Muster Cyber Notfallplan

Stand: 1. März 2023

Unternehmen

Erstellt am:

Erstellt von:

Leidenschaft
Möglichkeiten
Ideen
Entscheidungen
Menschen
Verantwortung
Scheitern
Besser scheitern
Gewinnen

Selbstverständlich selbständig.

VMG

WKO Landesinnung Bau STEIERMARK

Inhalt

1 Einleitung

Nachfolgende Unterlagen sollen einen kurzen Überblick über die Möglichkeit zur Errichtung eines Notfallplans darstellen. Der Notfallplan sollte auf den jeweiligen Bedarf des Unternehmens ausgerichtet sein und ist bei der Erstellung die Begleitung durch Spezialisten zu empfehlen.

Dieser Notfallplan sollte folgende Szenarien umfassen:
- Totalausfall
- Teilausfall wie zB
  - Verwaltung
  - Produktion
  - Handel
  - Einzelne Maschine (Schlüsselmaschine)...

Mögliche Ursachen:
- Cyber-Angriff
- Netzwerk-/Internetausfall
- Brand/Wasser
- ...

Ziel eines Notfallhandbuches ist es, eine dokumentierte Vorgehensweise beziehungsweise Hilfestellung für alle Phasen der Notfallbewältigung bereitzustellen, mit deren Unterstützung ein Unternehmen einen Notfall bewältigen und ihre kritischen Geschäftsprozesse fortführen kann.

Normalbetrieb	-	**Unterbrechung durch IT-Ausfall**	-	**Notbetrieb**	-	**Normalbetrieb**
		Feststellen des Ausfalls		Wiederherstellung		Nachbearbeitung
		erste Sofortmaßnahmen				
		Alarmierung und Ausruf des Notfalls				

Das Notfallhandbuch sollte in der Papierform bzw. als eine „offline" Kopie jederzeit verfügbar sein.

Das Notfallhandbuch ist nach Fertigstellung freizugeben und dem Adressatenkreis bekannt zu geben bzw. in regelmäßigen Abständen zu aktualisieren.

2 Organisation und Kommunikation

2.1 Notfallstab

Der Notfallstab übernimmt die Verantwortung für die gesamte Abwicklung eines IT-Notfalls. Die Leitung ist so zu besetzen, dass die gesamte Geschäftstätigkeit maximal entscheidungs- und handlungsfähig ist.

Es wird empfohlen, einen entsprechenden Plan mit den ausführenden Personen zu erstellen und die Tätigkeiten entsprechend aufzuteilen (Kommunikation, Alarmierung, Ergreifen von Sofortmaßnahmen...).

2.2 Notfallkommunikation

Abhängig von der Situation sind für den Notfallstab die folgenden Arbeitsweisen denkbar:

- Information/bei Bedarf: Die Mitglieder werden über eine Situation regelmäßig informiert, kommen aber nur bei besonderem Bedarf zusammen. Beispielsweise anwendbar in einfachen Situationen, die längere Wartezeiten beinhalten (um zB Anwendungen neu zu konfigurieren).
- Teilzeit: Die Mitglieder kommen regelmäßig zusammen, um eine Situation zu besprechen. Sie nehmen jedoch auch ihre anderen Tätigkeiten wahr.
- Vollzeit: Die Mitglieder arbeiten ausschließlich an der Bewältigung der Situation. Das ist notwendig bei komplexen Situationen, die eine hohe Arbeitslast generieren, zB umfangreicher Malware-Befall.

Vor allem in komplexen Situationen kann es notwendig sein, viele Stunden pro Tag und auch am Wochenende zu arbeiten. Deshalb sollte in solchen Fällen auch an Vertretungsmöglichkeiten gedacht werden.

2.2.1 Interne Kommunikation

- Wie erfolgt die Kommunikation bzw. welche Kommunikationsmittel stehen zur Verfügung?
- Was ist passiert – aktueller Status.
- Keine Kommunikation einzelner Mitarbeiter nach außen.
- Wie ist die weitere Vorgangsweise.

2.2.2 Kommunikation mit Geschäftspartnern

- Information über Lieferverzögerungen, Erreichbarkeit ...
- Kontakt mit IT-Dienstleister, Rechtsanwalt des Unternehmens, Versorgungsunternehmen, Telekommunikationsunternehmen

2.2.3 Kommunikation mit Behörden und Ämtern

Bei Bedarf sollte mit Ämtern (zB Finanzamt) Kontakt aufgenommen werden.

2.2.4 Öffentlichkeit

Je nach Situation sollte eine aktive Kommunikation an die Öffentlichkeit erfolgen. Dazu sollte ein Pressesprecher festgelegt werden.

2.3 Meldepflichten

Bei Datenschutzverstößen ist die Datenschutzbehörde zu informieren. Dies sollte unbedingt dokumentiert werden.

Eventuell Anzeige (je nach Situation) bei Polizei.

3 Erstmaßnahmen

3.1 Eintritt eines IT-Notfalls

- Verhinderung einer Schadensvergrößerung (zB Rechner vom Netz nehmen)
- Schadendokumentation durch zB fotografieren des Bildschirms
- Bei bestehender Cyberversicherung Kontakt mit Hotline

3.2 Alarmierung und Meldung

Welche Informationen sollen an wen weitergegeben werden?

4 Maßnahmen

4.1 Eintritt eines IT-Notfalls

- Protokollierung
- Wiederanlauf: Welche zeitkritischen Geschäftsprozesse bestehen bzw. benötigen ein IT-Service?
- Wie lange dauert die Durchführung?
- Welche Voraussetzungen sind erforderlich?

5 Wiederherstellung

- Alternative Organisation der Arbeit
- Mögliche Ersatzräumlichkeiten
- Wiederherstellung der IT-Infrastruktur (Server, Arbeitsplätze, Verkabelungen, Router ...)
- Externe Dienstleister

6 Meldung von Datenschutzverletzungen (Muster WKO)

Data BreachNotification[1]
(Art 34 EU-Datenschutzgrund-Verordnung (DSGVO))
Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

1. Name und Kontaktdaten des **Verantwortlichen**:

   a. Name und Anschrift:

   b. E-Mail-Adresse (und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.):

2. Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des **Datenschutzbeauftragten**[2]:

   a. Name und Anschrift:

   b. E-Mail-Adresse (und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.):

3. Beschreibung der **Art der Verletzung** des Schutzes personenbezogener Daten:

[1]Data Breach oder Datenpanne beschreibt den Verlust der Kontrolle über die Daten, siehe dazu auch das WKO-Merkblatt EU-Datenschutz-Grundverordnung (DSGVO): Meldung von Datenschutzverletzungen (Data BreachNotification).
[2]Sofern ein Datenschutzbeauftragter verpflichtend oder auf freiwilliger Basis bestellt wurde. Siehe dazu das WKO-Merkblatt EU-Datenschutz-Grundverordnung (DSGVO): Datenschutzbeauftragter.

4. Beschreibung der **wahrscheinlichen Folgen** der Verletzung des Schutzes personenbezogener Daten:

5. Beschreibung der **ergriffenen oder vorgeschlagenen Maßnahmen** zur Behebung der Verletzung:

   a. ggf. **Maßnahmen zur Abmilderung** der Auswirkungen der Verletzung:

Anhang: Data BreachNotification (Musterformular)

(Art 34 EU-Datenschutzgrund-Verordnung (DSGVO))
Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(Hinweis: Es wird darauf hingewiesen, dass es sich hier um ein fiktives Beispiel handelt. Bei der praktischen Umsetzung ist auf die konkreten Anwendungsfälle im Unternehmen abzustellen.)

1. Name und Kontaktdaten des **Verantwortlichen**:

   a. Name und Anschrift:

   Max Mustermann GmbH
   Neuer Weg 1
   ZZZZ Musterdorf

   b. E-Mail-Adresse (und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.):

   max@mustermann.at

2. ~~Name und Kontaktdaten (Anschrift, E-Mail und allenfalls weitere Kontaktdaten wie zB Tel.Nr.) des **Datenschutzbeauftragten**~~:

   a. ~~Name und Anschrift:~~[3]

   b. ~~E-Mail-Adresse (und allenfalls weitere Kontaktdaten wie z.B. Tel.Nr.):~~

3. Beschreibung der **Art der Verletzung** des Schutzes personenbezogener Daten:

   Einbruchdiebstahl, PC wurde entwendet.

[3] Wir gehen in unserem Beispiel davon aus, dass kein Datenschutzbeauftragter bestellt wurde.

4. Beschreibung der **wahrscheinlichen Folgen** der Verletzung des Schutzes personenbezogener Daten:

Weitergabe der Kundendaten, Weitergabe der Passwörter Kontaktaufnahme durch Unbefugte, Inanspruchnahme durch Unbefugte

5. Beschreibung der **ergriffenen oder vorgeschlagenen Maßnahmen** zur Behebung der Verletzung:

Anzeige bei der zuständigen Polizeidienststelle durch den Verantwortlichen, Zurücksetzen der Passwörter, Sperren der Kundenzugänge, Reaktivierung durch die Kunden

a. ~~ggf. **Maßnahmen zur Abmilderung** der Auswirkungen der Verletzung:~~

[4]Wir gehen in unserem Beispiel davon aus, dass keine weiteren Maßnahmen möglich waren.

WKO STEIERMARK

Leidenschaft
Möglichkeiten
Ideen
Entscheidungen
Menschen
Verantwortung
Scheitern
Besser scheitern
Gewinnen

Selbstverständlich selbständig.

Impressum: WKO Steiermark | Landesinnung Bau | Körblergasse 111 – 113 | 8010 Graz | T 0316/601-487 | Grafik: Stabstelle für Kommunikation & Marketing | Fotos: flashmovie - stock.adobe.com (Titelseite) | Ausgabe: 03/2023 | In der vorliegenden Broschüre haben wir uns konsequent um eine geschlechtsneutrale Formulierung bemüht. Sollte uns das nicht immer gelungen sein, möchten wir ausdrücklich festhalten, dass sämtliche Begriffe, Bezeichnungen und Funktionstitel für alle Geschlechter zu verstehen sind.