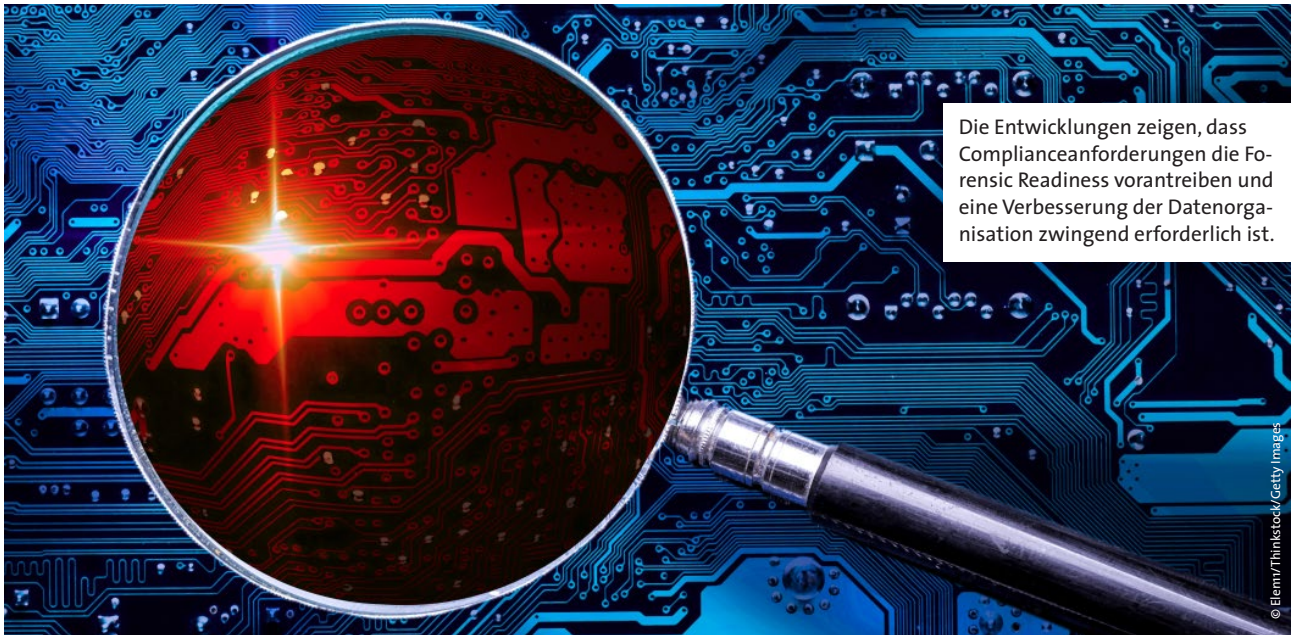
ComplianceBusiness
Ausgabe 2 // Juni 2019

Complianceanforderungen treiben die Forensic Readiness voran

Eine Verbesserung der Datenorganisation ist zwingend erforderlich

Von Hanno Baur

Die IT-Forensik kommt bei der Untersuchung von IT-Sicherheitsvorfällen zum Einsatz, wenn beispielweise externe Angreifer ins Firmennetz eindringen oder Malware in IT-Infrastruktur eingebracht wurde. Auch bei vermuteten Complianceverstößen, zum Beispiel Industriespionage, Korruption, Wettbewerbsdelikten, Arbeitsrechts-, Datenschutz-, Umwelt- oder Ethikverstößen, werden anlassbezogene Sonderuntersuchungen durchgeführt, bei denen häufig auf Methoden der IT-Forensik und/oder auf entsprechende Expertise aus der IT-Forensik zurückgegriffen wird.



Die Entwicklungen zeigen, dass Complianceanforderungen die Forensic Readiness vorantreiben und eine Verbesserung der Datenorganisation zwingend erforderlich ist.

Ähnlich wie in der IT-Sicherheit, die zum Beispiel die Empfehlungen bezüglich des kontinuierlichen Passwortänderungszwangs für Anwender zurückgenommen hat, sind auch die Methoden und Rahmenbedingungen der IT-Forensik einem stetigen Wandel ausgesetzt und müssen deswegen fortlaufend angepasst werden. Dieser Evolutionsdruck wird etwa durch die rechtlichen Rahmenbedingungen (die anlässlich des einjährigen Bestehens der DSGVO im vergangenen Monat gerade wieder intensiv diskutiert werden), den technologischen Fortschritt, Änderungen im Nutzungsverhalten und nicht zuletzt Prozessveränderungen ausgelöst. Bei Prozessveränderungen sorgen hier nicht nur eigene Prozesse für zusätzliche Dynamik, auch beispielsweise die Ablösung von Software, die längerfristig mit Sicherheitsupdates versorgt wird, durch Software, die einer kontinuierlichen Weiterentwicklung durch die Hersteller unterliegt – also die Umstellung von „Extended Support Releases“

ComplianceBusiness
Ausgabe 2 // Juni 2019

auf„Rolling Releases“ – wirkt sich hier auf die Methoden der IT-Forensik aus. Durch diese Umstellung der Softwareentwicklung ändern sich zum Beispiel die durch IT-Forensiker analysierten Artefakte, also die durch die Nutzung verursachten Daten, häufiger und unstetiger.

IT-Forensik und Complianceanforderungen

In der IT-Forensik wird in der Regel zwischen Live-Response- und Offlineanalysen (letztere oft auch als Postmortem-Analysen bezeichnet) unterschieden. Beim Live-Response wird an aktiven Systemen gearbeitet, wenn zum Beispiel flüchtige Daten für die Untersuchung des Sachverhalts gesichert werden müssen oder Systeme nicht ausgeschaltet werden können. Hierbei besteht die Gefahr, dass durch die Sicherungsvorgänge Daten zerstört werden und relevante Informationen verloren gehen. Bei der Offlineanalyse wird in der Regel mit einer forensischen Kopie gearbeitet. Hier kann es, bei richtigem Vorgehen, zu keinerlei Datenverlust kommen, und alle Arbeitsschritte können wiederholt und somit überprüft werden. Daten, die ausschließlich im flüchtigen Speicher vorgehalten werden, stehen so allerdings nicht zur Verfügung. Entsprechend muss bei der Planung möglicherweise das Vorgehen abgewogen werden. Unternehmen haben hierbei den Vorteil, dass sie ihre eigene Infrastruktur kennen und sich so im Rahmen einer strategischen Planung, oft auch als Forensic Readiness bezeichnet, entsprechend vorbereiten können. Hier haben die Complianceanforderungen, zum Beispiel die Meldefristen aus der DSGVO, eine Professionalisierung ausgelöst, die sich auch auf mittlere und kleine Unternehmen erstreckt und von der die IT-Forensik bei Sonderuntersuchungen profitiert. Die Information Governance, also ein geschäftlicher Ansatz zur Nutzung, Speicherung und Löschung von geschäftlichen Informationen, wurde entsprechend transparent gestaltet. Als weiteres Beispiel lässt sich das Geschäftsgeheimnisgesetz nennen, in dessen Rahmen sich gerade die Weiterentwicklung von Data Governance, also die Steuerung der Speicherung, Sicherung und des Austauschs von Daten, abzeichnet. Die damit einhergehenden Berechtigungseinschränkungen werden nicht nur die Sicherheit vor Cyberangriffen erhöhen, sondern auch den Aufwand von IT-Forensik-Untersuchungen reduzieren, wenn zum Beispiel Zugriffe auf Geschäftsgeheimnisse untersucht werden sollen.

Bei einigen Business-Applikationen, insbesondere im Cloudumfeld, sind mittlerweile „Beweissicherungsverfahren“, im Englischen in der Regel als „litigation hold“ bezeichnet, implementiert worden und erlauben die Präservation von elektronisch gespeicherten Informationen auf Knopfdruck.

Nicht alle Entwicklungen wirken sich allerdings arbeitserleichternd auf die IT-Forensik aus. Neben den gestiegenen Anforderungen und Dokumentationspflichten aus dem Datenschutz und der Datensicherheit ist hier die Tendenz zu nennen, Gesetze zur Nationalisierung der Datenverarbeitung und -speicherung einzuführen. Dadurch wird der IT-Forensik-Aufwand insbesondere bei multinationalen internen Investigationen deutlich erhöht.

IT-Forensik und Nutzungsverhalten

Durch die weiterhin kontinuierliche Verschiebung zu mobilen Geräten ist es wenig verwunderlich, dass auch die Notwendigkeit, mobile Geräte auszuwerten, weiterhin zunimmt. Global betrachtet, also ohne die Begrenzung auf interne Ermittlungen, sind Smartphones mittlerweile zur häufigsten Datenquelle aufgestiegen, gefolgt von PCs, einschließlich Laptops und Überwachungskamerasystemen. Technisch steht hierbei die meist ausgereifte Verschlüsselung einer physikalischen, forensischen Analyse entgegen und führt zu erheblichen Einschränkungen. Die große Anzahl an unterschiedlichen Applikationen auf mobilen Geräten führt zu einer ebenfalls steigenden Anzahl von Artefakten, die als Informationsquelle zur Verfügung stehen, aber auch zu einem erhöhten Auswertungsaufwand führen.

Auch bei den Angriffsmethoden sind Veränderungen zu beobachten, die sich über die Sicherheitsmaßnahmen auf das Nutzerverhalten auswirken. Advanced-Persistant-Threat(ATP)-Angriffsmethoden – dies sind hochtechnologisierte, fortgeschrittene und andauernde Angriffe auf die Informationstechnik durch wenige hochprofessionalisierte Angreifer – werden nachgeahmt und automatisiert und wandeln sich dadurch zu einer nun allgemeinen Bedrohung. So wurden zum Beispiel Spear-Phishing-Angriffe, also Angriffe, die wie ein „Speerangriff“ auf eine einzelne Person zielen und dafür individuell auf das Ziel zugeschnitten sind, automatisiert und zum Massenangriff weiterentwickelt. Um diesem, als Dynamit-Phishing bezeichneten Verfahren zu begegnen, wurde in vielen Unternehmen die Datenkommuni-

ComplianceBusiness
Ausgabe 2 // Juni 2019

kation mit Externen eingeschränkt und zum Beispiel der Empfang und Versand von Officedateien, welche Makros enthalten, unterbunden. Gleichzeitig werden aus dem Privaten gewohnte Kommunikationskanäle nicht oder nicht mit dem erwarteten Komfort angeboten. Die fehlenden Datenkanäle oder Messagingdienste werden dann häufig über private Geräte subsumiert. Diese sogenannte „Schatten-IT" kann bei internen Sonderuntersuchungen im Regelfall nicht mitanalysiert werden und schränkt die Erkenntnisgewinnmöglichkeiten der internen Ermittler ein. Hieraus ergibt sich oft auch eine Veränderung in der zu untersuchenden Fragestellung. Nun kann beispielsweise die Quellenidentifikation verstärkt in den Fokus rücken. Dann sind Analysen zum Beispiel nicht mehr auf Drucker/Kopierer ausgerichtet, auf denen ein geschütztes Dokument ausgedruckt oder kopiert wurde, sondern beschäftigen sich eher mit der Fragestellung, mit welchem Smartphone ein Dokument abfotografiert wurde. Entsprechend kann nun schon das Anzeigen eines Dokuments auf einem Bildschirm und nicht mehr das Kopieren der ganzen Datei – auf zum Beispiel einen USB-Datenträger – als einziges Indiz für eine Datenausleitung vorhanden sein.

Darknet und Co.

Durch internationale Zusammenarbeit hat die Polizei jüngst wieder einige Darknetmarktplätze geschlossen. Neben klassischer Polizeiarbeit kamen auch dabei Methoden, die der IT-Forensik zuzurechnen sind, zum Einsatz. Der gezielte Einsatz von VPNs, also virtuellen Netzwerken, mit denen sich Täter unter anderem anonymisieren können, ist nicht immer stabil möglich, und so kann ein einzelner Aussetzer des VPN-Dienstes den IT-Forensikern beispielsweise einen Hinweis auf eine verschleierte Identität geben. Zusätzlich können bei der IT-forensischen Ermittlung Informationen aus unterschiedlichen Jahren und unterschiedlichen Systemen miteinander kombiniert werden und dabei Spuren bis zu einem System verfolgt werden, auf dem eine nicht anonymisierte Identität verwendet wurde. Im Resultat vergleichbare Rahmenbedingungen könnten sich auch für Sonderuntersuchungen in Unternehmen ergeben. Die Vernetzung der ERP-Systeme wird fortlaufend verbessert, und über EDI-Schnittstellen (englisch für Electronic Data Interchange) werden externe Systeme angebunden. Wenn Vorsysteme nicht unter der Kontrolle des Unternehmens stehen, können diese Systeme nicht immer in die Untersuchung einbezogen werden. Hier liegt dann zwar keine gewollte Anonymisierung zugrunde, aber auch hier sind Systeme nicht einsehbar und können nur in Kooperation ausgewertet werden. Bis zur Umsetzung der EU-Whistleblowerrichtlinie, die bei Verstößen gegen EU-Recht wahrscheinlich Berichtseinsichtsrechte für die Hinweisgeber vorsieht, müssen hierfür Wege gefunden werden.

Zusammenfassung

Die Auswahl der hier aufgezeigten Entwicklungen macht deutlich, dass Complianceanforderungen die Forensic Readiness vorantreiben und eine Verbesserung der Datenorganisation deshalb zwingend erforderlich ist. Mobile Geräte wie Smartphones und Tablets dürfen bei internen Untersuchungen nicht ausgelassen werden und sollten auch in die strategische Vorbereitung aufgenommen werden. Zusätzlich führt die gestiegene Anzahl an Geräten und genutzten Systemen zu einer weiterhin stark steigenden Zahl an potentiellen Artefakten, die durch Methoden der IT-Forensik ausgewertet werden können, was wiederum neue Prozesse erfordert, die solches bewältigen können. Auch in Zukunft sind Möglichkeiten der Kooperation zwischen Unternehmen, die vernetzte Systeme nutzen, eine notwendige Voraussetzung für gewinnbringende IT-forensische Arbeit.

Hanno Baur

Manager, Ebner Stolz, Köln

Hanno.Baur@ebnerstolz.de
www.ebnerstolz.de