Cyber-Sicherheitsrat Deutschland e.V.

Werkzeugkasten Cybersicherheit

IT-Notfallplan

Definition, Einsatzgebiete & Diskussion

Wir sind wehrhaft

Cybersicherheit erscheint uns oft als unbezwingbare Aufgabe: ein **asymmetrisches Setting**, das Angreifern einen taktischen Vorteil gegenüber Sicherheitsexperten verschafft, wachsende Möglichkeiten und die **Professionalisierung von Cyberkriminellen**, **unklare Zuständigkeiten** und regulatorische Anforderungen bei IT-Sicherheitsinstitutionen und vieles mehr.

Das kann deprimieren.

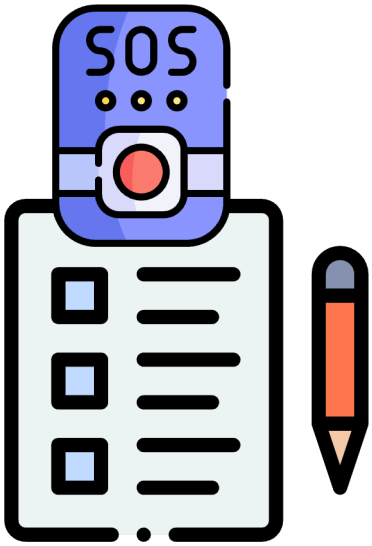
Was wir dabei oft vergessen sind die vielen Menschen, Ressourcen und Werkzeuge auf der anderen Seite, die tagtäglich daran arbeiten, Wirtschaft und Gesellschaft sicherer zu machen. In der Vergangenheit wurden **wirkungsvolle und starke Methoden** entwickelt, die nur an den richtigen Stellen genutzt werden müssen, um Angreifern einen Schritt voraus zu sein.
Es gibt für alles eine Lösung, man muss sie nur finden – vor allem im Bereich Cybersicherheit. Diese Publikationsreihe stellt übersichtsartig die wichtigsten **Methoden im Kampf gegen Cyberattacken** mit ihren Einsatzgebieten sowie Vor- und Nachteilen vor, damit zukünftig die richtigen Werkzeuge an den passenden Stellen parat stehen.

Ich wünsche Ihnen eine anregende Lektüre und interessante Einblicke in den Werkzeugkasten Cybersicherheit.

Hans-Wilhelm Dünn
Präsident
Cyber-Sicherheitsrat Deutschland e.V.

IT-Notfallplan – Was ist das?

Ein IT-Notfallplan ist eine Art Handbuch, das eine **Sammlung von Verfahren und Richtlinien** enthält, die bei einem IT-Notfall zu befolgen sind. Es beschreibt Handlungsschritte um Systeme und Daten des Unternehmens oder der Organisation zu schützen, die Sicherheit der Mitarbeiter und Kunden zu gewährleisten und den Geschäftsbetrieb aufrechtzuerhalten.
Ein IT-Notfall kann **verschiedene Ursachen** haben, wie z.B. Naturkatastrophen, menschliches Versagen, Cyberangriffe oder Hardwarefehler. Je nach Schadensereignis kommen verschiedene **Checklisten** zum Einsatz, die abgearbeitet werden.



Wie sind die Notfallpläne gestaltet?

Ein IT-Notfallplan beinhaltet verschiedene Komponenten, die alle dazu beitragen sollen, einen reibungslosen Ablauf im Falle eines Notfalls sicherzustellen. Er besteht stets aus einer **Kombination von technischen und organisatorischen Informationen**. Darin werden der Umfang der Notfallmaßnahmen beschrieben und die Verantwortlichkeiten der Mitarbeiter bei der Umsetzung des Plans aufgeführt.
Eine **Risikoanalyse** bewertet die Gefahren, die mit einem IT-Notfall einhergehen können und beschreibt die Maßnahmen, die ergriffen werden müssen, um diese zu minimieren. Eine detaillierte **Beschreibung der Notfallmaßnahmen** wird ebenfalls im Plan aufgeführt, wie beispielsweise die Abschaltung von Systemen, die Verlagerung von Arbeitsplätzen oder die Einleitung von Reparaturmaßnahmen. Sie dienen dazu, einen **Notbetrieb** sicherzustellen und mögliche Umgehungen (Workarounds) zu gewährleisten. Ein **Wiederherstellungsplan** ist ebenfalls Teil des IT-Notfallplans und umfasst die Verfahren zur Nutzung von Backups und Reaktivierung von Systemen. Der **Kommunikationsplan** legt fest, wie sich die Mitarbeiter während des Notfalls miteinander und mit anderen Interessengruppen wie Kunden oder Partnern in Verbindung setzen. Des Weiteren sind **Alarmketten** und -pläne wichtige Elemente eines solchen Plans.
Ein Verzeichnis von notfallrelevanten **Zugangsdaten** ist ebenfalls enthalten, um einen schnellen und sicheren Zugriff auf relevante Systeme zu gewährleisten. Zudem beinhaltet der IT-Notfallplan auch **Vertretungsregelungen**, um sicherzustellen, dass bei Abwesenheit von Schlüsselpersonen weiterhin angemessen auf Notfälle reagiert werden kann. Schließlich gibt es auch einen **Schulungs- und Testplan**, der die Vorbereitung der Mitarbeiter sowie den Ablauf von Tests zur Überprüfung der Wirksamkeit des Plans beschreibt.

Cyber-Sicherheitsrat Deutschland e.V.

Welche Chancen gibt es?

Unternehmen können sich in der Regel keine längere Ausfallzeit erlauben, da dies schnell zu Liquiditätsengpässen führt. Ein IT-Notfallplan kann dazu beitragen, die **Ausfallzeiten zu minimieren**, indem schnell auf Probleme reagiert wird und die erforderlichen Maßnahmen ergriffen werden, um den Geschäftsbetrieb des Unternehmens aufrechtzuerhalten.

Er kann dazu beitragen, die Systeme und **Daten des Unternehmens zu schützen**, indem Maßnahmen ergriffen werden, um Cyberangriffe zu verhindern oder darauf zu reagieren und die Integrität von Daten und Systemen zu gewährleisten. Indem sich die Belegschaft im Voraus mit potenziellen Gefahren auseinandersetzt, hilft der Notfallplan dabei, **Risiken zu erkennen und durch vorausschauende Maßnahmen zu verhindern**.

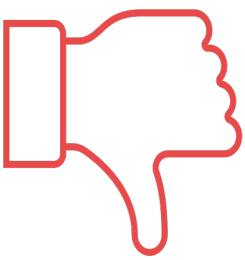
Nicht zuletzt dient er auch der **Sicherheit der Mitarbeiter und Kunden**, um sie und ihre persönlichen Daten zu schützen.

Welche Risiken gibt es?

Es handelt sich bei der Erstellung eines IT-Notfallplans nicht um eine einmalige Angelegenheit. Dieser muss vielmehr **regelmäßig aktualisiert** werden, um sicherzustellen, dass er relevant und wirksam bleibt. Dies erfordert **Zeit und Ressourcen**.

Ein IT-Notfallplan kann sehr komplex sein und erfordert die Beteiligung von vielen verschiedenen Abteilungen und Mitarbeitern, um seine Wirksamkeit zu gewährleisten. Deswegen ist es besonders wichtig, **klare Zuständigkeiten** zu definieren.

Ein IT-Notfallplan kann nicht alle potenziellen Risikofaktoren abdecken, mit denen ein Unternehmen oder eine Organisation möglicherweise konfrontiert wird. Es ist wichtig, sicherzustellen, dass der Plan so umfassend wie möglich ist und gleichzeitig einen **Rahmen für unvorhergesehene Ereignisse** bietet.



Wem nutzt ein IT-Notfallplan?

Ein IT-Notfallplan ist für Unternehmen und Organisationen jeglicher Größe und Art eine **wichtige Sicherheitsmaßnahme**. Ein solcher Plan bildet die Grundlage für die Implementierung weiterer Sicherheitsprozesse, beispielsweise eines Information Security Management System (**ISMS**), oder bei der Erfüllung von **Zertifizierungen** wie der ISO27001.
Er hilft dabei, auf potenzielle IT-Notfälle vorbereitet zu sein, die die Geschäftstätigkeit beeinträchtigen oder zum Stillstand bringen könnten.

Fazit

Insgesamt ist die Erstellung eines IT-Notfallplans für Unternehmen und Organisationen von **entscheidender Bedeutung für ein effektives Risikomanagement**.
Ein IT-Notfall kann eine Vielzahl von Ursachen haben, aber ein gut durchdachter Plan kann dazu beitragen, dessen Auswirkungen zu minimieren und den **Geschäftsbetrieb aufrechtzuerhalten**. Es ist wichtig, sicherzustellen, dass der Plan regelmäßig aktualisiert wird und die Verantwortlichkeiten klar definiert sind.

Cyber-Sicherheitsrat Deutschland e.V.