FAST DETECT

SACHVERSTÄNDIGENBÜRO
FÜR IT-FORENSIK

CASE STUDY

DATENLECK DURCH EINEN INNENTÄTER

DIE AUSGANGSSITUATION

In einer renommierten Aktiengesellschaft wurden vier höchst vertrauliche Vorstandspräsentationen anonym an private E-Mail-Adressen verschiedenster Mitarbeiter verschickt. Unter den Empfängern waren Mitglieder des Betriebsrats sowie Mitarbeiter der Rechts- und Marketingabteilung.

FAST-DETECT wurde beauftragt, den unautorisierten Versender der Dokumente zu identifizieren. Darüber hinaus sollte festgestellt werden, ob weitere vertrauliche Dokumente durch diese Person entwendet wurden.

DIE RAHMENBEDINGUNGEN

Auch bei firmeninternen Untersuchungen muss eine Vielzahl rechtlicher Vorschriften beachtet werden. So sind bei IT-forensischen Untersuchungen unter anderem das Bundesdatenschutzgesetz, das Betriebsverfassungsgesetz sowie die unternehmenseigenen IT-Richtlinien zu berücksichtigen.

Hinzu kommt, dass nur in seltenen Fällen bereits zu Beginn der Untersuchung direkt auf Daten einzelner Nutzer zugegriffen werden darf.

DAS VORGEHEN VON FAST-DETECT

1. Im ersten Schritt der IT-forensischen Untersuchung eruierte FAST-DETECT, dass Schreibzugriffe auf USB-Massenspeicher als Voreinstellung zwar unternehmensweit deaktiviert waren, aber dennoch etwa 25% aller Mitarbeiter dieses Recht nach einfacher Beantragung erhielten.
2. Alle Benutzer, die berechtigten Zugriff auf die relevanten Dokumente besaßen, wurden identifiziert.
3. Dann wurde überprüft, ob sich gegen einen oder mehrere dieser Benutzer ein Anfangsverdacht begründen ließ. Hierzu wurden im Rahmen der rechtlichen Möglichkeiten folgende Informationsquellen betrachtet:
   - Proxy-Protokolldateien zur Identifikation von auffälligen Internetzugriffen.
   - Hashanalyse zur Identifikation weiterer Speicherorte der relevanten Dateien.
   - Meta-Informationen der anonymen E-Mails sowie etwaige Metadaten der veröffentlichten Dateien.
4. Um den Anfangsverdacht gegen die identifizierten Benutzer zu erhärten, wurden folgende Spuren überprüft:
   - Nutzungsspuren von USB-Massenspeichern und deren Inhalte, inklusive der physisch nicht mehr zur Verfügung stehenden Inhalte.
   - Internethistorie der besuchten Websites – inklusive der Fragmente der gelöschten Internethistorie in den ungenutzten Speicherbereichen.
5. Durch verschiedene, festgestellte Spuren, u.a. die minimalen Spuren, die das Anschließen eines USB-Sticks hinterlässt, konnte das Endsystem (Client) identifiziert werden, mit dessen Hilfe man die Daten auf den Stick kopiert hatte.

ZUSAMMENFASSUNG

Tatbestand:	Entwendung von Firmendaten
Kunde:	Aktiengesellschaft
Auftrag:	Identifikation des Täters und des Umfangs der entwendeten Daten
Vorgehen:	1. Erhärtung eines Anfangsverdachts gegen Einzelpersonen. 2. IT-forensische Detailauswertung der Endgeräte dieser Einzelpersonen
Befund:	Vier relevante Dokumente wurden über ein hierfür eingerichtetes E-Mail-Konto und mit Hilfe eines USB-Sticks entwendet.
Ergebnis:	Identifizierung des Datenlecks, Beschreibung von Verbesserungsfeldern im Bereich der organisatorischen IT-Sicherheit sowie Vorschlag für sinnvolle technische Maßnahmen.

BEKANNTE SICHERHEITSRISIKEN

Die langjährige Erfahrung von FAST-DETECT bei der Aufklärung von Datenlecks zeigt, dass die Entwendung der Daten am häufigsten durch den Einsatz eines USB-Massenspeichers verursacht wird.

Als weitere Möglichkeiten werden Cloud-Speicherdienste, Unternehmens-E-Mail-Systeme und Webmailer genutzt.

DER BEFUND

FAST DETECT konnte zum in Frage kommenden Benutzerkreis Folgendes feststellen:

- 38 Benutzer hatten berechtigten Zugriff auf die relevanten Dokumente.
- Davon hatten 10 Benutzer genehmigten Schreibzugriff auf USB-Massenspeicher.
- Bei 4 der 38 Benutzer wurden auffällige Internetzugriffe festgestellt.
- Die Schnittmenge der drei Gruppen ergab genau einen Benutzer.

Die forensische Auswertung der Endgeräte des Benutzers ergab folgende Ergebnisse:

- Fragmente von zwei relevanten Dokumenten wurden im ungenutzten Speicherbereich als E-Mail-Anhang einer Entwurfs-E-Mail nachgewiesen. Das zugehörige E-Mail-Konto war zuvor bei Yahoo neu angelegt worden.
- Zwei weitere Dokumente wurden zwei Tage vor der Veröffentlichung auf einen USB-Stick kopiert. Bei diesem handelte es sich ausweislich der Nutzungsspuren um keinen unternehmenseigenen USB-Stick. Im Zuge des Kopiervorgangs wurden auch noch vier weitere Excel-Dokumente auf denselben Stick kopiert.
- Fragmente des ungenutzten Speicherbereichs lieferten auch den Hinweis darauf, weshalb zwei Dokumente mit Hilfe eines Webmailers und zwei weitere mit Hilfe eines USB-Sticks aus dem Unternehmen entwendet wurden: Eine Fehlermeldung wies darauf hin, dass Dokumente zu groß waren, um als E-Mail Anhang versendet zu werden

FABIAN UNUCKA
Sachverständiger für IT-Forensik

fabian.unucka@fast-detect.de

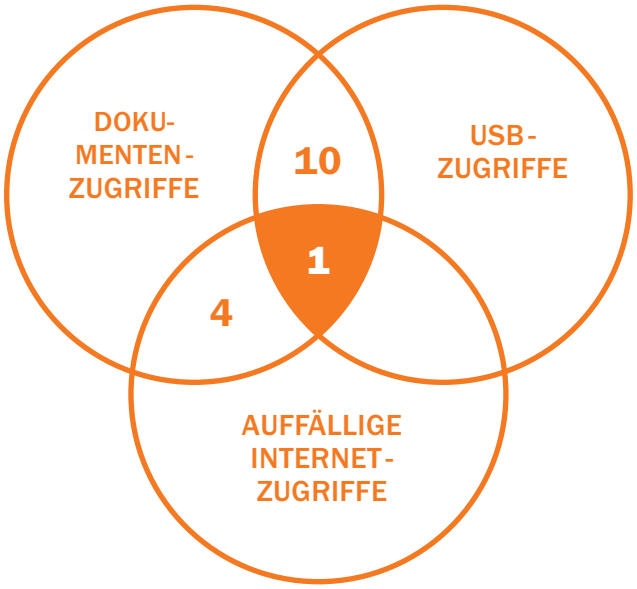

Abb. Einschränkung des Benutzerkreises

DAS ERGEBNIS

Aufgrund der Untersuchung von FAST-DETECT konnte sowohl das Datenleck wie auch ein Verdächtiger identifiziert werden. Außerdem wurden zahlreiche Ansatzpunkte zur Optimierung der IT-Sicherheit des Unternehmens aufgezeigt und konkrete technische Maßnahmen vorgeschlagen.

IDENTIFIZIERTES OPTIMIERUNGSPOTENTIAL

Zusätzlich zu den bereits ergriffenen Sicherheitsmaßnahmen des Unternehmens (z. B. Beschränkung des Schreibzugriffs auf USB-Massenspeicher) identifizierte FAST-DETECT während der Untersuchung weitere Verbesserungsfelder zur Steigerung der IT-Sicherheit und Forensic Readiness:

- Weitere Reduzierung der Schreiberlaubnisse für USB-Massenspeicher und jährliche Überprüfung der genehmigten Schreibzugriffe.
- Aktivierung der Dateiverfolgung für alle Vorstandsdaten und weitere sicherheitsrelevante Daten.
- Sperrung von Webmailern und Cloud-Speicherdiensten für Benutzer.

FAST-DETECT GmbH

Inselkammerstraße 12
82008 Unterhaching
Tel +49 89 204040-0
Fax +49 89 204040-299
Mail info@fast-detect.de
Web www.fast-detect.de

10/2018