ALARM
Awareness Labor KMU Informationssicherheit

# Niederschwelliges Sicherheitskonzept zum Thema Incident Response

für Geschäftsführung und IT-Verantwortliche

Thinking Objects GmbH

**Stand:** Mai 2023

IT-Sicherheit IN DER WIRTSCHAFT

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Das vorliegende **niederschwellige Sicherheitskonzept für KMU** ist eines von insgesamt sieben Sicherheitskonzepten, die im dreijährigen Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ der Technischen Hochschule (TH) Wildau verfasst werden.

Das Projekt „ALARM Informationssicherheit“ wird vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) gefördert.

## Projektlaufzeit

01.10.2020 – 30.09.2023

Das niederschwellige Sicherheitskonzept für KMU basiert auf Ergebnissen der im Projekt „ALARM Informationssicherheit“ durch den Unterauftragnehmer Thinking Objects (TO) GmbH in Pilotunternehmen durchgeführten „Vor-Ort-Angriffen“.

Das diesem Sicherheitskonzept zugrundeliegende Vorhaben wird mit Mitteln des Bundesministeriums für Wirtschaft und Klimaschutz unter dem Förderkennzeichen 01MS19002A gefördert.

Das Mittelstand-Digital Netzwerk bietet mit den *Mittelstand-Digital Zentren*, der Initiative *IT-Sicherheit in der Wirtschaft* und *Digital Jetzt* umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.it-sicherheit-in-der-wirtschaft.de.

# Inhaltsverzeichnis

# 1 Einleitung

Incident-Response Maßnahmen bezeichnen hier den Umgang mit IT-Sicherheits-Notfällen.

Im aktuellen Dokument wollen wir vor allem beschreiben, wie man mit Notfällen umgeht, die die Existenz des Unternehmens bedrohen können. Durch die in den letzten Jahren stark gestiegene Abhängigkeit aller Prozesse von der IT werden Hacker-Angriffe immer häufiger zu einer Bedrohung für das ganze Unternehmen.

Für kleinere sicherheitsrelevante Ereignisse helfen entsprechend festgelegte und standardisierte Prozeduren, deren Definition ist aber nicht Bestandteil dieses Dokumentes.

# 2 Vorbereitung

Der wichtigste Teil im Bereich der Incident-Response-Maßnahmen ist die Vorbereitung.

Hier ist der Vergleich mit der Feuerwehr sehr passend. Es werden sowohl personelle Ressourcen wie auch Technik, beispielsweise Fahrzeuge, vorgehalten und es finden regelmäßige Übungen statt, damit im Notfall jeder Handgriff sitzt. Aber auch hier gilt: kein Notfall ist wie der andere, das heißt die Reaktion auf die konkrete Notfall-Lage erfordert eine entsprechende Improvisation auf Basis der geübten Grundtechniken.

Notfall-Management im Bereich der IT-Security ist sehr ähnlich, viele Dinge müssen vorbereitet werden, um sie im Notfall tatsächlich einfach abrufen zu können.

## 2.1 Verantwortlichkeiten und Kompetenzen

Es ist wichtig vorab alle Verantwortlichkeiten und Kompetenzen zu klären und zu dokumentieren.

Wer stellt den IT-Notfall fest? Gibt es Unterschiede zwischen Bürozeiten, Nachtzeiten oder dem Wochenende und Feiertagen?

Wer darf die Abschaltung von Systemen durchführen? Wer darf Dienstleister beauftragen, die bei der Eindämmung des Vorfalls helfen können?

Wer eine Cyber-Versicherung abgeschlossen hat, sollte die Vorgaben dieser Police im Rahmen der Vorbereitung berücksichtigen.

## 2.2 Helfer und Dienstleister

Liegt ein IT-Sicherheitsvorfall vor, muss schnellstmöglich ein Krisenstab zusammengerufen werden. Die Zusammensetzung muss vorab geklärt sein. Wer aus der firmeneigenen IT-Organisation ist neben der Geschäftsführung Teil des Krisenstabes? Wer von meinen üblichen IT- und IT-Sicherheits-Dienstleistern ist Bestandteil des Krisenstabes? Gibt es hierfür einen entsprechenden Plan, wie diese auch außerhalb der Geschäftszeiten erreicht werden können?

Manchmal schreiben die Policen der Cyber-Versicherung vor, dass nur entsprechend akkreditierte Dienstleister im Schadensfall hinzugezogen werden dürfen. Dies muss vorab geprüft und berücksichtigt werden.

## 2.3 Notfall-IT

Um bei einem Totalverlust der IT-Zugriff auf Notfall-Pläne und Dokumentation zu haben, empfehlen wir einen, vom Active Directory unabhängigen Laptop als Notfall-Laptop vorzuhalten.

Hierauf sollte die entsprechende Dokumentation und Kontaktdaten für den Fall eines Falles als unabhängige Dokumente vorgehalten werden. Speziell wenn ansonsten beispielsweise Telefonnummern und E-Mail-Adressen alle aus den Online-Systemen stammen, sind diese Systeme im Falle des IT-Notfalls nicht verfügbar. Auch eine Kopie der wichtigsten Passwörter kann im Fall einer Wiederherstellung der Systeme von Grund auf notwendig sein. Das

gesamte System muss entsprechend verschlüsselt sein, um im Falle des Abhandenkommens keine Bedrohung für die IT-Systeme dazustellen.

Dieses System muss regelmäßig, je nach Komplexität der IT-Landschaft monatlich oder quartalsweise, mit aktualisierten Dokumenten versorgt werden. Auch die entsprechenden Updates des Betriebssystems sind durchzuführen.

Ebenfalls ist zu prüfen, ob vielleicht diese Informationen auch alle beim IT-Dienstleister des Vertrauens vorgehalten werden können. Dann ist nur sicherzustellen, dass man auch selbst in einem solchen Notfall Zugriff auf diese Information erhält.

## 2.4 Kommunikation

Im Falle eines IT-Sicherheitsnotfall sind, je nach Zeitpunkt des Ereignisses, Kunden, Partner und auch Beschäftigte zu Informieren.

Wir empfehlen hier entsprechende Möglichkeiten vorher durchzuspielen und zu verproben.

Es ist denkbar, dass der Web-Auftritt noch funktioniert, weil er unabhängig bei einer Agentur gehostet wird. Wer kann dort eine kurzfristig eine Meldung veröffentlichen? Oder gibt es einen Notfall-Webserver, der Inhaltlich vom Krisenstab gepflegt werden kann und auf den jeder Zugriff des eigentlichen Web-Auftrittes umgeleitet wird? So können vor allem Kunden und Partner erreicht werden.

Die eigenen Mitarbeiterinnen und Mitarbeiter kann man mit einem Aushang am Werkstor benachrichtigen, möglicherweise aber auch über andere Wege, um zu verhindern, dass diese im Falle des IT-Notfalls überhaupt zur Arbeit erscheinen.

## 2.5 Backup

Wichtigster Baustein in allen Wiederherstellungsszenarien ist ein Backup. Bei allen Totalverlusten sei es durch Feuer oder durch Cyber-Angriffe ist ein extern gelagertes Offline-Backup oftmals die letzte Rettung. Auch ein entsprechend abgesichert Cloud-Backup kann eine Möglichkeit sein, Daten wiederherzustellen.

Da extern gelagerte Backups grundsätzlich verschlüsselt werden sollten, muss sichergestellt werden, dass auch eine Entschlüsselung und Wiederherstellung der Backups beispielsweise bei einem logischen Totalverlust des Backup-Servers möglich ist. Dazu sollte eine entsprechend aufbewahrte Kopie des Schlüssels existieren.

# 3 IT Sicherheitsnotfall

Im Falle eines Falles müssen die definierten Prozesse greifen und umgesetzt werden. Der Sicherheitsnotfall muss ausgerufen werden, der Krisenstab muss zusammenkommen und es muss eine Bestandsaufnahme durchgeführt werden. Diese ersten Schritte erfolgen am besten anhand der verprobten Checklisten, die in der Vorbereitungsphase erstellt wurden.

Sind die ersten Abwehr- und Eindämmungsmaßnahmen entsprechend umgesetzt, der Schaden festgestellt und der Weg des Cyber-Einbruchs geklärt, ist das Vorgehen für die Wiederherstellung bzw. der Wiederaufbau festzulegen. Hier sind von der Reparatur der bestehenden Umgebung über eine Wiederherstellung aus den Backups bis hin zum kompletten Neu-Aufsetzen der Umgebung alle Optionen denkbar. Wichtig ist, dass sichergestellt werden kann, dass die Kriminellen keinen Zugriff mehr auf die Infrastruktur haben. Darum muss geklärt werden, wie die Angreifer auf die Systeme gekommen sind, um nicht entsprechend kompromittierte Benutzerkonten aus dem Backup wiederherzustellen oder Software-Versionen mit den gleichen Sicherheitslücken erneut zu installieren.

Nach jedem nennenswerten IT-Sicherheitsnotfall sind, nachdem der Betrieb wieder läuft, auch entsprechende Lessons-Learnd durchzuführen, um aus der Arbeit des Krisenstabes für den nächsten IT-Sicherheitsnotfall zu lernen.

Technische Hochschule Wildau
Technical University of Applied Sciences

Thinking Objects

**Thinking Objects GmbH**
Lilienthalstraße 2/1
70825 Korntal-Münchingen

Tel. +49 711 88770400
Fax. +49 711 88770449
**www.to.com**