Ich habe einen Vorfall – Checkliste

Organisatorisches

Nachstehende Checkliste wurde vom deutschen Bundesamt für Sicherheit in der Informationstechnik erstellt und für österreichische Unternehmen adaptiert.

Die Checkliste gliedert sich in organisatorische und technische Aspekte, **die teilweise parallel abgearbeitet werden können**. Sie ist in Form von Leitlinien und Leitfragen aufgebaut. Einzelne Schritte sind ggf. zyklisch zu wiederholen.

Rahmenbedingungen

1. Die vorliegende **Checkliste "Organisatorisches"** zur Bewältigung von IT-Notfällen kann keine präventiven Maßnahmen oder ein fehlendes Notfall-Management ersetzen.
2. Aufgrund der Allgemeingültigkeit, die einen weitverbreiteten Einsatz der Checkliste bei unterschiedlichen IT-Notfällen und in einem sehr heterogenen Umfeld der Betroffenen ermöglichen soll, kann eine Vielzahl der Punkte nur generischer Natur sein.
3. Die Checkliste zielt vor allem auf klein- und mittelständische Unternehmen, die noch keine Gelegenheit hatten, sich umfassend auf einen IT-Notfall vorzubereiten und damit eine Arbeitshilfe erhalten, um einen solchen strukturiert zu bewältigen. Einzelaspekte sind aber für Jedermann nutzbar.

In dem Dokument "**Ransomware: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall Version 1.1**" finden Sie diese Aspekte ausführlicher beschrieben und mit zusätzlichen Hintergrundinformationen.

Checkliste Organisatorisches

Bewahren Sie Ruhe und handeln Sie nicht übereilt.

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

1. Ist der IT-Sicherheitsverantwortliche, der Datenschutzbeauftragte, der IT-Betrieb informiert? Ein Beispiel dafür, was hier gemeldet werden sollte ist in der **IT-Notfallkarte** des BSI dargestellt.
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? Dies 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 potentiellen Opfer?

Welche Kommunikationsaspekte müssen berücksichtigt werden?

1. Falls noch nicht vorhanden, schaffen Sie die Rolle eines zuständigen Kommunikationsexperten, Pressesprechers oder ähnliches, um Informationen abgestimmt, gezielt und gebündelt zu verteilen, aber auch entgegen zu nehmen.
2. Umfassende Erläuterungen finden Sie im "**Leitfaden Krisenkommunikation**" des deutschen Bundesministeriums des Innern, für Bau und Heimat (BMI). Dieser wurde primär für die Bundesverwaltung und öffentliche Verwaltung entwickelt, enthält aber vor allem in den Kapiteln 5 und 6 sowie in Anlage 3 hilfreiche Grundsätze.
3. Vernachlässigen Sie nicht die betriebs-/ unternehmensinternen Benachrichtigungen Ihrer Mitarbeiter, ggf. bereits mit entsprechenden Sprachregelungen.
4. Prüfen Sie, wer informiert werden sollte oder muss.
5. Bestehen Meldepflichten?
    - Prüfen Sie, ob Sie im Fall einer Datenschutzverletzung Meldung an die Datenschutzbehörde erstatten und betroffene Personen informieren müssen. EU-Datenschutz-Grundverordnung (DSGVO): Meldung von Datenschutzverletzungen - WKO.at
    - Falls Sie Betreiber wesentlicher Dienster oder Anbieter digitaler Dienste im Sinne des NIS-Gesetzes sind und/oder freiwillige Meldung über einen Vorfall erstatten wollen, informieren Sie sich hier.
    - Haben Sie eine Versicherung für derartige Vorfälle, sollten Sie diese umgehend beiziehen.
6. Gelten für Sie im Falle von IT-Vorfällen vertragliche Informationspflichten, beispielsweise gegenüber Auftraggebern, Geschäftspartnern, Auftragnehmern oder Versicherungen, oder vergleichbare Compliance-Regeln?
7. Beziehen Sie auch Ihre Kunden und die Öffentlichkeit in Ihre Überlegungen mit ein.
8. Wollen Sie Strafanzeige stellen?
   Wenn Sie einen Verdacht auf Internetkriminalität haben und Hilfe oder Informationen benötigen, wenden Sie sich bitte an das Bundeskriminalamt:
   Meldestelle für Internetkriminalität
   E-Mail: against-cybercrime@bmi.gv.at
   Anzeige bei der Polizei
   Wenn Sie durch eine Straftat geschädigt wurden oder konkrete Hinweise auf einen Täter haben, können Sie die Straftat in jeder Polizeidienststelle zur Anzeige bringen.

Wird eine externe Unterstützung benötigt? Wenn ja, wo finde ich sie?

Wenn Ihr Unternehmen Opfer einer Cyberattacke, eines Cybercrime Angriffs, von Ransomware oder Verschlüsselungstrojanern wurde, rufen Sie das Callcenter der Cybersecurity Hotline der WKO unter 0800 888 133 an. Sie erhalten rund um die Uhr und kostenlos eine rasche telefonische Erstinformation und Notfallhilfe.

IT-Security-ExpertInnen stehen Ihnen mit hoher fachlicher Expertise und Erfahrung zur Seite und können Sie tatkräftig bei der Umsetzung unterstützen.

Im UBIT Firmen A-Z finden Sie IT-Security ExpertInnen aus ganz Österreich.

Falls Sie eine Cyberversicherung haben, wenden Sie sich an den Ansprechpartner Ihrer Versicherung.

Nachbereitung

1. Lernen Sie aus dem IT-Vorfall
2. Bereiten Sie sich auf den nächsten IT-Vorfall vor

Zu den **technische Aspekten**

Quelle: Bundesamt für Sicherheit in der Informationstechnik; adaptiert für österreichische Unternehmen