Definition und Abgrenzung

CYBERSICHERHEIT, IT-SICHERHEIT UND INFORMATIONSSICHERHEIT

Was ist der Zusammenhang zwischen Cybersicherheit, IT-Sicherheit und Informationssicherheit? Wo fängt das eine an, wo hört das andere auf und warum ist es nicht dasselbe? Diesen Fragen geht unser Autor in unserem Grundlagenartikel nach.

Sicherheit lässt sich aus zwei Perspektiven betrachten: die der Verteidiger sowie der Angreifer. Die Verteidiger ergreifen Sicherheitsmaßnahmen, um sich vor Angriffen zu schützen und die Angreifer tun alles, um die Sicherheitsmaßnahmen zu überwinden.

Derzeit besteht ein Ungleichgewicht, denn die professionellen Angreifer agieren momentan sehr erfolgreich. Das ist in erster Linie darauf zurückführen, dass Unternehmen allgemein noch unzureichend geschützt sind. Die aktuell genutzten Sicherheitsmechanismen auf den verschiedenen Ebenen sind durchweg insgesamt weder wirkungsvoll noch vollständig genug, um einen angemessenen und umfänglichen Schutz zu bieten. Hier muss sich etwas ändern, denn erfolgreich durchgeführte Angriffe verursachen Schäden, die Unternehmen existenziell gefährden.

Die Sicherheitslage verschlechtert sich von Jahr zu Jahr, wodurch das Schadensrisiko für alle Unternehmen und Organisationen steigt. Obwohl ständig neue Sicherheitstechnologien entwickelt werden, ist es bisher nicht gelungen, dieser negativen Tendenz entgegenzuwirken. Das Fazit kann daher nur lauten, dass sich im Bereich der Sicherheit grundlegend etwas ändern muss, um diesen Verlauf zu stoppen und die digitale Zukunft realisieren zu können.

Die Frage ist nun, welche Vorgehensweise hilft, die Sicherheitslage zu verbessern?

Die Darstellung des Zusammenhanges zwischen Cybersicherheit, Informationssicherheit und IT-Sicherheit verdeutlicht die unterschiedlichen Sichtweisen und Gemeinsamkeiten. IT-Sicherheit ist ein zentrales Element der Sicherheit, muss aber um definierte Aspekte in Richtung Cybersicherheit und Informationssicherheit erweitert werden.

DEFINITION: IT-SICHERHEIT

Mithilfe der IT-Sicherheit sollen vorhandene Risiken, die durch Bedrohungen auf IT-Systeme wirken, auf ein angemessenes Maß reduziert werden. IT-Sicherheit befasst sich daher mit IT-Sicherheitsmaßnahmen, die Daten, Informationen und Wissen auf IT-Systemen vor dem

Bild: Ar_TH - stock.adobe.com; fotohansel - stock.adobe.com

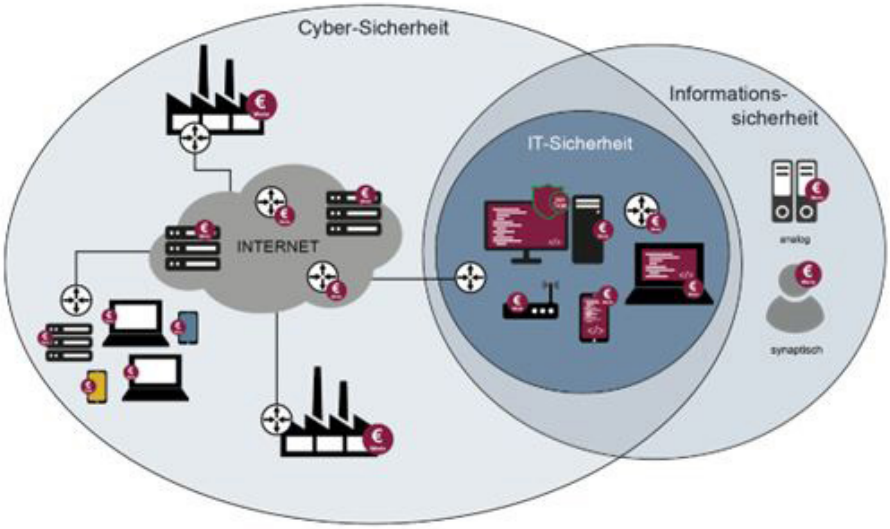

Abbildung 1: Zusammenhang Cybersicherheit, Informationssicherheit und IT-Sicherheit

Verlust von Vertraulichkeit, Authentifikation, Authentizität, Integrität, Verbindlichkeit, Verfügbarkeit und Anonymisierung/Pseudonymisierung schützen. Diese Aspekte werden auch als IT-Sicherheitsziele oder IT-Sicherheitsbedürfnisse und somit Grundwerte der IT-Sicherheit verstanden.

IT-Sicherheit beinhaltet zudem die Aspekte der Softwaresicherheit und Zuverlässigkeit von IT-Systemen. IT-Sicherheit schütz IT-Systeme, um Schäden für Unternehmen, Behörden, Organisationen und Personen zu vermeiden.

DEFINITION: CYBERSICHERHEIT

Cybersicherheit befasst sich mit allen Aspekten der IT-Sicherheit, wobei das Aktionsfeld auf den gesamten Cyberraum ausgeweitet wird. Mithilfe der Cybersicherheit sollen vorhandene Risiken, die durch Bedrohungen auf den Cyberraum wirken, auf ein angemessenes Maß reduziert werden.

Der Begriff Cyberraum umfasst in dieser Definition sämtliche mit dem globalen Internet verbundene IT-Systeme und IT-Infrastrukturen sowie deren Kommunikation, Anwendungen, Prozesse mit Daten, Informationen, Wissen und Intelligenzen. Aber auch die kriminellen Organisationen und weitere Angreifer gehören mit ihren immer intelligenteren Angriffsmethoden zum Cyberraum. Da der Cyberraum ein komplexes System mit vielen Abhängigkeiten und Akteuren ist, der nicht vollständig kontrolliert werden kann, sind die Herausforderungen für einen robusten, sicheren und vertrauenswürdigen Betrieb sehr groß.

Mit der zunehmenden Digitalisierung wird im Cyberraum auch die strikte Trennung zwischen Arbeit und Freizeit aufgelöst. Cyberangriffe im Cyberraum können die Unternehmen und Bürger treffen, aber auch zu erheblichen Beeinträchtigungen der gesellschaftlichen Lebensgrundlagen führen. Themen sind zum Beispiel Fake News, Deep Fake, Echokammern, mit denen Gesellschaften beispielsweise über Wahlen manipuliert werden können.

Aus diesem Grund spielt bei der Cybersicherheit die übergreifende Sichtweise auf den Cyberraum eine wichtige Rolle. IT-Sicherheit ist Teil der Cybersicherheit.

Zur Cybersicherheit gehören folgende Aspekte:

- IT-Infrastrukturen: wie zum Beispiel alle Autonome Systeme – selbstständige Netze (ca. 70.000), DNS-Infrastruktur, Webdienste, IP-Telefonie, Konferenzsysteme und soziale Medien
- Kommunikation: wie zum Beispiel IP, TCP, UDP, ICMP, QUIC, HTTP, SMTP, DNS, OSPF, BGP, IPSec und TLS/SSL
- Intelligenzen: künstliche Intelligenz und maschinelles Lernen und deren Anwendungen wie Assistenzsysteme, autonomes Fahren oder intelligente Angriffserkennungssysteme
- Angriffsmethoden: wie zum Beispiel Malware-Infiltrationen über manipulierte Webseiten und schadhafte E-Mail-Anhänge mithilfe von Phishing- und Social-Engineering-Angriffen sowie die daraus resultierenden Schadfunktionen der Malware. Dazu gehören beispielsweise Ransomware, Keylogger, Click-Fraud, Spam-Malware, DDoS-Malware, Staatstrojaner, Adware, trojanische Pferde und Spyware sowie Man-in-the-Middle-Angriffe, Angriffe mithilfe eines Software-Updates (Supply-Chain-Angriff), Angriffe auf die Verfügbarkeit von IT-Systeme (DDoS-Angriff) und Advanced Persistent Threats (APT).

DEFINITION: INFORMATIONSSICHERHEIT

Der Begriff Informationssicherheit befasst sich mit allen Aspekten der IT-Sicherheit, wird aber auf analoge und synaptische Informationen ausgeweitet. Informationssicherheit hat das Ziel,

Abbildung 2: Definition IT-Sicherheit (Bild: if(is))

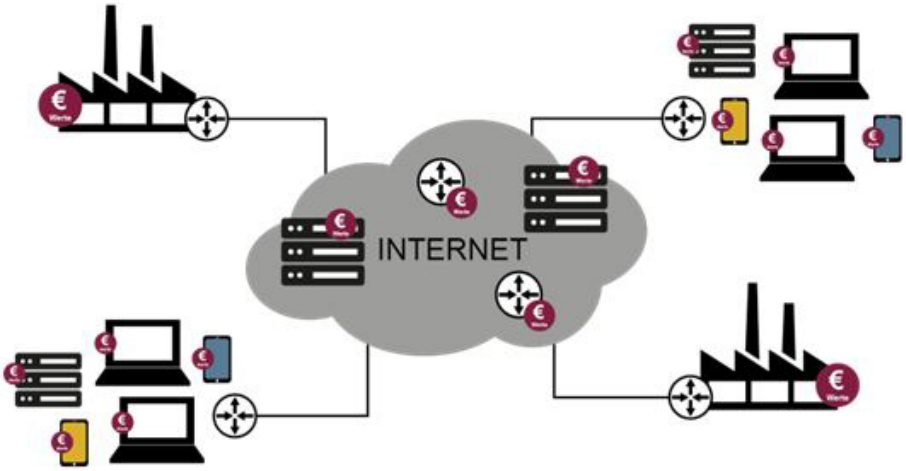

Abbildung 3: Definition Cybersicherheit (Bild: if(is))

Informationen während der Verarbeitung, Speicherung/Lagerung und Übertragung zu schützen. Die zu schützenden Informationen sind analog auf Papier (in Ordnern, Papierarchive ...), digital auf IT-Systemen oder auch in den Köpfen der Menschen gespeichert. IT-Sicherheit ist Teil der Informationssicherheit.

Informationssicherheit schütz analoge, digitale und synaptische Informationen. Damit werden Schäden für Unternehmen, Behörden, Organisationen und Personen vermieden und Risiken minimiert.

In der Praxis orientiert sich die Informationssicherheit im Rahmen des Informationssicherheitsmanagementsystems (ISMS) unter anderem an der ISO 27001 oder an IT-Grundschutz-Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI).

ISO-27001

ISO 27001 ist eine international anerkannte Norm, die von der International Organization for Standardization (ISO) herausgegeben wurde. Sie legt die Anforderungen für ein Informationssicherheitsmanagementsystem (ISMS) fest, dass die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen innerhalb eines Unternehmens gewährleisten soll. Das Ziel der Norm ist es, Unternehmen dabei zu helfen, Informationssicherheitsrisiken effektiv zu identifizieren, zu bewerten und zu behandeln. Die ISO 27001 Norm basiert auf einem risikobasierten Ansatz, bei dem das ISMS auf der Identifikation von Risiken, der Bewertung der Cybersicherheitsgefahren und Schwachstellen sowie der Implementierung von Kontrollen zur Risikominderung und -vermeidung basiert.

Ein solches ISMS kann in Unternehmen jeder Größe und Branche implementiert werden und ist darauf ausgerichtet, die IT-Sicherheit zu gewährleisten.

Aspekte der IT-Sicherheit sind zum Beispiel:

- Verfügbarkeit der IT-Systeme und -Prozesse gewährleisten.
- Sicherstellung der Vertraulichkeit der Informationen wie personenbezogenen Daten, geistigem Eigentum oder Betriebsgeheimnissen.
- IT-Risiken, mögliche Schäden und Folgekosten für das Unternehmen minimieren.
- Die Steigerung des Vertrauens gegenüber Partnern, Kunden und Öffentlichkeit erzielen.
- Die Sicherstellung der Compliance-Anforderungen garantieren.
- Mithilfe eines Schwachstellenmanagements Sicherheitslücken in IT-Systemen und Anwendungen zu identifizieren und beheben, um die Angriffsfläche zu minimieren und dadurch ein angemessenes Sicherheitsniveau zu gewährleisten.
- Die Kontrolle von IT-Risiken realisieren.

Die Norm umfasst verschiedene Anforderungen, darunter die Erstellung und Umsetzung von Informationssicherheitsrichtlinien und -prozessen, die Durchführung von Risikobewertungen und -management, die Einführung von Sicherheitskontrollen und -maßnahmen sowie das regelmäßige Monitoring und Überwachung des ISMS.

Unternehmen, die die Anforderungen der Norm erfüllen, können sich von unabhängigen Zertifizierungsstellen auditieren lassen und eine Zertifizierung gemäß ISO 27001 erhalten. Dabei werden die von dem Unternehmen erstellten Referenzdokumente gesichtet, eine Prüfung vor Ort durchgeführt und ein Auditbericht erstellt. Mit einer Zertifizierung kann die Wirksamkeit eines ISMS glaubwürdig nachgewiesen werden. Das kann das Vertrauen von Kunden, Partnern und anderen Interessengruppen stärken und auch bei der Einhaltung von Datenschutz– und Compliance-Vorschriften helfen.

IT-GRUNDSCHUTZ

Der IT-Grundschutz ist ein Konzept zur Absicherung von IT-Systemen und -Infrastrukturen gegen vorhandenen Risiken. Das IT-Grundschutz-Kompendium wurde vom BSI entwickelt und ist in drei Bereiche aufgeteilt:

1. Die Basisabsicherung setzt die Mindestanforderungen durch den Einsatz von Firewall-Systemen und Zutrittskontrollen um. Sie richtet

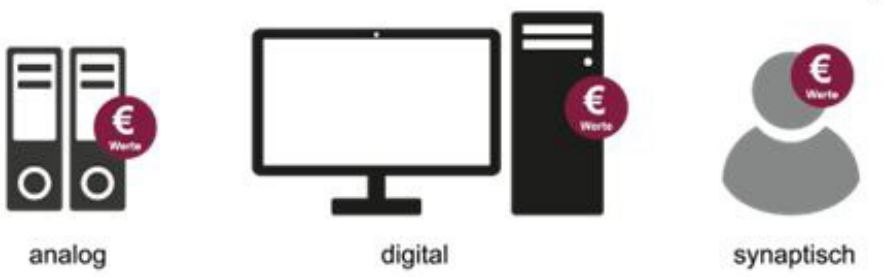

Abbildung 4: Definition Informationssicherheit (Bild: if(is))

sich vor allem an kleine und mittelständische Unternehmen.

2. Die Kernabsicherung dient dem Schutz von unternehmenskritischen Daten, wie zum Beispiel Produktions-, Kunden- oder Finanzdaten. Diese ist geeignet für Unternehmen, die noch kein ganzheitliches Informationssicherheitsmanagementsystem integriert haben.

3. Darüber hinaus gibt es die Standardabsicherung, die auf ein höheres Sicherheitsniveau durch eine Absicherung der gesamten Sicherheitsarchitektur abzielt.

Im Allgemeinen setzt sich IT-Grundschutz aus den Folgenden Schritten zusammen:

1. **Schutzziele bestimmen:** In diesem Schritt werden die Schutzziele definiert, die für die Organisation wichtig sind. Hierzu zählen beispielsweise die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen.

2. **Assets und Bedrohungen identifizieren:** Es werden die Assets (Werte) identifiziert, die in der Organisation geschützt werden müssen, sowie die Bedrohungen, denen sie ausgesetzt sind. Hierzu gehören beispielsweise Daten, Systeme, Netzwerke und Anwendungen sowie Bedrohungen wie Hackerangriffe oder menschliches Fehlverhalten.

3. **Risikoanalyse durchführen:** In diesem Schritt werden die identifizierten Assets und Bedrohungen bewertet und das daraus resultierende Risiko für die Organisation ermittelt. Hierbei werden auch die Auswirkungen eines erfolgreichen Angriffs auf die Organisation berücksichtigt.

4. **IT-Sicherheitsmaßnahmen zur Risikominimierung entwickeln:** Auf Basis der Ergebnisse der Risikoanalyse werden geeignete Cyber-Sicherheitsmaßnahmen zur Risikominimierung entwickelt. Hierbei kann es sich beispielsweise um technische IT-Sicherheitsmaßnahmen wie Firewalls oder Verschlüsselung sowie organisatorische Maßnahmen wie Schulungen für Mitarbeiter oder Regelungen für den Umgang mit Daten handeln.

5. **Maßnahmen implementieren und überprüfen:** Die entwickelten IT-Sicherheitsmaßnahmen werden umgesetzt und regelmäßig überprüft, um sicherzustellen, dass sie weiterhin wirksam sind und den Schutz der Assets gewährleisten.

Das IT-Grundschutzverfahren ist ein iterativer Prozess, der regelmäßig durchlaufen werden sollte, um sicherzustellen, dass die IT-Sicherheit in der Organisation kontinuierlich verbessert wird. Es ist ein bewährtes Verfahren, das Organisationen jeder Größe und Branche bei der Verbesserung ihrer Cybersicherheit unterstützt.

Der IT-Grundschutz des BSI ist ein Standard zur Informationssicherheit, welcher sich besonders in Unternehmen, die zur kritischen Infrastruktur gehören sowie bei öffentlichen Stellen etabliert hat.

INFORMATIONSSICHERHEITSMANAGEMENTSYSTEM (ISMS)

Ein ISMS ist ein strukturierter Ansatz zur Verwaltung der Informationssicherheit in einer Organisation. Es besteht aus einer Reihe von Prozessen, Sicherheitsrichtlinien, Verfahren und Kontrollen, die dazu dienen, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten. Ein ISMS basiert oft auf dem internationalen Standard ISO 27001, der die Anforderungen für ein Informationssicherheitsmanagementsystem festlegt. Auch im IT-Grundschutz ISMS im Fokus.

Die Implementierung umfasst mehrere Schritte:

- Kontextfestlegung: Die Organisation identifiziert den Anwendungsbereich des ISMS und legt die Ziele und Richtlinien fest.
- Risikobewertung: Eine systematische Bewertung der Informationssicherheitsrisiken wird durchgeführt, um Cybersicherheitsgefahren und Schwachstellen zu identifizieren.
- Risikobehandlung: Basierend auf den Ergebnissen der Risikobewertung werden geeignete Cybersicherheitsmaßnahmen ergriffen, um die Risiken zu reduzieren oder zu eliminieren.
- Implementierung der Kontrollen: Es werden IT-Sicherheitskontrollen und -maßnahmen implementiert, um die festgelegten Ziele zu erreichen. Dies umfasst technische, organisatorische und physische IT-Sicherheitsmaßnahmen.

Abbildung 5: Informationssicherheitsmanagementsystem (Bild: if(is))

- Überwachung und Überprüfung: Die Wirksamkeit der implementierten Kontrollen wird regelmäßig überwacht und überprüft, um sicherzustellen, dass sie angemessen funktionieren.
- Kontinuierliche Verbesserung: Das ISMS wird kontinuierlich verbessert, indem Schwachstellen identifiziert, IT-Sicherheitsvorfälle analysiert und Maßnahmen zur Verhinderung zukünftiger Vorfälle ergriffen werden.

ZUSAMMENFASSUNG

Das Thema Sicherheit ist ein komplexes und vielfältiges Thema. Anhand der Definition von IT-Sicherheit, Cybersicherheit und Informationssicherheit lassen sich die verschiedenen Perspektiven aufzeigen, die eingenommen werden können. Mithilfe etablierter Standrads wie der ISO 27001 und dem IT-Grundschutz können Unternehmen und Organisationen ein ISMS aufbauen, das Sicherheit strukturiert und damit so vollständig wie nur möglich umsetzt. ■

NORBERT POHLMANN
ist Professor für Cybersicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.