Informationssicherheit

Inhaltsverzeichnis

Inhaltsverzeichnis 1
§ 1 Begriffsbestimmung 1
§ 2 Verantwortlichkeiten 2
§ 3 Bezug zum Geheimschutz 2
§ 4 Pflichten Auftragnehmer 3
Anlage 1 „Informationssicherheit Meldung - Vorkommnis“ 4

§ 1
Begriffsbestimmung

1.1 Als **Informationssicherheit (InfoSichh)** im Sinne dieser Anlage bezeichnet man die Eigenschaft informationsverarbeitender und / oder -übertragender Informationstechnik (IT) und ihres Einsatzumfeldes, welche die Grundwerte der InfoSichh (siehe 1.2) sowie die weiteren Gewährleistungsziele (siehe 1.3) in dem geforderten Maß gewährleistet.

Der Begriff der InfoSichh entspricht dem der IT-Sicherheit und wird inhaltlich von Aspekten der Computersicherheit, Datensicherheit, Cyber Defence, Cyber-Sicherheit sowie den IT-relevanten Anteilen des Datenschutzes und der Militärischen Sicherheit bestimmt.

Der Begriff InfoSichh bezieht sich hierbei nicht ausschließlich auf IT, sondern auf alle Bereiche informationsverarbeitender Systeme wie auch operative Technologies (OT), Cloud-Dienste und Internet of Things (IoT).

1.2 Die drei **Grundwerte der InfoSichh** sind:

- **Vertraulichkeit** – Schutz vor unbefugter Informationsgewinnung / -beschaffung,
- **Verfügbarkeit** – Aufrechterhaltung der zugesicherten Nutzbarkeit von Informationen, IT-Diensten und -Funktionen sowie
- **Integrität** – Schutz vor unbefugten und unzulässigen Veränderungen von Informationen, IT-Diensten und Eigenschaften von IT sowie Nachweisbarkeit und Beweisbarkeit von IT-gestützten Aktionen.

1.3 Im Rahmen der InfoSichh sind – neben den oben definierten Grundwerten – zusätzlich mindestens die folgenden aus dem Datenschutz übertragenen **Gewährleistungsziele** zu betrachten.

- **Nichtverkettung** – Anforderung, dass Informationen nur für den Zweck verarbeitet und ausgewertet werden können, für den sie erhoben wurden und dass eine Verarbeitung nach Zwecken getrennt möglich ist.
- **Transparenz** – Anforderung, dass in einem unterschiedlichen Maße sowohl Nutzer als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt.

– **Intervenierbarkeit** – Anforderung, dass den Betroffenen in der Informationstechnik die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt werden können und die verarbeitende Stelle verpflichtet ist, die entsprechenden Maßnahmen umzusetzen. Dazu müssen die für die Verarbeitungsprozesse verantwortlichen Stellen jederzeit in der Lage sein, in die Datenverarbeitung vom Erheben bis zum Löschen der Daten einzugreifen.

§ 2
Verantwortlichkeiten

2.1 Die **Gesamtverantwortung** zur Sicherstellung der InfoSichh in den Verfahren des organbeliehenen Bundesbaus verbleibt beim Bauherrn. Bei Baumaßnahmen auf Liegenschaften der Bundeswehr liegt sie immer bei der Bundeswehr. Um die InfoSichh auch in den IT-Systemen der Auftragnehmer (AN) sicherzustellen, sind diesen besondere Pflichten aufzutragen.

2.2 Die Bauverwaltung übernimmt als Auftraggeber (AG) verantwortlich die Sicherstellung der InfoSichh in allen ihr übertragenen Aufgaben im Rahmen des Bundesbaus. Dies beinhaltet die Sicherstellung der InfoSichh in der von ihr selbst genutzten IT sowie die entsprechende Verpflichtung ihrer AN.

2.3 Der AN übernimmt verantwortlich die Sicherstellung der InfoSichh in allen an ihn beauftragten Leistungen. Der AN stellt sicher, dass geeignete personelle, technische und organisatorische Maßnahmen ergriffen werden, um im Rahmen der Auftragserfüllung die Risiken für die Sicherheit von Daten und Informationssystemen zu bewältigen und Informationssicherheitsvorkommnissen (InfoSichhVork) vorzubeugen. Ein InfoSichhVork liegt vor, wenn mindestens einer der Grundwerte gemäß. Nr. 1.2 gefährdet ist. Die Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheits- und Schutzniveau der Systeme gewährleisten, welches dem jeweils bestehenden Risiko angemessen ist. Grundsätzlich ist hierbei der jeweils aktuelle IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) maßgeblich.

Der AN stellt eigenverantwortlich sicher, dass die InfoSichh auch bei ggf. im Zuge der Unterbeauftragung oder konsortialen Zusammenarbeit hinzugezogenen weiteren AN eingehalten wird.

§ 3
Bezug zum Geheimschutz

3.1 Sämtliche zur Auftragserledigung überlassenen Unterlagen sind mit der notwendigen und angemessenen Sorgfalt zu handhaben. In diesem Zusammenhang ist immer sicherzustellen, dass ausschließlich berechtigte Personen Zugriff auf die Daten erhalten und dies nur, wenn es zur Auftragserfüllung erforderlich ist (Prinzip: Kenntnis nur wenn nötig).

3.2 Beim Umgang mit Verschlusssachen (VS) sind die Pflichten und Maßgaben des Geheimschutzhandbuchs des Bundesministeriums für Wirtschaft und Energie (BMWE) sowie der RiSBau zwingend einzuhalten. Für VS – Nur für den Dienstgebrauch (VS-NfD) gilt dies insbesondere für die Anlage 4 (VS-NfD Merkblatt) des Geheimschutzhandbuchs. Anforderungen zur elektronischen Verarbeitung von VS-NfD regelt insbesondere Teil 3 des VS-NfD-Merkblatts. Hierzu gehört das Herstellen und Einhalten der zugehörigen InfoSichh inkl. der Selbstakkreditierung des AN.

3.3 IT, die zur Verarbeitung von nicht öffentlichen, auftragsbezogenen Daten eingesetzt wird, in Fällen in denen das Geheimschutzhandbuch nicht gilt (kein Umgang mit VS), muss zumindest die Mindeststandards des BSI nach § 44 Abs. 1 Satz 1 BSIG (Link) sinngemäß erfüllen, bei Cloud-basierten Software-Diensten insbesondere den Mindeststandard BSI - Externe Cloud-Dienste. In einer InfoSichh-Umsetzungsbestätigung (Formular „VI.23 „Informationssicherheits-Umsetzungsbestätigung in Bauaufgaben“ zu dieser Anlage) erklärt der AN die Umsetzung dieser IT-Anforderungen. Die InfoSichh-Umsetzungsbestätigung ist dem AG bereits bei Vertragsschluss und folgend mindestens alle drei Jahre vorzulegen sowie auf Verlangen des AG zu aktualisieren. Falls eine Selbstakkreditierung nach VS-NfD-Merkblatt vorliegt, ersetzt diese die InfoSichh-Umsetzungsbestätigung.

§ 4
Pflichten Auftragnehmer

4.1 Auskunfts- und Zusammenarbeitspflicht

Der AN ist gegenüber dem Bauherrn sowie bei Bauaufgaben auf Liegenschaften der Bundeswehr gegenüber der Bundeswehr, hier vertreten insbesondere durch Angehörige des BAMAD sowie die jeweils zuständigen Beauftragten für militärische Sicherheit, Informationssicherheit oder Datenschutz, hinsichtlich aller Belange des Geheimschutzes, Datenschutzes und der InfoSichh uneingeschränkt auskunftspflichtig.

Im Falle eines InfoSichhVork, also der Gefährdung der Grundwerte der InfoSichh (vgl. 1.2), bspw. bei einem Cyber-Angriff beinhaltet die Auskunftspflicht insbesondere Angaben zum Hergang, zum eigenen Vorgehen, dem technischen Hintergrund und Angaben zur Beteiligung von bzw. Auswirkung auf weitere öffentliche Stellen sowie die Weitergabe IT-forensischer Erkenntnisse.

Der AN ist verpflichtet mit den Mitarbeitenden des AG sowie den genannten Stellen der Bundeswehr zusammenzuarbeiten, um jegliche Nachteile und/oder Schäden für die Bundeswehr oder die Sicherheit der Bundesrepublik Deutschland zu verhindern oder zu begrenzen, zum Beispiel durch Umsetzung vorgeschlagener Mitigationsmaßnahmen oder weitere Informationsbereitstellung.

4.2 Meldepflicht bei Bauaufgaben auf Liegenschaften der Bundeswehr

InfoSichhVork wie bspw. Cyber-Angriffe auf oder Datenabflüsse von durch den AN genutzten IT-Systemen oder Mitarbeitern sind durch den AN bei Feststellung des Vorfalls unter Verwendung des zugehörigen Formulars „Meldung Informationssicherheitsvorkommnis / Sicherheitsvorkommnis in Bauaufgaben“ unverzüglich und ohne schuldhaftes Zögern mit entsprechender Beschreibung und unter Angabe eines eigenen, erreichbaren Ansprechpartners vom AN an den AG sowie nachrichtlich an die zentrale Meldestelle beim Chief Security Officer Bundeswehr (CSO Bw) (CSOBwIncidents@bundeswehr.org) und den Chief Information Security Officer Infrastruktur (CISO Infra) (CISOInfra@bundeswehr.org) zu melden. Sollten zum Zeitpunkt der Meldung noch nicht alle in dem Formular geforderten Informationen vorliegen, so ist dies in dem jeweiligen Formularfeld entsprechend zu vermerken. Fehlende Informationen sind durch Aktualisierung des Formulars unverzüglich nachzureichen, wenn vorliegend.

Die Beschreibung des Vorfalls sollte Informationen enthalten, die es dem AG sowie der Bundeswehr ermöglichen, die Wahrscheinlichkeit und das Ausmaß des potenziellen Nachteils bzw. Schadens für Betroffene und Systeme zu bestimmen. Nachteilige bzw. schädliche Auswirkungen des Vorfalls sind durch sofortige Maßnahmen des AN zu begrenzen, welche ebenfalls in der Beschreibung zu benennen sind.

Der AN ergreift umgehend die für die unmittelbare Sicherheit der Betroffenen und Systeme notwendige Schutzvorkehrungen und geeigneten Schadensbegrenzungsmaßnahmen einschließlich entsprechender Benachrichtigungen.

Unberührt bleiben sonstige Melde- und Berichtspflichten an andere inländische Behörden wie die Meldung von Datenschutzverletzungen an die Bundesbeauftragte/ den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI), Meldepflichten an das BSI und Meldepflichten gemäß Geheimschutzhandbuch bzw. VS-NfD-Merkblatt. Gleiches gilt für die Zuständigkeiten anderer inländischer Behörden für schwerwiegende Betriebs- oder Sicherheitsvorfälle.

Anlage 1 „Informationssicherheit Meldung - Vorkommnis“

Meldung Informationssicherheitsvorkommnis / Sicherheitsvorkommnis in Bauaufgaben

Auftragnehmer	Bitte vollständige Anschrift und Kontakt für Rückfragen angeben.
Auftragsgegenstand	
Maximale Einstufung	
Art des Vorkommnisses	
Datum des Vorkommnisses	
Ort des Vorkommnisses	
Zuordnung der Täter („Motiv“)	bspw.: politisch, terroristisch, kriminell (bspw. finanziell) motiviert (…)
Datum dieser Meldung	

Die Meldung ist zu senden an:
auftraggebende Stelle, CSOBwIncidents@bundeswehr.org, CISOInfra@bundeswehr.org

Sachverhaltsdarstellung in eigenen Worten	
Sind Informationen abgeflossen? Wenn ja, bitte Umfang so genau wie möglich angeben.	
Sind diese Informationen oder Teile hiervon als VS-NfD oder höher eingestuft? Wenn ja, bitte Einstufung und Umfang so genau wie möglich angeben.	

Welche Informationen ligen zum Auftragsgegenstand bei Ihnen vor? Bitte Art der Informationen, Einstufung, Dateiformate und Qualität angeben (z.B. Entwurfsplanung, Ausführungsplanung etc.).	
Waren eingestufte Informationen VS-konform verschlüsselt abgelegt?	
War der zugehörige Schlüssel physisch getrennt abgelegt (z.B. USB-Stick)?	
Wurde die Polizei informiert und wurde Strafanzeige gestellt? Wenn ja, wo und unter welchem Aktenzeichen?	
Ist außer der Polizei noch jemand mit der Durchführung der IT-forensischen Ermittlungen beauftragt? Wenn ja, wer?	
Wie wurden vor Wiederherstellung der Systeme Spuren für eine IT-forensische Auswertung gesichert?	
Wie wurde vor Wiederherstellung der Systeme sichergestellt, dass von den Tätern in den Systemen keine dauerhafte Backdoor verankert wurde?	