Bundesamt
für Sicherheit in der
Informationstechnik

CON.9 Informationsaustausch

1. Beschreibung

1.1. Einleitung

Informationen werden zwischen Sendenden und Empfangenden 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

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. 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 Empfangende versendet werden.

Schutzbedürftige Informationen können versehentlich in falsche Hände gelangen, falls das Personal nicht ausreichend sensibilisiert und geschult wird. So werden können z. B. Datenträger weitergegeben werden, 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, übermittelt werden. In weiteren Fällen werden z. B. vertrauliche Unterlagen versehentlich an die falsche Person 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 Angriffe abgegriffen oder beeinflusst werden.

Bei Angriffen können Informationen vorsätzlich gestohlen werden, wenn sie nicht ausreichend geschützt werden. So kann bei einem Angriff z. B. ein Datenträger auf dem Postweg abfangen oder unbemerkt der Inhalt einer ungeschützt versendeter E-Mails gelesen werden. Außerdem können bei Angriffen ungeschützte Informationen verändert werden, während sie übertragen werden und so beispielsweise Schadsoftware in Dateien eingespielt werden.

2.5. Unzulängliche Anwendung von Verschlüsselungsverfahren

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

Falls das kryptographische Verfahren bei einem Angriff bekannt ist, können die verschlüsselten Daten und der zugehörige Schlüssel abfangen werden, wenn die Verschlüsselungsverfahren nicht sachgerecht anwendet werden. Mitarbeitende, 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. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Informationssicherheitsbeauftragte (ISB)
Weitere Zuständigkeiten	Fachverantwortliche, Benutzende, Zentrale Verwaltung

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

CON.9.A1 Festlegung zulässiger Empfangender (B) [Zentrale Verwaltung]

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

Die zentrale Verwaltungsstelle MUSS festlegen, wer welche Informationen erhalten und weitergeben darf. Es MUSS festgelegt werden, auf welchen Wegen die jeweiligen Informationen ausgetauscht werden dürfen. Alle Beteiligten MÜSSEN vor dem Austausch von Informationen sicherstellen, dass die empfangende Stelle die notwendigen Berechtigungen für den Erhalt und die Weiterverarbeitung der Informationen besitzt.

CON.9.A2 Regelung des Informationsaustausches (B)

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

Falls schutzbedürftige Daten übermittelt werden, MUSS die Institution die Empfangenden darüber informieren, wie schutzbedürftig die Informationen sind. Falls die Informationen schutzbedürftig sind, MUSS die Institution die Empfangenden darauf hingewiesen werden, dass diese die Daten ausschließlich zu dem Zweck nutzen dürfen, zu dem sie übermittelt wurden.

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

Fachverantwortliche MÜSSEN die Mitarbeitenden über die Rahmenbedingungen jedes Informationsaustauschs informieren. Die Fachverantwortlichen MÜSSEN sicherstellen, dass die Mitarbeitenden 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 diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

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

Bei einem regelmäßigen Informationsaustausch mit anderen Institutionen SOLLTE die Institution die 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 (S) [Benutzende]

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

Die Institution SOLLTE Anleitungen bereitstellen, die vorgeben wie unerwünschte Restinformationen vom Austausch auszuschließen sind.

Jede Datei und jedes Dokument SOLLTE vor der Weitergabe auf unerwünschte Restinformationen überprüft werden. Unerwünschte Restinformationen SOLLTEN vor der Weitergabe aus Dokumenten und Dateien entfernt werden.

CON.9.A6 Kompatibilitätsprüfung des Sende- und Empfangssystems (S)

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

CON.9.A7 Sicherungskopie der übermittelten Daten (S)

Die Institution SOLLTE 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 diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

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

Bevor vertrauliche Informationen an andere Institutionen weitergeben werden, SOLLTE die zentrale Verwaltung informiert werden. Die zentrale Verwaltung SOLLTE eine Vertraulichkeitsvereinbarung mit der empfangenden Institution abschließen. Die Vertraulichkeitsvereinbarung SOLLTE regeln, wie die Informationen durch die empfangende Institution aufbewahrt werden dürfen. In der Vertraulichkeitsvereinbarung SOLLTE festgelegt werden, wer bei der empfangenden Institution 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.