Bundesamt
für Sicherheit in der
Informationstechnik

CON: Konzepte und Vorgehensweisen

CON.9: Informationsaustausch

1 Beschreibung

1.1 Einleitung

Informationen werden zwischen Sender und Empfänger über unterschiedliche Kommunikationswege übertragen, wie z .B. persönliche Gespräche, Telefonate, Briefpost, Wechseldatenträger oder Datennetze. Regeln zum Informationsaustausch stellen sicher, dass vertrauliche Informationen nur an berechtigte Personen weitergegeben werden. Solche Regelungen sind besonders dann notwendig, wenn Informationen über externe Datennetze übermittelt werden.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, den Informationsaustausch zwischen verschiedenen Kommunikationspartnern abzusichern. Mithilfe dieses Bausteins lässt sich ein Konzept zum sicheren Informationsaustausch erstellen.

1.3 Abgrenzung und Modellierung

Der Baustein CON.9 *Informationsaustausch* ist einmal auf den gesamten Informationsverbund anzuwenden, wenn Informationen mit Kommunikationspartnern, die nicht dem Informationsverbund angehören, ausgetauscht werden sollen.

Die Absicherung von Netzverbindungen wird in anderen Bausteinen des IT-Grundschutz-Kompendiums behandelt, siehe Schicht NET *Netze und Kommunikation.* Anforderungen an Wechseldatenträger (siehe Baustein SYS.4.5 *Wechseldatenträger*) und die Weiterverarbeitung in IT-Systemen außerhalb des Informationsverbunds werden ebenfalls nicht in diesem Baustein berücksichtigt.

2 Gefährdungslage

Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein CON.9 *Informationsaustausch* von besonderer Bedeutung.

2.1 Nicht fristgerecht verfügbare Informationen

Der Informationsaustausch kann gestört, verzögert oder unterbrochen werden.

Informationen treffen verzögert oder nicht vollständig ein oder werden zu langsam verarbeitet, wenn die eingesetzte Technik Übertragungsfehler erzeugt. Unter Umständen endet der Austausch von Informationen vollständig, weil Schnittstellen oder Betriebsmittel nicht leistungsfähig genug sind oder ausfallen.

Geschäftsprozesse können erheblich beeinträchtigt werden, wenn erforderliche Fristen zur Lieferung von Informationen nicht eingehalten werden. Im Extremfall werden vertraglich vereinbarte Fristen gebrochen, weil eine Datenübertragung durch technisches oder menschliches Versagen scheitert.

2.2 Ungeregelte Weitergabe von Informationen

Schutzbedürftige Informationen können in die Hände unbefugter Personen gelangen.

Es kann nicht beeinflusst werden, wer eine Information erhält und nutzt, wenn z. B. im Vorfeld eines Informationsaustauschs versäumt wurde, eine Vertraulichkeitsvereinbarung abzuschließen. Das Risiko des Datenmissbrauchs erhöht sich ebenfalls, wenn die Vertraulichkeitsvereinbarung unpräzise oder lückenhaft formuliert wurde.

2.3 Weitergabe falscher oder interner Informationen

Schutzbedürftige Informationen können an unbefugte Empfänger versendet werden.

Schutzbedürftige Informationen können versehentlich in die Hände unbefugter Empfänger gelangen, wenn Mitarbeiter nicht ausreichend sensibilisiert und geschult sind. So werden z. B. Datenträger weitergegeben, auf denen sich Restinformationen wie unzureichend gelöschte Alt-Daten befinden. Andere Restinformationen sind ungelöschte interne Kommentare, die versehentlich in einem elektronischen Dokument, z. B. als E-Mail-Anhang, an einen externen Empfänger übermittelt werden. In weiteren Fällen werden z. B. vertrauliche Unterlagen versehentlich an den falschen Empfänger verschickt, weil klare Handlungsvorgaben für den Umgang mit vertraulichen Unterlagen fehlen.

2.4 Unberechtigtes Kopieren oder Verändern von Informationen

Informationen und Daten können unbemerkt durch Angreifer abgegriffen oder beeinflusst werden.

Angreifer können Informationen vorsätzlich stehlen, wenn sie nicht ausreichend geschützt werden. So kann ein Angreifer z. B. Datenträger auf dem Postweg abfangen oder unbemerkt den Inhalt ungeschützt versendeter E-Mails lesen. Außerdem kann ein Angreifer ungeschützte Informationen verändern, während sie übertragen werden und so beispielsweise Schadsoftware in Dateien einspielen.

2.5 Unzulängliche Anwendung von Verschlüsselungsverfahren

Der Schutz von Informationen während der Übertragung mithilfe kryptographischer Verfahren kann von Angreifern unterlaufen werden.

Ein Angreifer, der das kryptographische Verfahren kennt, kann die verschlüsselten Daten und den zugehörigen Schlüssel abfangen, wenn Mitarbeiter die Verschlüsselungsverfahren nicht sachgerecht anwenden. Mitarbeiter, die nicht ausreichend geschult wurden, könnten z. B. den Schlüssel gemeinsam mit den Daten auf demselben Datenträger verschicken. Darüber hinaus werden beispielsweise oft Schlüssel verwendet, die zu leicht zu erraten sind.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.9 *Informationsaustausch* aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte (ISB) für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**

Grundsätzlich zuständig	Informationssicherheitsbeauftragter (ISB)
Weitere Zuständigkeiten	Fachverantwortliche, Benutzer, Zentrale Verwaltung

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein CON.9 *Informationsaustausch* vorrangig erfüllt werden:

CON.9.A1 Festlegung zulässiger Empfänger [Zentrale Verwaltung, Benutzer] (B)

Die zentrale Verwaltungsstelle MUSS sicherstellen, dass durch die Weitergabe von Informationen nicht gegen rechtliche Rahmenbedingungen verstoßen wird.

Die zentrale Verwaltungsstelle MUSS festlegen, welche Empfänger welche Informationen erhalten und weitergeben dürfen. Es MUSS festgelegt werden, auf welchen Wegen die jeweiligen Informationen ausgetauscht werden dürfen. Jeder Mitarbeiter MUSS vor dem Austausch von Informationen sicherstellen, dass der Empfänger die notwendigen Berechtigungen für den Erhalt und die Weiterverarbeitung der Informationen besitzt.

CON.9.A2 Regelung des Informationsaustausches [Zentrale Verwaltung, Benutzer] (B)

Bevor Informationen ausgetauscht werden, MUSS der Informationseigentümer festlegen, wie schutzbedürftig die Informationen sind. Der Informationseigentümer MUSS festlegen, wie die Informationen bei der Übertragung zu schützen sind.

Falls schutzbedürftige Daten übermittelt werden, MUSS der Informationseigentümer den Empfänger darüber informieren, wie schutzbedürftig die Informationen sind. Falls die Informationen schutzbedürftig sind, MUSS der Informationseigentümer den Empfänger außerdem darauf hinweisen, dass dieser die Daten ausschließlich zu dem Zweck nutzen darf, zu dem sie übermittelt wurden.

CON.9.A3 Unterweisung des Personals zum Informationsaustausch [Fachverantwortliche] (B)

Der Fachverantwortliche MUSS alle Mitarbeiter über die Rahmenbedingungen jedes Informationsaustauschs informieren. Der Fachverantwortliche MUSS sicherstellen, dass die Mitarbeiter wissen, welche Informationen sie wann, wo und wie weitergeben dürfen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein CON.9 *Informationsaustausch*. Sie SOLLTEN grundsätzlich erfüllt werden.

CON.9.A4 Vereinbarungen zum Informationsaustausch mit Externen [Zentrale Verwaltung] (S)

Bei einem regelmäßigen Informationsaustausch mit anderen Institutionen SOLLTE die Institution Rahmenbedingungen für den Informationsaustausch formal vereinbaren. Die Vereinbarung für den Informationsaustausch SOLLTE Angaben zum Schutz aller vertraulichen Informationen enthalten.

CON.9.A5 Beseitigung von Restinformationen vor Weitergabe [Benutzer] (S)

Zusätzlich zu den allgemeinen Schulungsmaßnahmen SOLLTE die Institution die Benutzer über die Gefahren von Rest- und Zusatzinformationen in Dokumenten und Dateien informieren. Den Benutzern SOLLTE vermittelt werden, wie sie Rest- und Zusatzinformationen in Dokumenten und Dateien vermeiden können.

Die Institution SOLLTE jeden Benutzer anleiten, wie unerwünschte Restinformationen vom Austausch auszuschließen, sind.

Die Benutzer SOLLTEN jede Datei und jedes Dokument vor der Weitergabe auf unerwünschte

Restinformationen überprüfen. Die Benutzer SOLLTEN unerwünschte Restinformationen aus Dokumenten und Dateien entfernen.

CON.9.A6 Kompatibilitätsprüfung des Sender- und Empfängersystems (S)

Vor einem Informationsaustausch SOLLTE überprüfen werden, ob die eingesetzten IT-Systeme und Produkte auf Sender- und Empfängerseite kompatibel sind.

CON.9.A7 Sicherungskopie der übermittelten Daten [Benutzer] (S)

Die Benutzer SOLLTEN eine Sicherungskopie der übermittelten Informationen anfertigen, falls die Informationen nicht aus anderen Quellen wiederhergestellt werden können.

CON.9.A8 Verschlüsselung und digitale Signatur (S)

Die Institution SOLLTE prüfen, ob Informationen während des Austausches kryptografisch gesichert werden können. Falls die Informationen kryptografisch gesichert werden, SOLLTEN dafür ausreichend sichere Verfahren eingesetzt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein CON.9 *Informationsaustausch* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

CON.9.A9 Vertraulichkeitsvereinbarungen [Zentrale Verwaltung, Benutzer] (H)

Bevor vertrauliche Informationen an Externe weitergeben werden, SOLLTE der Benutzer die zentrale Verwaltung informieren. Die zentrale Verwaltung SOLLTE eine Vertraulichkeitsvereinbarung mit den Empfängern abschließen. Die Vertraulichkeitsvereinbarung SOLLTE regeln, wie die Informationen auf der Empfängerseite aufbewahrt werden dürfen. In der Vertraulichkeitsvereinbarung SOLLTE festgelegt werden, wer auf der Empfängerseite Zugriff auf welche übermittelten Informationen haben darf.

4 Weiterführende Informationen

4.1 Wissenswertes

Die International Organization for Standardization (ISO) beschreibt in ihrem Standard *ISO/IEC 27001:2013*, Kap. 13.2 Anforderungen an den Austausch von Informationen.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein CON.9 *Informationsaustausch* von Bedeutung.

G 0.14 Ausspähen von Informationen (Spionage)

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.22 Manipulation von Informationen

G 0.25 Ausfall von Geräten oder Systemen

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.45 Datenverlust