Informationsblatt – Meldung und Erkennung von IT-sicherheits- und

Allgemein

In nahezu allen Bereichen der Bundesanstalt für Immobilienaufgaben (BImA) ist die Aufrechterhaltung der Funktionsfähigkeit in ihren Kernprozessen an eine zuverlässige und insbesondere auch sichere Informationstechnik gekoppelt. Um die *Vertraulichkeit, Integrität* und *Verfügbarkeit* der Daten sicherzustellen, sind die Erfassung und Analyse sicherheitskritischer Ereignisse (IT-Sicherheitsvorfälle) und die Initiierung sowie Umsetzung geeigneter Maßnahmen zur Vermeidung und Behebung in der BImA in einen fortwährenden, bereichsübergreifenden Sicherheitsprozess eingebunden. Dies entspricht den Vorgaben der „*IT-Sicherheitsleitlinie der Bundesanstalt für Immobilienaufgaben“* - sie bildet die Grundlage des Informationssicherheitsprozesses. In der **„***Richtlinie für Meldewege und Maßnahmen bei IT-Sicherheitsvorfällen in der Bundesanstalt für Immobilienaufgaben“* sind die entsprechenden Grundschutzanforderungen und Maßnahmen zur Behandlung von IT-Sicherheitsvorfällen festgelegt. Die Maßgaben sowohl der Sicherheitsleitlinie als auch der Richtlinie sind zu beachten.

In einigen Arbeitsbereichen der BImA ist der Umgang mit Verschlusssachen mit dem Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH Teil der täglichen Aufgabenwahrnehmung. Dienstliegenschaften bzw. Teile davon können zudem als Sicherheitsbereiche ausgewiesen bzw. kann dort der Zugang zu Verschlusssachen mit dem Geheimhaltungsgrad VS-VERTRAULICH und höher relevant sein. Verschlusssachen unterliegen dem Schutzbereich des Sicherheitsüberprüfungsgesetzes (SÜG) und der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschluss-sachenanweisung -VSA -). Daraus resultieren besondere Voraussetzungen für den Zugang zu sowie für den Umgang mit Verschlusssachen abhängig vom jeweiligen Geheimhaltungsgrad.

Weiterhin finden auch die Bestimmungen der Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes (BDSG) entsprechende Anwendung, um Betroffene davor zu schützen, dass diese beim Umgang mit ihren personenbezogenen Daten durch Dritte in ihrem grundgesetzlich geschützten Persönlichkeitsrecht nicht beeinträchtigt werden. Die zu beachtenden Regelungen und Maßnahmen, worunter auch die Meldung von Datenschutzvorfällen zählt, sind in der „*Datenschutzrichtlinie für die Bundesanstalt für Immobilienaufgaben“* ausgeführt.

Die vorgenannten Dokumente können bei der Vergabestelle angefordert werden.

Erkennung von IT-sicherheits- sowie geheimschutzrelevanten Vorfällen

Als IT-Sicherheitsvorfall wird ein unerwünschtes Ereignis bezeichnet, das Auswirkungen auf die Informationssicherheit hat und in der Folge große Schäden nach sich ziehen kann.
Ein IT-Sicherheitsvorfall ist jedes Vorkommnis, bei dem die Grundwerte der Informationssicherheit

- *Vertraulichkeit* (Schutz vor unbefugter Preisgabe),
- *Verfügbarkeit* (Schutz vor Verlust und Ausfall) oder
- *Integrität* (Schutz vor Manipulation bzw. Verfälschung)

von Daten bzw. IT-Systemen in unzulässiger Weise verletzt werden und eine Verletzung oder Gefährdung des Geheim- bzw. Sabotageschutzes und / oder des Datenschutzes vorliegt oder zu erwarten ist. Typische Folgen von IT-Sicherheits- und Geheim- bzw. Sabotageschutzvorfällen können die Ausspähung, Manipulation oder Zerstörung von Daten bzw. Verschlusssachen sein.

Sicherheitsvorfälle können durch eine Vielzahl von Ereignissen ausgelöst werden und sind Vorkommnisse,

a) die einen Verstoß gegen die geltenden Sicherheitsrichtlinien der BImA darstellen,
   Beispiele: Weitergabe von Passwörtern, Arbeiten mit fremden Benutzerkennungen, Zutritt von Unbefugten zu IT-Räumen,
b) die einen Verstoß gegen relevante gesetzliche Vorschriften oder Verwaltungsvorschriften
   (z. B. DSGVO, SÜG, VSA) darstellen,
   Beispiele: Unrechtmäßige Speicherung und Auswertung von Personendaten, ungeeigneter Umgang mit vertraulichen Informationen oder Verschlusssachen,
c) die die Sicherheit von Daten, Netzen und IT-Systemen der BImA in einer Weise beeinträchtigen, die den im IT-Sicherheitskonzept festgelegten Schutzbedarf verletzen,
   Beispiele: Fehlerhaft eingerichtete Zugriffsmöglichkeiten auf Informationen, Computerviren, Schadsoftware, unbefugtes Kopieren von Datenbeständen
d) die die vorhandenen Sicherheitsmechanismen oder Sicherheitssysteme der BImA ganz oder teilweise außer Funktion setzen,

Beispiele: längerfristiger Ausfall der unterbrechungsfreien Stromversorgung (USV), Umgehen von Firewalls oder E-Mail-Filtern, Deaktivieren von Virenscannern auf den APCs, Verlust von Zugangsschlüsseln

e) die darauf hinweisen, dass ein Vorfall nach a) bis d) versucht wurde oder bevorsteht.
Beispiele: Unerklärliches Systemverhalten, Verdächtige Einträge in Protokolldateien der Server und Firewalls

Erkennen von Datenschutzvorfällen

Eine „Verletzung des Schutzes personenbezogener Daten“ liegt in jeder Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden. Dies kann z. B. der Fall sein, wenn Hacker im Rahmen eines Cyber-Angriffs personenbezogene Daten abgreifen oder wenn Datenträger (z. B. USB-Sticks, Festplatten, Laptops) mit personenbezogenen Daten verloren gehen oder gestohlen werden.

Wie und wem kann ein Vorfall gemeldet werden?

IT-Sicherheitsvorfälle oder Schadensmeldungen von Dienstleistenden, sind der bzw. dem IT-Sicherheitsbeauftragten per E-Mail an IT-Sicherheit@bundesimmobilien.de zu melden.

Geheim- bzw. Sabotageschutzvorfälle sind umgehend und ausschließlich dem Stabsbereich Geheimschutz per E-Mail an geheimschutz@bundesimmobilien.de zu melden. Dies gilt auch bei auftretenden Fragestellungen mit geheim- und sabotageschutzfachlichem Zusammenhang.

Wird Kenntnis von einem möglichen Verdacht für einen Datenschutzvorfall erlangt, ist der IT-Servicedesk telefonisch unter 0228 37787-600 zu benachrichtigen. Zur Meldung per E-Mail verwenden Sie bitte folgende E-Mail-Adresse IT-Servicedesk@bundesimmobilien.de und die Angabe „Meldung eines Datenschutzvorfalls“ im Betreff.

Zur Bearbeitung des Vorfalls wird benötigt:

1. eine kurze Beschreibung dessen, was zu welcher Zeit an welchem Ort bemerkt wurde (was, wann, wo)
   und bei einem **IT-Sicherheitsvorfall**
2. Bezeichnung des betroffenen Systems;

3. soweit bekannt, die Angabe, ob das betroffene System zur Verarbeitung oder Speicherung personenbezogener Daten verwendet wird.

und bei einem **Datenschutzvorfall**

2. welche personenbezogenen Daten welcher Personen(-gruppe) betroffen sind
3. ggf. das Verarbeitungssystem und
4. mögliche Bedrohungsszenarien.

und bei einem **Geheimschutzvorfall**

2. welcher Geheimhaltungsgrad der Verschlusssache betroffen ist.

Was geschieht mit der Meldung?

Alle Meldungen werden vertraulich behandelt. Nur ein sehr kleiner Personenkreis hat direkten Zugriff auf die Meldungen.

Zur Abwehr akuter schwerwiegender Störungen und Gefahren können unabhängig davon temporär

1. die Anwenderinnen bzw. Anwender von der Nutzung der IT-Infrastruktur der BImA ausgeschlossen werden,
2. die Internet-Verbindung zu den betroffenen Endgeräten oder Subnetzen unterbrochen werden.

Diese Sofortmaßnahmen sind auf den Zeitraum beschränkt, in dem die Störung oder Gefahr vorliegt.

Bei einem Datenschutzvorfall obliegen der BImA Informationspflichten. U. a. sind die bzw. der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und in Abhängigkeit des Risikos die betroffenen Personen zu informieren.