DER.2.2: Vorsorge für die IT-Forensik

1 Beschreibung

1.1 Einleitung

IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Datennetzen zur Aufklärung von Sicherheitsvorfällen in IT-Systemen.

IT-Sicherheitsvorfälle forensisch zu untersuchen, ist immer dann notwendig, wenn entstandene Schäden bestimmt, Angriffe abgewehrt, zukünftige Angriffe vermieden und Angreifer identifiziert werden sollen. Ob ein IT-Sicherheitsvorfall forensisch untersucht wird, entscheidet sich, während der Vorfall behandelt wird. Eine IT-forensische Untersuchung im Sinne dieses Bausteins besteht aus den folgenden Phasen:

- Strategische Vorbereitung: In dieser Phase werden Prozesse geplant und aufgebaut, die sicherstellen, dass eine Institution IT-Sicherheitsvorfälle forensisch analysieren kann. Sie ist auch dann notwendig, wenn die Institution über keine eigenen Forensik-Experten verfügt.
- Initialisierung: Nachdem die verantwortlichen Mitarbeiter entschieden haben, einen IT-Sicherheitsvorfall forensisch zu untersuchen, werden die vorher geplanten Prozesse angestoßen. Des Weiteren wird der Untersuchungsrahmen festgelegt und es werden Erstmaßnahmen durchgeführt.
- Spurensicherung: Hier werden die zu sichernden Beweismittel ausgewählt und die Daten forensisch gesichert. Dabei wird zwischen Live-Forensik und Post-Mortem-Forensik unterschieden: Die Live-Forensik stellt sicher, dass flüchtige Daten, wie z. B. Netzverbindungen oder RAM, von einem laufenden IT-System gesichert werden. Bei der Post-Mortem-Forensik hingegen werden forensische Kopien von Datenträgern erstellt.
- Analyse: Die gesammelten Daten werden forensisch analysiert. Dabei werden die Daten sowohl für sich als auch im Gesamtzusammenhang betrachtet.
- Ergebnisdarstellung: Die relevanten Untersuchungsergebnisse werden zielgruppengerecht aufbereitet und vermittelt.

1.2 Zielsetzung

Der Baustein zeigt auf, welche Vorsorgemaßnahmen notwendig sind, um IT-forensische Untersuchungen zu ermöglichen. Dabei wird vor allem darauf eingegangen, wie die Spurensicherung vorbereitet und durchgeführt werden kann.

Führen Forensik-Dienstleister Spurensicherungen ganz oder teilweise durch, gelten die Anforderungen auch für die Dienstleister. Durch vertragliche Vereinbarungen und Prüfungen kann dabei sichergestellt werden, dass sich der Dienstleister auch daran hält.

1.3 Abgrenzung und Modellierung

Der Baustein DER.2.2 *Vorsorge für die IT-Forensik* ist für den gesamten Informationsverbund einmal anzuwenden.

Der Baustein befasst sich mit Vorsorgemaßnahmen, die grundlegend für spätere IT-forensische Untersuchungen sind.

Wie die eigentliche forensische Analyse durchgeführt wird, ist daher nicht Thema dieses Bausteins. Es werden keine Anforderungen beschrieben, die sicherstellen, dass Angriffe erkannt werden. Diese sind im Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* enthalten und werden im vorliegenden Baustein vorausgesetzt. Auch werden keine Kriterien und Prozesse erläutert, anhand derer die Verantwortlichen entscheiden können, ob ein IT-Sicherheitsvorfall forensisch untersucht werden muss oder nicht. Die Entscheidung darüber wird getroffen, während der Sicherheitsvorfall behandelt wird (siehe DER.2.1 *Behandlung von Sicherheitsvorfällen*).

Ebenso bezieht sich der Baustein nicht auf IT-forensische Untersuchungen bei Straftaten.

Letztlich geht der Baustein auch nicht darauf ein, wie sich IT-Infrastrukturen bereinigen lassen, nachdem sie angegriffen worden sind (siehe dazu DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle*). Die dort beschriebenen Tätigkeiten können jedoch durch die Ergebnisse von IT-forensischen Untersuchungen maßgeblich unterstützt werden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein DER.2.2 *Vorsorge für die IT-Forensik* von besonderer Bedeutung:

2.1 Verstoß gegen rechtliche Rahmenbedingungen

Für IT-forensische Untersuchungen werden oft alle für notwendig befundenen Daten kopiert, sichergestellt und ausgewertet. Darunter befinden sich meistens auch personenbezogene Daten von Mitarbeitern oder externen Partnern. Wird darauf z. B. unbegründet und ohne Einbeziehung des Datenschutzbeauftragten zugegriffen, verstößt die Institution gegen gesetzliche Regelungen, etwa wenn dabei die Zweckbindung missachtet wird. Auch ist es möglich, dass aus den erhobenen Daten beispielsweise abgeleitet werden kann, wie sich Mitarbeiter verhalten, oder es kann ein Bezug zu ihnen hergestellt werden. Dadurch besteht die Gefahr, dass auch gegen interne Regelungen verstoßen wird.

2.2 Verlust von Beweismitteln durch fehlerhafte oder unvollständige Beweissicherung

Werden Beweismittel falsch oder nicht schnell genug gesichert, können dadurch wichtige Daten verloren gehen, die später nicht wiederhergestellt werden können. Im ungünstigsten Fall führt das zu einer ergebnislosen forensischen Untersuchung. Mindestens ist jedoch die Beweiskraft eingeschränkt.

Die Gefahr, wichtige Beweismittel zu verlieren, steigt stark an, wenn Mitarbeiter die Werkzeuge zur Forensik fehlerhaft benutzen, Daten zu langsam sichern oder zu wenig üben. Oft gehen auch Beweismittel verloren, wenn die Verantwortlichen flüchtige Daten nicht als relevant erkennen und sichern.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins DER.2.2 *Vorsorge für die IT-Forensik* aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte (ISB) für die Erfüllung der

Anforderungen zuständig. 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 Umsetzung 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, Datenschutzbeauftragter, Institutionsleitung

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein DER.2.2 *Vorsorge für die IT-Forensik* vorrangig erfüllt werden:

DER.2.2.A1 Prüfung rechtlicher und regulatorischer Rahmenbedingungen zur Erfassung und Auswertbarkeit [Datenschutzbeauftragter, Institutionsleitung] (B)

Werden Daten für forensische Untersuchungen erfasst und ausgewertet, MÜSSEN alle rechtlichen und regulatorischen Rahmenbedingungen identifiziert und eingehalten werden (siehe ORP.5 *Compliance Management (Anforderungsmanagement)*). Auch DARF NICHT gegen interne Regelungen und Mitarbeitervereinbarungen verstoßen werden. Dazu MÜSSEN der Betriebs- oder Personalrat sowie der Datenschutzbeauftragte einbezogen werden.

DER.2.2.A2 Erstellung eines Leitfadens für Erstmaßnahmen bei einem IT-Sicherheitsvorfall (B)

Es MUSS ein Leitfaden erstellt werden, der für die eingesetzten IT-Systeme beschreibt, welche Erstmaßnahmen bei einem IT-Sicherheitsvorfall durchgeführt werden müssen, um möglichst wenig Spuren zu zerstören. Darin MUSS auch beschrieben sein, durch welche Handlungen potenzielle Spuren vernichtet werden könnten und wie sich das vermeiden lässt.

DER.2.2.A3 Vorauswahl von Forensik-Dienstleistern (B)

Verfügt eine Institution nicht über ein eigenes Forensik-Team, MÜSSEN bereits in der Vorbereitungsphase mögliche geeignete Forensik-Dienstleister identifiziert werden. Welche Forensik-Dienstleister infrage kommen, MUSS dokumentiert werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein DER.2.2 *Vorsorge für die IT-Forensik*. Sie SOLLTEN grundsätzlich erfüllt werden.

DER.2.2.A4 Festlegung von Schnittstellen zum Krisen- und Notfallmanagement (S)

Die Schnittstellen zwischen IT-forensischen Untersuchungen und dem Krisen- und Notfallmanagement SOLLTEN definiert und dokumentiert werden. Hierzu SOLLTE geregelt werden, welche Mitarbeiter für welche Aufgaben verantwortlich sind und wie mit ihnen kommuniziert werden soll. Darüber hinaus SOLLTE sichergestellt werden, dass die zuständigen Ansprechpartner stets erreichbar sind.

DER.2.2.A5 Erstellung eines Leitfadens für Beweissicherungsmaßnahmen bei IT-Sicherheitsvorfällen (S)

Es SOLLTE ein Leitfaden erstellt werden, in dem beschrieben wird, wie Beweise gesichert werden sollen. Darin SOLLTEN Vorgehensweisen, technische Werkzeuge, rechtliche Rahmenbedingungen und Dokumentationsvorgaben aufgeführt werden.

DER.2.2.A6 Schulung des Personals für die Umsetzung der forensischen Sicherung (S)

Alle verantwortlichen Mitarbeiter SOLLTEN wissen, wie sie Spuren korrekt sichern und die Werkzeuge zur Forensik richtig einsetzen. Dafür SOLLTEN geeignete Schulungen durchgeführt werden.

DER.2.2.A7 Auswahl von Werkzeugen zur Forensik (S)

Es SOLLTE sichergestellt werden, dass Werkzeuge, mit denen Spuren forensisch gesichert und analysiert werden, auch dafür geeignet sind. Bevor ein Werkzeug zur Forensik eingesetzt wird, SOLLTE zudem geprüft werden, ob es richtig funktioniert. Auch SOLLTE überprüft und dokumentiert werden, dass es nicht manipuliert wurde.

DER.2.2.A8 Auswahl und Reihenfolge der zu sichernden Beweismittel [Fachverantwortliche] (S)

Eine forensische Untersuchung SOLLTE immer damit beginnen, die Ziele bzw. den Arbeitsauftrag zu definieren. Die Ziele SOLLTEN möglichst konkret formuliert sein. Danach SOLLTEN alle notwendigen Datenquellen identifiziert werden. Auch SOLLTE festgelegt werden, in welcher Reihenfolge die Daten gesichert werden und wie genau dabei vorgegangen werden soll. Die Reihenfolge SOLLTE sich danach richten, wie flüchtig (volatil) die zu sichernden Daten sind. So SOLLTEN schnell flüchtige Daten zeitnah gesichert werden. Erst danach SOLLTEN nichtflüchtige Daten wie beispielsweise Festspeicherinhalte und schließlich Backups folgen.

DER.2.2.A9 Vorauswahl forensisch relevanter Daten [Fachverantwortliche] (S)

Es SOLLTE festgelegt werden, welche sekundären Daten (z. B. Logdaten oder Verkehrsmitschnitte) auf welche Weise und wie lange im Rahmen der rechtlichen Rahmenbedingungen für mögliche forensische Beweissicherungsmaßnahmen vorgehalten werden.

DER.2.2.A10 IT-forensische Sicherung von Beweismitteln [Fachverantwortliche] (S)

Datenträger SOLLTEN möglichst komplett forensisch dupliziert werden. Wenn das nicht möglich ist, z. B. bei flüchtigen Daten im RAM oder in SAN-Partitionen, SOLLTE eine Methode gewählt werden, die möglichst wenige Daten verändert.

Die Originaldatenträger SOLLTEN versiegelt aufbewahrt werden. Es SOLLTEN schriftlich dokumentierte kryptografische Prüfsummen von den Datenträgern angelegt werden. Diese SOLLTEN getrennt und in mehreren Kopien aufbewahrt werden. Zudem SOLLTE sichergestellt sein, dass die so dokumentierten Prüfsummen nicht verändert werden können. Damit die Daten gerichtlich verwertbar sind, SOLLTE ein Zeuge bestätigen, wie dabei vorgegangen wurde und die erstellten Prüfsummen beglaubigen.

Es SOLLTE ausschließlich geschultes Personal (siehe DER.2.2.A6 *Schulung des Personals für die Umsetzung der forensischen Sicherung*) oder ein Forensik-Dienstleister (siehe DER.2.2.A3 *Vorauswahl von Forensik-Dienstleistern*) eingesetzt werden, um Beweise forensisch zu sichern.

DER.2.2.A11 Dokumentation der Beweissicherung [Fachverantwortliche] (S)

Wenn Beweise forensisch gesichert werden, SOLLTEN alle durchgeführten Schritte dokumentiert werden. Die Dokumentation SOLLTE lückenlos nachweisen, wie mit den gesicherten Originalbeweismitteln umgegangen wurde. Auch SOLLTE dokumentiert werden, welche Methoden eingesetzt wurden und warum sich die Verantwortlichen dafür entschieden haben.

DER.2.2.A12 Sichere Verwahrung von Originaldatenträgern und Beweismitteln [Fachverantwortliche] (S)

Alle sichergestellten Originaldatenträger SOLLTEN physisch so gelagert werden, dass nur ermittelnde und namentlich bekannte Mitarbeiter darauf zugreifen können. Wenn Originaldatenträger und Beweismittel eingelagert werden, SOLLTE festgelegt werden, wie lange sie aufzubewahren sind. Nachdem die Frist abgelaufen ist, SOLLTE geprüft werden, ob die Datenträger und Beweise noch weiter aufbewahrt werden müssen. Nach der Aufbewahrungsfrist SOLLTEN Beweismittel sicher gelöscht oder

vernichtet und Originaldatenträger zurückgegeben werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein DER.2.2 *Vorsorge für die IT-Forensik* 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.

DER.2.2.A13 Rahmenverträge mit externen Dienstleistern (H)
Die Institution SOLLTE Abrufvereinbarungen bzw. Rahmenverträge mit Forensik-Dienstleistern abschließen, damit IT-Sicherheitsvorfälle schneller forensisch untersucht werden können.

DER.2.2.A14 Festlegung von Standardverfahren für die Beweissicherung (H)
Für Anwendungen, IT-Systeme bzw. IT-Systemgruppen mit hohem Schutzbedarf sowie für verbreitete Systemkonfigurationen SOLLTEN Standardverfahren erstellt werden, die es erlauben, flüchtige und nichtflüchtige Daten möglichst vollständig forensisch zu sichern.

Die jeweiligen systemspezifischen Standardverfahren SOLLTEN durch erprobte und möglichst automatisierte Prozesse umgesetzt werden. Sie SOLLTEN zudem durch Checklisten und technische Hilfsmittel unterstützt werden, z. B. durch Software, Software-Tools auf mobilen Datenträgern und IT-forensische Hardware wie Schreibblocker.

DER.2.2.A15 Durchführung von Übungen zur Beweissicherung (H)
Alle an forensischen Analysen beteiligten Mitarbeiter SOLLTEN regelmäßig in Form von Übungen trainieren, wie Beweise bei einem IT-Sicherheitsvorfall zu sichern sind.

4 Weiterführende Informationen

4.1 Wissenswertes

Das BSI gibt in dem „Leitfaden IT-Forensik“ weiterführende Informationen in die Thematik und kann auch als Nachschlagewerk für einzelne praxisbezogene Problemstellungen dienen.

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27042:2015 und 27043:2015 01:2013 Vorgaben für die Durchführung von forensischen Analysen.

Das Infomation Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel TM 2.4 Forensik Investigations Vorgaben für die Durchführung von forensischen Analysen.

Der Request for Comments (RFC) 3227 „Guidelines for Evidence Collection and Archiving“ gibt in seinem Leitfaden Hinweise zur grundlegenden Vorgehensweise bei einer forensischen Sicherung.

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 DER.2.2 *Vorsorge für die IT-Forensik* von Bedeutung.

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.22 Manipulation von Informationen

G 0.25 Ausfall von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.37 Abstreiten von Handlungen

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen