IT-Forensik / Security Incident Handling

Erste Hilfe im Schadensfall

Antago GmbH | Heinrichstraße 10 | D 64283 Darmstadt
Tel.: +49 . 6151 . 428568 . 0 | Fax: +49 . 6151 . 428568 . 1
E-Mail: sicherheit@antago.info | Web: http://www.antago.info
HRB 89141 | Geschäftsführerin: Frau Silke Thielmann

Sitz der Gesellschaft: Darmstadt | Registergericht: Darmstadt
Steuer-Nr.: 007 228 03 203 | Ust-IDNr.: DE 27 237 9849
Konto-Nr.: 0133 106 971 | BLZ: 508 526 51 | Sparkasse Dieburg
IBAN: DE07 5085 2651 0133 1069 71 | BIC: HELADEF1DIE

Inhalt

Einleitung

Vermehrt dringen Sicherheitsvorfälle mit entsprechenden Konsequenzen an die Öffentlichkeit. Regelmäßig ist in der aktuellen Presse vom Abfluss sensitiver Informationen wie Kundendaten, Passwörtern, Konto- und Kreditkartendaten und vielem mehr zu lesen.

Jedoch treffen diese Vorfälle bei weitem nicht nur die bekannten Big Player mit einer scheinbar stark ausgeprägten IT-Sicherheit. Auch viele kleine und mittelständische Unternehmen haben mit Angriffen auf ihre informationsverarbeitenden Strukturen, sprich die IT, zu kämpfen. Die Folgen reichen von kurzfristiger Mehrarbeit in der IT zur Behebung der Situation bis hin zu großen finanziellen und den Ruf des Unternehmens betreffenden Schäden.
Neben dem Diebstahl von sensitiven Daten kommt es vermehrt zu Taten durch entlassene oder verärgerte (ehemalige) Mitarbeiter, durch Konkurrenten aus dem In- und Ausland, zu Industriespionage, Erpressung, gezielter Rufschädigung, versehentlich oder unwissentlich geteilten Informationen und vielem anderen mehr.

Im Falle des Falles sind viele Unternehmen jedoch nicht oder nur unzureichend auf einen solchen Security Incident vorbereitet. Hier wollen wir Sie mit ersten Informationen unterstützen!

Über dieses Paper

Dieses Paper richtet sich ausdrücklich an Personen und Unternehmen, die keine eigene Expertise im Bereich IT-Forensik und Incident Handling vorhalten und im Schadensfall auf externe Unterstützung angewiesen sind. Darüber hinaus ist es so formuliert, dass auch nicht-technischen Mitarbeitern ein Verständnis der Thematik ermöglicht wird. Es ist daher auch für die Information der Geschäftsführung und solcher Mitarbeiter geeignet, die über keine tieferen IT-Security-Kenntnisse verfügen, aber im Rahmen Ihrer Tätigkeit viele – auch sensitive - Daten verarbeiten oder im Schadensfalle das weitere Vorgehen einleiten oder verantworten müssen oder sollen.

Das Paper soll Ihnen erste Informationen geben, wie Sie im Falle eines IT-Sicherheitsvorfalls zu dessen Bearbeitung beitragen können und welche Maßnahmen und Entscheidungen getroffen und bedacht werden sollten, um für Ihr Unternehmen den Schaden und dessen Folgen so gering wie möglich zu halten.

Dazu führen wir Sie in Begrifflichkeiten des Security Incident Handling und der IT-Forensik ein und geben Ihnen wichtige Tipps, wie Sie zu einer optimalen Behandlung des Vorfalls beitragen und hinzugezogene Fachleute bei Ihrer Arbeit unterstützen können.

Fragestellungen

Bei einem Sicherheitsvorfall oder Verdacht auf einen Sicherheitsvorfall müssen sich die beteiligten Akteure schon vor Beginn der ersten Maßnahmen einige grundlegende Fragen stellen, um die richtigen Schritte für das jeweils individuelle Szenario einzuleiten. Die sorgfältige Beantwortung dieser Fragen trägt maßgeblich zu einer erfolgreichen Behandlung des Sicherheitsvorfalls bei.

Störfall oder Sicherheitsvorfall

Handelt es sich bei dem Vorfall um ein sicherheitsrelevantes Problem oder ist es tatsächlich nur ein Störfall? Im Falle eines Störfalles ist die Problemlösung in der Regel einfach: Die Störung wird beseitigt und das System wieder in einen benutzbaren Zustand versetzt.

Handelt es sich jedoch um einen Sicherheitsvorfall, der eine Täterermittlung und anschließende Strafverfolgung sinnvoll oder gar zwingend notwendig macht, muss mit entsprechender Sorgfalt vorgegangen werden, um nicht mögliche Beweise und Indizien zu vernichten oder für eine Gerichtsverwertbarkeit unbrauchbar zum machen.

In diesem Fall greifen Störfall-Lösungen meist nur sehr begrenzt, oftmals wird sogar ein etwaiger finanzieller Ausfall oder sicherheitsrelevante Vorfälle ignoriert, um das System schnellstmöglich wieder in Betrieb zu nehmen. Bei dieser Vorgehensweise wird die Verfolgung der Täter unwahrscheinlich, eine Kompensation für den Schaden findet nicht statt. Das wissen auch die Täter, sie können sich im Umfeld der Computerkriminalität noch immer einer geringen Aufklärungsquote erfreuen. Während ein Diebstahl eines physischen Gegenstandes nahezu immer zur Anzeige durch den Betroffenen gebracht wird, werden Identitätsdiebstähle, Datenentwendungen und Datenveränderungen kaum angezeigt. Aufgrund der abstrakten Thematik setzen die Täter auf das Gefühl der Machtlosigkeit und die trügerische, eigene Sicherheit der Anonymität.

Tatsachen- und Täter-Ermittlung vs. Schadensbegrenzung

Wenn ein Sicherheitsvorfall festgestellt wird, gilt es sich im allerersten Schritt zu fragen, wie mit dem Vorfall umgegangen werden soll. Ist eine Ermittlung der Tat (Wer, Was, Wann, Wie etc.) notwendig, und zu welchem Zweck. Und wie groß ist der vorhandene und noch zu erwartende Schaden?

Hier gilt es auf Basis der vorliegenden Informationen abzuwägen.

Eine schnelle Behebung des Sicherheitsvorfalls durch einen Eingriff in die oder Ausschalten der Systeme kann zur Vernichtung oder Kompromittierung wichtiger Indizien und Beweise führen und eine weitere (Straf-)Verfolgung unmöglich machen.

Eventuell ist es ausreichend, den Vorfall zu beheben und eine etwaige Sicherheitslücke so zu schließen, dass kein weiterer gleicher Vorfall mehr eintreten kann und keine weiteren Systeme geschädigt werden. Dies kann dann sinnvoll sein, wenn kein weiterer monetärer Schaden entstanden ist und eine Täterermittlung nicht von weiterem Interesse ist oder dieser eine geringe Erfolgschance zugerechnet wird. Hier können spezialisierte IT-Security-Unternehmen oder entsprechend qualifizierte Mitarbeiter der eigenen IT-Abteilung unterstützen, geeignete Maßnahmen identifizieren und diese umsetzen. Ist jedoch durch einen weiteren Betrieb der betroffenen Systeme ein immenser Schaden für das Unternehmen und / oder Dritte zu erwarten, kann es notwendig und sinnvoll sein, diese einfach „vom Strom“ zu nehmen.

Wie im Einzelfall vorgegangen werden sollte, hängt vom Vorfall, dem möglichen Schaden und dem betroffenen System ab. Entscheidend ist jedoch, sich vor der ersten Maßnahme über deren Konsequenzen im Klaren zu sein, da diese grundlegend über den weiteren Verlauf des Incident Handlings entscheidet.

Ist es gewünscht oder gar notwendig, den Sachverhalt genau zu rekonstruieren und Indizien und Beweise für ein einzuleitendes (Straf-)Verfahren zu sichern, ist eine Behebung der Sicherheitslücke oder des Störfalls nur insofern angezeigt, wie keine Beweise und Indizien unbrauchbar gemacht werden. Es sollte unbedingt umgehend ein Spezialist für Incident Handling, forensische Sachverständige und ein Rechtsbeistand, ggf. gar Ermittlungsbehörden hinzugezogen werden.

Wie Sie mit dem Sicherheitsvorfall umgehen, sollte von der Geschäftsführung oder zuständigen Abteilung unter Beratung mit Anwälten, der hauseigenen Rechtsabteilung und der internen IT sowie Security-Spezialisten entschieden werden. Im Idealfall hat Ihr Unternehmen eine Richtlinie zum Security Incident Handling, an die Sie sich halten können. In der Realität liegen diese jedoch in den wenigsten, und wenn, dann meist nur in sehr großen Unternehmen, vor.

In jedem Fall gilt vor allem eines:
Ermitteln Sie nicht auf eigene Faust. Eine forensische Untersuchung basiert auf der Grundlage unveränderter Daten und einer geschlossenen, nachvollziehbaren Asservatenhandhabung. IT-Systeme verändern bereits dann Daten und Zugriffsstatistiken wenn Sie als Benutzer davon ausgehen, dass Sie nichts verändert haben. Das beginnt mit Änderungen an Zugriffszeiten von Dateien, geht über zu automatischen Datenträgeroptimierungen (die möglicherweise vom Täter gelöschte - aber noch immer auf dem Datenträger vorhandene - Indizien zerstören) und endet leider nicht bei von Tätern erstellten Programmen, die eine Rückverfolgung und Indizienerhebung stören oder verhindern sollen. Ab dem Zeitpunkt des festgestellten Sicherheitsvorfalls sollte an dem betroffenen System keine Änderung mehr vorgenommen werden – je länger es in Betrieb bleibt, desto schwerer wird eine genaue, gerichtete Analyse.

Erste Schritte

1

Beantwortung der grundlegenden Fragen:

- Was ist passiert?
- Was wollen wir erreichen?
- Wann ist es passiert?
- Wie ist es passiert?
- Wer ist der Täter oder kommt als solcher in Frage?
- Welcher Schaden ist entstanden oder wird noch entstehen?

Dies muss geschehen, ohne dass zu diesem Zeitpunkt die betroffenen Systeme verändert werden. Können einige Fragen nur durch Veränderung (also Nutzung) der Systeme beantwortet werden, müssen diese zu diesem Zeitpunkt erst einmal ausgeklammert werden, bis eine Entscheidung über das weitere Vorgehen getroffen wurde.

2

Entscheidung für oder gegen Abschaltung der Systeme

Entscheidung, ob ein Abschalten der Systeme zur Schadensbegrenzung unbedingt notwendig ist, oder ob die Beweissicherung und Täterermittlung im Vordergrund stehen soll oder muss. Hier dienen die Antworten auf die Fragen aus Schritt 1 als Entscheidungsbasis.

3

Hinzuziehen eines oder mehrerer Spezialisten

Hinzuziehen von Spezialisten für das Handling von IT- Sicherheitsvorfällen. Ggf. Hinzuziehen eines Rechtsbeistandes, um den Sachverhalt rechtlich betrachten zu lassen.

- Welche Ziele wurden definiert und können diese durch interne Mitarbeiter erfüllt werden?
- Liegt eine Straftat vor?
- Kann oder muss diese zur Anzeige gebracht werden?
- Müssen aufgrund gesetzlicher Bestimmungen andere Behörden oder Betroffene informiert werden (z.B. beim Abfluss personenbezogener Daten etc.)?
- Ist eine Analyse der Daten und Systeme u.a. in Bezug auf das Bundesdatenschutzgesetzt zulässig und rechtmäßig oder müssen Schritte eingeleitet werden, um eine Rechtmäßigkeit herzustellen?

Auf Basis der Empfehlung des Rechtsbeistandes ggf. Stellen einer Anzeige und somit Einschalten von Strafverfolgungs- und Ermittlungsbehörden.

4

Sammlung und Aufbereitung der zur Verfügung stehenden Informationen

Alle hilfreichen Informationen sollten gesammelt und aufbereitet werden, damit diese für das weitere Incident Handling zur Verfügung stehen. Hier sollte nicht vorab in Bezug auf den Vorfall interpretiert oder aussortiert werden, sondern alle Informationen möglichst vollständig und sachlich korrekt vorliegen.

Einzubindende Organisationen und externe Unterstützung

Nicht viele Unternehmen haben die Möglichkeit, die Expertise für IT-Forensik und Security Incident Handling im eigenen Haus vorzuhalten. Organisationen und Personen, die Sie im Schadensfall unterstützen können sind u.a.:

- **Geschäftsführung: ein Sicherheitsvorfall muss immer an eine entscheidungsbefugte Stelle im Unternehmen eskaliert werden. Im Regelfall ist dies die Geschäftsführung oder eine von dieser benannte Stelle im Unternehmen, wie z.B. ein IT-Security Verantwortlicher oder die interne Sicherheit. Hier gilt es, schnell die Freigabe der notwendigen Maßnahmen und Ressourcen zu erhalten.**
- **Interne Rechtsabteilung oder Rechtsanwälte:** Fachanwälte für IT-Recht, Arbeitsrecht, Strafrecht, Datenschutz zur Beurteilung rechtlicher Aspekte des Sicherheitsvorfalls.
- **Externer oder interner Datenschutzbeauftragter:** der Datenschutzbeauftragte kann Sie bei der Bewertung des Sachverhaltes und der Koordination weiterer Schritte unterstützen.
- **Security-Spezialisten:** Zur Koordination und Beurteilung von Maßnahmen sowie zur Ermittlung von Sicherheitslücken etc., benötigt es die Expertise von Security-Spezialisten mit Erfahrung im Bearbeiten von Sicherheitsvorfällen.
- **Systemhäuser / IT-Dienstleister:** Sofern Sie Ihre IT nicht selbst betreuen, ist es wichtig, Ihren Dienstleister in den Prozess mit einzubeziehen. Dieser kann wichtige Informationen zu den betroffenen Systemen liefern und bei der Umsetzung der identifizierten Maßnahmen unterstützen.
- **Anerkannte IT-Forensiker:** Sofern eine Aufklärung angestrebt wird, sollten Sie zur beweissicheren Analyse von Datenträgern einen IT-Forensiker hinzuziehen. Oft verfügen IT-Security-Unternehmen über diese Expertise und stellen sie im Rahmen des Security Incident Managements mit zur Verfügung.
- **Staatliche Ermittlungsbehörden:** Im Falle einer vermuteten oder offensichtlichen Straftat sollten in Absprache mit Ihrem Rechtsbeistand staatliche Ermittlungsbehörden eingeschaltet und Strafanzeige gestellt werden.

Wichtig für eine erfolgreiche Umsetzung ist hier, dass alle Beteiligten Hand in Hand und unter Koordination einer definierten Instanz, meist des Spezialisten für Security Incident Handling, arbeiten.

Hilfreiche Informationen für Ermittler

Grundsätzlich gilt: Um so mehr fundierte, korrekte und sachliche Informationen den Ermittlern zeitnah vorliegen, umso besser und umfassender kann die vorliegende Situation bewertet werden. Hilfreiche Informationen, die Sie bereits vor Eintreffen der Ermittler zusammen- und zur Verfügung stellen können, sind (je nach Situation und betroffenen Systemen):

Wie wurde der Vorfall erkannt?

- Wurde er durch einen Benutzer festgestellt oder hat ein automatisches System Alarm geschlagen?
- Wurde der Vorfall durch Mitarbeiter aus der IT-Abteilung erkannt ?
- Meldeten externe Dienstleister eine Abweichung von der Norm oder wurden die Informationen von Strafverfolgungsbehörden oder der Presse zur Verfügung gestellt?
- Wo ist es passiert? Steht das betroffene System in einem Bereich mit beschränktem Besucherzugang, befindet es sich in einem eher öffentlichen Bürobereich mit Kundenzutritt, ist es ein Serversystem in einem Rechenzentrum oder ist es ein Gerät, dass Mitarbeiter in ihr Home Office mitnehmen?

Wann ist es passiert?

- Steht der Zeitpunkt genau fest?
- Ist es ein relativ kleiner Zeitrahmen oder wurde über Monate das Problem nicht erkannt oder sich darum gekümmert?

Erstellen Sie eine Timeline mit allen Ihnen zur Verfügung stehenden Informationen und stellen Sie diese den Ermittlern zur Verfügung.

Was ist passiert?

- Welches System wurde kompromittiert (Laptop, Smartphone, Server, Telefonanlage etc.)?
- Welche Daten wurden kompromittiert (gestohlen, verändert, gelöscht etc.)?

Zeichnet es sich ab, dass ein geschäftskritisches System kompromittiert wurde, stellen sich weitere Fragen:

- Sind neben dem bekannten Vorfall weitere Systeme betroffen?
- Sind mit dem kompromittierten System vernetzte Systeme oder Anwendungen in Gefahr?
- Betrifft der Sicherheitsvorfall nur interne Benutzer oder auch externe?
- An welcher Stelle hat sich der Sicherheitsvorfall ereignet?

Hier sind Netzpläne, Protokolle, technische Dokumentation etc. zur Einsicht und Bewertung hilfreich.

Wie ist es passiert?

- Ist dieser Vorgang nachzuvollziehen?
- Über welche Wege ist der Angreifer in die Systeme eingedrungen?
- Wurden bekannte Sicherheitslücken ausgenutzt?
- Wurden User-Accounts für den Angriff genutzt?
- Ist Schadcode auf die Systeme gelangt?
- Wenn ja, über welchen Weg ist Schadcode auf die Systeme gelangt?

Und falls dies geklärt werden kann: Wer hat es getan bzw. könnte es getan haben?

- Wurde beispielsweise ein Mitarbeiter dabei ertappt, wie er Daten entwendete?
- Gibt es aktuell Personen, die mit einer Schädigung des Unternehmens gedroht haben (entlassene oder verärgerte Mitarbeiter, Konkurrenten, Partner)?
- Veränderte ein Besucher an einem nicht überwachten Bürocomputer Projektdaten?
- Gab es eine Schutzgelderpressung mit darauffolgender oder voran gegangener Serverattacke?
- Wurden Zugangsdaten verwendet, die nur einem einzelnen Mitarbeiter oder einem spezifischen Personenkreis zuzuordnen sind?

Fazit

Im Falle des Falles gilt es Ruhe zu bewahren und die nächsten Maßnahmen und Handlungen gut zu durchdenken und rechtlich abzusichern. Sie können einiges dazu beitragen, dass der Sicherheitsvorfall sachgerecht behandelt und nicht durch etwaige voreilige Handlungen der Schaden für das Unternehmen noch vergrößert wird.
Wenden Sie sich im Zweifelsfall daher frühzeitig an Spezialisten, die Sie im weiteren Prozess unterstützen und beraten.
Nnehmen Sie sich die Zeit, das Thema „Was tun im Schadensfall" im Unternehmen zu diskutieren und zu definieren. Vorzugsweise, bevor der Fall der Fälle eintritt!

Glossar

Das folgende Glossar gibt Ihnen einen Überblick über die in diesem Paper verwendeten Begrifflichkeiten. Das Glossar ist nicht vollständig in Bezug auf alle für die IT-Forensik relevanten Begrifflichkeiten, ermöglicht dem Leser jedoch ein Verständnis der häufigsten Grundbegriffe und damit ein Basisverständnis in der Zusammenarbeit mit IT-Forensikern und Ermittlern.

- **Asservat:** Ein Asservat bezeichnet ein Verwahrstück, dass zur Indizienerhebung in der Forensik dient. Es wird gesichert verwahrt und wird in der Regel nach Abschluss der Ermittlungen zurückgegeben (physisches Asservat) oder je nach Vorgabe des Kunden eingelagert oder vernichtet (digitales Asservat).
- **Beweis:** In der Kriminalistik ist ein Beweis eine Tatsache oder ein Erfahrungssatz aufgrund derer die richterliche Überzeugung eintritt, dass eine Behauptung wahr oder unwahr ist.
- **Flüchtige Daten:** Daten, die bei einem Ausschalten eines Systems unwiederbringlich gelöscht / überschrieben werden, wie z.B. Daten im Prozessor oder Arbeitsspeicher, Routing-Tabellen, Kernel-Statistiken, CPU Cache etc. Darüber hinaus flüchtige Daten im Netzwerk, welche über dieses gesendet und empfangen werden.
- **Forensisches BackUp**: Eine forensische Datensicherung von Datenträgern, um auf diesen Images die notwendigen Analysen durchführen zu können, ohne den Originaldatenträger zu kompromittieren (siehe Image).
- **Gerichtsfeste Beweissicherung:** Die eingesetzten Methoden müssen von Seiten der Fachwelt allgemein akzeptiert sein, ihre Robustheit und Funktionalität muss nachgewiesen sein. Die

Beweissicherung muss mit gleichem Ergebnis wiederholbar sein. Durch die Untersuchung und Sicherung dürfen die Beweismittel nicht verändert werden.

- **Image:** Physisches Datenträgerabbild, das zur forensischen Analyse der Daten (nicht-flüchtige Spuren) genutzt wird. Images müssen immer mit speziellen forensischen Tools erstellt werden, um die Beweissicherheit des Originaldatenträgers nicht zu gefährden. Das Abbild muss u.a. vollständig sein und mit der Berechnung einer kryptografischen Checksumme abgeschlossen werden, um die Unveränderheit (Integrität) des Images nachweisen zu können. Auf den Originaldatenträger darf bei dieser Vorgehensweise unter keinen Umständen Daten verändert werden.
- **Indiz:** Informationsbruchstück, das alleinstehend noch nicht zur Analyse des Vorfalls ausreicht. Potenzielle Indizien müssen so gehandhabt werden, dass sie nachweislich nicht verfälscht werden.
- **IT-Forensik:** Das BSI definiert in seinem Leitfaden zur IT-Forensik den Begriff wie folgt „IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung, insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems."
- **Live-Forensik:** Untersuchung während des Vorfalls mit Schwerpunkt auf der Gewinnung und Untersuchung von flüchtigen Daten. Auch als Online-Forensik bezeichnet.
- **Nichtflüchtige Daten:** Daten, die bei einem Ausschalten der Systeme erhalten bleiben, wie zum Beispiel auf Festplatten, USB-Sticks oder anderen Massenspeichern.
- **Post-Mortem-Analyse:** Untersuchung nach dem Vorfall, meist von speziell für die Analyse nach forensischen Methoden erzeugten Images (Datenträgerabbildern) des eigentlichen Datenträgers. Der Schwerpunkt liegt auf der Gewinnung und Untersuchung von gelöschten, umbenannten sowie anderweitig versteckten und verschlüsselten Dateien von Massenspeichern. Auch als Offline-Forensik bezeichnet.
- **Security Incident Handling:** Behandlung / Umgang mit einem / Management eines Sicherheitsvorfalls.
- **Writeblocker:** Gerät, dass eingesetzt wird, um sicher zu stellen, dass bei dem Erstellen einer forensischen Sicherung nicht schreibend auf den Originaldatenträger zugegriffen wird. Durch Einsatz dieses Tools wird während des Sicherungsvorgangs die Beweissicherheit des Originaldatenträgers erhalten.

Weiterführende Informationen

Weiterführende Informationen bietet Ihnen unter anderem der kostenfreie Leitfaden „IT-Forensik“ des BSI – Bundesamt für Sicherheit in der Informationstechnik sowie die einschlägige Literatur.

Vermehrt werden darüber hinaus auch Veranstaltungen und Seminare zu den Themen Cyber Crime und IT-Forensik angeboten, z.B. auf den bekannten IT-Fachmessen wie der it-sa in Nürnberg oder der CEBIT in Hannover sowie auf diversen anderen Messen und Kongressen.

Über die Autoren

Silke Thielmann ist Gesellschafterin und Geschäftsführerin der Antago GmbH. Zusammen mit Ihrem Team betreut Sie Unternehmen aus Industrie und Handel sowie dem Gesundheitswesen aller Branchen und Größen im Bereich der Informationssicherheit.

Martin Alberstadt ist Security Consultant der Antago GmbH mit Schwerpunkt auf IT-Forensik. Darüber hinaus ist er ein ausgewiesener Linux-Spezialist und beschäftigt sich seit vielen Jahren mit Kleinst-Linux-Systemen.

