Michael LANG · Hans LÖHR

IT-Sicherheit

Technologien und Best Practices für die Umsetzung im Unternehmen

HANSER

HANSER

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

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
Ausstattung patentrechtlich geschützt. Kösel FD 351, Patent-Nr. 0748702

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

Inhalt

Hagen Lauer, Nicolai Kuntze

2.1 Einleitung

2.1.1 Trends

2.1.2 Herausforderungen

2.1.3 IT-Sicherheit vs. Sicherheit

2.1.4 Schutzziele

2.2 Grundprinzipien der IT-Sicherheit

2.2.1 Kenne die Bedrohungen

2.2.2 Sicherheit und Wirtschaftlichkeit

2.2.3 Keine „Security through Obscurity“

2.2.4 Security by Design

2.2.5 Prinzip der geringsten Berechtigung

2.2.6 Trennung der Verantwortlichkeiten

2.2.7 Zugriffskontrolle

2.2.8 Defense in Depth

2.2.9 Der Mensch als Faktor

2.2.10 Design for Resilience

2.3 Literatur

3 Organisation des IT-Sicherheitsmanagements im Unternehmen

Markus Nauroth

3.1 Einführende Bemerkungen

3.2 Imperative des IT-Sicherheitsmanagements

3.2.1 Sicherheit ist aktiv und proaktiv

3.2.2 Routine

3.2.3 Sicherheit liegt in der Verantwortung eines jeden

3.2.4 Worst-Case-Szenario

3.2.5 Es bedarf vieler Unterstützer

3.2.6 Denken wie ein Angreifer

3.2.7 Mehrschichtige Verteidigung verwenden

3.3 Grundlegende Pfeiler einer IT-Sicherheitsorganisation

3.3.1 Gängige Organisationsstrukturen nach organisatorischem Reifegrad

9 Der Chief Information Security Officer in der Praxis

Andreas Reisch

Nicolai Kuntze, Hagen Lauer

12.3 Was läuft schief?

12.3.1 Zu viel Vertrauen in andere

12.3.2 Zu wenig Management-Fokus

12.3.3 Sicherheits-Features zu teuer oder nicht genutzt

12.3.4 Es ist noch nie etwas passiert – und das bleibt auch so

12.3.5 Never change a running system

12.3.6 Sensibilisierung und Weiterbildung zu teuer/aufwendig

12.4 Was ist zu tun?

12.4.1 Cybersicherheit allgemein

12.4.2 Cybersicherheit in der Automatisierung

12.5 Praxisbeispiel: Einführung von Cybersicherheit in der Produktion (Orientierung an ISA/IEC 62443)

12.5.1 Audit

12.5.2 Festlegen eines Sicherheitslevels

12.5.3 Risikobeurteilung

12.5.4 Defense in Depth

14.2 Vergabeverfahren in Deutschland

14.2.1 Grundsätze und Aspekte

14.2.2 Verfahrensarten

14.2.3 Elektronische Vergabeplattformen

14.3 IT-Sicherheit im Vergabeverfahren

14.3.1 TOM im Vergabeverfahren

14.3.2 Die Gestaltung der Vergabeunterlagen

14.3.3 Die Planung des Vergabeverfahrens

14.3.4 Die Verfahrensdurchführung

14.3.5 Die elektronische Kommunikation

14.3.6 Der Umgang mit Verschlusssachen

14.4 Kennzeichnen von Geschäftsgeheimnissen

14.5 Rechtschutzmöglichkeiten

14.6 Strafbarkeit im Vergabeverfahren

14.7 Bietertipps zum Umgang mit Vergabestellen und zur Erstellung von Angeboten

Herausgeber, Autorin und Autoren

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).

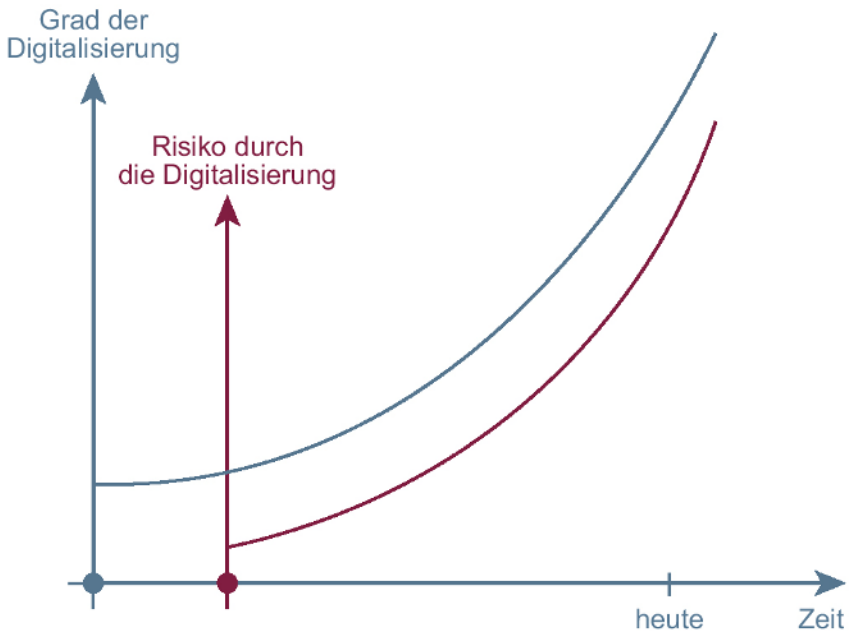

Bild 1.1 Entwicklung der Digitalisierung und des korrespondierenden Risikos

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 unterschiedlichen 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**