Erste Hilfe

bei einem

IT-Sicherheitsvorfall

Version: v1.2 (Oktober 2023)

INVASE
SECURITY IN BUSINESS

Zielsetzung

IT-Sicherheitsvorfälle nehmen an Häufigkeit und Intensität zu, die Wahrscheinlichkeit betroffen zu sein ist entsprechend hoch. Und dennoch: Die Mehrheit der deutschen Unternehmen ist nicht ausreichend auf IT-Sicherheitsvorfälle vorbereitet. Solche Vorbereitungen sind mit Aufwänden verbunden – um die Zeitspanne bis zu etablierten Vorkehrungen zu überbrücken, soll dieses Dokument bei einem IT-Sicherheitsvorfall unterstützen.
Bitte beachten Sie, dass diese Checkliste keine fundierten, individuell auf Ihr Unternehmen zugeschnittene Vorkehrungen ersetzen kann.
Die Vorbereitung auf einen Vorfall und die Fähigkeiten einem solchen Vorfall zu begegnen, sind unersetzlich.

Diese Checkliste wird fortlaufend aktualisiert. Die stets neueste Version finden Sie unter diesem Link:

https://www.invase.io/erste-hilfe-bei-einem-it-sicherheitsvorfall

Über uns

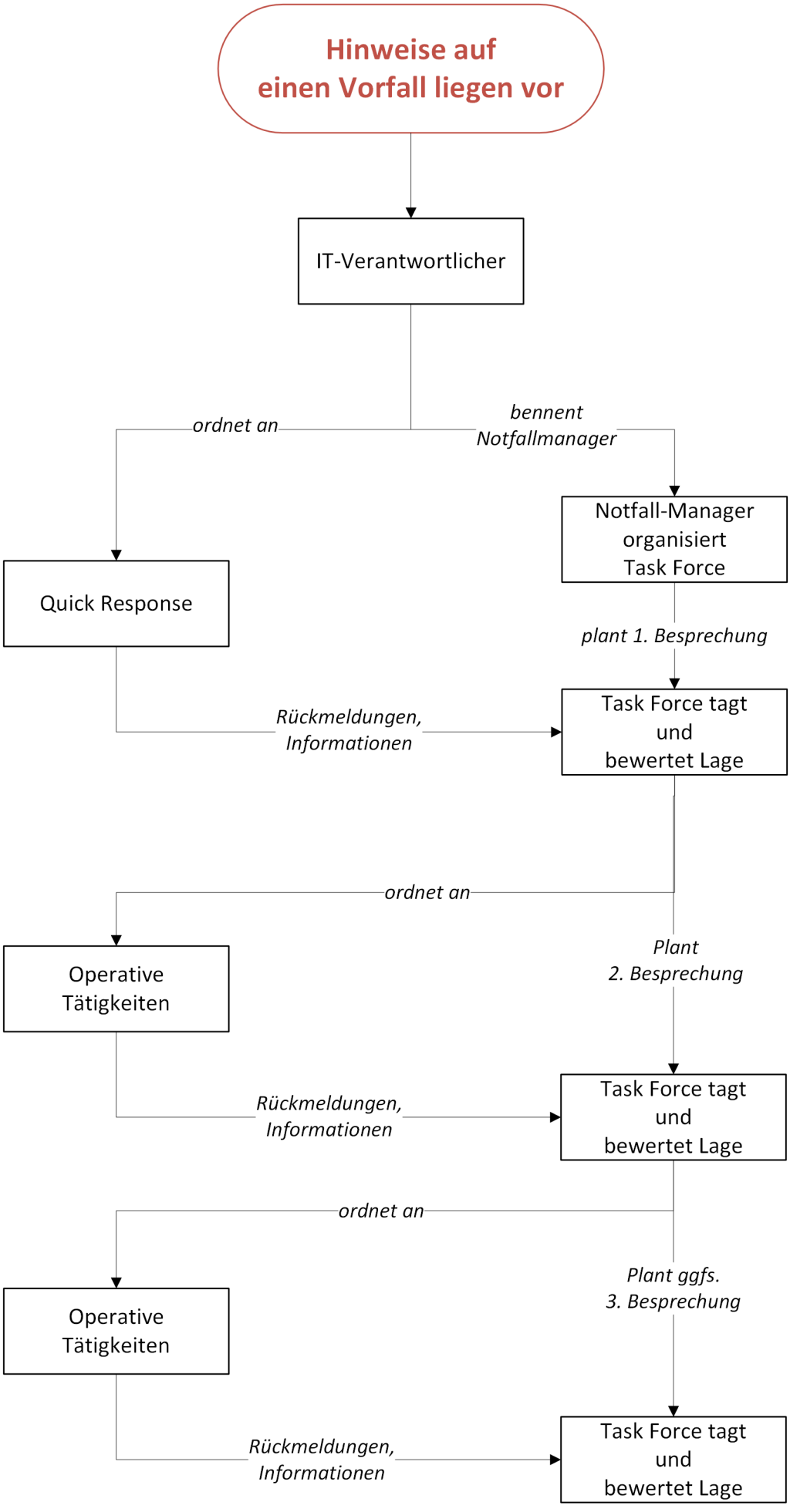
INVASE steht für Information, Value und Security. Unser Schwerpunkt liegt in der ganzheitlichen Etablierung der Informationssicherheit auf allen Ebenen unserer Kundenunternehmen, unabhängig ihrer Branchen, für eine belastbare Unternehmenssicherheit.

Ziel ist stets der effiziente Schutz von Unternehmenswerten – Security in Business.

Dabei bringen wir Erfahrungswerte, insbesondere aus kritischen Umfeldern wie Finanzinstituten, Versicherungen, Telekommunikationsunternehmen, Behörden, Katastrophenschutz, Militär- und IT-Dienstleister mit ein. Unser Leistungsangebot reicht von der Prävention bis zur Nachbehandlung von Sicherheitsvorfällen, Risikomanagement, ISMS, Datenschutz und Governance.

Unser Beratungsportfolio finden Sie unter folgendem Link:

https://www.invase.io/beratungsportfolio-invase-io


Hinweise auf
einen Vorfall liegen vor
IT-Verantwortlicher
ordnet an
bennent
Notfallmanager
Quick Response
Notfall-Manager
organisiert
Task Force
plant 1. Besprechung
Rückmeldungen,
Informationen
Task Force tagt
und
bewertet Lage
ordnet an
Operative
Tätigkeiten
Plant
2. Besprechung
Rückmeldungen,
Informationen
Task Force tagt
und
bewertet Lage
ordnet an
Operative
Tätigkeiten
Plant ggfs.
3. Besprechung
Rückmeldungen,
Informationen
Task Force tagt
und
bewertet Lage

Grundregeln für unmittelbare Reaktionen

Ruhe bewahren, Kontrolle behalten

Hektische Reaktionen oder unbedachte Handlungen verschlimmern die Lage eher, als dass sie helfen.

Task Force bilden

Benennen Sie für diesen Vorfall einen **Notfall-Manager,** dieser steuert und koordiniert, arbeitet jedoch **nicht** operativ.
Sammeln Sie interne Experten mit folgenden Schwerpunkten, um die Sachlage zu ermitteln und Gegenmaßnahmen einzuleiten:

- Infrastruktur/Netzwerke (insb. Schwerpunkte wie z.B. Routing, Firewalls,)
- Zentrale IT-Services (IAM, Fileserver, E-Mail-Server, etc.)
- Client-Management (Verwaltung von Endgeräten und Group Policies)
- (Krisen-)Kommunikation nach Intern und Extern
- Datenschutz / Compliance / Recht
  (Einbindung Staatsanwaltschaft oder Polizei, ggfs. Meldepflichten an Behörden o.ä.)

Lage richtig einschätzen

Sammeln und ordnen Sie innerhalb der Task Force alle vorliegenden Informationen. Trennen Sie so weit möglich zwischen Fakten und Vermutungen, unterscheiden Sie zwischen Symptomen und tatsächlichen Ursachen. Sollten Indizien vorliegen, die für Folgeaktivitäten kritisch sind, muss der Notfall-Manager auf Basis der Experten-meinungen entscheiden, ob diesen nachgegangen werden soll, um belastbare Erkenntnisse zu erlangen.

Schadensbegrenzung hat Priorität

Es ist wichtig, dass die Schadensursache begrenzt wird, bevor Dienste wiederhergestellt werden. Besonders bei Vorfällen mit Schadsoftware kann diese weiter um sich greifen. Ein brennendes Haus muss gelöscht werden, bevor man es in Stand setzt.

Dienstleister hinzuziehen, falls vorhanden Cyber-Versicherung informieren

Spezialisierte Dienstleister für Sicherheitsvorfälle helfen bei akuten Situationen. Gute Cyber-Versicherungen können geeignete Dienstleister direkt beauftragen und zur Unterstützung beistellen.

Checkliste

Quick Response

- [ ] Sachlage durch IT-Verantwortlichen bewertet.
(Liegt ein Vorfall vor? Sind geschäftskritische Prozesse oder Informationen gefährdet?)

- [ ] Backup-Systeme vom Netzwerk getrennt, Integrität der Backups geprüft. (Insbesondere für Disaster Recovery)

- [ ] Befallene / betroffene Systeme und/oder Netzwerkbereiche isoliert.

- [ ] Falls erforderlich: Internetverbindung für betroffene Systeme getrennt;
(Ggfs. komplette Isolierung aller Systeme vom Internet; unternehmenskritische System herunterfahren).

- [ ] Schadensbegrenzung verifiziert.

- [ ] Vorfall bisher so weit wie möglich nachvollzogen und dokumentiert.

- [ ] Privilegierte Accounts (z.B. Admin-Accounts) und deren Aktivitäten werden überwacht.

Bildung der Task Force

- [ ] Notfall-Manager benannt.
- [ ] Task-Force gebildet.
- [ ] Interne Kommunikation geklärt und erfolgt.
  (inkl. Melde- und Eskalationswege)
- [ ] Informationen zur ersten Lageeinschätzung gesammelt.
- [ ] Prüfung der zur Verfügung stehenden Ressourcen.
  (Sind ggfs. mehr Menschen oder externe Expertise notwendig?)
- [ ] Falls notwendig: IT-(Sicherheits-)Dienstleister alarmiert.
- [ ] Falls vorhanden: Cyber-Versicherung informiert und nach Unterstützung erkundigt.
- [ ] Log-Dateien, System-/Anwendungs-Protokolle, Notizen, Screenshots gesichert.
- [ ] Nicht benötigte privilegierte Accounts deaktiviert.

1. Besprechung der Task Force

- [ ] Sachlage simpel und verständlich beschrieben und allen Teilnehmern kommuniziert.
- [ ] Betroffene Systeme und Daten aufgelistet. (insbesondere Datenschutzrelevante Daten)
- [ ] Alle weiteren notwendigen Aktivitäten gesammelt.
- [ ] Aktivitäten priorisiert und delegiert.
- [ ] Sammlung weiterer Daten, Informationen, Indizien über anomale Aktivitäten. (Hohe Rechenleistungen, hohe Netzwerklast, abnorme Berechtigungen einzelner Nutzer etc.)
- [ ] Weitere Vorgehen dokumentiert und begründet.
- [ ] Zeitpunkt und Teilnehmerkreis der 2. Besprechung geplant. (Idealerweise gleicher Teilnehmerkreis.)

2. Besprechung der Task Force

- [ ] Präsentation der aktuellen Sachlage, Zwischenerfolge/Misserfolge, offener Aktivitäten.
- [ ] Kommunikation mit Fachbereichen koordiniert, um geschäftskritische Prozesse zu identifizieren.
- [ ] Priorisierung der Wiederherstellung definiert.
  (z.B. zentrale IT-Services, Kern-Netzwerke, kritische Business-Anwendungen, etc.)
- [ ] Umgang mit kompromittierten Systemen geklärt.
  (z.B. Löschung; oder Aufbewahrung zwecks forensischer Untersuchung)
- [ ] Vorgehen dokumentiert und begründet.
- [ ] Notwendigkeit, Zeitpunkt, Teilnehmerkreis der 3. Besprechung geplant.
  (idealerweise erweiterter Teilnehmerkreis,
  plus Ansprechpartner der geschäftskritischen Fachbereiche)

3. Besprechung der Task Force

- [ ] Präsentation der aktuellen Sachlage, Zwischenerfolge/Misserfolge, offener Aktivitäten.
- [ ] Offene Aktivitäten aufgelistet, priorisiert, delegiert.
- [ ] Wiederherstellung der kritischen Systeme initiiert, durch Fachbereiche unterstützt.
- [ ] Interne Kommunikation definiert und delegiert.
- [ ] Ggfs. externe Kommunikation vorbereitet.
  (Zielgruppe: Behörden, Kunden, IT-Dienstleister, Presse, etc.)
- [ ] Entscheidungen und Vorgehen dokumentiert und begründet.
- [ ] Notwendigkeit, Zeitpunkt, Teilnehmerkreis einer weiteren Besprechung geplant;
  Agenda: Punkte der 3. Besprechung wiederholen.

4. Lessons Learned - Planung von Aktivitäten

(Nach erfolgreicher Wiederherstellung)

- [ ] Dokumentiertes Vorgehen sammeln und auswerten.
- [ ] Entscheidung über forensische Nachuntersuchung des Vorfalls. (z.B. Klärung auf weiterhin bestehende Kompromittierung)
- [ ] Erkenntnisse spezifizieren und Verbesserungen definieren.
- [ ] Notfallpläne, auch mit Fachbereichen, erstellen.
- [ ] Business Continuity Management anstreben.
- [ ] Maßnahmen zur Resilienz der IT-Landschaft treffen, Detektions- und Abwehrmöglichkeiten durch Experten prüfen lassen.
- [ ] Cyber-Resilienz als strategisches Unternehmensziel aufnehmen.

Vorfälle bewältigen

Ein IT-Sicherheitsvorfall ist in den meisten Fällen geprägt von Mangelverwaltung: Es fehlen Informationen, Zeit und genügend (erprobtes) Personal. Insbesondere, wenn keine nennenswerten Vorkehrungen getroffen wurden, ist die Chance gering den Vorfall ohne großen Schaden zu überstehen. Schnell wird aus einem Vorfall ein Desaster der ohne fremde Hilfe nicht mehr beherrschbar wird.
Deshalb ist es unabdingbar zu jeder Zeit Ruhe zu bewahren und zwischen belastbaren Erkenntnissen und Vermutungen strikt zu unterscheiden. Indizien werden auch im Katastrophenfall Teil der Entscheidungsgrundlage sein, weil auch dann nur mit vorliegenden Informationen gearbeitet werden kann.

Hektik, Chaos und Emotionen führen unweigerlich zu Kontrollverlust.

Vorbereitung ist unersetzlich

Die Vorbereitung auf einen IT-Sicherheitsvorfall ist unumgänglich, und der Aufwand ist beträchtlich. Jedoch sind die wirtschaftlichen Folgen unvorbereitet einem Vorfall entgegenzustehen deutlich höher. Zumindest auf *wahrscheinliche* Vorfälle muss sich jedes Unternehmen vorbereiten. Auch eine Cyber-Versicherung kann im Schadensfall mit Experten für DFIR (Data Forensics and Incident Response) aushelfen, sodass im akuten Schadensfall Experten hinzugezogen werden können, die bei der Bewältigung unterstützen. Fast alle Punkte unserer Checkliste können ganz oder teilweise vorbereitet werden. Planspiele und realistische Übungen geben wertvolle Hinweise auf Unzulänglichkeiten in den Abwehrmechanismen.

Externe Expertise

Die gute Nachricht: Experten für IT-Sicherheitsvorfälle gibt es glücklicherweise hinreichend. Diese können auch im akuten Vorfall hinzugezogen werden, sowohl aus der Privatwirtschaft als auch über Behörden.

Kontaktdaten

BSI-Notfall-Hotline:
TEL: 0800 - 274 1000 (Service-Zeiten: 8:00 Uhr bis 18:00 Uhr)

Zentrale Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft:
https://www.allianz-fuer-cybersicherheit.de/dok/12430116

Für weitere Informationen zu Beratungen, Vorbereitungen oder Schulungen kontaktieren Sie uns gerne:

TEL: +49 (0)2153 97041 60 E-Mail: contact@invase.io

https://www.invase.io

Disclaimer / Haftungsbeschränkung
Die Inhalte dieses Dokumentes wurden mit größtmöglicher Sorgfalt recherchiert und erstellt. Fehler im Bearbeitungsvorgang sind dennoch nicht auszuschließen. Hinweise und Korrekturen senden Sie bitte an

✉ contact@invase.io

Jegliche Haftung für Schäden, Beeinträchtigungen, Datenverluste, entgangene Gewinne oder anderweitiger Konsequenzen, die konkret, mittelbar oder unmittelbar im Zusammenhang mit der Benutzung dieses Dokumentes entstehen, wird ausgeschlossen, soweit diese nicht auf Vorsatz oder grober Fahrlässigkeit beruhen. Dies gilt gleichsam für die Verletzung des Körpers, des Lebens oder der Gesundheit. Dieses Dokument dient als Leitfaden und Orientierungshilfe und ersetzt keine Vorbereitung auf IT-Sicherheitsvorfälle. Unternehmen jeder Art unterliegen u.a. Verpflichtungen sich sorgfältig, angemessen und wirksam auf IT-Sicherheitsvorfälle oder ähnlicher Beeinträchtigungen vorzubereiten. Dieses Dokument entbindet nicht von derartigen Verpflichtungen. Eine sach- und fachgerechte Vorbereitung und (Nach-)Behandlung von IT-Sicherheitsvorfällen bedarf professioneller Kenntnisse, die nicht durch die Inhalte oder Anwendung dieses Dokumentes ersetzt werden können. Wir begründen durch die Bereitstellung dieser Informationen kein Vertragsangebot über Auskünfte, Beratung oder ähnliche Vertragsbeziehungen.
Alle aus oder in Verbindung mit dieser Website entstehenden Rechtsstreitigkeiten unterliegen ausschließlich deutschem Recht. Gerichtsstand ist der Sitz der Gesellschaft INVASE Heimers & Schild GbR.

Urheberrecht

Impressum

INVASE.IO – Security in Business
INVASE – Information | Value | Security

INVASE Heimers & Schild GbR

Briefanschrift	Düsseldorfer Str. 14 41334 Düsseldorf
Telefon	+49 (0)2153 97041 60
E-Mail	contact@invase.io
Internetpräsenz	https://www.invase.io