Typische Fehler in der IT-Sicherheit

Praxismanagement Bublitz-Peters verweist Sie auf die typischen Fehler, die viele nach einem Cyberangriff (z. B. Hackerangriff oder Datendiebstahl) machen. Außerdem werden Sie lernen, welche Schritte Sie stattdessen unternehmen sollten.

Beispielsituation

Vor kurzem hatten Sie einen Praktikanten in Ihrer Praxis. Kurze Zeit nachdem er aufhörte, bekommen Sie eine anonyme Erpressernachricht, dass wenn Sie nicht sofort 100.000€ zahlen, die sensiblen Daten Ihrer Patienten im Internet veröffentlicht werden. Ihnen kommt der Verdacht, dass es sich hierbei um einen Fall von Datendiebstahl des ehemaligen Praktikanten handeln könnte. Da Sie den Verdacht so schnell wie möglich klären möchten, lassen Sie von Ihrem internen IT-Beauftragten sofort den PC auf Aktivitäten während des Praktikums, mit den Log-In Daten des Praktikanten überprüfen.

Um den Rechner zu untersuchen, führt der Mitarbeiter Ihrer IT-Firma folgende Schritte durch:

- Er schaltet den Rechner an.
- Er meldet sich mit den Daten des Praktikanten bei dem PVS an und überprüft die Verzeichnisse.
- Es werden Dateien auf einen externen USB-Stick kopiert.
- Der IT-Mitarbeiter installiert eine Untersuchungssoftware, die die auf dem Rechner befindlichen Daten überprüft.
- Er schaltet den Rechner aus.

Da die Ergebnisse der Untersuchung Ihren Verdacht bestätigen, schalten Sie professionelle IT-Forensiker ein, die ein Gutachten für Sie erstellen sollen.

Professionelle Spurensicherung

Die hinzugezogenen IT-Forensiker überprüfen den Rechner. Während der Untersuchung stellen sie jedoch fest, dass einige der zu untersuchenden Daten fehlen oder verfälscht wurden. Ursache dafür ist vermutlich die vorherige Überprüfung durch Ihren Mitarbeiter. Auch die Zeitstempel der Aktionen sind verändert worden und dadurch der Datendiebstahl nicht auf seinen ursprünglichen Zeitpunkt zurück zu verfolgen. Dadurch ist nicht mehr nachvollziehbar, ob wirklich der Praktikant für den Datenklau verantwortlich war. Anschließend analysieren die IT-Forensiker den Rechner auf Spuren einer externen Speichermediennutzung (z. B. USB-Sticks oder Festplatten). Eventuell hat der Praktikant Daten auf einen USB-Stick kopiert. Durch das Anschließen eines USB-Sticks während Ihrer Vorabuntersuchung, wurden allerdings auch diese Spuren korrumpiert.

Praxismanagement Bublitz-Peters GmbH & Co. KG
Rohrbacher Str. 28, 69115 Heidelberg
Telefon: 0 62 21- 43 85 00
Telefax: 0 62 21- 43 85 01 10
e-mail: info@bublitz-peters.de
www.bublitz-peters.de

Sitz der Gesellschaft: Heidelberg
Amtsgericht Mannheim, HRA 701358
Geschäftsführerin:
Silke Bublitz-Peters
Steuer-Nr.: 32074/02988
USt-Id-Nr.: DE 258372570

Die Experten konnten für ihr Gutachten nahezu keine verwertbaren Spuren finden, die dem Praktikanten einwandfrei zugeordnet werden können. Er kann nun gerichtlich nicht belangt werden.

Wie Sie richtig vorgehen

Anhand dieses Beispiels können Sie sehen, dass eine eigenständige Untersuchung eines Systems erhebliche Folgen haben kann. IT-Forensiker sind in der Lage, digitale Spuren zu finden, diese gerichtsfest zu sichern, zu analysieren und zu dokumentieren. Dies ist allerdings nur möglich, wenn die zu sichernden Spuren noch vorhanden und unverändert sind.

Hier unsere Tipps, wie Sie sich im Ernstfall verhalten sollten (das gilt sowohl für einen Angriff von außen z. B. über Schadsoftware wie einen Virus, als auch Angriffe von innen, wie einen Datenklau per USB-Stick):

- Sobald der Vorfall entdeckt wird, lassen Sie den betroffenen Rechner angeschaltet. Durch das Herunterfahren, wird eine Analyse des Arbeitsspeichers unmöglich.
    - Führen Sie keinesfalls Updates durch, bis die professionelle Spurensicherung stattgefunden hat. Updates könnten wichtige Daten überschreiben. Trennen Sie am besten die Netzwerkverbindung. Somit vermeiden Sie automatische Updates sowie andere Veränderungen am System durch Netzwerkaktivitäten.
- Nutzen Sie unbedingt einen anderen Rechner in der Zwischenzeit. Durch eine Nutzung des betroffenen Geräts, können wichtige Daten und Dateien nachhaltig verändert oder vollständig gelöscht werden.
- Setzen Sie den Rechner nicht neu auf, dadurch werden fast alle Spuren gelöscht.
- Führen Sie keine eigenständigen Untersuchungen durch. Für ein Gerichtsverfahren ist ein objektives Gutachten einem eigenen vorzuziehen.
- Installieren Sie keine Untersuchungstools oder andere Software, da diese auf jede einzelne Datei zugreifen und dadurch sämtliche Zeitstempel verändern.
- Durchsuchen Sie keine Ordner oder Dateien die relevant sind. Auch dieser Vorgang kann forensisch-relevante Daten verändern oder löschen.
- Schließen Sie keine USB-Geräte an, da hierbei Spuren entstehen, die für eine professionelle Prüfung relevanten Spuren überdecken können.

Nicht in die Falle tappen

Die Versuchung, bei einem IT-Sicherheitsvorfall selbst schnell zu handeln und eine Untersuchung durchzuführen, ist groß. Oftmals besteht Zeitdruck und Unsicherheit, ob es überhaupt einen Vorfall gab. Dann wird versucht, dies vorab zu klären. Dadurch werden allerdings häufig Beweisen und Spuren unwiderruflich vernichtet. Digitale Spuren sollten Sie also so ähnlich behandeln, wie Sie es mit physikalischen Spuren und Beweisen bei einem Gewaltverbrechen tun würden. Belassen Sie Beweismittel unberührt und holen Sie Experten hinzu.