Incident Response und Forensik

cirosec

Incident Response und Forensik

Incident Response und Forensik

Der Einbruch eines Hackers in die Web-Applikation des Unternehmens, ein Mitarbeiter, der vertrauliche Daten an ein Konkurrenzunternehmen versendet, ein Wurm, der sich im Unternehmen ausbreitet, kinderpornographische Bilder auf der Festplatte eines Angestellten – dies alles sind Beispiele für Vorfälle, die Unternehmen gerne vermeiden würden. Dennoch kommen sie immer wieder vor.

Wenn der Verdacht auf einen IT-Sicherheitsvorfall besteht, ist es entscheidend, möglichst früh die richtigen Schritte zu unternehmen, um nicht mehr Schaden anzurichten, als möglicherweise schon entstanden ist.

In der Praxis zeigt sich, dass in den meisten Fällen keine ausreichenden Eskalationsprozeduren und Leitfäden für richtiges Handeln bei Sicherheitsvorfällen existieren. Bei dem Verdacht, dass gerade ein Hacker sein Unwesen auf den Firmenservern treibt, werden in Hektik oder sogar Panik meist wichtige Spuren zerstört und eine Analyse des Tathergangs ist danach oft nicht mehr möglich.

Um im Fall der Fälle nicht hilflos und mit leeren Händen dazustehen, sollte man sich rechtzeitig über das so genannte „Incident Handling“ im Unternehmen Gedanken machen. Die Zielsetzung liegt dabei in der Definition von Prozessen, die im Ernstfall einzuhalten sind, um eine angemessene Reaktion zu ermöglichen. Dazu müssen unter anderem Zuständigkeiten und Befugnisse sowie Handlungsanweisungen für die korrekte Sammlung und Sicherung relevanter Daten definiert werden. Ebenso müssen vorbereitende Maßnahmen geplant und durchgeführt werden, damit im Ernstfall die benötigten Informationen oder Protokolle überhaupt technisch verfügbar sind.

Bei einem konkreten Verdacht auf einen Sicherheitsvorfall muss schnell und richtig gehandelt werden. Die im Vorfeld definierten Sofortmaßnahmen müssen in Abhängigkeit vom Verdacht und von der Art und Kritikalität des betroffenen Systems durchgeführt werden. Darüber hinaus muss der Vorfall an das Incident Handling Team eskaliert werden. Das Team sollte entsprechend dem Vorfall gegebenenfalls auch Vorgesetzte, Rechtsabteilung, Personalvertretung und Personalabteilung involvieren. Dann gilt es, die Spuren bzw. Daten zu sammeln und zu sichern.

Die konkrete Durchführung von Sofortmaßnahmen des Incident Handlings kann meist nur sinnvoll von den eigenen Mitarbeitern vor Ort durchgeführt werden, da in diesem Fall genaue Kenntnisse der firmeninternen Strukturen sowie ein schnelles Handeln erforderlich sind. Allerdings ist auch externe Unterstützung möglich, wenn im Vorfeld schon klare Absprachen getroffen wurden.

Anschließend stehen die Analyse des Tathergangs und die gerichtsfeste Durchführung und Aufbereitung der forensischen Analyse im Vordergrund. Die Auswertung der Daten kann sehr gut von externen Experten übernommen werden. Durch ihre regelmäßige Tätigkeit verfügen sie über ein großes Maß an Erfahrung, um so beispielsweise den Tathergang rekonstruieren zu können und die sogenannte „Nadel im Heuhaufen“ zu finden.

UNTERSTÜTZUNG DURCH CIROSEC

Beratung/Erarbeitung von Incident-Handling-Konzepten

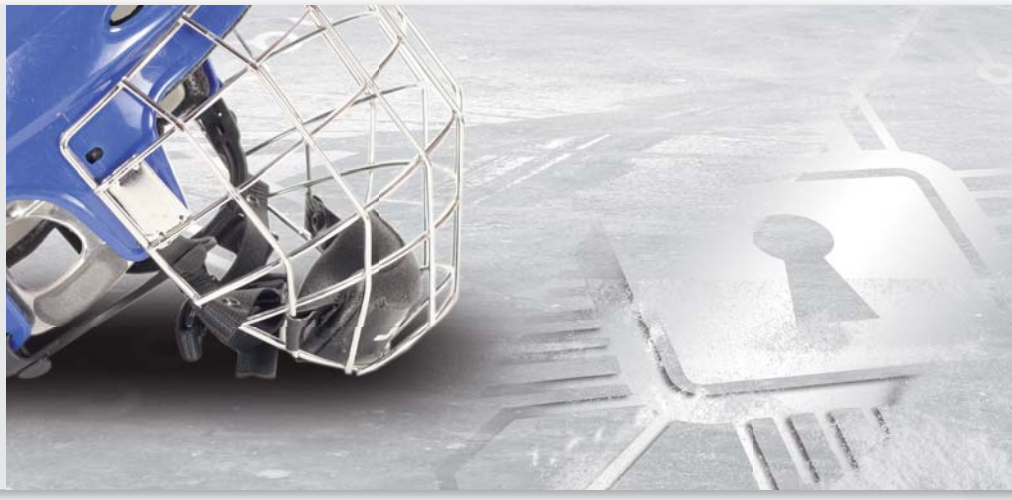
Die erfahrenen Berater der cirosec GmbH erarbeiten in enger Abstimmung mit Ihnen Konzepte, vorbereitende Maßnahmen und unterstützen bei der Gestaltung von Prozessen sowie der Festlegung von Verantwortlichkeiten und Handlungsanweisungen, damit Sie auf den Ernstfall vorbereitet sind.

Enthalten sein können darin beispielsweise auch Vorgehensweisen zur Sammlung und Sicherung relevanter technischer Daten im Fall eines Verdachts bzw. eines konkreten Sicherheitsvorfalls und eine Zusammenstellung von forensischen Analysemöglichkeiten zur gezielten Auswertung der zuvor gesammelten technischen Daten.

Ebenso müssen typischerweise die Protokollierungseinstellungen relevanter Systeme optimiert werden, damit im Ernstfall auch genügend auswertbare Spuren vorhanden sind.

Wir unterstützen Sie bei der Auswahl geeigneter Werkzeuge für die Durchführung von Sofortmaßnahmen durch die eigenen Mitarbeiter.

Zur Vorbereitung auf den Ernstfall beraten wir Sie umfassend, damit Sie Ruhe bewahren und zielgerichtet reagieren können.



Forensische Analyse

Auf Anfrage kommen Berater der cirosec GmbH zu Ihnen, um bei der Sicherung von Spuren und der Analyse der Daten nach einem Sicherheitsvorfall zu helfen. Dabei können beispielsweise folgende Teilaspekte eine Rolle spielen:

- Rekonstruktion des Tathergangs oder des Infektionswegs über die Analyse von Protokollen oder Analyse der Festplatten- oder Speicherabbildern
- Suche nach Schwachstellen, die den Einbruch ermöglicht haben
- Untersuchung von laufenden Systemen, um weitere Spuren zu sammeln oder den Umfang des Vorfalls einzugrenzen
- Analyse von Dateien oder Programmen, um beispielsweise die Funktionen einer Malware zu analysieren
- Ermittlung der betroffenen Komponenten
- Analyse strukturierter und unstrukturierter Daten
- Unterstützung bei der Ermittlung des entstandenen Schadens.

TRAININGS UND SCHULUNGEN

Training Forensic Extrem

In diesem Training werden aktuelle technische Methoden der IT-Forensik und des Incident Handlings sowie die damit verbundenen rechtlichen und organisatorischen Rahmenbedingungen und Möglichkeiten vorgestellt. Anhand vieler Fallbeispiele und Übungen wird das richtige Vorgehen bei einem Verdacht auf Hacker-Einbruch, Datenmissbrauch, Datendiebstahl, Datenlöschung oder auch bei unberechtigter Nutzung von firmeneigenen Kommunikationsmöglichkeiten erörtert.

Die Schulung teilt sich in einen technischen Teil, in dem Werkzeuge für eine forensische Analyse vorgestellt und in Übungen eingesetzt werden, und in einen rechtlichen/organisatorischen Teil, in dem auch die rechtlichen Rahmenbedingungen für Inhouse-Ermittlungen gegen Verdächtige dargestellt werden, auf.

Im technischen Teil lernt jeder Teilnehmer anhand vieler Übungen, die er auf einem zur Verfügung gestellten Laptop selbst nachvollzieht, Spuren in IT-Systemen zu suchen, richtig zu sichern und zu interpretieren.

Im rechtlichen/organisatorischen Teil wird ein Rechtsanwalt detailliert auf die Vorgehensweise nach der Entdeckung von Einbrüchen eingehen. Fall für Fall wird die Sammlung, Sicherung und Auswertung gerichtsfester digitaler Spuren als Beweismittel zur erfolgreichen Rechtsverfolgung durchgespielt.

Dabei wird berücksichtigt, welche Tätergruppe in Betracht kommt, welches übergeordnete Ziel (z. B. Schädigung der Firma) der Angriff wirklich hatte, was geschützt werden muss und welches Schadenspotenzial der Angriff hatte. Ebenso wird erörtert, welche Beweismittel durch eigene Ermittlungen beschafft werden können, welche nur unter Einschaltung Dritter oder der Polizei und inwieweit eine Strafanzeige gegen Verdächtige hilft.

Nach Abschluss des Trainings sind die Teilnehmer in der Lage, die Wege eines Einbrechers nachzuvollziehen. Sie wissen, wie sie im Falle eines Systemeinbruchs reagieren müssen und welche Anforderungen an die gerichtsfeste Sammlung, Speicherung und Auswertung digitaler Spuren als Beweismittel gestellt werden müssen.

CIROSEC – IHR PARTNER IN DER IT-SICHERHEIT

Wir sind ein spezialisiertes Unternehmen mit Fokus auf IT- und Informationssicherheit und beraten unsere Kunden im deutschsprachigen Raum.

Das cirosec-Team zeichnet sich dabei durch seine zahlreichen Experten aus, die als Buchautoren oder Referenten internationaler Kongresse bekannt sind und den Kunden individuell mit technischem und strategischem Sachverstand beraten.

Darüber hinaus verfügen wir über langjährige Erfahrung in der Konzeption und Integration von Sicherheitsprodukten in komplexen Umgebungen. Bekannt sind einige der Mitarbeiter auch durch erfolgreiche Research-Tätigkeit, da sie immer wieder neue, noch nicht gemeldete Schwachstellen in Standardsoftwareprodukten finden.

Das Leistungsspektrum umfasst die Bereiche:

- Konzepte, Reviews und Analysen
- IT-Sicherheitsmanagement-beratung (ISO 27001, Risikomanagement, Erstellung von Prozessen, Policies, Richtlinien)
- Durchführung von Audits und Penetrationstests
- Incident Response und Forensik
- Trainings
- Konzeption, neutrale Evaluationen und Implementation von Produkten und Lösungen.

Typische Themen im Umfeld von Produkten und Lösungen sind:

- Moderne Schutzmaßnahmen für Unternehmen (z. B. WAFs, Schutz vor DDoS und gezielten Angriffen)
- Sicherheit im internen Netz (z. B. LAN-Zugangskontrolle, 802.1x, NAC/NAP, IPS)
- Bring your own Device, Mobile/Wireless Security
- Werkzeuge für ISMS, Verwundbarkeits- und Risikomanagement
- Nachvollziehbarkeit administrativer Zugriffe.

v01CRS-13-1929-DE130628 · Bildquellen: istockphoto, shutterstock

cirosec GmbH
Ferdinand-Braun-Straße 4 | 74074 Heilbronn | Deutschland
T +49 7131 59455-0 | F +49 7131 59455-99 | www.cirosec.de

cirosec