# Anhang 1: Notfall-Karte

|  |
| --- |
| IT-SECURITY INCIDENT? |
| Step 1: Start forensic log book Add first information: WHAT – WHERE – WHEN – WHO |
| Step 2: Inform Management **eMail: ...**  - Phone Number: **+49 ....** |
| Step 3: Inform .... (relevant local authorities if necessary) *Add here contact data* |
| Step 4: Perform ad-hoc protection measures DARK SITES – DISCONNECT – SHUTDOWN |
| Step 5: Perform forensic backup *Add here contact data of your IT-forensics service provider* |
| Step 6: Analyze Now you can start investigating –  ideally in cooperation with your IT-forensics service provider |
| Step 7: Re-activate Once you know what happened, and after cleaning up the systems  GO BACK TO NORMAL MODE |
| Step 8: Document and learn |

# Vorlage forensisches Logbuch

|  |  |
| --- | --- |
| Um welchen Vorfall handelt es sich? | Kurze Bezeichnung |
| Wer ist für Aufklärung verantwortlich? | Kurze Angabe der Kontaktdaten |
| Welche weiteren Personen und Dienstleister sind an der Aufklärung beteiligt? | Kurze Angabe der Kontaktdaten mit der jeweiligen Rolle, fortlaufende Ergänzung |
| Wann wurde der Vorfall gemeldet? | Möglichst genaue Angabe mit Uhrzeit |
| Durch wen erfolgte die Meldung? | Kurze Angabe der Kontaktdaten |
| Wie wurde der Vorfall bemerkt? | Information durch Partner, Zugriff auf Dienste oder Daten durch Mitarbeiter |
| Welche Auswirkungen hat der Vorfall? | Einschränkung der Verfügbarkeit, Verletzung der Vertraulichkeit oder Integrität, Verlust oder Manipulation von Daten, interne oder auch externe Auswirkungen |
| Welche Dienste oder Daten sind nach aktuellem Kenntnisstand betroffen? | Auflistung der Dienste und Daten |
| Welche Systeme sind nach aktuellem Kenntnisstand betroffen? | Auflistung der Systeme |
| Welche Dokumentationen sind vorhanden? | Sammeln der Dokumentationen, Verweis auf Dateinamen und kurze Angabe des Inhalts |
| Wurde der Vorfall an zuständige Ermittlungsbehörden gemeldet? | Nur optional falls eine Meldepflicht besteht |
| Welche Notfallmaßnahmen wurden ergriffen? | Abschaltung von Systemen, Trennung vom Netz, Erzeugung von Datensicherungen |
| Wurde eine forensische Datensicherung durchgeführt? | Dienstleister, Datum, Ort der Ablage |
| Wie wurde der Vorfall analysiert? | Verwendete Logdateien, Verwendung von Tools, Überprüfte Systeme, Überprüfung der Konfiguration |
| Welche Erkenntnisse wurden aus der Analyse gewonnen? | Ursachen für den Vorfall, betroffene Systeme, Dienste oder Daten, Verweis auf detaillierte Berichte |
| Wie erfolgte die Wiederherstellung? | Wiederhergestellte Systeme, Dienste oder Daten, Anpassung Sicherheitsrichtlinien und technischer oder organisatorischer Maßnahmen |
| Wurde der Vorfall extern kommuniziert? | Nur optional und abgestimmt, Geschäftspartner, Pressevertreter |