Juli 2024

IT-NOTFALL HANDBUCH

LEITFADEN UND ERSTE SCHRITTE

Erstellt von
SYSTAG GmbH

Gutenbergstr. 47 72555 Metzingen
07123 9 20 20
info@systag.com
www.systag.com

Inhalt

Zweck & Definition

Risikobewertung

Kritische Geschäftsprozesse

ToDos im IT-Notfall

Kommunikationsplan

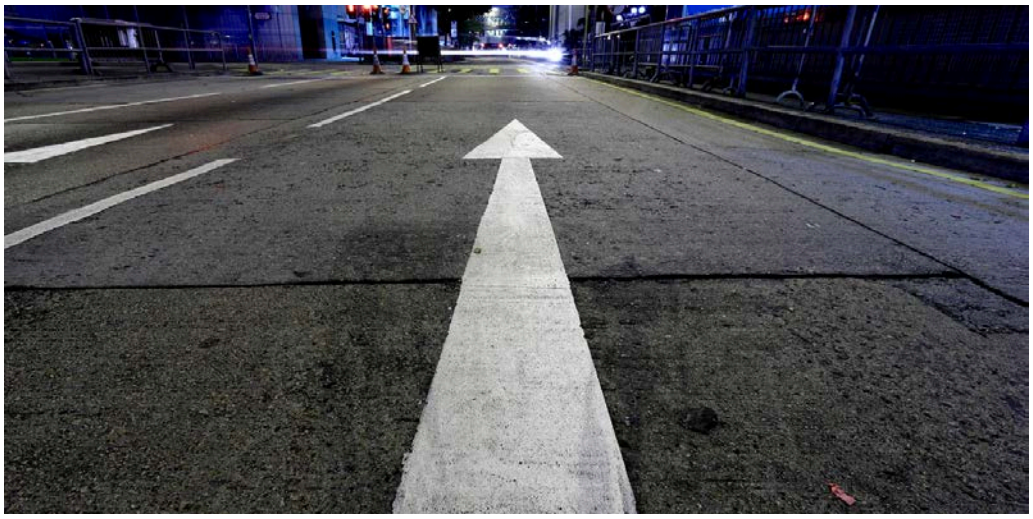
Wiederherstellungsplan

Präventation und Schulung

Dokumentation und Revision

Kontaktinformationen

ZWECK des IT-Notfallhandbuchs



Das IT-Notfallhandbuch soll sicherstellen, dass im Fall eines IT-Notfalls schnell und effizient gehandelt wird, um Schäden zu minimieren und den Geschäftsbetrieb so schnell wie möglich wiederherzustellen.

WAS IST ein IT-Notfall

Bei welchen Szenarien kann es zu einem IT-Notfall kommen, hier einige Beispiele:

- Hardware-Ausfälle
- Cyberangriffe
- Datenverlust
- Naturkatastrophen

! Unterschied zwischen Betriebsstörung und IT-Notfall definieren!

RISIKEN

bewerten

Identifikation potenzieller IT-Risiken

Welche Risiken bestehen für unsere IT. Hier einige Beispiele:

- Server- und Hardware-Ausfälle
- Netzwerkausfälle
- Malware und Cyberangriffe
- Feuer, Überflutung und andere Naturkatastrophen

Bewertung der Auswirkungen

Welche Auswirkungen hätten eben diese Risiken auf unser Unternehmen. Zum Beispiel:

- Finanzielle Verluste
- Datenverlust und Datenschutzverletzungen
- Schlupflöcher in der Geschäftskontinuität
- Reputationsschäden
- Produktionsausfall etc.

KRITISCHE Geschäftsprozesse

Identifizierung kritscher Geschäftsprozesse und Anwendungen

Welche Zusammenhänge bestehen, und wo sind die Prioritäten?

Hier wird definiert welche Prozesse kritisch sind und welche Anwendungen dafür benötigt werden.

Identifikation der Handlungsoptionen

Wie können wir im Ernstfall gegensteuern, welche Handlungsoptionen haben wir und wie stellen wir unsere kritischen Geschäftsprozesse und Anwendungen schnellstmöglich wieder her.

NOTFALL

Organisation

Notfallteam

Wer ist für was im Falle eines Notfalls verantwortlich? Zuständigkeiten und Kontaktdaten der Mitglieder des Notfallteams.

Rollen und Verantwortlichkeiten

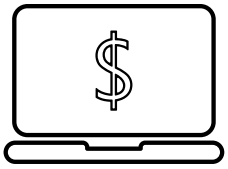
Wer hat welche Rolle im Falle eines IT-Notfalls? Folgende Rollenverteilung wäre möglich:

- Notfallkoordinator
- IT-Spezialisten
- PR-Manager
- Sicherheitspersonal

ToDos im NOTFALL

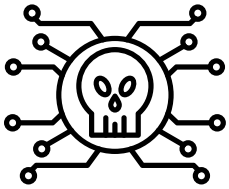
Welche Maßnahmen müssen im jeweiligen Notfall unmittelbar ergriffen werden. Erstmaßnahmen bei verschiedenen Notfällen:

Hardware-Ausfall



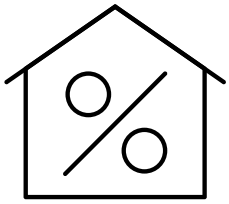
Server abschalten, Ersatzhardware in Betrieb nehmen, betroffene Systeme überprüfen und reparieren

Cyberangriff



Betroffene Systeme sofort vom Netz nehmen, IT-Sicherheitsunternehmen benachrichtigen, Sicherheitslücken schließen.

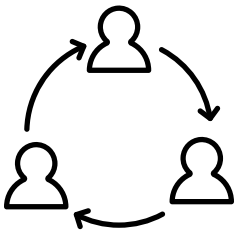
Datenverlust



Datenwiederherstellungssoftware nutzen, externe Backup-Systeme aktivieren, betroffene Systeme checken

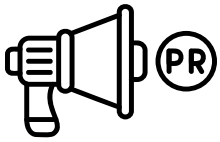
Hier werden für alle möglichen Ausfallszenarien die entsprechenden Gegenmaßnahmen definiert und festgehalten.

KOMMUNIKATIONSPLAN



INTERN

- Benachrichtigung der Mitarbeitenden über festgelegte Kommunikationskanäle (E-Mail, Intranet)
- Regelmäßige Statusupdates



EXTERN

- Vorlagen für Pressemitteilungen
- Informationen für Kunden und Partner
- Ansprechpartner für Medienanfragen

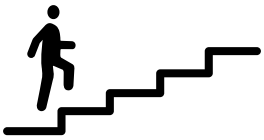
ALARMIERUNGSKETTE

Phase 01	• ToDo
Phase 02	• ToDo
Phase 03	• ToDo
Phase 04	• ToDo

Hier wird definiert, wie im Falle eines IT-Notfalls kommuniziert wird. Sowohl intern als auch extern.Wer wird über was, wann informiert? Wer muss einbezogen werden?

WIEDERHERSTELLUNGSMASSNAHMEN

Schritt-für-Schritt-Anleitung zur Wiederherstellung



- Priorisierung der Systeme zur Wiederherstellung
- Dokumentation aller genutzten Ressourcen (Hardware, Software)
- Überprüfung der Systemsicherheit nach Wiederherstellung

RESSOURCEN

- Liste mit benötigter Hardware und Software zur Wiederherstellung
- Welche externen Dienstleister und Lieferanten werden als Unterstützung benötigt

SCHRITT-FÜR-SCHRITT

Schritt 01
- ToDo

Schritt 02
- ToDo

Schritt 03
- ToDo

Schritt 04
- ToDo

Schritt 05
- ToDo

Hier wird definiert - in welcher Reihenfolge die Systeme und Anwendungen wiederhergestellt werden.

PRÄVEN
-TION

UND SCHULUNG

Regelmäßige Schulungen:

- IT-Sicherheitsschulungen für alle Mitarbeitenden
- Notfallübungen, um die Wirksamkeit des Plans zu testen

Sicherheitsvorkehrungen

- Installation und regelmäßige Aktualisierung von Sicherheits- und Anti-Virus-Software
- Implementierung einer starken Passwortpolitik

DOKUMENTATION UND REVISION

Regelmäßige Überprüfungen

- Jährliche Überprüfung und Aktualisierung des IT-Notfallhandbuchs
- Anpassung des Handbuchs je nach gewonnenen Erfahrungen und neuen Bedrohungen

Dokumentation

- Protokollierung aller Maßnahmen während eines Notfalls
- Feedback zur Verbesserung des Notfallhandbuchs

Bei Fragen, wenden Sie sich bitte an:

Ihre Ansprechpartnerin

Franka Theis

Strategic Account Managerin Cyber Security
franka.theis@systag.com
+49 7123 9 20 20

Bitte beachten Sie, dass dies ein Leitfaden zur Erstellung eines IT-Notfallhandbuchs ist und keine vollständige Vorlage dafür.