Leitfaden

Cyber-Security

Bundesverband

Herausgeber: ASW Bundesverband
Autoren: Wolf-Rüdiger Moritz (Infineon Technologies AG), Marcel Knop und Prof. Timo Kob (beide HiSolutions AG)
Titelfoto: fotolia.com: ©duncanandison
Stand: April 2016, Nr. 2

Der gesamte Inhalt des Leitfadens ist urheberrechtlich geschützt. Alle Rechte sind vorbehalten. Jede Verwertung, insbesondere Vervielfältigung von Informationen durch etwa die Verwendung von Texten, Textteilen oder Bildmaterial, bedarf der ausdrücklichen, schriftlichen Zustimmung durch den ASW Bundesverband (Allianz für Sicherheit in der Wirtschaft e. V.).

Der ASW Bundesverband und die Autoren sind um die Richtigkeit und Aktualität der Informationen bemüht. Eine Haftung oder Garantie dafür sowie für die Vollständigkeit der zur Verfügung gestellten Informationen, einschließlich der Haftung gegenüber Dritten, kann jedoch nicht übernommen werden. Der ASW Bundesverband und die Autoren haften weder für direkte noch indirekte Schäden, die durch die Nutzung der Informationen entstehen.

© Allianz für Sicherheit in der Wirtschaft e. V., 2016

Inhalt

1. Definition und Bedrohungen

Unser Privat- und Berufsleben ist mittlerweile durchdrungen von vernetzten IT-Systemen. Dies wird mit dem Begriff „Cyber“ beschrieben – also der Integration von IT-Systemen in das menschliche Alltagsleben.

IT-Systeme sind jedoch die komplexesten von Menschenhand erzeugten Systeme überhaupt. Und Komplexität ist der größte Feind von Sicherheit. Die hieraus zwangsläufig entstehenden Sicherheitslücken können durch die zunehmende Vernetzung der IT-Systeme von immer mehr Angreifern missbraucht werden. **Mit Cyber-Sicherheit ist also die Sicherheit der in unser Alltagsleben integrierten IT-Systeme gemeint.**

Cyber-Security ist ein mehrdimensionales, disziplinübergreifendes Phänomen und **kann nur im Zusammenwirken aller erforderlichen Fachgebiete wirksam erreicht werden.**

Bezüglich der Angriffe ist zwischen **gezielten und ungezielten Angriffen** zu unterscheiden. Ungezielte Angriffe suchen vor allem nach IT-Systemen, die eine bestimmte Schwachstelle aufweisen, unabhängig davon, welches Unternehmen oder System hiervon betroffen ist. Ziel dieser Angriffe ist häufig der Missbrauch der IT-Ressourcen (Rechenkapazität, Speicher, Netzwerk) des Opfers, beispielsweise zur Versendung von unerwünschten Werbenachrichten per E-Mail (auch Spam genannt).

Gezielte Angriffe haben einzelne Systeme, Benutzer oder Unternehmen im Fokus. Ziel dieser Angriffe ist meist die Erlangung von Zugang zu geschützten IT-Systemen und deren Daten. Hierdurch sind Szenarien wie Datenabfluss oder schwerwiegende Eingriffe in die Funktion unternehmensinterner Arbeitsabläufe möglich.

Prominentes Beispiel hierfür ist der „gehackte“ Hochofen aus dem BSI-Jahresbericht, dessen Betrieb durch einen gezielten Hackerangriff stillgelegt wurde.

Als Tätergruppen kann man meist unterscheiden zwischen einzelnen Privatpersonen, Hacker- oder Aktivistengruppen, aber auch zunehmend Organisationen mit kriminellen Hintergründen, sowie regierungsnahe Einrichtungen, hier insbesondere die Geheimdienste.

Eine Vielzahl von Studien belegt, dass **Cyber-Kriminalität** und Schäden, die durch Störung von IT-Systemen entstehen, immer mehr an Bedeutung gewinnen und als **einer der größten Risikofaktoren in Unternehmen** angesehen werden können.

2. Themengebiete

Cyber-Sicherheit gliedert sich in eine Vielzahl unterschiedlicher Themengebiete auf:

Physische Sicherheit:

Quasi sämtliche von IT-Systemen genutzten Kontrollmechanismen basieren auf der Voraussetzung, dass **kein unautorisierter Zugriff auf die Hardware-Komponenten** erfolgen kann. Hat ein Angreifer physischen Zugang zum IT-System, können Festplatten ausgebaut oder alternative Systemstart-Verfahren gewählt werden, um die logischen Kontrollverfahren außer Kraft zu setzen.

Asset Management und IT-Risiko-Analysen:

IT-Systeme haben unterschiedliche Anforderungen an die IT-Sicherheit. Während manche Systeme eine besonders hohe Verfügbarkeit verlangen (beispielsweise IT-Systeme in der Produktion) haben andere Systeme besonders hohe Anforderungen an die Wahrung der Vertraulichkeit (beispielsweise Systeme in der Personalverwaltung). Um eine Übersicht über alle vorhandenen Systeme im Unternehmen oder in der Institution zu haben, ist es notwendig, eine **Aufstellung aller IT-Systeme** zu erstellen. Ist diese Übersicht einmal vorhanden, werden durch Risiko-Analysen die jeweiligen **Schutzbedarfe der Systeme ermittelt**, die Systeme entsprechend ihrer **Schutzklassen gruppiert** und daraufhin **Schutzmaßnahmen konzipiert**.

Personelle Sicherheit:

Um zu verhindern, dass nicht vertrauenswürdige, nicht ausreichend kompetente oder unzuverlässige Personen mit der Verarbeitung von sensiblen Informationen beauftragt werden, können durch **Screening-Verfahren im Bewerbungs-Prozess** von Unternehmen und Instituten Prüfungen angestellt werden, die den Werdegang des jeweiligen Bewerbers verifizieren. Diesen Prüfverfahren sind jedoch insbesondere in Deutschland und Europa enge Grenzen durch Datenschutzgesetze gesteckt. In anderen Ländern, wie beispielsweise den USA, sind intensivere Prüfungen möglich.

Einsatz von Kryptografie:

Techniken zur Verschlüsselung von Daten werden an sehr vielen Stellen der Informationstechnik eingesetzt, um die Vertraulichkeit oder Integrität von Datenverarbeitungs- oder Übertragungsprozessen zu ermöglichen. Die zugrundeliegende Mathematik und Technik ist jedoch in aller Regel sehr komplex. Es gilt, die **richtigen kryptologischen Verfahren** und ihre jeweiligen Parameter korrekt auszuwählen und zu konfigurieren. Fehler resultieren dabei häufig darin, dass Verschlüsselungen von Angreifern gebrochen oder umgangen werden können. Daher ist die Festlegung von geeigneten kryptografischen Verfahren von jedem Unternehmen oder Institut durch geeignete Spezialisten festzulegen. Dies erfolgt häufig auf der vorangegangenen Risikoanalyse der jeweiligen IT-Systeme oder Prozesse, da aus diesen die Höhe der jeweiligen Anforderungen abgeleitet werden kann.

Betrieb der IT-Systeme:

„Eine Mauer ist nur so stark wie die Menschen, die sie bewachen." (Dschinghis Khan). Auch IT-Systeme sind keine statischen Konstrukte sondern können aufgrund einer Vielzahl von Änderungen, Ergänzungen und der Aktivitäten ihrer verschiedenen Benutzer über ihren Einsatzzeitraum hinweg als quasi lebendige Objekte verstanden werden. Um Risiken, die aus diesen Gefahren entstehen, abzufangen ist die Umsetzung einer Vielzahl von Maßnahmen notwendig. Hierzu gehört die **richtige Konfiguration der unterschiedlichen IT-Systeme**, die stets **zeitnahe Installation von Security-Patches**, um bekannt gewordene Sicherheitslücken zu schließen, das **Berechtigungsmanagement** der verschiedenen Benutzer, die **Protokollierung der Systemvorgänge**, geeignete **Backup-Verfahren** zur Datensicherung, und nicht zuletzt das generelle **Änderungsmanagement**, um fehlerhafte oder unautorisierte Änderungen an den IT-Systemen zu vermeiden.

Entwicklung und Wartung von IT-Systemen:

Unternehmen oder Institute, die eigene IT-Systeme oder Anwendungen erstellen, müssen besondere **Sorgfalt beim Entwicklungsprozess** walten lassen. Neben einer Vielzahl von allgemeinen Projektrisiken muss insbesondere die IT-Sicherheit beim Entwicklungsprozess berücksichtigt werden. Hierbei gilt es primär, die **Komplexität** des Vorhabens zu **reduzieren**, indem Vorgaben erstellt werden, die den Programmierern als Vorlage dienen, um sicherheitsrelevante Komponenten der Software zu gestalten. Hierdurch wird das Risiko reduziert,

dass die mit der Programmierung beauftragten Personen individuelle Entscheidungen treffen und hierdurch unterschiedliche IT-Sicherheitslevel innerhalb der Software entstehen. Zudem wird hierbei definiert, in welchem Umfang Software getestet werden muss, bevor sie produktiv genutzt werden kann. Die Vergangenheit hat gezeigt, dass quasi jede veröffentlichte Software eine große Anzahl von Sicherheitsmängeln hatte, die erst im Laufe des Betriebs entdeckt und behoben wurden.

Management von ausgelagerten Prozessen und IT-Systemen:

Unternehmen und Institute, die sich dafür entscheiden, einzelne Elemente oder den ganzen IT-Betrieb an externe Dienstleistungsunternehmen auszulagern, können hierdurch die operativen Aufwände zum Systembetrieb auslagern, allerdings nicht die Verantwortung für den Betrieb der Systeme. Sie sind daher zum Teil auch gesetzlich dazu verpflichtet, **angemessene Kontrollverfahren** einzurichten, um den **ordnungsgemäßen IT-Betrieb auch bei externen Unternehmen zu überwachen**. Hierdurch soll erreicht werden, dass die extern betreuten IT-Systeme den gleichen (oder vergleichbaren) Sicherheitsstandards genügen, wie die in Eigenregie betriebenen Systeme.

Sicherheitsvorfallbehandlung:

Um Störungen der IT-Systeme während des produktiven Betriebs zeitnah zu erkennen und angemessen darauf reagieren zu können, ist die Einführung und Nutzung eines **einheitlichen Verfahrens** notwendig. Hierbei werden Vorkommnisse erfasst, qualifiziert und den entsprechenden Abteilungen zur Behebung des Vorfalls weitergeleitet. Typischerweise werden Vorfälle unterschieden nach:

Störung

Einfacher Vorfall, der ohne Zuhilfenahme anderer Organisationseinheiten gelöst werden kann.

Notfall

Arbeitsprozesse werden unterbrochen, Hilfsmaßnahmen auf Basis konkreter Planungen werden angewendet.

Krise

Vorfall mit besonderer Schwere, der nicht mehr durch das Notfall-Management allein bewältigt werden kann.

3. Management-Systeme für Informationssicherheit

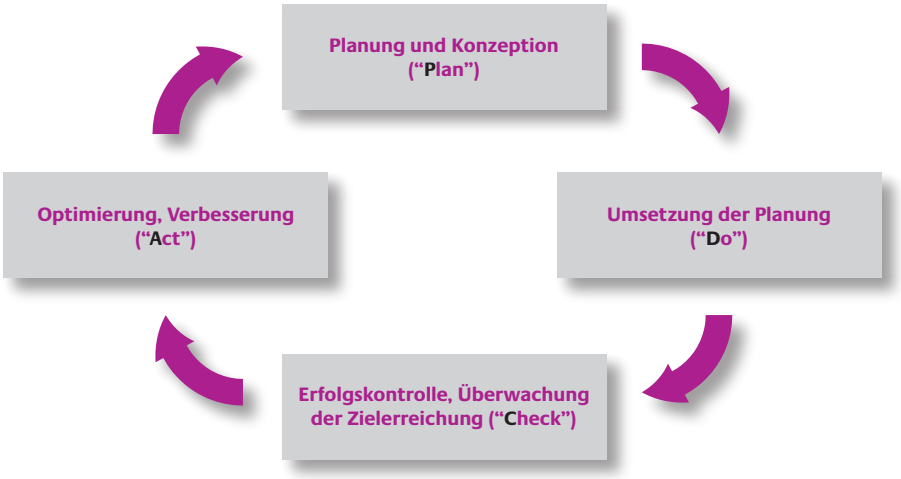
Damit die im vorangegangenen Abschnitt dargestellten Maßnahmen jeweils angemessen ausgestaltet werden, und auch Änderungen zeitnah berücksichtigt werden können, haben sich verschiedene Management-System-Standards etabliert. Allen Management-Systemen ist gemein, dass sie in einem zyklischen Prozess arbeiten und somit in der Lage sind, Änderungen im Bereich der IT-Sicherheit zeitnah und angemessen zu bearbeiten. Als Management-Systeme haben sich dabei **zwei Standards am Markt etabliert**: zum einen der **100-1 des Bundesamtes für Sicherheit in der Informationstechnik** (BSI) und des Weiteren der **ISO/IEC 27001**.

Während der BSI-Standard 100-1 vor allem im deutschsprachigen Raum, und hier insbesondere von Behörden und staatsnahen Unternehmen eingesetzt wird, ist der ISO/IEC 27001 bei privatwirtschaftlichen Unternehmen und internationalen Unternehmen weit verbreitet. Fachlich unterscheiden sich die Standards 100-1 und ISO/IEC 27001 durch ihre technische Detaillierung. Während der 100-1-Standard recht spezifische informationstechnische und risikospezifische Vorgaben macht, sind die Risiko- und Maßnahmenbeschreibungen im ISO/IEC 27001 vergleichsweise generisch und bedürfen einer weitergehenden Interpretation.

Beide Management-Systeme erlauben eine Zertifizierung, die dazu genutzt wird, Dritten gegenüber die Qualität des eigenen IT-Security-Managements zu belegen. Grundsätzlich haben die beiden Standards das gleiche Vorgehen bei der Schaffung und Etablierung eines Information Security Management Systems:

1. **Definition von Verantwortlichkeiten**
2. **Definition des Anwendungsbereichs**
3. **Risiko-Assessment der IT-Umgebung**
4. **Implementierung von Kontrollen**
5. **Wirksamkeitsprüfungen der Kontrollen**

Dieser Prozess wird kontinuierlich durchlaufen und ist bekannt als „PDCA-Zyklus“ (Plan-Do-Check-Act). In der nachfolgenden Abbildung ist der Prozess visualisiert:



4. Gesetze und Regularien zur IT-Sicherheit

Im Sommer 2015 wurde vom Deutschen Bundestag das IT-Sicherheitsgesetz verabschiedet. Es verpflichtet die Betreiber kritischer Infrastrukturen zur Einhaltung von Mindeststandards im Bereich der IT-Sicherheit. Derzeit besteht allerdings noch Unklarheit darüber, welche Unternehmen genau zum Kreis der Betreiber kritischer Infrastrukturen zählen und wie genau die Mindeststandards im Bereich IT-Sicherheit aussehen sollen. Es ist zu erwarten, dass in den nächsten Wochen und Monaten mit einer Klärung dieser Sachverhalte zu rechnen ist.

Zudem bestehen noch weitere Gesetze mit Bezug zur IT-Sicherheit:

- Bundesdatenschutzgesetzt (**BDSGB**): Das BDSGB verpflichtet alle datenverarbeitenden Stellen, durch geeignete technische wie auch organisatorische Maßnahmen die Gewährleistung der datenschutzrechtlichen Anforderungen sicherzustellen.
- Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (**KonTraG**): Das KonTraG verbessert die Kontrolle und Transparenz in Aktiengesellschaften und auch in größeren GmbHs. Der Vorstand einer AG und insbesondere auch die Geschäftsführung einer GmbH ist verpflichtet, geeignete Maßnahmen zur frühzeitigen Erkennung von Entwicklungen zu treffen, die den Fortbestand der Gesellschaft konkret gefährden. Um dies zu gewährleisten, bedarf es eines Überwachungssystems, das in der Lage ist, kritische Situationen frühzeitig zu erkennen.
- Mindestanforderungen an das Risikomanagement (**MaRisk**): Für Unternehmen aus dem Finanzdienstleistungssektor sind Anforderungen für das Management und Controlling von operationellen Risiken definiert, zu denen auch IT-Risiken zählen.

- Payment Card Industry Data Security Standard (**PCI-DSS**): PCI-DSS ist eine Sammlung von IT-Sicherheitsanforderungen, die Unternehmen erfüllen müssen, wenn sie Kreditkartendaten von Dritten speichern oder verarbeiten.
- **GxP**: Unternehmen aus dem Pharma- und Medizinsektor müssen spezifischen good practices folgen, in denen auch Anforderungen an die IT-Sicherheit definiert sind. Die Einhaltung dieser Standards ist Voraussetzung zum Marktzugang und deren Einhaltung wird in der Regel von den zuständigen Behörden überwacht.
- Des Weiteren bestehen einige weitere Gesetze, dei den Missbrauch von IT-Systemen bzw. von Daten unter Strafe stellen:

Tatbestand	Paragraf	Strafdrohung	Verfolgung	Versuch
Ausspähen von Daten	202a StGB	Bis zu 3 Jahre oder Geldstrafe	Offizialdelikt	nicht strafbar
Computerbetrug	263a StGB	Bis zu 5 Jahre oder Geldstrafe	Offizialdelikt	strafbar
Erschleichen von Leistungen	265a StGB	bis zu 1 Jahr oder Geldstrafe	Offizialdelikt	strafbar
Fälschung beweiserheblicher Daten / techn. Aufzeichnungen	268 StGB, 269 StGB	bis zu 5 Jahre oder Geldstrafe	Offizialdelikt	strafbar
Datenveränderung	303a StGB	bis zu 2 Jahre oder Geldstrafe	auf Antrag	strafbar
Computersabotage	303b StGB	bis zu 10 Jahre oder Geldstrafe	in der Regel auf Antrag	strafbar
Unerlaubte Verwertung urheberrechtlich gesch. Werke	106, 108 UrhG	bis zu 3 Jahre oder Geldstrafe	in der Regel auf Antrag	strafbar

5. Audit von IT-Sicherheit

Die Sicherheit von IT-Systemen, -Infrastrukturen und -Prozessen kann auf unterschiedliche Weisen untersucht werden:

- **Penetrationstests**: Sie werden eingesetzt, um spezifische Anwendungen auf mögliche Sicherheitslücken zu untersuchen. Hierzu wird meist in manueller Handarbeit versucht, in das System einzudringen und aus applikationsinternen Berechtigungsstrukturen auszubrechen. Diese Untersuchung wird meist bei Systemen mit hohen Sicherheitsanforderungen angewendet, bevor sie in den Produktivbetrieb gehen.

- **Schwachstellenscans**: Hierbei werden größtenteils automatisierte Tests durchgeführt, um IT-Systeme auf allgemein bekannte Schwachstellen zu untersuchen. Dabei wird im Unterschied zum Penetrationstest keine besondere Analyse einzelner Systeme durchgeführt. Auch applikationsinterne Tests werden hierbei nicht durchgeführt. Durch die weitgehende Automatisierung dieser Tests kann eine Vielzahl von Systemen in kurzer Zeit untersucht werden. Dieses Verfahren wird daher häufig eingesetzt, um sämtliche aus dem Internet erreichbaren IT-Systeme eines Unternehmens oder Instituts auf Sicherheitslücken zu testen.

- **Firewall-Audits**: Weder Penetrationstests noch Schwachstellenscans können Aussagen darüber treffen, ob und wie gut interne Netzwerke gegenüber dem Internet und anderen Drittnetzwerken abgesichert sind. Aussagen hierüber können nur durch ein Firewall-Audit getroffen werden. Bei diesem Audit werden die Regelwerke (Welche Systeme/Netze dürfen mit welchen anderen Systemen/Netzen kommunizieren?) auditiert und die Firewall-Infrastruktur insgesamt (bestehend aus mehreren Komponenten zur Filterung des Netzwerk-Verkehrs) auf sogenannte Single-Point-of-Failures sowie Fehler-und Ausfalltoleranz untersucht.

ASW Bundesverband

Allianz für Sicherheit
in der Wirtschaft e. V.

Bayerischer Platz 6
10779 Berlin

Telefon: +49 (0)30 246 37 175
Telefax: +49 (0)30 200 77 056
info@asw-bundesverband.de

www.asw-bundesverband.de

Bundesverband