Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

Handreichung "Security by Design"

Leitfaden für die Entscheidungsebene

2023

Danksagung

Diese Publikation wurde im TeleTrusT-Arbeitskreis "Security by Design", einem Untergremium der TeleTrusT-AG "Recht", erarbeitet. TeleTrusT bedankt sich bei den nachstehenden Personen für ihre Mitwirkung sowie für die aktive Mitgestaltung dieser Handreichung.

Projektleitung

Rolf Blunk, IFIT, Leiter des TeleTrusT-AK "Security by Design"

Autoren (Auszug)

Adolf, Alexander - Condition-ALPHA
Bartels, RA Karsten U. LL.M - HK2 Rechtsanwälte
Burgstaller, Prof. Dr. Peter, LL.M - FH Hagenberg (Oberösterreich)
Drexler, Harald - Cybersec (Oberösterreich)
Egle, Monika - ditis
Haar, Jan - Bundesdruckerei
Hammer, Jonas - esatus
Hempel, Christopher - esatus
Hollay, Christopher
Huisgen, Dr. Philip - Datakom
Kolmhofer, Prof. DI Robert - FH Hagenberg (Oberösterreich)
Richter, Thorsten - ditis
Rieken, Dr. Ralf - Uniscon
Schmidt, Peter - ditis
Schütz, Anna Katharina - esatus

Redaktion

Abou Nasser, Morad - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Mühlbauer, Dr. Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)

In dieser Publikation werden zahlreiche Anglizismen verwendet, da sie sich in der zugrundeliegenden Fachdiskussion branchentypisch verfestigt haben.

Impressum

Herausgeber:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
E-Mail: info@teletrust.de
https://www.teletrust.de

V 2_2023-05

Inhalt

Verwendungshinweis

Diese Handreichung versteht sich als Ausgangspunkt bei der Ermittlung von gesetzlichen IT-Sicherheitsmaßnahmen, die dem Stand der Technik entsprechen. Sie ersetzt eine technische, organisatorische oder rechtliche Beratung oder Bewertung im Einzelfall nicht.

Glossar

Bedrohung	Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch den oder das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann. Beispiele für Bedrohungen sind höhere Gewalt, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen. Trifft eine Bedrohung auf eine Schwachstelle (insbesondere technische oder organisatorische Mängel), so entsteht eine Gefährdung.
Schwachstelle	Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.
Gefährdung	Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt / eine Ressource einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt / eine Ressource.
Safety	Safety ist ein Zustand des Schutzes von Mensch und Umwelt vor potenziellen Schäden oder etwas, das zum Schutz und zur Vorbeugung von Schäden entwickelt wurde. Beim Menschen sind sowohl physische als auch psychische Schäden einzubeziehen.
Cyber-Sicherheit	Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der klassischen IT-Sicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein.

1 Ausgangssituation, Motivation, und Zielsetzung

1.1 Ausgangssituation

Kunden, Analysten und Produkthersteller sind sich einig: Die Digitalisierung von Produkten, Prozessen und Dienstleistungen ist in allen Branchen angekommen. Von der Automobilindustrie und deren Zulieferern über den Maschinen- und Anlagenbau bis hin zu Konsumgüterherstellern. Viele Produkte haben eine digitale Komponente und sind mit dem Internet verbunden - das sogenannte Internet of Things (IoT).

In jüngster Vergangenheit haben eine Vielzahl erfolgreicher Cyber-Angriffe gezeigt, dass schlecht oder gar nicht abgesicherte IoT-Komponenten sehr effektive Werkzeuge sein können, um IT-Infrastrukturen erfolgreich anzugreifen. Cyber-Erpressung durch Ransomware, wie auch verteilte Angriffe über Botnetze stellen mittlerweile die Hauptbedrohungen für Unternehmen dar. Die Anzahl an entdeckten Schwachstellen in IoT-Komponenten nimmt ebenfalls stetig zu. Dies unterstreicht die Notwendigkeit wirkungsvolle Sicherheitsmechanismen zu einem Kernelement der digitalisierten Welt zu machen.

Internationale, europäische und nationale Gesetzesinitiativen sowie Anforderungen aus dem privatwirtschaftlichen Bereich regulieren zunehmend die Cyber-Sicherheit digitaler Produkte und Dienstleistungen. Die Europäische Kommission sowie der nationale Gesetzgeber haben diese Risiken und Probleme ebenfalls erkannt und reagieren hierauf mit unterschiedlichen Gesetzen, Verordnung und Richtlinien. Beispielsweise: IT-Sicherheitsgesetz (ITSiG), EU-Datenschutzgrundverordnung (EU-DSGVO)[1], Richtlinie zur Netz- und Informationssicherheit (EU-NIS-Richtlinie)[2], EU Cyber Resilience Act (CRA), UNECE-Regelung 155/156, EU-Maschinenverordnung. Teilweise sehen diese Regulierungen bei Nichteinhaltung empfindliche Strafen für Unternehmen vor oder versagen gar die Inverkehrbringung von Produkten mit digitalen Bestandteilen im europäischen Wirtschaftraum.

1.2 Motivation

Um am Markt zu bestehen, ist es für Produkthersteller unabdingbar, die Anforderungen der Cyber-Sicherheit aus Gesetzesinitiativen und Kundenvorgaben in ihren digitalisierten Produkten und Dienstleistungen umzusetzen.

Die Umsetzung der "Security by Design"-Prinzipien lässt sich sehr gut in ein Informationssicherheitsmanagementsystem (ISMS), z.B. gemäß der ISO/IEC 2700x-Normenreihe, integrieren und kann dazu führen, dass die Anforderungen eines solchen ISMS leichter erfüllt werden können.

Ohne die Umsetzung der Anforderung Cyber-Sicherheits-Compliance auf Basis von "Security by Design" droht nicht nur ein Imageverlust und die Beschädigung der bestehenden Marke durch unzuverlässige digitale Produkte, Prozesse und Dienstleistungen. Es ist auch damit zu rechnen, dass Umsatzeinbußen durch nicht erfüllte Kunden-Compliance-Anforderungen und haftungsrechtliche Risiken für den Produkthersteller konkrete finanzielle Auswirkungen haben werden.

1.3 Zielsetzung

Um Anforderungen der Cyber-Sicherheit effektiv und effizient umzusetzen, gilt es diese nicht als isolierte Funktionen eines Produkts oder Service zu realisieren. Vielmehr sind sie als integrierte Produkteigenschaften wie unter anderem Gebrauchsfunktionen, Benutzerfreundlichkeit oder Qualität umzusetzen.

Die Anforderungen aus den "Security by Design"-Prinzipien sind in den gesamten Produktlebenszyklus einzubringen und zu integrieren - von der ersten Idee bis zum Erreichen des End-of-Life eines Produktes. In der Umsetzungsverantwortung sind alle am Produkt beteiligten Unternehmensbereiche wie beispielsweise Produktmanagement, Entwicklung, Beschaffung, Fertigung, Vertrieb, Logistik, Service, aber auch Stakeholder aus dem Bereich der Compliance z.B. Datenschutzbeauftragter, Compliance-Beauftragte, Cybersecurity-Manager einzubinden.

Die vorliegende TeleTrusT-Handreichung soll Hersteller digitalisierter Produkte, Prozesse und Dienstleistungen unterstützen, die "Security by Design"-Prinzipien in ihren Produktlebenszyklus zu integrieren (siehe Kapitel 3) und gibt hierfür organisatorische Handlungsempfehlungen (siehe Kapitel 4).

[1] DSGVO: Verordnung (EU) 2016/679
[2] NIS2: Richtlinie (EU) 2022/2555

2 Grundverständnis "Security by Design"

"Security by Design" ist ein Prinzip, das sicherstellt, dass Sicherheitsanforderungen bereits zu Beginn des Entwicklungsprozesses systematisch ermittelt und berücksichtigt werden, um spätere Aufwände zur Behebung von Sicherheitslücken zu verhindern oder zu minimieren.

Das "Security by Design"-Prinzip ist nicht neu und im Grunde genommen eine Anleitung zum Bau und Betrieb sicherer Systeme. Es wird seit etlichen Jahren bereits von führenden Unternehmen wie Apple, Microsoft, Google, Adobe, Oracle etc. praktiziert. Es kann und sollte komplementär mit anderen Prinzipien (z.B. "Privacy by Design") umgesetzt werden.

Hersteller von digitalisierten Produkten, Prozessen und Dienstleistungen werden mit "Security by Design" in die Lage versetzt, gesetzliche und regulatorische Vorgaben zur IT-Sicherheit sowie diesbezügliche marktübliche und kundenspezifische Anforderungen einzuhalten und ggf. entsprechende Zertifizierungen zu erhalten.

"Security by Design" ist ebenso eine unabdingbare Voraussetzung, um Gefährdungen der Betriebssicherheit (functional safety) von Produkten und Diensten durch Sicherheitslücken abzuwehren. Ebenso ist die Einhaltung von "Security by Design"-Prinzipien, die Grundvoraussetzungen für die Gewährleistung von "Privacy by Design"-Prinzipien, die zum Schutz der Privatsphäre bei Verarbeitung personenbezogener Daten von der EU-DSGVO gefordert werden.

"Security by Design" ist für Unternehmen kein "nice to have", sondern zwingendes "Muss", um mit Produkten, Prozessen und Dienstleistungen erfolgreich in den Markt einzutreten, am Markt agieren und bestehen zu können. Der Erfolg des herstellenden bzw. anbietenden und/oder betreibenden Unternehmens hängt essenziell davon ab, dass die "Security by Design"-Prinzipien über den gesamten Lebenszyklus aktiv und konsequent angewandt werden.

Bei der Umsetzung der Maßnahmen nach den "Security by Design"-Prinzipien ist die einfache Anwendbarkeit von Sicherheitsmaßnahmen im Nutzungskontext im Sinne des "Usable Security"-Prinzips zu berücksichtigen. Fehlende Anwendbarkeit kann zu Nutzungsfehlern oder zum Umgehen von Sicherheitsmaßnahmen und damit letztlich zu Sicherheitsproblemen führen.

Als eine grundlegende und qualitätsentscheidende Kernmaßnahme für den gesamten weiteren Lebenszyklus nach den "Security by Design"-Prinzipien hat sich die sorgfältige Planung und Durchführung einer strukturierten Bedrohungsmodellierung (Threat Modeling) während der frühen Ideen- bzw. Konzept-Phase als "Best-Practice-Vorgehen" erwiesen.

Hierbei werden in einem moderierten Dialog zwischen allen, für das jeweilige Planobjekt relevanten, Stakeholdern zunächst die für das Unternehmen schützenswerten Assets identifiziert. Risikobewertungen für relevante Bedrohungslagen werden in der Folge von allen Beteiligten vorgenommen und entsprechende IT-Sicherheits- und Datenschutzanforderungen dokumentiert.

Damit liegen als Ergebnis spezifisch dokumentierte und von allen Stakeholdern mitgetragene Schutzziele und geplante Sicherheits- und Datenschutzmaßnahmen als zu überprüfende Soll-Vorgaben für den gesamten weiteren Lebenszyklus mit den nachfolgend modellhaft beschriebenen Phasen vor.

3 Produkt-Lebenszyklus / Product Lifecycle

Eine am Markt etablierte, gut geführte und gepflegte Marke gehört zu den essenziellen Werten eines Unternehmens. Oft nutzen Unternehmen diese etablierten Marken, um ihre innovativen digitalen Produkte und Services am Markt zu platzieren. Häufig wird dabei vergessen, dass die digitalen Komponenten eines Produktes ebenso wie das physische Produkt selbst, einem Produkt-Lebenszyklus unterworfen sind.

Um den Markenwert nicht zu beschädigen ist es unabdingbar, dass auch digitale Produkte durch ein Produkt-Lebenszyklus-Management / Product Lifecycle Management (PLM) über den kompletten Lebenszyklus hinweg begleitet werden. Integraler Bestandteil sind dabei die Fragestellungen, wie verfügbar, wie zuverlässig und wie nachhaltig ein digitales Produkt in der Kundenbeziehung sein muss, um am Markt zu bestehen und den Markenwert in einer digitalen Welt zu stärken und nicht durch mangelnde IT-Sicherheit zu gefährden.

Eine wichtige Komponente, um dieser Herausforderung nachhaltig gerecht zu werden, sind die "Security by Design"-Prinzipien. Elementare Grundlage ist die Integration der Sicherheitsanforderungen in allen Phasen des Produkt-Lebenszyklus-Management / Product Lifecycle Management (PLM). Man spricht dann von einem Sicheren-Produkt-Lebenszyklus-Management / Secure Product Lifecycle Management.

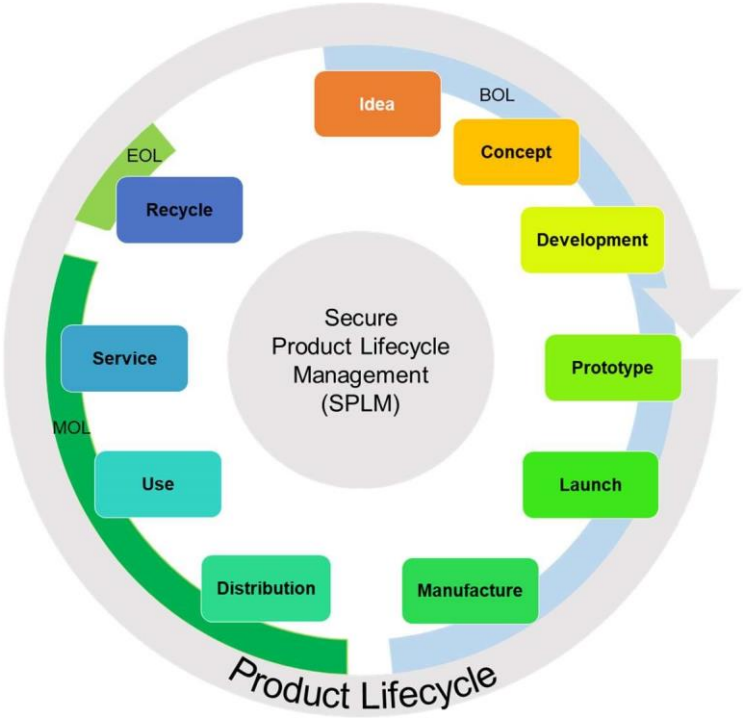

Abbildung 1: Sicheres-Produkt-Lebenszyklus-Management / Secure Product Lifecycle Management (SPLM)

3.1 Sicherer-Produkt-Lebenszyklus / Secure Product Lifecycle (SPL)

Die "Security by Design"-Prinzipien sind in das Produkt-Lebenszyklus-Management / Product Lifecycle Management (PLM) integriert und begleiten alle Phasen des Lebenszyklus: Man spricht vom Sicheren-Produkt-Lebenszyklus-Management / Secure Product Lifecycle Management (SPLM).

Grundlegende Voraussetzung für ein SPLM ist die Einbindung aller Phasen in ein Qualitäts- und Informationssicherheitsmanagementsystem. Auf Basis dieses Managementsystems haben alle am Produkt beteiligten Unternehmensbereiche z.B. Produktmanagement, Entwicklung, Beschaffung, Fertigung, Vertrieb, Logistik, Service, aber auch Stakeholder aus dem Bereich der Compliance z.B. Datenschutzbeauftragter, Compliance-Beauftragte, Cybersecurity-Manager, Verantwortung im Kontext der Cybersecurity im Produkt zu übernehmen.

3.1.1 Entstehungsphase / Beginning of Life (BOL)

Die Entstehungsphase eines Produkts durchläuft verschiedene Reifegrade: Von der Idee, über die Konzeption und der Entwicklung eines Prototyps entsteht ein marktreifes Produkt. Die "Security by Design"-Prinzipien begleiten auch die Entstehungsphase. Daraus ergeben sich Anforderungen, die in den nachfolgenden Kapiteln näher erläutert werden.

3.1.1.1 Idee / Idea

Bereits während der Konkretisierung von Produktideen ist die Klärung folgender Punkte wichtig:

- Ist das Thema "Product Security" ein Alleinstellungsmerkmal / Unique Selling Point (USP)? Wird das Produkt mit einem "Product Security Image" am Markt erfolgreicher? Sind dafür Zertifizierungen notwendig?
- Wo, in welchem physikalischen Umfeld (z.B. Outdoor, im Privathaushalt, Kraftwerk etc.) und in welchem logischen Umfeld (z.B. im Netzwerk, vor oder hinter einer Firewall etc.) soll das Produkt eingesetzt werden?
- Wie hoch sind die Sicherheitsanforderungen, die der Markt an das Produkt stellt?

3.1.1.2 Konzept / Concept

In der Konzeptphase eines Produkts sind folgende Fragen zu beantworten:

- Wie hoch ist der Schutzbedarf der Daten und Schutzobjekte hinsichtlich der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit?
- Gibt es Compliance-Anforderungen (Normen, Gesetze, Branchen-Standards, Kundenanforderungen, interne Regelungen, etc.) an das Produkt?
- Welche digitalen Bedrohungsszenarien würden die Sicherheit des Produkts gefährden oder die Marke beschädigen?
- Wie können die identifizierten Bedrohungen ausreichend abgeschwächt werden?
- Welche Sicherheitsanforderungen müssen eingesetzte Dritt-Anbieter- / Third-Party Komponenten erfüllen?
- Welche Sicherheitsanforderungen sind bei der Auswahl von Dienstleistern zu beachten?
- Welche Konzepte zur Erkennung von Sicherheitsvorfällen müssen verfolgt werden und welche Möglichkeiten zur Auswertung sind notwendig?

3.1.1.3 Entwicklung / Development

Nachdem die Fragestellungen aus den Phasen "Idee" und "Konzept" beantwortet und festgeschrieben sind, gilt es unter Berücksichtigung der "Security by Design"-Prinzipien ein marktfähiges Produkt mit angemessenen Schutzmaßnahmen zu entwickeln. Dazu zählen insbesondere:

- Die Systemarchitektur hat Sicherheitsanforderungen durch ein Sicherheitskonzept angemessen zu berücksichtigen.
- Der Systementwurf muss daraufhin überprüft werden, ob alle relevanten Bedrohungen ausreichend abgeschwächt sind.
- Allgemein anerkannte Methoden zur sicheren Implementierung müssen angewendet werden.
- Die sichere Implementierung wird mit geeigneten Mitteln (beispielsweise statische und dynamische Codeanalyse) überprüft.
- Alle Dritt-Anbieter- / Third-Party-Lieferanten und Komponenten müssen abhängig von deren Kritikalität in die Überprüfung eingebunden werden.
- Die Integrität der Entwicklungsumgebung und der eingesetzten Werkzeuge muss durch geeignete technische und organisatorische Maßnahmen geschützt werden.

3.1.1.4 Prototyp / Prototype

Während dieser Phase werden die Sicherheitsfähigkeiten des Produkts unter realen Bedingungen in deren physischen und logischen Einsatzort überprüft. Geeignete Prüfungen sind z.B.:

- Automatisierte Schwachstellensuche im Produkt
- Penetrationstests.

3.1.1.5 Einführung / Launch

In dieser Phase muss die Organisation auf den sicheren Betrieb vorbereitet werden. Hierzu sind folgende Punkte zu berücksichtigen:

- Aufbau einer Organisation zur regelmäßigen Überprüfung aller verwendeter Komponenten und Bibliotheken auf Schwachstellen sowie das Etablieren eines Schwachstellenmanagements.
- Aufbau und etablieren einer Organisation zur Sicherstellung von Wartung und Support, insbesondere für das Patch- und Defektmanagement.
- Erstellen von Kundendokumentation zum zweckmäßigen und sicheren Betrieb des Produkts.
- Dem Kunden gegenüber muss in transparenter Art und Weise vermittelt werden, wie und wie lange Sicherheitsupdates für das Produkt verfügbar sind.

3.1.1.6 Herstellung / Manufacture

Neben den üblichen Qualitätssicherungsmaßnahmen muss in der Produktionsphase die gleichbleibende Sicherheit des Produkts gewährleistet werden. Dazu sind folgende Punkte zu berücksichtigen:

- Sicherstellung der Rückverfolgbarkeit aller Informationen zum Produkt. Hierzu zählen beispielsweise ein Verzeichnis der Seriennummern und ausgelieferten Hard- und Software-Komponenten, Firmware, Betriebssysteme, Bibliotheken und deren Versionen. Dies ist die notwendige Basis, um ein Schwachstellenmanagement zu betreiben.
- Schutz der Integrität der Produktionsumgebung, um insbesondere sicherzustellen, dass keine manipulierten Komponenten in die Produktion übernommen werden. Dies bedeute: Sicherstellung der Herkunft der installierten Software, der verarbeiteten Daten, der Konfigurationen mittels geeigneter Verfahren sowie ausreichende Schutzmechanismen gegen nachträgliche Manipulation.

3.1.2 Nutzungs- und Service-Phase / Middle of Life (MOL)

Nach der Fertigung beginnt die "Middle of Life" Phase. Das Produkt wird an den Endkunden ausgeliefert und durch die Serviceorganisation betreut. Hier werden Daten über Fehler, Defekte, Wartungsarbeiten, Kundenerfahrungen etc. gesammelt. Diese Datenerhebung ist für die Fehlerbehebung und Weiterentwicklung des Produktes notwendig.

3.1.2.1 Distribution

Die Distribution-Organisation muss befähigt werden, Produkte sicher im festgelegten Einsatzszenario in den Verkehr zu bringen. Dieses bedeutet insbesondere:

- Für die Auslieferung digitaler Komponenten (Software, Konfigurationsdateien etc.) sind geeignete Verfahren zur Wahrung der Integrität und Herkunft anzuwenden.
- Kundendokumentation zum zweckmäßigen und sicheren Betrieb des Produkts wird bereitgestellt und während des zugesagten Support-Zeitraums aktuell gehalten.

3.1.2.2 Nutzung / Use

Der Betreiber muss befähigt werden, Produkte sicher im festgelegten Einsatzszenario zu betreiben. Dazu ist es erforderlich, dass der Hersteller folgende Punkte erfüllt:

- Es muss ein Schwachstellenmanagement betrieben werden, um auf Schwachstellen zu reagieren.
- Über ein Incident-Management wird sichergestellt, dass Sicherheitsprobleme zeitnah erkannt, untersucht, behandelt und behoben werden.
- Ebenso werden server- bzw. cloudseitige Komponenten stets auf einem aktuellen, sicheren und gesetzeskonformen Stand gehalten. Für weitere Details sei auf die TeleTrusT-Handreichung "Cloud Supply Chain Security"[3] der TeleTrusT-Arbeitsgruppe "Cloud Security" hingewiesen.

3.1.2.3 Service

Die Service-Organisation muss in der Lage sein, über geeignete Kommunikationswege die Kunden über Sicherheits-Patches, Sicherheitsprobleme, deren Auswirkung und mögliche Ausgleichsmaßnahmen zu informieren. Darüber hinaus gibt es bereits bei Sicherheits- und Datenschutzvorfällen gesetzliche Regelungen hinsichtlich der Meldepflichten (inkl. Meldefristen).

Des Weiteren ist über einen geeigneten Service-Prozess sicherzustellen, dass Daten bei Rückläufern und Reparaturen dem Schutzbedarf angemessen behandelt werden.

3.1.3 Nutzungsende / End of Life (EOL)

Am Nutzungsende / die "End of Life" Phase umfasst alle Schritte, die mit der Einstellung des Supports, der Außerbetriebnahme und Entsorgung des Produkts zu tun haben.

3.1.3.1 Recycle / Auslaufzyklus

Bereits beim Design des Produkts müssen die Anforderungen an das "End of Life" (EoL) sowie den "End of Support" (EoS) berücksichtigt werden:

- EoS: Es muss sichergestellt werden, dass Kunden rechtzeitig über das Ende des Supports informiert werden. Hier sind Hinweise auf mögliche Sicherheitsauswirkungen auf Schutzobjekte und Schutzziele zu geben.

[3] Publikationen der TeleTrusT-AG "Cloud Security"

- EoL: Im Produkthandbuch müssen die Verfahren zur sicheren Außerbetriebnahme sowie der sicheren und fachgerechten Entsorgung beschrieben werden. Dies umfasst zum einen technische Möglichkeiten zur Löschung sensibler Daten (z.B. Schlüsselmaterial, personenbezogene Daten etc.), aber auch die sichere physikalische Entsorgung bzw. das Recycling von Geräten.

3.2 Sicheres-Produkt-Lebenszyklus-Management-System / Secure Product Lifecycle Management System (SPLMS)

Um die Anforderungen des "Security by Design"-Konzepts vorausschauend, nachhaltig und effizient in einer Organisation zu implementieren, ist ein SPLMS unerlässlich.

3.2.1 Ziele

Die Ziele eines SPLMS sind insbesondere:

- Vermeidung von Organisationsverschulden und Nachweis der Erfüllung von Kundenanforderungen und rechtlichen Vorgaben
- Effizientes Management der Sicherheitsanforderungen während des kompletten Produkt-Lebenszyklus / Product Lifecycle
- Transparenz der Produktrisiken durch Integration des Produkt-Lebenszyklus / Product Lifecycle in das interne Kontrollsystem

3.2.2 Methodik

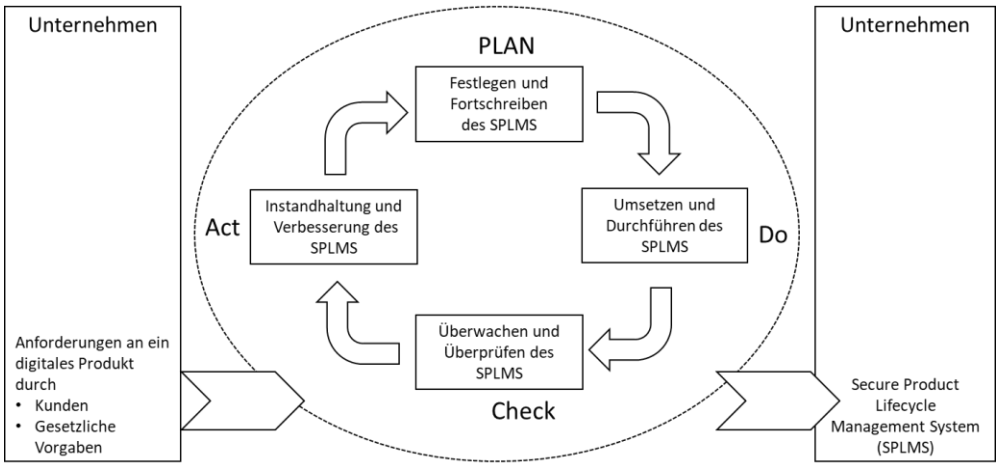

Abbildung 2: Methodik eines Sicheren-Produkt-Lebenszyklus-Management-Systems / Secure Product Lifecycle Management Systems (SPLMS)

In der betrieblichen Praxis hat sich beim Aufbau von Managementsystemen der PDCA-Zyklus (Plan-Do-Check-Act), auch Demingkreis genannt, als sinnvoll erwiesen. Gesteuert von den Anforderungen der Kunden und der gesetzlichen Vorgaben werden Management-Prozesse definiert, kontinuierlich verbessert, auf geänderte Anforderungen angepasst sowie nachhaltig und effizient in der Unternehmensorganisation umgesetzt.

3.2.3 Struktur

Die Dokumentation des Sicheren-Produkt-Lebenszyklus-Management-Systems / Secure Product Lifecycle Management System (SPLMS) wird in Anlehnung an andere Managementsysteme in der Regel durch einen hierarchischen Aufbau charakterisiert und lässt sich in Form einer Pyramide veranschaulichen.

Abbildung 3: Struktureller Aufbau eines Sicheren-Produkt-Lebenszyklus-Management-Systems / Secure Product Lifecycle Management Systems (SPLMS)

- **Leitlinie:** Durch die Leitlinie gibt die Unternehmensleitung die Grundsätze für die Entwicklung digitaler Produkte verbindlich vor. Sie legt die Ziele, Verantwortlichkeiten und die grundsätzliche Sicheres-Produkt-Lebenszyklus-Management-Organisation / Secure Product Lifecycle Management Organisation im Unternehmen fest.

- **Managementprozesse:** Die Managementprozesse beschreiben die grundsätzlichen Vorgaben zum SPLMS. Dazu gehören insbesondere: Schutzbedarf-, Risiko-, Dokumentations-, Audit-, Qualifikations-, Entwicklungs-, Software-Qualitäts-, Security-, Datenschutz-, Dienstleister-, Defekt-, Schwachstellen- und Incidentmanagement.

- **Zielgruppenorientierte Richtlinien:** Um die grundsätzlichen Vorgaben der Managementprozesse in den unternehmerischen Alltag zu integrieren, sind zielgruppenorientierte Richtlinien sinnvoll. In global agierenden Unternehmen müssen beim Erstellen der Richtlinien rechtliche, infrastrukturelle und kulturelle Einflussfaktoren an den jeweiligen Unternehmensstandorten berücksichtigt werden. Als typische Zielgruppen für spezifische Richtlinien haben sich in der Praxis u.a. folgende Gruppen herauskristallisiert: Produktmanagement, Systemarchitektur, Entwicklung, Qualitätssicherung, Anforderungsmanagement, Einkauf, IT, Service, Vertrieb, Datenschutzverantwortlicher und Personal.

- **Konkrete Hilfestellung und Werkzeuge**: Um die zielgruppenorientierten Richtlinien effektiv und effizient umzusetzen, empfiehlt es sich, den unterschiedlichen Zielgruppen entsprechende Hilfestellungen und Werkzeuge an die Hand zu geben, wie beispielsweise Formulare, Checklisten, konkrete Arbeitsanweisungen und Kollaborationswerkzeuge.

4 Handlungsempfehlung

"Security by Design" ist für Unternehmen ein zwingendes "Muss", um mit Produkten, Prozessen und Dienstleistungen erfolgreich am Markt agieren und bestehen zu können.

Was ist also zu tun, um die "Security by Design"-Prinzipien für das eigene Unternehmen nachhaltig einführen zu können?

Eindeutiges Commitment der Unternehmensführung ist zwingend.

Zuallererst bedarf es einer klaren Kommunikation der Geschäftsführung respektive des Vorstands, dass "Security by Design" eine zwingende Voraussetzung im Produktentwicklungs- und Produktionsprozess sein muss. Dabei ist darauf zu achten, dass nicht nur zukünftige Produkte, Prozesse und Dienstleistungen zu betrachten sind, sondern auch die, die derzeit am Markt positioniert sind.

"Security by Design" ist, allem voran, die Weiterentwicklung der gesamten Organisation.

Bei "Security by Design" handelt es sich nicht um technische Vorgaben, sondern um eine Maßgabe der Organisationsentwicklung, welche die gesamte Organisation betrifft. Die Organisation muss sich anpassen. Die handelnden Akteure haben sich nach den Prinzipien von "Security by Design" auszurichten und in weiterer Folge zu verhalten.

Ausreichende Ressourcen- und finanzielle Mittelbereitstellung sind unerlässlich.

Um die "Security by Design"-Prinzipien erfolgreich im Unternehmen einzuführen, bedarf es neben des uneingeschränkten Management Commitments auf allen Ebenen einer ausreichenden Bereitstellung von Ressourcen und finanziellen Mitteln.

Damit darf "Security by Design" nicht nur als Absichtserklärung eines mittleren Managements für das Unternehmen und seine Partner verstanden werden. Ein nachhaltiger Nutzen wäre kaum gewährleistet. Zu hoch wäre die Gefahr, dass das Unternehmen mit seinen Produkten und Dienstleistungen am Markt keinen Absatz mehr findet.

"Security by Design" ausrichten auf Compliance-Vorgaben und gesetzliche Bestimmungen

Wesentlich ist zu definieren, welche Compliance-Vorgaben umgesetzt werden müssen. Strebt das Unternehmen beispielsweise eine Zertifizierung nach einer Norm an, hat es spezielle Branchen-Vorgaben seitens Partner, Verbände oder gar Gesetzgeber zu erfüllen, sind für die Erschließung von Export-Ländern besondere zusätzliche Compliance-Vorgaben zu berücksichtigen.

Eindeutige Zuordnung der Verantwortung von "Security by Design" innerhalb der Organisation

Eine eindeutige Zuordnung der Umsetzungsverantwortung innerhalb der Organisation ist entscheidend für den Erfolg der Einführung. Hierbei ist die Regelung wichtig, ob die jeweilige Instanz lediglich für die Einführung der Compliance-Normen zuständig ist oder, ob nach erfolgreichem Abschluss der Einführung diese mit der nachfolgenden dauerhaften Betreuung der Normumsetzung beauftragt ist.

Normen sind regelmäßigen Anpassungen unterworfen und diese Änderungen sind für das Unternehmen zu interpretieren und schließlich umzusetzen. Auch ist eine nachhaltige Überprüfung der Umsetzungsstände in den eigenen Organisationen regelmäßig zu überprüfen.

Lassen sich verschiedene vergleichbare Compliance-Vorgaben bündeln oder sind die Vorgaben von internen Regelwerken zur Einhaltung einer Produktionsqualität wenig unterschiedlich, so lassen sich Synergieeffekte erzielen. Der Vorteil darin liegt insbesondere in der Tatsache, dass sich Regelprozesse zur Einführung und Prüfung von Compliance-Vorgaben wenig unterscheiden und die Lernkurve hier wesentlich effizienter genutzt werden kann.

Der Vorteil für eine dezentralisierte Verantwortungsverteilung liegt in der meist größeren Nähe zu Informationskreisen einer Compliance-Vorgabe, so dass Änderungs- und Anpassungsanforderungen schneller identifiziert und somit deutlich im eigenen Produktions- und Leistungsprozess berücksichtigt werden können.

Stringente Vorgehensweise ist bei der Einführung geboten.

Um ein SPLMS zu konzipieren, einzuführen und zu betreiben, hat sich in der Praxis die etablierte Projekt-Vorgehensweise als effizient erwiesen.

Abbildung 4: SPLMS Projekt-Vorgehensweise

Alle betroffenen Organisationsbereiche sind einzubeziehen.

Sämtliche am Produkt oder an der Dienstleistung beteiligten Unternehmensbereiche sind dabei einzubinden wie beispielsweise: Produktmanagement, Entwicklung, Beschaffung, Fertigung, Vertrieb, Logistik, Service, aber auch Stakeholder aus dem Bereich der Compliance z.B. Datenschutzbeauftragter, Compliance-Beauftragte und Cybersecurity-Manager.

Dauerhafte Einbindung der Unternehmensführung im Projekt ist erforderlich.

Um das Management Commitment jederzeit sicherstellen zu können und das Management über die Änderungsanforderungen der eigenen Organisation informiert zu halten, ist dabei dringend zu empfehlen, dass ein Vertreter des Projekt-Steuerungsteams in regelmäßigen Abständen an die Unternehmensführung berichtet.

5 TeleTrusT-Position

Anliegen des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT) ist es, dazu beizutragen, dass Deutschland in einer global vernetzten Welt ein sicherer Ort für digitale und vernetzte Unternehmen und Verbraucher ist. Hierzu fördert der Verband die Zusammenarbeit staatlicher Stellen mit der Industrie, um nicht nur einerseits zu gewährleisten, dass Deutschland vor Cyber-Angriffen geschützt bleibt, sondern auch, um dafür Sorge zu tragen, dass Anwender vernetzter Produkte und Dienste in die Lage versetzt werden ihre digitale Souveränität zu wahren. Hierzu gilt es sicherzustellen, dass über den gesamten Lebenszyklus eines vernetzten Produktes hinweg angemessene und wirksame Sicherheitsmechanismen zum Einsatz kommen.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.