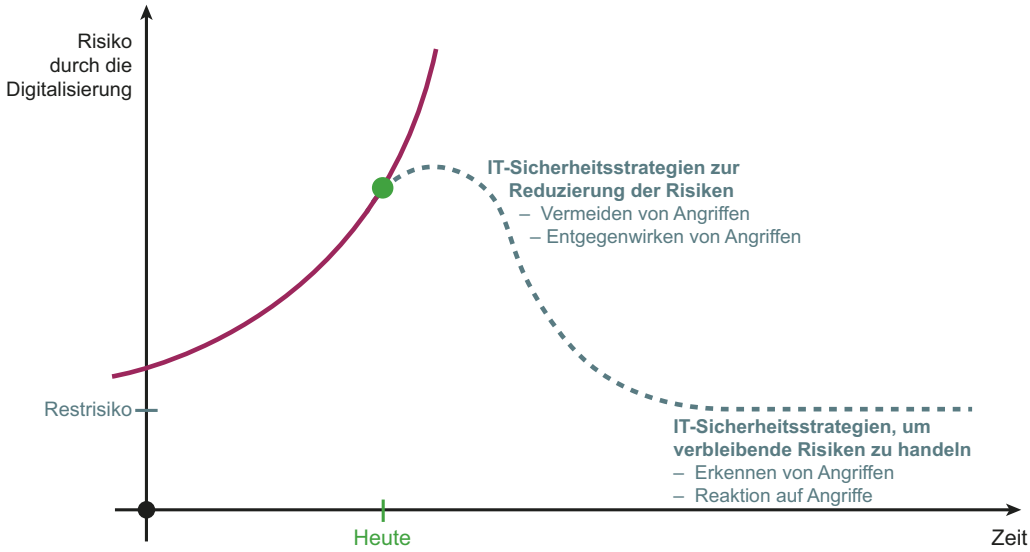

Bild 1.2 IT-Sicherheitsstrategien, um die Risiken der Digitalisierung zu managen

Im Folgenden werden die vier prinzipiellen IT-Sicherheitsstrategien beschrieben, die helfen können, IT-Sicherheitsmechanismen in strategische Ziele einzuteilen, um die Risiken der Digitalisierung zu managen. So können deren Wirkung auf Angriffe und den Schutz der Werte besser verstanden und geeignete IT-Sicherheitsstrategien ausgesucht sowie umgesetzt werden.

1.3.1 Vermeiden von Angriffen

Eine generelle IT-Sicherheitsstrategie zum Schutz der Werte eines Unternehmens ist die Idee, einen Schaden durch Angriffe zu vermeiden – die sogenannte Vermeidungsstrategie. Durch diese Vorgehensweise wird eine Reduzierung der Angriffsfläche und damit die Reduzierung der Risiken erreicht.

Im Folgenden werden unterschiedliche Prinzipien der Vermeidung erfolgreicher Angriffe aufgezeigt:

1. **Prinzip der Datensparsamkeit**
   Ein Aspekt der Vermeidungsstrategie ist das Prinzip der Datensparsamkeit, das heißt, so wenige wertvolle Daten generieren wie möglich und nur so viele wie nötig. Das Prinzip: Daten, die nicht auf IT-Systemen vorhanden sind, können nicht angegriffen werden. Daher sollten nur Daten gespeichert werden, die wirklich notwendig sind. Abgeleitete Daten, Zusammenfassungen und so weiter sollten nicht permanent erfasst, sondern bei Bedarf automatisiert neu berechnet werden.
2. **Nur sichere IT-Technologien, -Produkte und -Dienste verwenden**
   Ein weiteres Prinzip der IT-Sicherheitsstrategie Vermeiden von Angriffen ist: „Keine Technologien, Produkte und Dienste mit bekannten Schwachstellen verwenden“. Dazu müssen natürlich die entsprechenden Schwachstellen bekannt sein, damit ihnen begegnet werden kann. Beispiele von IT-Lösungen, bei denen dieses Prinzip umgesetzt werden kann, sind Browser, Betriebssysteme und Internet-Dienste. Hilfreich ist hier die Realisierung einer Zwei-Hersteller-Strategie beispielsweise bei Browsern. Diese ermöglicht, dass, wenn bei einem Browser Schwachstellen bekannt werden, unmittelbar der zweite Browser, ohne bekannte Schwachstelle, mit allen Einstellungen weiterverwendet werden kann.
3. **Fokussierung**
   Aus Studien ist bekannt, dass im Schnitt circa fünf Prozent aller vorhandenen Daten in Unternehmen besonders schützenswert sind. Welche Daten zu den fünf Prozent gehören und von daher besonders schützenswert sind, wissen die Verantwortlichen in der Regel nicht genau. Generell sind dies unter anderem Daten, die dem Unternehmen einen hohen Schaden verursachen, wenn sie in die Hände des Wettbewerbs fallen würden, also beispielsweise das geistige Eigentum des Unternehmens, Kalkulationsdaten oder Kundendaten. Aus diesem Grund ist eine Schutzbedarfsanalyse notwendig, um diese unternehmenskritischen Daten auf den vorhandenen IT-Systemen zu identifizieren und deren IT-Schutzbedürfnisse genau zu kennen. Mit dem exakten Wissen, welche Daten für das Unternehmen besonders schutzbedürftig sind, werden die Verantwortlichen in die Lage versetzt, sich auf möglichst wenige IT-Systeme zu konzentrieren und diese besonders zu schützen. So sind zum Beispiel, wie in Bild 1.3 aufgezeigt, nur auf dem IT-System in der Mitte besonders sicherheitsrelevante Werte gespeichert sind, die schlussfolgernd der IT-Schutzbedürfnisse spezifisch und besonders geschützt werden müssen.
4. **Reduzierung von IT-Möglichkeiten**
   Die Reduzierung der IT-Möglichkeiten ist ein weiteres Prinzip zur Vermeidung von Angriffen. Nicht notwendige Software vom IT-System entfernen, nicht verwendete Funktionen einer Anwendung deaktivieren oder Kommunikationsmöglichkeiten zum Beispiel mithilfe von Routern und Firewall-Systemen reduzieren, all diese Maßnahmen helfen, die potenziellen Angriffsflächen zu verringern.

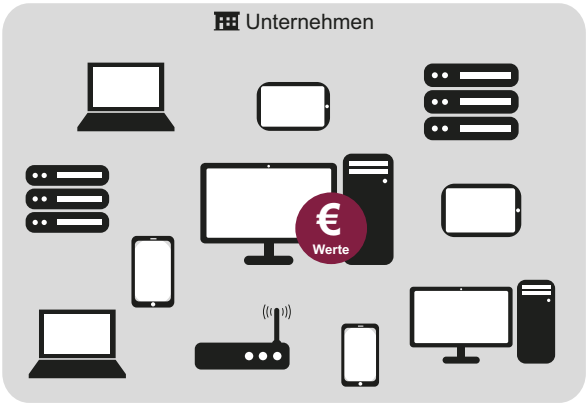

Bild 1.3 Idee der Fokussierung

5. **Sicherheitsbewusste Mitarbeiter**
   Security Awareness, also das Vorhandensein eines Sicherheitsbewusstseins, ist ein weiterer wichtiger Punkt der Vermeidungsstrategie. Sicherheitsbewusstsein setzt sich aus Wissen und einer bestimmten Einstellung der Mitarbeiter zusammen, beides dient dazu, die IT mit all ihren Werten zu schützen. Das relevante Wissen erstreckt sich hierbei über die Werte eines Unternehmens, die zu schützen sind, den Schutzbedarf dieser Werte sowie die Bedrohungen, die auf diese Werte wirken; aber auch unter anderem darüber, welche organisatorischen Regelungen einzuhalten sind, oder die richtige Nutzung von IT-Sicherheitsmaßnahmen zum Schutz der Werte. Mit der Einstellung ist gemeint, dieses Wissen zu verinnerlichen und zum Schutz des Unternehmens aktiv umzusetzen.
6. **Bewertung der Vermeidungsstrategie**
   Das Vermeiden von Angriffen ist die beste IT-Sicherheitsstrategie, um Schäden zu reduzieren. Leider ist die Vermeidungsstrategie jedoch praktisch nur eingeschränkt umsetzbar, da eine bestimmte Anzahl an IT-Systemen und Daten benötigt wird, um die gewünschten digitalen Aktivitäten umzusetzen. Das Vermeiden von Angriffen reduziert zwar die Angriffsfläche, aber für die gewollten IT-Anwendungen und -Dienste sowie die erforderliche Kommunikation etwa mit Kunden oder Dienstleistern muss eine weitere IT-Sicherheitsstrategie, wie das Entgegenwirken von Angriffen, zum Einsatz kommen, um die vorhandenen Risiken weiter zu minimieren.

1.3.2 Entgegenwirken von Angriffen

Das Entgegenwirken von Angriffen ist die meistverwendete IT-Sicherheitsstrategie, um das vorhandene Risiko zu minimieren und damit Schäden zu vermeiden. Dazu werden IT-Sicherheitsmechanismen verwendet, die eine hohe Wirkung gegen bekannte Angriffe zur Verfügung stellen. Die Stärke der Wirkung eines IT-Sicherheitsmechanismus hängt prinzipiell von unterschiedlichen Aspekten ab. Außerdem müssen die Fachkenntnisse, Gelegenheit und Ressourcen der Angreifer bei der Diskussion der Wirksamkeit betrachtet werden. Da Angriffe immer ausgefeilter, komplexer und intelligenter werden, müssen IT-Sicherheitsmechanismen kontinuierlich optimiert werden, um die notwendige Wirkung aufrechtzuhalten (Pohlmann 2019b).

IT-Sicherheitsmechanismen, die gegen spezielle Angriffe wirken, sind zum Beispiel:

- **Verschlüsselung**
  (Datei-, Festplatten-, E-Mail-Verschlüsselung, VPN-Systeme, SSL/TLS ...)
  Die Verschlüsselung sorgt dafür, dass keine unerlaubten Informationen im Klartext gelesen werden können.
- **Multifaktor-Authentifikationsverfahren**
  Mithilfe einer Multifaktor-Authentifikation wird verhindert, dass unerlaubte Nutzer Zugriff auf das IT-System oder den IT-Dienst erhalten.
- **Anti-Malware-Lösungen**
  Anti-Malware-Lösungen sorgen dafür, dass illegales Aufspielen und kriminelles Nutzen von Malware auf IT-Systemen nicht umgesetzt werden können.
- **Anti-DDoS-Verfahren**
  Mithilfe von Anti-DDoS-Verfahren wird die erfolgreiche Umsetzung von DDoS-Angriffen verhindert.
- **Signaturverfahren**
  Die Nutzung von Signaturverfahren ermöglicht es zu verhindern, dass digitale Handlungen geleugnet werden können.
- **Hardware-Sicherheitsmodule**
  Mithilfe von Hardware-Sicherheitsmodulen (Smartcards, TPMs, High-Level Security Modules) wird der unerlaubte Zugriff auf Sicherheitsinformationen und die unerlaubte Nutzung von Kryptografie-Funktionen mit Schlüssel unterbunden.

Da Angreifer zunehmend schneller mehr, aber auch neue Angriffsmethoden entwickeln und umsetzen sowie die potenziellen Ressourcen für Angriffe immer leistungsstärker werden, müssen die IT-Sicherheitsmechanismen, die diese abwehren sollen, kontinuierlich und zeitnah verbessert werden.

Bewertung des Entgegenwirkens

Die IT-Sicherheitsstrategien „Entgegenwirken von Angriffen“ ist eine naheliegende Vorgehensweise, digitale Werte angemessen zu schützen. IT-Sicherheitsmechanismen sollten dem Stand der Technik genügen, um mittels einer hohen Wirkung einen angemessenen IT-Sicherheitslevel zu erzielen. Momentan stehen nicht genügend, beziehungsweise nicht schnell genug, wirkungsvolle IT-Sicherheitstechnologien, -lösungen und -produkte gegen die immer intelligenteren Angriffe zur Verfügung oder werden nicht angemessen und vollumfänglich genug eingesetzt. Das dokumentiert die Vielzahl der professionell durchgeführten und daher erfolgreichen Angriffe. Da es keine hundertprozentige IT-Sicherheit gibt und somit immer ein Restrisiko bleibt, muss mit weiteren IT-Sicherheitsstrategien gegen die verbleibenden Risiken vorgegangen werden.

1.3.3 Erkennen von Angriffen

Wenn Angriffen mithilfe von IT-Sicherheitsmechanismen nicht angemessen oder vollständig entgegengewirkt werden oder eine Vermeidung die Angriffsfläche nicht ausreichend redu-

zieren kann, bleibt noch die Strategie, Angriffe erkennen und zu versuchen, den Schaden so schnell wie möglich zu minimieren.

In diesem Bereich spielen prinzipiell Frühwarn- und Lagebildsysteme eine besondere Rolle, da sie Lagebilder erstellen und Warnungen erzeugen, wenn die Bedrohungslage ungewöhnlich groß ist und gerade umgesetzte Angriffe erkannt werden.

Hier ist die Idee, dass in einem definierten Bereich (etwa IT- und Kommunikationsinfrastruktur, Endgeräte oder Server) nach Angriffssignaturen oder Anomalien gesucht wird. Bei Erkennen eines Angriffs werden die Hintergründe analysiert und adäquate Gegenmaßnahmen eingeleitet, um weitere Schäden zu verhindern oder zumindest zu reduzieren.

Bewertung des Erkennens

Die IT-Sicherheitsstrategie „Erkennen von Angriffen“ ist sehr hilfreich, hat aber definierte Grenzen, da es keine hundertprozentige Erkennungsrate gibt. Aus diesem Grund wird es in der Zukunft wichtig, auf diesem Gebiet durch mehr und bessere Sensoren sowie einen unternehmensübergreifenden Austausch viele sicherheitsrelevante Informationen verfügbar zu machen, aber auch durch den Einsatz von KI-Systemen die Erkennungsraten so weit wie möglich zu steigern. Zudem ist es wichtig, schnell und angemessen zu reagieren. Daher müssen die IT-Sicherheitsstrategien „Erkennen von Angriffen“ und „Reaktion auf Angriffe“ zusammen betrachtet werden.

1.3.4 Reaktion auf Angriffe

Wenn Angriffe erkannt werden, gilt es, so schnell wie möglich mit passenden Aktionen zu reagieren.

1. **Automatisierte Reaktion**
   Wenn ein Angriff erkannt wird, können zum Beispiel sofort und (halb-)automatisiert Firewall-Regeln oder E-Mail-Server-Regel so reduziert werden, dass nur noch die wichtigen Prozesse für das Unternehmen aufrechterhalten bleiben. Durch die Reduktion der Angriffsfläche lassen sich die potenziellen Schäden so gut wie möglich verringern.
2. **Definition von Befugnissen, Informationsflüssen, Entscheidungsprozessen und Kommunikationsstrategien**
   Für das gesamte Abschalten der Internetverbindung oder die Notwendigkeit des Herunterfahrens vieler IT-Systeme, etwa bei großen Ransomware-Angriffen, müssen in der Regel die Verantwortlichkeiten sowie die damit verbundenen Rechte definiert sein. Um schneller handeln zu können, ist es notwendig, die erforderlichen Informationsflüsse und Reaktionsmöglichkeiten exakt ausgearbeitet und vereinbart zu haben. Wichtig für ein angegriffenes Unternehmen sind somit ein sehr kurzer Entscheidungsprozess, effiziente Pfade für die Informationsverteilung sowie klar definierte Befugnisse der Akteure, um im Notfall schnell und verantwortungsvoll reagieren zu können. Zudem muss die Kommunikationsstrategie bezüglich Mitarbeitern, Kunden, Regulierungsbehörden und Medien sorgfältig geplant sein, um einen hohen Imageschaden zu vermeiden.
3. **Digitale Forensik**
   Grundsätzlich ist die digitale Forensik eine streng methodisch vorgenommene Datenanalyse auf Datenträgern und von IT-Systemen und Kommunikationsnetzwerken zur

Aufklärung von Vorfällen durch forensische Sicherung von digitalen Beweisen sowie zur Analyse der digitalen Beweismittel. In Sinne einer Reaktion lässt sich durch die Analyse eines Angriffes gewährleisten, dass eventuell vorhandene Lücken geschlossen, vorhandene IT-Sicherheitsmaßnahmen optimiert oder weitere integriert werden, damit das Unternehmen zukünftig besser geschützt ist.

4. **Notfallplanung**
   Wichtig ist auch, dass es bereits getestete Reaktionskonzepte (Notfallplanungen) gibt, in denen die richtige Vorgehensweise im Krisenfall definiert ist, aber auch welche Personen die Rechte haben, die entsprechenden Reaktionen auszulösen. Besonders relevant ist dabei, alle definierten Abläufe in ausreichendem Maße mit allen Mitarbeitern zu trainieren, damit im Ernstfall die adäquaten Reaktionen schnell und erfolgreich umgesetzt werden können.

Bewertung der Reaktion

Die IT-Sicherheitsstrategie „Reagieren auf Angriffe“ hilft, Schäden zu vermeiden oder zu minimieren. Es kann jedoch nur reagiert werden, wenn Angriffe erkannt werden. Notwendig ist, die Reaktionskonzepte vorher definiert sowie getestet zu haben, um im Ernstfall schnell und wirkungsvoll reagieren zu können.

1.4 Umsetzung eines angemessenen IT-Sicherheitslevels

Der Stand der Technik bezeichnet die am Markt verfügbare Bestleistung einer IT-Sicherheitsmaßnahme, um ein gesetzliches IT-Sicherheitsziel zu erreichen (TeleTrusT 2021).

Das Technologie- und IT-Sicherheitsniveau „Stand der Technik“ ist angesiedelt zwischen dem innovativeren Technologiestand „Stand der Wissenschaft und Forschung“ und dem bewährten Technologiestand „allgemein anerkannte Regeln der Technik“ (siehe Bild 1.4).

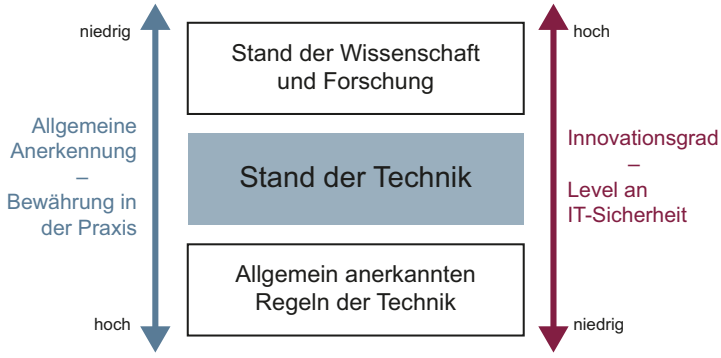

Bild 1.4 Angemessener IT-Sicherheitslevel durch den Stand der Technik

Stand der Technik Der Stand der Technik bezeichnet die am Markt verfügbare Bestleistung einer IT-Sicherheitsmaßnahme, um das entsprechende IT-Sicherheitsziel zu erreichen. IT-Sicherheitslösungen, die dem Stand der Technik genügen, bieten einen angemessenen Level an IT-Sicherheit für den aktuellen Grad der Digitalisierung.

Stand der Wissenschaft und Forschung Technische IT-Sicherheitsmaßnahmen im Stadium „Stand der Wissenschaft und Forschung" haben einen hohen Innovationsgrad sowie IT-Sicherheitslevel, sind sehr dynamisch in ihrer Entwicklung und gehen mit der Erreichung der Marktreife (oder zumindest mit ihrer Markteinführung) in das Stadium „Stand der Technik" über. Dort nimmt die Dynamik ab, etwa durch die Standardisierung der Prozesse.

Allgemein anerkannte Regeln der Technik Auch technische Maßnahmen im Stadium „allgemein anerkannte Regeln der Technik" sind am Markt verfügbar. Ihr Innovationsgrad ist geringer, sie haben sich jedoch in der Praxis bewährt und werden oftmals in den entsprechenden Standards beschrieben. Jedoch ist im Stadium „allgemein anerkannte Regeln der Technik" das Entgegenwirken von innovativen Angreifern nicht mehr so wirkungsvoll. Einige Beispiele hierfür sind: Die Nutzung von Passwörtern für die Authentifikation oder die Nutzung von nicht mehr sicheren Kryptografie-Algorithmen etwa bei Signaturen, Authentifikation oder Verschlüsselung. Aber ebenso Anti-Malware-Lösungen, die überwiegend auf der Basis der Signaturerkennung funktionieren, oder Firewall-Systeme, die keine sicheren Regeln nutzen oder umsetzen können, gehören – in Anbetracht der aktuell sehr dynamischen Digitalisierung – in diese nicht mehr angemessene Kategorie.

Verfügbare Bestleistung einer IT-Sicherheitsmaßnahme Unter anderem im „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)" und in der „EU-Datenschutz-Grundverordnung (DSGVO)" ist vorgeschrieben, dass sich die IT-Sicherheitsmaßnahmen an dem Stand der Technik orientieren. Daher kommt diesem eine hohe Bedeutung zu, auch aus der Sicht der Haftung im Schadensfall.

1.5 IT-Sicherheitsmechanismen, die gegen Angriffe wirken

Im Folgenden werden einige IT-Sicherheitsmechanismen beschrieben, die gegen Angriffe wirken (Pohlmann 2019b).

1. Verschlüsselung

Das Ziel der Verschlüsselung besteht darin, Daten in einer solchen Weise einer mathematischen Transformation zu unterziehen, dass es einem Unbefugten unmöglich ist, die Originaldaten aus den transformierten, verschlüsselten Daten zu rekonstruieren. Damit die verschlüsselten Daten für ihren legitimen Nutzer dennoch verwendbar bleiben, muss es diesem jedoch möglich sein, durch Anwendung einer inversen Transformation daraus wieder die Originaldaten zu generieren (siehe Bild 1.5).

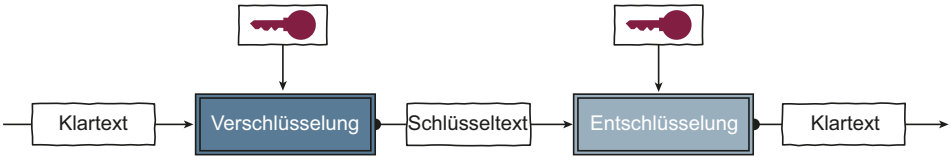

Bild 1.5 Verschlüsselung

Die Verschlüsselung wird zur Übertragung und Speicherung vertraulicher Daten verwendet, die nur dem legitimen Empfänger/Besitzer zugänglich sein sollen. Anwendungsfälle sind unter anderem: Datei-, Festplatten-, E-Mail-Verschlüsselung, IPSec-Verschlüsselungssysteme, SSL/TLS-Absicherung.

Im Bereich Verschlüsselung gibt es bei den meisten Unternehmen noch einen großen Nachholbedarf. Aus diesem Grund sollte ein Konzept erarbeitet werden, wie die Verschlüsselung und eine dazu notwendige IT-Sicherheitsinfrastruktur umgesetzt werden können.

Kryptoagilität Beim Einsatz von Verschlüsslungssystemen sollte auf die Kryptoagilität geachtet werden. Die Kryptoagilität ermöglicht es einem IT-Sicherheitssystem, auf ein alternatives neues Kryptosystem (unter anderem bezüglich kryptografischer Algorithmen, Schlüssellänge, Schlüsselgenerierungsverfahren, technischer Umsetzung) sehr schnell umzuschalten, ohne wesentliche Änderungen am IT-System oder IT-Sicherheitssystem (wie Systemarchitekturen oder Protokolle) vorzunehmen. Damit kann garantiert werden, dass ein IT-Sicherheitssystem kontinuierlich ein Mindestniveau an IT-Sicherheit halten kann.

In Bezug auf die wichtigsten Angriffsvektoren, wie Man-in-the-Middle (MITM), hilft Verschlüsselung, diese zu verhindern.

2. Authentifikationsverfahren

Authentifikation bezeichnet einen Prozess, in dem überprüft wird, ob der Nutzer (Mitarbeiter, Kunde und andere Personen), der gerade auf ein IT-System zugreifen möchte, echt ist. Bei der Authentifikation wird mit der Erbringung eines oder mehrerer Nachweise bestätigt, ob es sich um den Nutzer mit der angegebenen und behaupteten digitalen Identität handelt (siehe Bild 1.6).

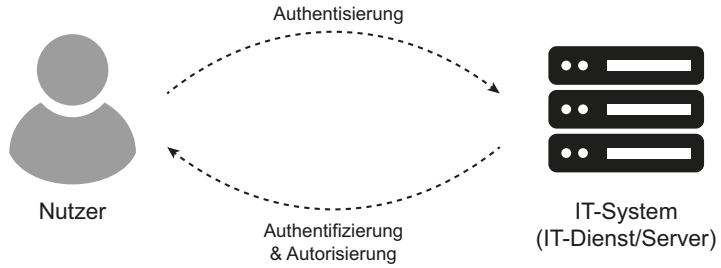

Bild 1.6 Authentifikation, Authentisierung & Autorisierung

- **Authentisierung (Sichtweise Nutzer):**
  Der Nutzer authentisiert sich gegenüber einem IT-System (etwa Endgerät, Server, IT-Dienst oder Cloud), indem er einen Nachweis über seine digitale Identität erbringt, zum Beispiel den Nutzernamen.

- **Authentifizierung (Sichtweise IT-System):**
  Das IT-System (etwa Endgerät, Server, IT-Dienst oder Cloud) überprüft den Nachweis, um die Echtheit der digitalen Identität eines Nutzers im Rahmen der Authentifizierung festzustellen.
- **Autorisierung (Sichtweise IT-System):**
  Wenn die Echtheit der digitalen Identität eines Nutzers erfolgreich verifiziert werden konnte, kann das IT-System (etwa Endgerät, Server, IT-Dienst oder Cloud) dem Nutzer definierte Rechte einräumen.

Klassen von Authentifizierungsverfahren Es werden verschiedene Klassen von Authentifizierungsverfahren unterschieden, bei denen unterschiedliche Aspekte eine Rolle spielen und diverse Charakteristika berücksichtigt werden müssen.

1. *Wissen:* Bei dieser Klasse von Authentifizierungsverfahren wird über einen Nachweis der Kenntnis von Wissen die Echtheit eines Nutzers überprüft. Beispiele von Wissen sind: Passwort, PIN oder Antwort auf eine bestimmte Frage (Sicherheitsfrage).
2. *Besitz:* Verwendung eines Besitztums für das Authentifizierungsverfahren ist eine weitere Klasse. Beispiele für Besitz sind: Neuer Personalausweis, SIM-Karte im Smartphone und weitere Hardware-Sicherheitsmodule, wie Smartcard oder USB-Stick. In der Regel wird in diesem Bereich der Besitz von geheimen Schlüsseln mithilfe von Challenge-Response-Verfahren nachgewiesen, die in den Hardware-Sicherheitsmodulen sicher gespeichert sind.
3. *Sein:* Bei dieser Klasse von Authentifizierungsverfahren muss der Nutzer gegenwärtig sein. Beispiele von Sein sind: Biometrische Merkmale wie Fingerabdruck, Gesichtsgeometrie oder Iris.
4. *Weitere unterstützende Faktoren (Reputation, Standort, Zeit, Technologie):* Es können noch weitere unterstützende Faktoren für die Beurteilung der Echtheit des Nutzers herangezogen werden. Beispiele sind: Vergangene Transaktionen des Nutzers (Reputation), verwendete Endgeräte und Software des Nutzers (Technologie), Standort und Zeit des Authentisierungsprozesses.

Multifaktor-Authentifizierung Stand der Technik heute ist die Multifaktor-Authentifizierung. Mit einer Multifaktor-Authentifizierung (MFA) kann flexibel agiert und mit einer höheren Vertrauenswürdigkeit authentifiziert werden. Ein Beispiel für eine Multifaktor-Authentifizierung ist: Es wird als Basis eine digitale Signatur einer Zufallszahl mithilfe eines Hardware-Sicherheitsmoduls (etwa Smartcard, USB-Stick oder Sicherheitsmodul im Smartphone) umgesetzt, das mit einem Passwort oder PIN aktiviert werden muss. Um den Nutzerbezug zu verstärken, muss der Nutzer noch mithilfe eines Fingerabdrucks oder der Gesichtserkennung seine Gegenwärtigkeit zusätzlich verifizieren lassen.

Konzept der risikobasierten und adaptiven Authentifizierung Die adaptive Authentifizierung entscheidet auf der Basis der Vertrauenswürdigkeit des zugreifenden Nutzers, der Kritikalität der konkreten Anwendung/Aktion und der Rahmenbedingungen des aktuellen Zugriffs, welche Klassen von Authentifikationsverfahren zum Einsatz kommen sollen. Dieser risikoorientierte Ansatz erhöht das allgemeine Sicherheitsniveau und vermindert die Anzahl nicht notwendiger starker Authentifizierungen. Es wird das Optimum zwischen Sicherheit und Komfort angestrebt. Umgesetzt werden Konzepte der adaptiven Authentifizierung mithilfe von Mehrfaktor-Authentifizierung (MFA), die flexibel, in Abhängigkeit vom gerade notwendigen Sicherheitsniveau oder von Risiken, die passenden Klassen von Authentifikationsverfahren auswählt.