**Notfallplan IT**

***Vorfall – Was ist zu tun?***



**Hilfe zur Selbsthilfe**

* Checkliste Organisatorisches (Anlage 1)
* Checkliste Technik (Anlage 2)

**Kontakt zum Service Center (Hotline)**

Zur richtigen Einschätzung des IT-Sicherheitsvorfalls, kann telefonische Hilfe beim BSI eingeholt werden.

***Bundesamt für Sicherheit in der Informationstechnik (BSI)***

***Hotline-Nummer: 0800-274 1000***

***Service-Zeiten: 8:00 Uhr bis 18:00 Uhr***

Das Cyber-Sicherheitsnetzwerk ist ein freiwilliger Zusammenschluss von qualifizierten Helferinnen und Helfern, die sich bereit erklären, ihr individuelles Fachwissen zur Behebung von IT-Sicherheitsvorfällen zur Verfügung zu stellen.

**Digitale Ersthelfer**

Aufgabe der Digitalen Ersthelfer ist es, Betroffene, insbesondere Verbraucherinnen und Verbraucher, bei der Behebung von kleineren IT-Störungen- und IT-Sicherheitsvorfällen mit Ersthilfe zu unterstützen.

Digitale Ersthelfer im Unternehmen: XXXXXKontaktdaten IT-intern einfügen

**Vorfall-Praktiker**

Vorfall-Praktiker sind geschulte IT-Fachleute mit IT-Sicherheitserfahrung. Sie unterstützen KMU telefonisch innerhalb ihre Servicezeiten bei der Behebung von IT-Sicherheitsvorfällen und leisten so schnelle Erst Hilfe.

Vorfall Praktiker: XXXXXKontaktdaten IT-Dienstleister einfügen

**Vorfall-Experten**

Die Vorfall-Experten sind vom BSI personenzertifizierte IT-Fachleute mit nachgewiesener Expertise bei der Behandlung von IT-Sicherheitsvorfällen. Im Rahmen der Digitalen Rettungskette sind sie soweit qualifiziert, dass sie in der Lage sind, den Vorfall tiefer zu analysieren und entsprechende Hilfestellung zu geben – ggf. auch vor Ort.

Folgender Link enthält die aktuell registrierten Vorfall-Experten: „[**Vorfall-Experten**](https://www.allianz-fuer-cybersicherheit.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Qualifizierung/Vorfall_Experten/Suche/suche_node.html)“

**IT-Sicherheitsdienstleister für Vorfallbehandlung**

Die vom BSI zertifizierten IT-Sicherheitsdienstleister für Vorfallbehandlung stellen ganze Teams aus Vorfall-Experten und IT-Spezialisten zur Verfügung, die aus diesem Grund auch komplexe und zeitaufwändigere IT-Sicherheitsdienstleister geeignet betreuen können.

Folgender Link enthält die aktuell registrierten IT-Sicherheitsdienstleister:

 „[**IT-Sicherheitsdienstleister**](https://www.allianz-fuer-cybersicherheit.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Anerkennung-von-Stellen-und-Zertifizierung-IT-Sicherheitsdienstleister/Vorfallbearbeitung/Liste-IT-Sicherheitsdienstleister_Vorfall-Experte/liste-it-sicherheitsdienstleister_Vorfallbearbeitung_node.html)“

**Anlage 1 - Checkliste Organisatorisches**

***Ruhe bewahren und nicht übereilt handeln!***



**Wissen alle, die intern davon wissen müssen vom mutmaßlichen IT-Notfall?**

1. Ist der IT-Sicherheitsverantwortliche, der Datenschutzbeauftragte, der IT-Betrieb informiert?
2. Ist die Geschäftsleitung informiert?
3. Müssen weitere interne Stellen informiert werden?

**Organisieren Sie sich. Richten Sie einen Krisenstab (oder eine Projektgruppe) ein. Verteilen Sie Rollen und Zuständigkeiten.**

1. Wer trifft die relevanten Entscheidungen?
2. Wer macht was bis wann?

**Sammeln Sie möglichst schnell und möglichst viele Informationen, um fundierte Entscheidungen treffen zu können.**

1. Was ist eigentlich passiert?
2. Wie ist es aufgefallen?
Wurde es durch Externe gemeldet? Dann halten Sie den Kontakt zu diesen aufrecht, sofern dort gewünscht, um zu verhindern, dass der Vorfall aus einem Gefühl der Vernachlässigung vorzeitig publik gemacht wird.
3. Welche Auswirkungen kann es direkt auf das Unternehmen, seine Kerndienstleistungen oder auf wesentliche Produktionsprozesse haben?
	* Muss der Weiterbetrieb um jeden Preis gewährleistet werden? Wirkt sich möglicherweise negativ auf forensische Beweissicherung und Analyseergebnisse aus.
	* Besteht ausreichend zeitlicher Spielraum, um das Problem umfassender zu analysieren und zu bewältigen?
	* Ist eine Strafverfolgung vorgesehen? Muss deshalb beweissicher gehandelt werden? Erfordert i.d.R. umsichtigeres und aufwändigeres Vorgehen.
4. Welche Auswirkungen kann es auf Kunden, Partner oder die Öffentlichkeit haben?
	* Ergibt sich daraus zusätzlicher Handlungsbedarf?
5. Warum ist es uns passiert? Gibt es Hinweise auf ein gezieltes Vorgehen? Sind wir nur eines von vielen potenziellen Opfer?

**Welche Kommunikationsaspekte müssen berücksichtigt werden?**

1. Benennung eines Kommunikationsexperten, Pressesprechers oder ähnliches, um Informationen abgestimmt, gezielt und gebündelt zu verteilen, aber auch entgegenzunehmen.
2. Betriebs-/ unternehmensinternen Benachrichtigungen an die Mitarbeiter, ggf. bereits mit entsprechenden Sprachregelungen.
3. Wer muss noch informiert werden?
4. Bestehen Meldepflichten?
	* Im Falle einer damit verbundenen relevanten Datenschutzverletzung, ist der IT-Vorfall an die zuständige Datenschutzaufsichtsbehörde zu melden.
5. Gelten im Falle von IT-Vorfällen vertragliche Informationspflichten, beispielsweise gegenüber Auftraggebern, Geschäftspartnern, Auftragnehmern oder Versicherungen, oder vergleichbare Compliance-Regeln?
6. Kunden und die Öffentlichkeit in Überlegungen miteinbeziehen
7. Soll der IT-Vorfall freiwillig gemeldet werden (ggf. anonymisiert / pseudonymisiert), um die Warnung potenziell weiterer Betroffener zu ermöglichen?
8. Soll eine Strafanzeige gestellt werden?

**Anlage 2 - Checkliste Technik**

**Keine Anmeldung mit privilegierten Nutzerkonten auf einem potenziell infizierten System.**

1. Existieren Benutzerkonten mit unnötigen, privilegierten Rechten?
2. Sind Hinweise zu erkennen, ob diese privilegierten Rechte durch Unbefugte / Angreifer – möglicherweise in jüngster Vergangenheit – eingerichtet wurden?

**Sicherstellen, dass nur vollständige und aktuelle Informationen über das Netzwerk verwendet werden.**

1. Das / die betroffene(n) System(e) identifizieren.

Nicht nur auf das Offensichtliche beschränken. Es sollte in Betracht gezogen werden, dass weitere Systeme ebenfalls betroffen sind und noch auf Befehle des Angreifers warten.

1. Betroffene Systeme vom internen produktiven Netzwerk und dem Internet trennen.
	* Dazu das Netzwerkkabel ziehen.
	* Gerät nicht herunterfahren oder ausschalten, sofern eine technische Analyse beabsichtigt ist.
	* Gegebenenfalls forensische Sicherung inkl. Speicherabbild (selbst, durch Dienstleister oder Strafverfolgungsbehörden) erstellen, sofern eine Strafverfolgung eingeleitet werden soll.
	* Erst danach AV-Programme einsetzen, da diese ggf. Änderungen sowohl am flüchtigen als auch persistenten Speicher vornehmen könnten.
2. Infizierte lokale Systeme grundsätzlich als vollständig kompromittiert betrachten. Eine punktuelle Bereinigung ist nur mit umfassendem Fachwissen erfolgversprechend. Im Regelfall sollte eine komplette Neuinstallation eingeplant werden.
3. Alle auf betroffenen Systemen gespeicherten bzw. nach der Infektion eingegebenen Zugangsdaten ebenfalls als kompromittiert betrachten.
4. Im Fall einer Kompromittierung des Active Directory (AD) auch das gesamte Netz als kompromittiert betrachten.

**Sofern bisher noch kein ausreichendes Netzwerk-Monitoring und Logging aktiviert war, ist eine Abstimmung mit dem Datenschutzbeauftragten notwendig (und ggf. Betriebs-/ Personalrat), um noch andauernde Angriffe oder Datenabflüsse feststellen zu können.**

1. Als Best-Practice gilt das auch vom BSI empfohlene Full-Packet-Capturing im Netzwerk.
	* Am Mirror-Port an internen, zentralen Netzkoppelelementen können ggf. die Kommunikation der infizierten, internen Systeme untereinander oder der lokalen Command & Control Server erkannt werden.
	* Am Übergang zwischen LAN und WAN können ggf. die externen C&C-Server festgestellt werden.
	* Vielfach werden Angriffe zuerst durch Externe als Unregelmäßigkeiten festgestellt und an Betroffene gemeldet. Um eine solche Meldung nachvollziehen zu können, muss an der Firewall geloggt werden.
2. Einrichtung dedizierte Protokollserver. Optimalerweise werden diese außerhalb des Produktiv-/ Büronetzes über eine Schnittstelle im "Promiscuous"-Mode betrieben. Angreifer können i.d.R. eigene Defensivmaßnahmen ergreifen, um ein Logging zu verhindern oder zu erschweren. Im Einzelfall können ungeschützte Logdaten durch den Angreifer manipuliert werden.
3. Erkennbare Täterzugänge blockieren.

**Verfügbarkeit der aktuellen, sauberen, integren Backups prüfen. Die Aufbewahrung sollte offline erfolgen. Online-Sicherungen können ggf. beiläufig oder bewusst kompromittiert worden sein.**

**Ggf. können wichtige Daten auch an abgesetzten Außenstellen oder auf Systemen von Mitarbeitern im Urlaub befinden.**