

Empfehlungen zu Entwicklung und Bereitstellung von in Kritischen Infrastrukturen eingesetzten Produkten

Version 2.0 vom 01.12.2022

Erstellt durch Themenarbeitskreis Lieferanten/Hersteller des UP KRITIS

www.upkritis.de

Download dieses Dokuments unter www.bsi.bund.de/dok/980540



Änderungshistorie

<i>Datum</i>	<i>Version</i>	<i>Bearbeitung</i>	<i>Autor</i>	<i>Status</i>
29.11.2018	1.00	Final – bestätigt	Plenum UP KRITIS	Freigegeben
01.12.2022	2.00	Final – bestätigt	Plenum UP KRITIS	Freigegeben

Tabelle 1: Änderungshistorie

Version 0.0 - 0.5 Zusammenstellen der Inhalte
Version 0.6 - 0.8 Review
Version 0.9 Version zur Freigabe im Plenum
Version 1.0 Vom Plenum freigegebene Version
... und zyklisch in dieser Aufteilung weiter

Bundesamt für Sicherheit in der Informationstechnik
Referat WG 13 – Geschäftsstelle UP KRITIS
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-5098
E-Mail: upkritis@bsi.bund.de
Internet: www.upkritis.de
© Bundesamt für Sicherheit in der Informationstechnik 2023

Inhalt

1	Einleitung.....	4
2	Grundlagen.....	5
3	Ziele	7
4	Herstellung eines Produktes.....	8
4.1	Security-Funktionalität im Umfeld „kDL“.....	8
4.2	Entwicklung von Produkten	8
4.3	Produktion des Produktes.....	10
4.4	Vertrieb des Produktes	11
4.5	Transparenz	11
5	Bereitstellung des Produktes.....	13
5.1	Übergabe und Inbetriebnahme des Produktes.....	13
5.2	Servicelevel während des Betriebs	13
5.3	Supportlaufzeit und Lebensdauer.....	13
6	Incident Handling.....	14
6.1	Informations- und Meldepflichten.....	14
6.2	Vertragliche Unterstützungsleistung bei Incidents.....	14
6.3	Unterstützungsleistung bei fehlender Vereinbarung	14
7	Zusammenfassung.....	15
8	Definitionen und Abkürzungen.....	16
9	Literatur	17

1 Einleitung

Für den Betrieb der kritischen Dienstleistungen setzen wir als Betreiber Produkte ein, die Hersteller und Dienstleister bereitstellen. Von deren Qualität bezüglich Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität hängt wesentlich die Qualität der kritischen Dienstleistung ab.

In der derzeit gültigen Gesetzgebung, insbesondere im IT-Sicherheitsgesetz, liegt die Verantwortung für die kritische Dienstleistung zurzeit nur am Ende der Supply-Chain-Kette beim Betreiber der Kritischen Infrastruktur. Damit bleiben bisher zwei wesentliche Leistungsanteile zu Erbringung der kritischen Dienstleistungen unbeachtet. Zum einen ist das der Entwicklungs- und Herstellungsprozess und zum anderen der Bereitstellungs- und Betriebsprozess der *Produkte*, die in den kritischen Dienstleistungen benötigt werden.

In absehbarer Zukunft wird der EU Cyber Security Act (SCA) darüber hinaus weitere verbindliche Anforderungen wie der EU Cyber Resilience Act (CRA) an Hersteller und Produkte adressieren, die hier als Grundlage vorausgesetzt werden.

Hersteller und Dienstleister, die Sicherheitsaspekte bereits bei der Entwicklung, Produktion und Bereitstellung von Produkten berücksichtigen, sind für die Betreiber verlässlichere Partner, um die für die Gesellschaft kritischen Dienstleistungen nachhaltig anbieten zu können.

Eine Transparenz über Sicherheits- und Verfügbarkeitseigenschaften von Produkten auf der einen Seite und deren Einsatzanforderungen bei den Betreibern Kritischer Infrastrukturen auf der anderen Seite sind elementare Voraussetzungen für einen effektiven Betrieb der kritischen Dienstleistung. In diesem Sinn kann dieses Dokument auch die Betreiber bei der Stellerauswahl unterstützen, um sicherheitsrelevante Themen zu adressieren.

Dieses Dokument beschreibt, wie die Mitwirkung der Hersteller und Dienstleister gestaltet werden müsste, um die Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität kritischer Dienstleistungen auf einem hohen Niveau gemeinsam sicherzustellen.

2 Grundlagen

Die Betreiber Kritischer Infrastrukturen haben eine besondere Verpflichtung, ihre Dienstleistungen bezüglich Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität auf einem hohen Niveau anzubieten und bereitzustellen.

Für den Betrieb der kritischen Dienstleistung setzen die Betreiber *Produkte und Dienstleistungen* (im Folgenden nur als *Produkte* bezeichnet) ein. In diesem Dokument beziehen sich die Autoren ausschließlich auf Produkte und Hersteller im Sinne einer Werkleistung und Werklieferung. Sowohl „klassische“ Produkte als auch aus Einzelprodukten zusammengefügte Lösungen unterliegen den beschriebenen Anforderungen und Empfehlungen. Hersteller sind dabei Erzeuger von Geräten und Systemen sowie Produzenten einer funktionsfertigen Lösung im Sinne des Werkrechts. Von der Produktqualität bezüglich Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität hängt damit wesentlich auch die Qualität der vom Betreiber einer kritischen Infrastruktur bereitgestellten Dienstleistung ab. Weisen solche *Produkte* eine Störung¹ auf, kann dies auch zu einer Störung der kritischen Dienstleistung (kDL) führen.

Für KRITIS-Betreiber stellt dieses Dokument ein Spiegelbild dessen dar, worauf er und sie achten sollten.

Plattformen wie Cloud (IaaS, PaaS) und Hosting werden in diesem Dokument nicht weiter als Funktionalität für die kDL betrachtet. Diese werden im Dokument „Anforderungen an Lieferanten“ [1] behandelt.

Die Verwendung von *Produkten*, deren Sicherheitsniveau den Anforderungen der kritischen Dienstleistung angemessen ist, kann die Komplexität der Sicherheitsmaßnahmen reduzieren und erleichtert die Etablierung und Aufrechterhaltung der Qualitätskriterien für die kDL. Die kDL kann dabei aber nur so gut sein wie die einzelnen *Produkte*, die für die kDL eingesetzt werden (Prinzip des schwächsten Gliedes in einer Kette bzw. Umgebung).

Freiwillige Transparenz und Maßnahmen der *Hersteller* sowie direkte gesetzliche Anforderungen an Mindestqualitäten in Bezug auf die Sicherheit und Funktionalität der von *Herstellern* bereitgestellten *Produkte* könnten diese Komplexität verringern.

Resultierend aus seinen Verpflichtungen der Daseinsfürsorge und Fürsorgepflicht hat der Gesetzgeber bisher Sicherheitsanforderungen für große Betreiber von kritischen Dienstleistungen (kDL) aus definierten Wirtschaftssektoren in Deutschland über das IT-Sicherheitsgesetz (IT-SiG) im BSI-Gesetz (BSiG) und für verschiedene Branchen zusätzlich in Spezialgesetzgebungen festgeschrieben.

In diesen Gesetzgebungen, hier insbesondere im IT-SiG, liegt die Verantwortung für die Verfügbarkeit der kritischen Dienstleistung vollumfänglich beim Betreiber der Kritischen Infrastruktur (KRITIS) am Ende der Supply-Chain-Kette. Entsprechend verbleibt auch die Verantwortlichkeit gegenüber den (Aufsichts-)Behörden im Störfall grundsätzlich beim Betreiber. Mit dem IT-SiG 2.0 (2021) ergibt sich, in speziellen Fällen, zusätzlich eine Verantwortung und Mitwirkungspflicht für Hersteller nach § 9b BSiG.

Nicht nur aufgrund der Vorgaben des IT-SiG sind Betreiber verpflichtet, adäquate Sicherheitsmaßnahmen für die kritischen Dienstleistungen zu ergreifen. Sie sollten deshalb mit ihren *Herstellern* immer entsprechende Vereinbarungen schließen, die diese Maßnahmen unterstützen und absichern. Es gibt aber auch bestimmte gesetzliche Anforderungen, die bisher nur mittels sehr aufwendiger kommerzieller Vereinbarungen mit einem oder mehreren *Herstellern* umgesetzt werden können. Nicht zu allen gesetzlichen Anforderungen ist dies auch nachhaltig möglich. Darüber hinaus müssen die Betreiber einer kritischen Dienstleistung viele Vereinbarungen separat mit *Herstellern* verhandeln oder durch entsprechendes Design in den IT-Architekturen für Sicherheit durch Redundanzen und oder zusätzliche Elemente sorgen – siehe hierzu auch „Anforderungen an Lieferanten...“ [1].

¹ Störungen sind Beeinträchtigungen in der Funktion eines Produkts, worunter auch bereits das Bekanntwerden einer (IT-)Schwachstelle des Produkts verstanden wird.

Dieses Dokument wendet sich primär an *Hersteller* von IT-basierenden *Produkten*, die von KRITIS-Betreibern eingesetzt werden. Gleichzeitig soll das Dokument auch als Werkzeug für KRITIS-Betreiber dienen, um die angebotenen *Produkte und Dienstleistungen* an den Empfehlungen in diesem Dokument zu spiegeln.

Gleichzeitig darf auch die Perspektive auf Anlagen mit IT-Schnittstellen bzw. das Schnittstellenthema an sich nicht vernachlässigt werden. Dazu finden sich zusätzlich weiterführende Informationen in „Anforderungen an netzwerkfähige Industriekomponenten“ [2] und „Sicherheitsspezifische Empfehlungen für Maschinenbauer und Integratoren“ [3].

3 Ziele

Aktuell müssen die Betreiber der kDL sehr oft die Sicherheit der kDL durch vielfältige zusätzliche Maßnahmen um die eingesetzten IT-Produkte herum sicherstellen, um die eigentlichen KRITIS-Anlagen „von außen“ zu schützen (Mehrfach-Firewalls, manuelle Netztrennung, paralleler Betrieb, um ganze Anlagen austauschen zu können usw.). Die Sicherheit der KRITIS-Anlagen wird heute in der Regel nicht ausreichend durch die Anlagen selber erzeugt, sondern durch aufwendige Zusatzmaßnahmen des Betreibers, die die Sicherheitsdefizite vor Ort ausgleichen. Bei der Nutzung von Clouddiensten stellt es sich erfahrungsgemäß aufwändiger dar, Sicherheitsdefizite in der Cloudumgebung und oder beim Betreiber auszugleichen.

Die Notwendigkeit von aufwendigen Zusatzmaßnahmen soll unter anderem durch *Produkte* mit höheren Sicherheitsstandards und Sicherheitsfunktionen reduziert werden.

Das Dokument zeigt auf, welche Anforderungen *Hersteller* von Produkten für Kritische Infrastrukturen erfüllen bzw. nach welchen Prinzipien *Produkte* hergestellt werden sollten, um die Betreiber in die Lage zu versetzen, ihre kritischen Dienstleistungen adäquat zu betreiben.

- Ziel 1: Die *Hersteller* werden animiert, IT- und Funktionssicherheit als einen integrativen Mehrwert und heutzutage notwendigen und selbstverständlichen Teil der Produktqualität zu sehen. Dazu gehört auch, dass die Hersteller Transparenz darüber schaffen, welchen Funktionsumfang das *Produkt* hat und welche fremden *Produkte* verwendet wurden (Software wie Hardware). Darüber hinaus ist es unumgänglich bei der Inbetriebnahme beim Kunden die Funktionalität auf die Anforderungen des Kunden einzustellen².
- Ziel 2: Die Betreiber von kDL werden in die Lage versetzt, *Produkte* gegen eine Menge von Sicherheitsanforderungen zu analysieren, zu bewerten und angemessen sicher zu betreiben.
- Ziel 3: Der Gesetzgeber wird unterstützt, über die Betreiber von kDL hinaus auch die Hersteller in der Gesetzgebung zu betrachten. *Hersteller* sollen aus Sicht der Wirtschaft vergleichbar in die Pflicht genommen werden.

² z. B. Pflichtenheft und Abnahme als gemeinsame Aufgabe

4 Herstellung eines Produktes

4.1 Security-Funktionalität im Umfeld „kDL“

Um die heute noch immer notwendige Menge von Zusatzmaßnahmen zur Absicherung der IT zu verringern, sollen neue Produkte bereits Sicherheitsfunktionen in sich tragen. In einigen Fällen sind das zwingende Anforderungen (**MUSS**).

Im Folgenden findet sich eine (unvollständige) Liste von Ansätzen:

- Sicherheitsrelevante Ereignisse in einem Produkt **MÜSSEN** für Systeme zur Angriffserkennung auswertbar sein (siehe auch § 8a, BSIG) – Stichwort SIEM, Security-Logs, Funktionslogs, Konfigurationslogs
- Bei Produkten mit multifunktionaler Ausprägung **MÜSSEN** voneinander unabhängige Funktionalitäten einzeln deaktivierbar sein (Härtung je nach Einsatzfall)
- Schnittstellen **SOLLEN** nach dem Stand der Technik zur aktiven Übermittlung von Monitoring-Daten, insbesondere für Security-Alarme, bereitgestellt werden.
- Selbstschutzfunktionen **SOLLEN** von innen gegen ungewollte Veränderung, z. B. Hashkontrolle, Signaturen oder andere und oder Angabe von „Kontrolldaten von außen“, insbesondere bei OT-Komponenten, implementiert sein.
- Eine Überprüfung auf sicherheitstechnische Eignung, Schwachstellen und Updatefähigkeit sowie ein Nachweis benutzter Software-Bibliotheken Dritter **SOLLEN** dokumentiert sein.
- Die Übernahme von Uhrzeiten aus einer externen zentralen Quelle **SOLL** über geschützte Protokolle (z. B. gemäß RFC 2030 / RFC 1305) erfolgen.
- Anstelle der bisher häufig verwendeten MAC-Adressen-Identifikation oder ähnlichen einfachen Verfahren **SOLL** in neuen Produkten die Möglichkeit von zertifikatsbasierter Identifikation möglich sein. Dabei **SOLL** die Austauschfähigkeit von Zertifikaten sichergestellt werden.

4.2 Entwicklung von Produkten

Die Entwicklung eines neuen *Produktes* durchläuft üblicherweise verschiedene Phasen – von der strategischen Planung bis zur Realisierung. In der Regel steht die angestrebte Funktionalität im Fokus der Entwicklungsarbeiten.

Das zeigt sich bei der Entwicklung vor allem durch den Fokus, dass die Soft- oder Hardware die definierten Anforderungen erfüllt und alle Funktionen fehlerfrei ausführbar sind. Die Sicherheitsaspekte und die Resilienz stehen nur sehr selten im Vordergrund und müssen sich bis heute überproportional der Wirtschaftlichkeit unterordnen. Dies erhöht die Wahrscheinlichkeit von Sicherheitslücken, die dann während des Lebenszyklus eines *Produktes* gefunden und ausgenutzt werden können. Diese müssen dann schnellstmöglich in teuren und aufwendigen Patch-Zyklen oder durch den vollständigen Austausch von Produkten (Stichwort IoT) beseitigt werden.

Deshalb besteht für die *Hersteller* von Produkten eine wesentliche Anforderung darin, neben der Funktionsfähigkeit auch die Sicherheit für die vorgesehenen Anwendungsfälle gründlich zu prüfen. Bei der Entwicklung von Produkten sollte ein *Hersteller* einsatzbezogene Business Impact- und Bedrohungsanalysen bereits beim Design berücksichtigen. Das beinhaltet auch missbräuchliche Anwendungsfälle sowie die Anwendung in schwierigen Situationen. Bereits im Entwicklungsprozess müssen entsprechende Gegenmaßnahmen bei der Spezifikation des *Produktes* berücksichtigt werden (Stichwort und Ziel: Resilienz).

Es sind die eingesetzten Secure-Coding-Practices sowie die Vorgaben zur sicheren Softwareentwicklung bei der Bereitstellung des Produktes gegenüber dem Betreiber nachzuweisen.

Im Minimum gibt es zwei Grundsätze in der Entwicklung, die IT-basierende *Produkte* berücksichtigen sollten, um den heutigen Anforderungen Genüge zu tun.

1. Security by design (SbD):

SbD soll hier nicht einfach nur als Technik verstanden werden, sondern als eine Philosophie und Maßnahme während des Entwicklungsprozesses³. Es muss bereits im Entwicklungsprozess berücksichtigt werden, wie IT-Sicherheit grundsätzlich in das *Produkt* implementiert, geprüft und gesichert werden kann. Bei möglichen und im Lebenszyklus mit statistischer Sicherheit zu erwartenden neuen Schwachstellen sollten diese überhaupt und dann mit möglichst geringem Aufwand beseitigt werden können.

Beispiel 1: In vielen Systemen findet man heute noch fest kodierte Parameter (z. B. IP-Adressen, Ports und Passwörter). Das ist nicht nur in kleinen und häufig agil entwickelten *IoT*-Lösungen oder einfachen APPs, sondern durchaus auch in ernstzunehmenden Industrielösungen, zu sehen.

→ Ergebnis: Die erkannte Schwachstelle lässt sich nicht beheben, das *Produkt* müsste komplett ausgetauscht (neu entwickelt) werden.

Beispiel 2: Eine produktinterne Kommunikation zwischen einzelnen Bausteinen wird über bestimmte TLS/SSL-Version ausgeführt. Sollte das verwendete Protokoll zu irgendeinem Zeitpunkt korumpiert werden, hat der *Hersteller* einen Mechanismus vorzusehen, den Protokollstack nachträglich gesichert auszutauschen.

→ Ergebnis: Das *Produkt* müsste nicht getauscht werden.

Beispiel 3: Anfang 2018 wurde ein Designfehler in (sehr vielen) CPUs öffentlich, über den vertrauliche Informationen ausgelesen werden können. Eine nachträgliche Designanpassung ist nicht möglich. Es kann nur mit umgebenden SW-Anteilen der Bereich so gut wie möglich abgesichert werden.

→ Ergebnis: Das (Teil-) *Produkt* muss absehbar getauscht werden oder es müssen Leistungseinbußen durch einen Workaround hingenommen werden.

2. Privacy by design (PbD):

Privacy by design ist ein eng verbundener Bestandteil von IT-Sicherheit und ist in allen Produkten zu beachten, die im Einsatz für KDL (auch) personenbezogenen Daten verarbeiten. Hier soll mittels „Datenschutz durch Technik“ sichergestellt werden, dass grundsätzlich Datenschutz und Privatsphäre bereits während der Entwicklung in das *Produkt* implementiert werden können.

Hierzu sind 7 Grundprinzipien beschrieben:

- Proaktiv, nicht reaktiv; als Vorbeugung und nicht als Abhilfe.
Wurden die Daten einmal öffentlich, ist es zu spät. Der *Hersteller* muss Ereignisse voraussehen, die in die Privatsphäre vordringen können, um diese zu verhindern, bevor sie geschehen können.
- Datenschutz als Standardeinstellung („Privacy by Default“).
Einzelpersonen sind nicht gefordert, selbst etwas für den Schutz ihrer Privatsphäre zu unternehmen – Der *Hersteller* hat den Schutz bereits systemimmanent als Standardeinstellung vorzunehmen (z. B. personenbezogene Daten nur durch Einwilligung per Opt-In an Dritte).
- Der Datenschutz ist in das Design eingebettet.
Alles, was für den Datenschutz nötig ist, hat der *Hersteller* im Design, die Architektur der IT-Systeme und die Geschäftsprozesse zu integrieren.
- Sowohl volle Funktionalität als auch volle Datensicherheit.
Der *Hersteller* kommt allen berechtigten Interessen und Zielen entgegen. Die Vortäuschung falscher, künstlich erzeugter Gegensätze wie Datenschutz versus Sicherheit wird vermieden.

³ Ein mögliches Vorbild für das „Security by Design“-Prinzip ist ein großer SW-*Hersteller*. Dieser *Hersteller* entschloss sich 2002 als Reaktion auf die stark ansteigende Zahl von Sicherheitslücken, den Entwicklungsprozess vollständig zu ändern und mit einem 14-stufigen Security-Prozess zu unterlegen, der seitdem stringent eingehalten wird.

-
- Durchgängige Sicherheit – Schutz während des gesamten Lebenszyklus.
Der *Hersteller* muss Privacy by Design bereits vor der Ersterfassung der Information im System sicherstellen und wirkt damit auf den gesamten Lebenszyklus der Daten bis ans Ende.
 - Sichtbarkeit und Transparenz – für Offenheit sorgen.
Der *Hersteller* muss durch unabhängige Prüfungen gewährleisten, dass im System unabhängig von Geschäftsprozessen oder Technologien die angekündigten Maßnahmen erfolgreich implementiert sind.
 - Für eine nutzerzentrierte Gestaltung sorgen.
Vor allem von den System-Architekten und Betreibern (von IT-Systemen) wird gefordert, dass für sie die Interessen der Nutzer an erster Stelle stehen. Sie sorgen für eine nutzerzentrierte Gestaltung.

Ergebnis: *Produkte*, die *Privacy by design* berücksichtigen, besitzen grundsätzlich einen Wettbewerbsvorteil gegenüber sonst gleichwertigen Produkten.

Für den Betreiber einer Kritischen Infrastruktur, der ein *Produkt* im Umfeld der kDL zu nutzen plant, sollten diese Analysen, die Designprozesse und die implementierten Maßnahmen so weit wie möglich transparent gemacht werden.

Transparenz ist ein wesentlicher Faktor von IT- und Funktions-Sicherheit.

Sollten bereits im Design Restrisiken erkennbar sein, müssen diese proaktiv aufgezeigt werden. Nur dann hat der Betreiber einer kritischen Infrastruktur die Möglichkeit, entweder bei der Integration des *Produktes* in seinem Betrieb weitere Maßnahmen zu ergreifen, die diese Restrisiken weiter reduzieren oder im Idealfall vollständig kompensieren, oder ein anderes *Produkt* mit passenderen Eigenschaften einzusetzen.

Weiterführende Anforderungen an Test von Komponenten und Maßnahmen findet man in [4].

4.3 Produktion des Produktes

Die Spezifikation eines *Produktes* beschreibt seine Konstruktion, Fähigkeiten und Eigenschaften und ist das Ergebnis des Entwicklungsprozesses. Werden diese *Produkte* in einer kritischen Infrastruktur eingesetzt, wird eine adäquate Verlässlichkeit des Produkts und des Herstellers vorausgesetzt. Es muss transparent sein, unter welchen Voraussetzungen das *Produkt* fehlerfrei funktioniert. Der *Hersteller* muss Erkenntnisse über das Verhalten des *Produktes* außerhalb der vorgegebenen Rahmenbedingungen ermitteln und dem Betreiber gegenüber transparent machen, denn diese können aus verschiedensten Gründen verletzt werden (z. B. Umgebungstemperatur zu hoch). Je umfangreicher die Erkenntnisse über das Verhalten des Produktes außerhalb der Rahmenbedingungen dem Betreiber bekannt sind (z. B. automatische Abschaltung), desto zielgerichteter kann dieser weiteren Maßnahmen im Vorfeld ergreifen (z. B. zusätzliche Kühlung).

Aus diesem Grund ist es neben der sicheren Entwicklung⁴ von entscheidender Bedeutung, dass das *Produkt* entsprechend der Spezifikation fehlerfrei und mit resilienten Eigenschaften produziert wird. Um das zu verifizieren, muss jedes fertige Produkt immer einer Qualitätskontrolle unterzogen werden. Die dazugehörigen Abläufe sollten dem Betreiber einer Kritischen Infrastruktur in einer angemessenen Tiefe durch entsprechende Dokumentation transparent gemacht werden. Das Ergebnis der Qualitätskontrolle des ausgelieferten *Produktes* muss dokumentiert und dem Betreiber einer Kritischen Infrastruktur mit dem *Produkt* beigestellt werden.

Unabhängig davon gibt es einen weiteren Ansatz zur Verbesserung der Sicherheit, der am Ende einer Produktion und vor der Auslieferung eines Produktes zum Tragen kommen sollte.

⁴ Vergleiche zum Beispiel ISO 26262

1. Security by default:

Unter diesem Punkt wird die Voreinstellung der Parameter und Variablen eines *Produktes* ab Werk (Werksvoreinstellungen) verstanden, die ohne Zutun eines potentiellen Käufers/Betreibers bereits zur Auslieferung vorliegen. Diese sollen so gesetzt sein, dass alle Prinzipien der IT-Sicherheit soweit wie möglich berücksichtigt werden. Den Werkseinstellungen soll die maximale Sicherheit und nicht die maximale Bedienbarkeit zu Grunde liegen.

Beispiel 1: Ein voreingestelltes Masterpasswort wird deutlich kommuniziert und eine Funktion im *Produkt* erzwingt eine Änderung des Masterpasswortes bei Inbetriebnahme sofort oder spätestens nach einer angemessenen Zeit x.

Beispiel 2: Nicht benötigte bzw. genutzte Netzwerk-Protokolle sind in den Werkseinstellungen deaktiviert (z. B. Fernzugriff per SSH).

2. Privacy by default:

Ebenso wie unter Security by default wird auch hier die Werksvoreinstellung der möglichen Parameter und Variablen erwartet, die dem Ziel des „Datenschutz durch datenschutzfreundliche Voreinstellungen“ Rechnung trägt.

Ziel dieser Maßnahmen ist es, ab Beginn einer Nutzung eines *Produktes* einen „sicheren“ Zustand zu haben, der nur durch bewusstes Handeln verändert wird.

Die weiterführenden Anforderungen an Test von Komponenten und Maßnahmen aus [4] finden auch in diesem Schritt sinnvoll Anwendung.

4.4 Vertrieb des Produktes

Die Erfüllung der in 4.1 und 4.3 genannten Anforderungen sollte, soweit machbar, dem potenziellen Käufer (Betreiber einer Kritischen Infrastruktur) schon in der Angebotsphase durch eine angemessene Dokumentation transparent gemacht werden, damit er bereits in dieser Phase ggf. notwendige weitere Maßnahmen in seiner Kalkulation berücksichtigen kann.

Produkte die vom *Hersteller* für den Einsatz in einer Anlage gem. BSI-KritisV vorgesehen sind, sollten vom *Hersteller* mit einem entsprechenden Gütesiegel versehen werden. Im Minimum soll eine Selbsterklärung im Sinn der nachfolgend beschriebenen Anforderung an die Transparenz zu IT-Sicherheits-Aspekten zur Verfügung gestellt werden.

4.5 Transparenz

Im Folgenden eine mögliche, hier bewusst unvollständige, Checkliste mit Informationen, die ein *Hersteller* einem Betreiber zusätzlich zu den im ProdSG und anderen Normen genannten Anforderungen zur Verfügung stellen sollte:

- Verschlüsselte Kommunikation im *Produkt* zwischen den einzelnen Teilen/Bausteinen inklusive Benennung der Endpunkte der Verschlüsselung
- Eingesetzte Verschlüsselungstechnologien nach Stand der Technik
- Updatemöglichkeiten für das *Produkt* inklusive Updateprozess
- Verhalten des *Produkts* außerhalb der definierten Betriebsumgebung (z. B. Sicherheitsabschaltung, Warnmeldung an Betreiber, ... bis hin zur erwarteten Zerstörung)
- Schnittstellen des *Produkts* und Kommunikation mit anderen Produkten (Anbindung an ein Internet/Intranet, verwendete Protokolle/Ports, ...)

-
- Falls sicherheitsrelevante Cloudverbindungen eingerichtet sind, Information darüber, zu welchem RZ, in welchen Ländern das geschieht
 - Kontrolle und oder Prüfung des Clouddienstleisters am C5-Katalog des BSI
 - Art der Zugriffskontrollen und der Protokolle
 - Supportkonzept und -dauer: Sicherstellung durch den *Hersteller*, dass sein *Produkt* auch nach dem Verkauf weiterhin beobachtet wird, automatische Sicherheitsupdates erhält und im Bezug zur Cybersicherheit geprüft wird.
 - Ergebnisse und Liste der durchgeführten Penetrationstests
 - Mögliche Liste von technisch-organisatorischen Maßnahmen (TOMs) zum Schutz des *Produktes*, im Entwicklungs-, Herstellungs- und Verkaufsprozess:
 - Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle),
 - Verhinderung des unbefugten Lesens, Kopierens, Veränderns, Löschsens oder Entfernens von Datenträgern (Datenträgerkontrolle),
 - Verhinderung der unbefugten Eingabe von ... Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten ... Daten (Speicherkontrolle),
 - Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle),
 - Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten ... Daten Zugang haben (Zugriffskontrolle),
 - Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen ... Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle),
 - Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche ... Daten zu welcher Zeit und von wem ... eingegeben oder verändert worden sind (Eingabekontrolle),
 - Gewährleistung, dass bei der Übermittlung von Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle),
 - Gewährleistung, dass eingesetzte Systeme im Störfall wiederhergestellt werden können (Wiederherstellbarkeit),
 - Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit),
 - Gewährleistung, dass gespeicherte ... Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität),
 - Gewährleistung, dass ... Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle)
 - Dokumentation der Wertschöpfungs- und Lieferkette (Stichwort Supplychain)

5 Bereitstellung des Produktes

5.1 Übergabe und Inbetriebnahme des Produktes

Aus dem Einsatz eines *Produktes* für die Bereitstellung kritischer Dienstleistungen ergeben sich besondere Anforderungen an das *Produkt* an sich, den Umgang mit und die Nutzung des *Produktes*.

Abhängig von den vertraglichen Vereinbarungen ist eine Übergabe und Begleitung der Inbetriebnahme in der Art und Weise durch den *Hersteller* anzubieten, dass das *Produkt* möglichst störungsfrei in den Bereitstellungsprozess der kritischen Dienstleistung aufgenommen werden kann. Dabei ist klar, dass Unterbrechungen bei der Inbetriebnahme nicht immer auszuschließen sind. Vielmehr soll gewährleistet werden, dass das Produkt seinen Betrieb möglichst störungsfrei aufnimmt. Da nicht immer alle Störungsmöglichkeiten bei der Inbetriebnahme im Vorfeld abschätzbar sind, muss der *Hersteller* die Inbetriebnahme so lange unterstützen, bis diese mit vollumfänglicher Funktion des *Produktes* abgeschlossen ist und die kritische Dienstleistung bereitgestellt und funktionsüberprüft ist. Betreiber sollen ein risikobasiertes Change-Management bei der Ausschreibung der Beschaffung vorsehen, dass bei Eintreten von größeren Risiken den Rückbau auf eine stabile Version vorsieht.

5.2 Servicelevel während des Betriebs

Während des Betriebes muss die Verantwortlichkeit für die Wartung des *Produktes* eindeutig geklärt sein. Welche Aufgaben hier der Betreiber der Kritischen Infrastruktur und welche Aufgaben der *Hersteller* übernimmt, muss zwischen beiden Parteien vereinbart werden.

Weiterführende Details und Hinweise sind dem Dokument „Anforderungen an Lieferanten“ [1] zu entnehmen.

5.3 Supportlaufzeit und Lebensdauer

Die Mindestsupportlaufzeit eines *Produktes* muss durch den Hersteller bei Vertragsbeginn offengelegt und im Vertrag dokumentiert werden. Informationen über die erwartete Lebensdauer des Produktes und/oder wesentlicher Komponenten (Obsoleszenz) sollen vom Hersteller bereitgestellt werden.

Nur so besteht für den Betreiber einer Kritischen Infrastruktur die Möglichkeit, den Nutzungszeitraum bezüglich der Risiken zu betrachten. Eine Option für die Verlängerung der Supportlaufzeit über die Mindestlaufzeit hinaus ist vertraglich zu regeln. Die damit verbundenen wirtschaftlichen Rahmenbedingungen muss der Betreiber einer Kritischen Infrastruktur berücksichtigen (z. B. Ausschreibungen dauern länger als erwartet).

6 Incident Handling

6.1 Informations- und Meldepflichten

Der *Hersteller* muss sich verpflichten, Fehler in seinen Produkten, die Auswirkungen auf den Betrieb kritischer Infrastrukturen haben können, dem Betreiber aktiv mitzuteilen. Das kann auch über öffentlich erreichbare Plattformen (z. B. CERT-Bund, CVE u. a.) erfolgen.

Genauso muss der Betreiber dem *Hersteller* Erkenntnisse über relevante Schwachstellen und Schwächen in den eingesetzten Produkten mitteilen.

Diese können ähnlich gestaltet werden wie die Meldeverpflichtungen der Betreiber kritischer Infrastrukturen gegenüber dem BSI⁵.

Weiterführende Informationen zur Handhabung von Schwachstellen werden in [5] beschrieben.

6.2 Vertragliche Unterstützungsleistung bei Incidents

Der Betreiber einer Kritischen Infrastruktur sollte die Unterstützung durch den *Hersteller* im Falle einer Störung möglichst genau vereinbaren. Darauf basierend besteht für beide Seiten die Möglichkeit, die Risiken auch betriebswirtschaftlich zu kalkulieren.

6.3 Unterstützungsleistung bei fehlender Vereinbarung

Ein *Hersteller* muss bei Störfällen im Sinne des IT-Sicherheitsgesetzes auch bei einer ggf. fehlenden Vereinbarung mit dem Betreiber seine Unterstützungsleistung im Rahmen seiner verfügbaren Ressourcen auf Anfrage bereitstellen. Sich daraus ergebende Aufwände, die nicht vertraglich vereinbart sind, kann der *Hersteller* selbstverständlich in Rechnung stellen.

⁵ Siehe FAQ des BSI zu Meldekriterien

7 Zusammenfassung

Für den Betrieb der kritischen Dienstleistung setzen die Betreiber *Produkte und Dienstleistungen* (im Folgenden nur als *Produkte* bezeichnet) ein. In diesem Dokument beziehen sich die Autoren ausschließlich auf Produkte und Hersteller im Sinne einer Werkleistung und Werklieferung. Sowohl „klassische“ Produkte als auch aus Einzelprodukten zusammengefügte Lösungen unterliegen den beschriebenen Anforderungen und Empfehlungen. Hersteller sind dabei Erzeuger von Geräten und Systemen sowie Produzenten einer funktionsfertigen Lösung im Sinne des Werkrechts.

Plattformen wie Cloud (IaaS, PaaS) und Hosting werden in diesem Dokument nicht weiter als Funktionalität für die KDL betrachtet. Diese werden im Dokument „Anforderungen an Lieferanten“ [1] behandelt.

Dieses Dokument ist zur Orientierung gedacht, die in B3S und weiteren Dokumenten und Regelungen beim Betreiber der Kritischen Dienstleistungen konkretisiert werden müssen

Autorengruppe im TAK Lieferanten/Hersteller

Christian Behre

Christian Daniel

Daniel Fengler

Sven Greven

Andreas Jünger – Sprecher

Christian Sachgau – Leiter

Patrick Schlüter

Lars Schmidt

Philipp Töbich

Thomas Wienand

8 Definitionen und Abkürzungen

<i>Abkürzung</i>	<i>Erläuterung</i>
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz
BSI-KritisV	BSI-Kritisverordnung
C5	Cloud Computing Compliance Control Catalogue (BSI)
CE	EU-Verordnung 765/2008
Hersteller	<i>Hersteller</i> im Sinne dieses Dokumentes sind <i>Hersteller</i> , Lieferanten, Integratoren und Dienstleister, von denen <i>Produkte</i> in einer Anlage eingesetzt werden, die zum Betrieb von kritischen Dienstleistungen benötigt wird. Im Dokument wird der Begriff <i>Hersteller</i> synonym für alle Kategorien verwendet.
ICS	Industrial Control Systems (Industrielle Steuerungssysteme, Automatisierungssysteme)
IoT	Internet of Things
IT-SiG	IT-Sicherheitsgesetz
kDL	kritische Dienstleistung
KRITIS	Kritische Infrastruktur
Kritische Infrastruktur	Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.
Produkt	<i>Produkte</i> im Sinne dieses Dokumentes sind IT-basierende <i>Produkte</i> , Systeme und Dienstleistungen, die in oder für eine einer Anlage eingesetzt werden, die zum Betrieb von kritischen Dienstleistungen benötigt wird.
Software	Mit Software ist in diesem Dokument Soft- und Firmware gemeint.

9 Literatur⁶

- [1] Best-Practice-Empfehlungen für Anforderungen an Lieferanten zur Gewährleistung der Informationssicherheit in Kritischen Infrastrukturen, UP KRITIS
<https://www.bsi.bund.de/dok/upk-anforderungen-lieferanten>
- [2] Anforderungen an netzwerkfähige Industriekomponenten, BSI
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_067.html
- [3] Sicherheitsspezifische Empfehlungen für Maschinenbauer und Integratoren, BSI
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_106.pdf?__blob=publicationFile&v=1
- [4] ICS-Security-Kompendium für Hersteller und Integratoren, BSI
<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.html>
- [5] Handhabung von Schwachstellen – Empfehlungen für Hersteller, BSI
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_019.pdf?__blob=publicationFile&v=1

Der UP KRITIS stellt sektorübergreifende Publikationen hier zur Verfügung:

<https://www.bsi.bund.de/dok/upk-publikationen>

⁶ Stand der angegebenen Links: Oktober 2022