Handbuch
IT-Notfallmanagement

Version x.x vom 00.00.0000

Diese Vorlage dient lediglich als Beispiel und beinhaltet nicht den kompletten Inhalt.

Für eine umfassende Beratung kontaktieren Sie uns gerne.

– Klassifizierung –

Freigabe

	Datum	Unterschrift
Erstellt von: Steve Secure Security Manager IS-FOX GmbH		
Genehmigt: Jesse Chief Vors. der Geschäftsführung IS-FOX GmbH		

Versionshistorie

Version	Datum	Autor	Änderungen
x.x	00.00.0000	Steve Secure	Erstellung Erstversion

Mitgeltende Unterlagen

Dokument	Veröffentlichung

Inhaltsverzeichnis

1 Allgemeines

1.1 Zielgruppe & Geltungsbereich

Dieses Handbuch ist für sämtliche Mitarbeiter der IS-FOX GmbH (ISF) mit allen Organisationseinheiten, Tochterunternehmen und Niederlassungen verbindlich, die an der Vorbereitung und Umsetzung von Maßnahmen im Bereich IT-Notfallmanagement sowie der Bewältigung von IT-Notfällen beteiligt sind.

1.2 Zweck

Das vorliegende Handbuch dient als Rahmenwerk zur Vorbereitung und Reaktion auf Ereignisse und Situationen in Bezug auf IT-Sicherheit, in denen die präventiven Maßnahmen das Eintreten eines Notfalls nicht abwenden konnten. Es soll ebenfalls Anwendung finden bei akuten Bedrohungen, die unverzügliche Aktivitäten erfordern, da ein Schadenseintritt bei ISF mit hoher Wahrscheinlichkeit zu erwarten ist. Auch, wenn dieses Dokument ausschließlich Fälle mit Bezug auf IT-Sicherheit adressiert, so ist die Nomenklatur bewusst so neutral gewählt, dass dieses Dokument als Vorlage für andere Notfall-Szenarien genutzt werden kann.

Das Ziel besteht darin, mit Hilfe einer funktionierenden Aufbau- und Ablauforganisation die nur bedingt vorhersehbaren Vorfälle möglichst zielgerichtet, zügig, nachhaltig und unter weitgehender Vermeidung zusätzlicher Beeinträchtigungen zu bearbeiten und soweit möglich zu beseitigen.

Das IT-Notfallmanagement stellt dabei die Ebene zwischen der routinemäßigen Behandlung von (Sicherheits-)Vorfällen (sog. Störungen) mit nur geringen Auswirkungen bis hin zu Major Incidents mit Security Bezug und Krisenfällen mit erheblichen Auswirkungen (siehe Kap. 1.3 Definitionen) dar.

Die im Kapitel 2 (Vorbereitung für IT-basierte Notfälle) beschriebenen Maßnahmen sind darauf ausgerichtet, bestmögliche Vorkehrungen für das Eintreten eines Notfalls zu treffen. Demgegenüber soll mit dem in Kapitel 3 (Management eines IT-basierten Notfalls) aufgeführten Prozessablauf Hilfestellungen bei der tatsächlichen Bewältigung eines Notfalls bzw. der Durchführung einer Übung gegeben werden.

1.3 Definitionen

Die nachstehenden Definitionen gelten für alle relevanten Bereiche bzw. auslösenden Ursachen. Ereignisse in Bezug auf IT-Sicherheit stellen somit eine (mögliche) Teilmenge dar.

Die Regelungen in Bezug auf IT-Notfallmanagement werden auch für sich daraus entwickelnde Krisensituationen angewendet, solange hierfür keine übergeordneten Regelungen (unternehmensweites Krisenmanagement) etabliert sind.

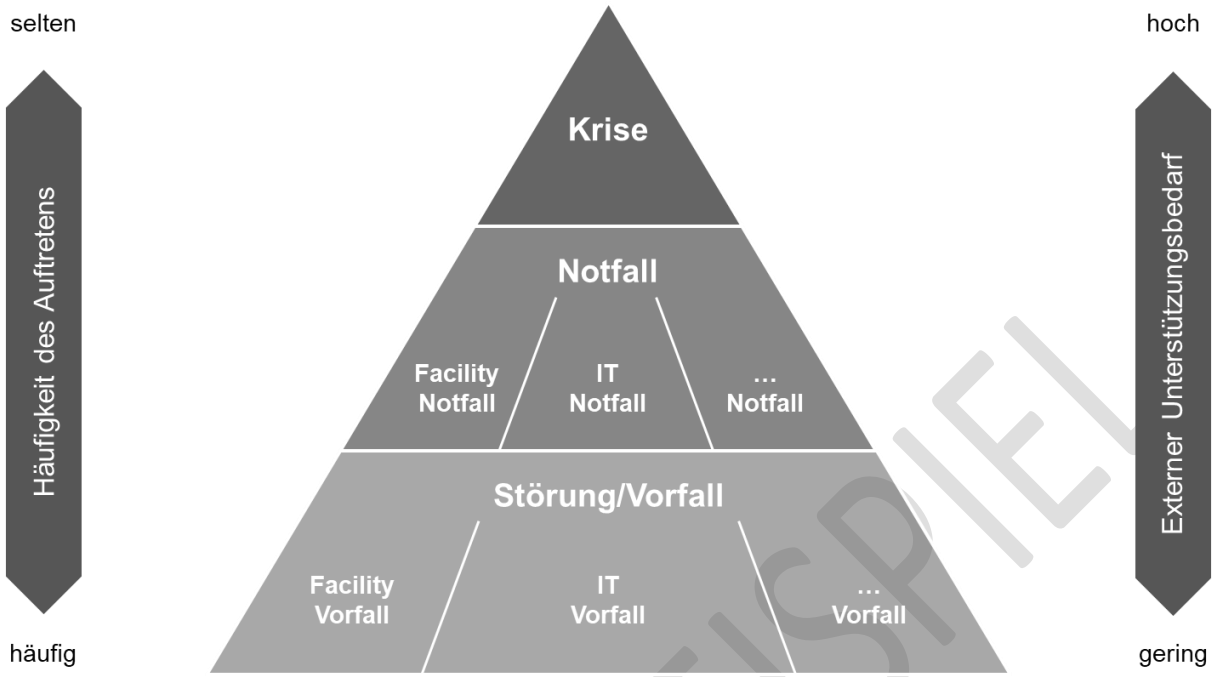

Abbildung 1: Eskalationsstufen von Störungen

Krise:

Unerwartetes Ereignis oder unerwartete Situation, die zu einer Unterbrechung von Geschäftsprozessen oder einer Beeinträchtigung der Geschäftstätigkeit bzw. des Ansehens von ISF oder Auswirkungen auf die körperliche und/oder geistige Unversehrtheit von Personen hat. Die durch eine Krise entstehenden Schäden sind aus Sicht des Unternehmens bzw. der betroffenen Personen als erheblich und/oder nicht nur von kurzfristiger Dauer einzustufen. Für die Bewältigung der Krise stehen aufgrund der Einmaligkeit der Konstellation nur bedingt im Voraus festgelegte Verfahren und Dokumentationen zur Verfügung. Zur Lagebewertung, Analyse von Ursachen und Lösungsmöglichkeiten sowie für die Planung und Umsetzung von Interimslösungen wird eine interdisziplinär zusammengesetzte Krisenorganisation benötigt, die für die Dauer der Krise (mehrere Stunden bis hin zu Wochen oder Monaten) etabliert wird. Zusätzlich kann die Einbindung externer Kräfte zur Schadensbegrenzung, Ursachenermittlung sowie Krisenbewältigung sinnvoll und erforderlich sein.

Katastrophen stellen einen Sonderfall von Krisen dar, indem sie zeitlich und örtlich kaum begrenzbar sind und großflächige Auswirkungen auf Menschen, Infrastrukturen und/oder Werte haben. Die Bewältigung einer Katastrophe erfordert die Unterstützung externer Kräfte und steht häufig unter Einbindung oder Leitung einer externen Katastrophenschutzorganisation.

Notfall:

Unerwartetes Ereignis oder unerwartete Situation mit erheblichen, jedoch zeitlich bzw. unter Umständen örtlich/regional absehbaren Auswirkungen, die nicht im Rahmen des Tagesgeschäftes bzw. des Störungsmanagements beseitigt werden kann. Die Ursachenermittlung und Behandlung erfordern die kurzfristige Bereitstellung entsprechender Ressourcen, möglicherweise aus unterschiedlichen Bereichen sowie evtl. externer Spezialisten. Im Rahmen der Analyse des Notfalls ist die Erfordernis zur Eskalation als Krise zur prüfen.

Störung:

Ereignis oder Situation, in der Prozesse oder Ressourcen von ISF nicht wie vorgesehen funktionieren oder die Auswirkungen auf die Unversehrtheit von Personen hat. Die durch eine Störung entstehenden Schäden sind aus Sicht des Unternehmens bzw. der betroffenen Personen als gering und/oder zeitlich absehbar einzustufen. Für die Störungsbehebung reichen im Regelfall Ressourcen aus dem Tagesgeschäft aus.

Bereit, Ihr ISMS aufzubauen?

Lassen Sie uns gemeinsam starten!

Kontaktieren Sie uns jetzt für eine individuelle Beratung und Unterstützung.