Der Sicherheitsvorfall

Die Unternehmens-IT ist bereits bei vielen Unternehmen der Dreh- und Angelpunkt der internen und externen Kommunikation, Organisation sowie der Steuerung von Prozessen. Im Zuge der Digitalisierung wird der Anteil der elektronischen Datenverarbeitung noch weiter zunehmen. Daher ist es sehr wichtig, dass die interne IT (sowohl im Büro als auch in der Produktion) reibungslos funktioniert. Durch eigen- aber auch fremdverursachte Fehler kann diese Funktionsfähigkeit beeinträchtigt werden.

Wann wird von einem Sicherheitsvorfall gesprochen?

Als Sicherheitsvorfall wird in einem Unternehmen ein Ereignis bezeichnet, das die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen, Geschäftsprozesse, IT-Dienste, IT-Systeme oder IT-Anwendungen mit hohem oder sehr hohem Schutzbedarf derart beeinträchtigt, dass ein großer Schaden für das Unternehmen / Behörde / Kunden / Geschäftspartner entstehen kann. (BSI Grundschutz M 6.122)

Wie kann ich die Ursachen von einem Sicherheitsvorfall ermitteln?

Sicherheitsvorfälle können sowohl zufällige Ereignisse z. B. Brände und Stromausfälle, als auch bewusste oder unbewusste menschliche Eingriffe in die IT-Systeme als Ursache haben. Hierbei bietet eine Spezialdisziplin der Informatik, die IT-Forensik, eine geeignete Hilfestellung, die Sie durch Experten erhalten können. Typische Ziele der IT-Forensik (in Anlehnung an BSI Grundschutz M 6.126) sind: Methoden und Schwachstellen zu identifizieren, die zu einem Systemvorfall geführt haben, daraus entstandene Schäden zu erkennen, mögliche Angreifer zu identifizieren und Beweise für weitere juristische Aktionen zu sichern. Eine typische Folgekette einer IT-forensischen Analyse besteht aus der strategischen und operativen Vorbereitung, Datensammlung, Datenuntersuchung, Datenanalyse und der Dokumentation.
Anhand dieses Prozesses sollten auch Sie Ihr Vorgehen bei einem Sicherheitsvorfall orientieren, um effektive Handlungsweisen umzusetzen. Die 10 goldenen Regeln unterstützen Sie hierbei.

Mittelstand 4.0-Kompetenzzentrum Chemnitz

Als Mittelstand 4.0-Kompetenzzentrum Chemnitz unterstützen wir Sie als kleines und mittelständisches Unternehmen! Wir zeigen Ihnen die technologischen und wirtschaftlichen Potenziale der Digitalisierung, Vernetzung und Anwendung von Industrie 4.0 und begleiten Sie auf dem herausfordernden Weg in eine digitale Zukunft. Mit der Expertise und Erfahrung unserer Partner wollen wir das Thema Industrie 4.0 für Sie als Unternehmen greifbar machen, Ihre Führungskräfte und Mitarbeiter qualifizieren und die Umsetzung der Digitalisierung bei Ihnen vor Ort unterstützen. Unsere Angebote umfassen ein umfangreiches Leistungsportfolio – von der Sensibilisierung über den Kompetenzaufbau bis hin zur Umsetzung im Unternehmen. Die Leistungsbereiche bauen aufeinander auf und werden vor Ort in den Unternehmen, in den Testumgebungen der Partner und auf unserer Onlineplattform angeboten. Im Rahmen unserer kostenfreien und praxisnahen Angebote können Sie sich intensiv mit diesen Themen beschäftigen.

Dabei bearbeiten wir folgende Themenfelder:

- **Menschen machen's! –**
  Der Mensch in der digitalen Arbeitswelt.
- **Alles Unternehmen! –**
  Das Unternehmen für morgen aufstellen.
- **Leistung bringen! –**
  Den Prozess digital verbessern.
- **Produkte gestalten! –**
  Das Produkt für den Nutzer machen.
- **Recht behalten! –** Recht, Sicherheit & Schutz beim digitalen Miteinander.
- **Sicher bleiben! –**
  Digitalisieren und vernetzen, aber sicher.

Was ist Mittelstand-Digital?

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie (BMWi) ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Der DLR Projektträger begleitet im Auftrag des BMWi die Projekte fachlich und sorgt für eine bedarfs- und mittelstandsgerechte Umsetzung der Angebote. Das Wissenschaftliche Institut für Infrastruktur und Kommunikationsdienste (WIK) unterstützt mit wissenschaftlicher Begleitung, Vernetzung und Öffentlichkeitsarbeit.

Weitere Informationen finden Sie unter:
www.mittelstand-digital.de

Impressum

Text und Redaktion:
Roland Hallau, Mittelstand 4.0-Kompetenzzentrum Chemnitz

Herausgeber:
Mittelstand 4.0-Kompetenzzentrum Chemnitz
c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH
Bruno-Wille-Straße 9, 39108 Magdeburg
Tel.: +49 391 74435-24 • Fax: +49 391 74435-11
E-Mail: rhallau@tti-md.de
Geschäftsführer: Dr. Michael Klaeger, Marko Wunderlich
Amtsgericht Stendal, HRB 104429
Umsatzsteuer-Identifikationsnummer: DE 139 310 185

Grafische Konzeption und Gestaltung:
toolboxx-media UG (haftungsbeschränkt)

Druckerei: KOCH-DRUCK

Bildnachweis: rvlsoft, momius, viz4biz – Fotolia.com; gorodenkoff, scyther5 – iStock

Magdeburg, April 2019

Mittelstand 4.0 Kompetenzzentrum Chemnitz

Betrieb 4.0 machen!

Was tun bei einem Sicherheitsvorfall?

10 Goldene Regeln aus der Praxis

www.mittelstand-digital.de

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

10 Goldene Regeln, die wirklich helfen

Mit einem Vorfall sicher umgehen!

Die 10 Goldenen Regeln sollen Ihnen helfen, die Funktionsfähigkeit Ihrer IT-Systeme effizient zu schützen und im Schadensfall wiederherzustellen. Diese Tipps stammen aus der betrieblichen Praxis kleiner und mittlerer Unternehmen sowie dem Handwerk. Sie wurden in enger Zusammenarbeit mit Unternehmen erarbeitet. Weiterführende Informationen und Anregungen rund um das Thema Datensicherung und Datensicherheit finden Sie unter

www.betrieb-machen.de

IT-Forensik Hacker

Sicherheitsvorfall Manipulation Schadsoftware Quarantäne Backup Sensibilisierung Zugangsdaten Netzwerkkomponenten Protokoll Verantwortlichkeiten Systemwiederherstellung

Wie sollten Sie sich richtig vorbereiten?

Regel 1: Schaffen Sie Maßnahmen zur Unterstützung der IT-Forensik

Um überhaupt ein sicherheitsrelevantes Ereignis zu erkennen und im Anschluss zu analysieren, ist es notwendig, geeignete Maßnahmen zu realisieren, die den IT-forensischen Prozess unterstützen. Hierzu können z. B. Systeme mit Inspektionsmöglichkeiten zur Datenpaketanalyse oder auch Überwachungs- und Monitoringsysteme zum Einsatz kommen. Wichtig ist, dass auch notwendige Logging-Mechanismen geschaffen bzw. aktiviert werden, welche häufig in Betriebssystemen und Netzwerkgeräten Anwendung finden. Eine Sammlung dieser Logs kann auf einem zentralen Server erfolgen.

Regel 2: Bereiten Sie Ihre Organisation auf einen Vorfall vor

Eine Grundlage zur Bearbeitung von Sicherheitsvorfällen ist die Vorbereitung des Umgangs mit diesen. Neben der Definition von Vorfällen und Sicherheitszielen ist es wichtig, dass Ihre IT-Systeme bekannt sind (z. B. Netzwerkplan, eingesetzte Hard- und Software, Konfiguration). Bestimmen Sie verantwortliche und zu kontaktierende Personen im Unternehmen und machen Sie sich über geeignete Stellen Gedanken, die Sie bei einer Untersuchung des Vorfalls unterstützen (IT-Dienstleister bzw. -Forensiker). Das alles sollten Sie in einem sogenannten Notfallplan verfasst haben und beispielsweise mit Checklisten ergänzen, die beschreiben, wie mit Sicherheitsvorfällen proaktiv umzugehen ist.

Regel 3: Lernen Sie selbst, sicherheitsrelevante Ereignisse zu erkennen

Sicherheitsvorfälle zu erkennen, ist eine sehr komplexe Aufgabenstellung, da diese sich je nach Vorfall unterscheiden können. Zudem zeigen sich Auswirkungen häufig erst nach Tagen oder Wochen. Der Kernaspekt ist aber, dass alle Personen im Unternehmen aufmerksam sind und Unregelmäßigkeiten am IT-System melden. Dabei ist es wichtig, dass die Mitarbeiter auch wissen, ob es sich um einen Sicherheitsvorfall handelt (siehe Regel 2) und dementsprechend sensibilisiert sind. Weiterhin unterstützen Sie auch unter Umständen die aus Regel 1 bekannten technischen Hilfsmittel, da diese sicherheitsrelevante Vorfälle automatisch erkennen, teilweise selbständig verhindern oder Lösungsmöglichkeiten aufzeigen können.

Wie sollten Sie sich bei einem Eintritt eines sicherheitsrelevanten Ereignisses verhalten?

Regel 4: Ruhe bewahren, aber besonnen und zügig handeln

Dies ist eine Grundregel und schützt die Anwendung der weiteren Regeln. Fehler durch hektisches oder panisches Handeln können zu einer Kettenreaktion führen und eine effiziente Wiederherstellung der Unternehmens-IT beeinträchtigen. Eine durchdachte, aber trotzdem schnelle Reaktion auf den Sicherheitsvorfall kann für Sie Kosten einsparen, Schaden für Ihre Kunden abwenden und u. U. eine notwendige forensische Analyse des Vorfalls vereinfachen. Orientieren Sie sich dafür an Ihren vorgeschriebenen Regeln des Notfallplans!

Regel 5: Überblick verschaffen

Versuchen Sie, in Ihren ersten Schritten zu ermitteln, was vorgefallen ist und welche wesentlichen Systeme betroffen sind. Hierzu sollten vom Mitarbeiter, welcher den Vorfall erkannt hat, folgende Fragen beantwortet oder in einer Checkliste abgearbeitet werden:

- Was ist vorgefallen?
- Wann und wo ist der Vorfall aufgetreten?
- Welche Systeme und Objekte sind betroffen (Netzwerkkomponenten, Software, Daten usw.)?
- Was sind aktuelle Auswirkungen?
- Gibt es eine Vermutung für die Ursache (infizierte E-Mail, Technikausfall etc.)?
- Sind bereits Maßnahmen durchgeführt worden (z. B. Herunterfahren des Rechners, Trennen der Netzwerkverbindung)?

Regel 6: Verhindern Sie eine weitere Ausbreitung

Falls es sich um den Befall einiger Komponenten im Netzwerk mit Schadsoftware handelt, sollten Sie diese unter Quarantäne stellen, vom Netzwerk entkoppeln und alle Zugänge sperren. Eine weitere Möglichkeit ist das Herunterfahren der Systeme. Hierbei muss aber beachtet werden, dass Informationen zum Schädling bzw. Angriff, die noch im Hauptspeicher vorhanden sein können, verloren gehen. Ferner kann auch das Herunterfahren ein weiterer Auslöser zur Einnistung von weiteren Schadprogrammen sein!

Regel 7: Untersuchen und analysieren Sie den Vorfall

Häufig ist es zur Ableitung weiterer Maßnahmen notwendig, die Ursachen des Vorfalls zu analysieren. Möglicherweise ergeben sich dann auch einfachere Varianten zum Umgang. Jeder Angriff hinterlässt zudem Spuren, sei es durch eine eingesetzte Schadsoftware oder durch Kommunikation im Netzwerk. Erkenntnisse darüber könnten Aufschluss über den Vorfall liefern. Es ist beispielsweise in einigen Fällen möglich, durch forensische Datenanalysen im Hauptspeicher von Systemen, Schlüssel für Dateien auszulesen, die von sogenannter „Ransomware" (Erpressungssoftware) kodiert und somit unlesbar gemacht wurden. Vermeiden Sie daher das Verändern von Daten (Spurenverwischung)!

Regelmäßige Sicherung der Daten

Für eine Wiederherstellung der IT-Systeme sind regelmäßige Backups notwendig, um kosten- und zeitintensive Datenrettungen oder unstrukturiertes Installieren von Programmen zu vermeiden. Bei den Backups sollten Sie auf geplante Zeitintervalle, die Aktualität, die Vollständigkeit und auch auf die Korrektheit der gesicherten Daten achten. Mehr Informationen können Sie in unserem Flyer „Wie sichere ich meine Daten? – 10 Goldene Regeln für die Sicherung von Daten" im Wissensbereich auf der Seite www.betrieb-machen.de finden.

Regel 8: Leiten Sie geeignete Maßnahmen ab und handeln Sie danach

In Abhängigkeit der Ergebnisse aus Regel 7 sollten Sie die Maßnahmen priorisieren, um eine zügige und korrekte Wiederherstellung der Systeme zu ermöglichen. Im Sinne der 80-20-Regel (Pareto-Effizienz) erzielen bereits 20 % (also die wichtigsten) Maßnahmen 80 % des gewünschten Effektes. In der Regel werden bei den betroffenen IT-Systemen kompromittierte Dateien gelöscht und durch Backups wieder eingespielt. Dabei ist darauf zu achten, dass die Backups selbst nicht von den Schadprogrammen betroffen sind. Dazu ist eine geeignete Analyse durchzuführen.

Anschließend sollte die Funktionsfähigkeit der IT-Systeme überprüft und die bekannten Sicherheitslücken, die zum Vorfall geführt haben, geschlossen werden (z. B. durch Patches, Änderungen im Netzwerkplan oder neue Handlungsanweisungen für die Mitarbeiter).

Was sollten Sie abschließend unternehmen?

Regel 9: Dokumentieren Sie den Sicherheitsvorfall und die Maßnahmen

Achten Sie darauf, dass die Vorfälle, auch im Ablauf, ausreichend dokumentiert werden. Dies kann mithilfe eines Protokolls erledigt werden. Es bietet sich an, ein Standardprotokoll für einen IT-Sicherheitsvorfall anzulegen. Hierbei sollten sowohl der eigentliche Vorfall selbst, als auch die Lösungsmaßnahmen dokumentiert werden. Hilfreich sind dabei auch Fotos, Screenshots und genaue Zeitangaben.

Regel 10: Ziehen Sie Lehren aus dem Sicherheitsvorfall

Im Sinne eines ständigen Verbesserungsprozesses sollten Sie aus dem gesamten Vorfall lernen, um zukünftig die Schwachstellen zu vermeiden, durch die sich der Vorfall ereignen konnte. Denkbar wären Konfigurationsänderungen an den technischen Systemen, Systemerweiterungen, organisatorische Anpassungen und die laufende Schulung bzw. Sensibilisierung von Mitarbeitern. Passen Sie auch dementsprechend Ihre Dokumentationen an!

Häufige Fehler beim Umgang mit IT-Sicherheitsvorfällen aus der Praxis sind:

- Backups werden nicht gepflegt,
- Vorfälle nicht kommuniziert („Lessons learned"),
- keine ausreichende Sensibilisierung der Mitarbeiter,
- kaum technische Hilfsmittel zur Erkennung,
- befallene Systeme sind zu lang online,
- Ressourcen zur Problembehandlung nicht ausreichend,
- Behinderung der Datenforensik und
- keine Dokumentation.

Weitere Informationen finden Sie unter nebenstehendem QR-Code oder unter: **www.betrieb-machen.de**