Einsatz von digitaler Forensik in Unternehmen und Organisationen

Stefan Meier, Günther Pernul

Lehrstuhl Wirtschaftsinformatik I - Informationssysteme
Universität Regensburg
Universitätsstraße 31
D-93053 Regensburg
stefan.meier@ur.de
guenther.pernul@ur.de

Abstract:
Zielgerichtete und hoch spezialisierte Angriffe auf die IT-Systeme erschweren es zunehmend die Systeme abzusichern und für alle Angriffsszenarien entsprechende Maßnahmen im Vorfeld zu etablieren. Aus diesem Grund ist es nötig die Täterverfolgung zu forcieren, anstatt nur in abwehrende IT-Sicherheitsmaßnahmen zu investieren. Zur Verfolgung von Tätern eignen sich besonders Methoden aus dem Bereich der digitalen Forensik. Mithilfe der durch digitale forensische Untersuchungen gewonnenen hieb- und stichfesten digitalen Beweise ist es nicht nur möglich einen IT-Sicherheitsvorfall umfassend aufzuklären, sondern auch die Täterverfolgung einzuleiten. Die gesammelten digitalen Spuren können dann letzten Endes auch vor Gericht verwendet werden. Inwieweit Organisationen bereits in der Lage sind solche digitalen forensischen Untersuchungen durchzuführen ist bisher in der Literatur jedoch noch nicht umfassend geklärt. Deshalb wurde im Rahmen der in diesem Paper präsentierten Studie der tatsächliche Status Quo der digitalen Forensik in Unternehmen und Organisationen umfassend untersucht. Die Ergebnisse der Studie zeigen, dass aktuell noch ein erheblicher Aufholbedarf besteht. Weiter hat die Studie gezeigt, dass auch die Wissenschaft gefordert ist, entsprechende Methoden bereitzustellen.

1 Motivation und Zielsetzung

Zielgerichtete Angriffe auf Unternehmensnetze wie der Angriff auf das Playstation Network[1] von Sony oder der erfolgreiche Angriff auf den IT-Sicherheitsspezialisten RSA[2] (EMC Corporation) haben gezeigt, dass es für Unternehmen unabdingbar ist sich mit dem Thema digitale Forensik zu beschäftigen. Die erfolgreichen Angriffe zeigen, dass heute kein Unternehmensnetzwerk vor einem Angriff sicher ist. Auch die Abschottung von IT-Systemen vom Internet ist keine ausreichende Garantie mehr für die Sicherheit von IT-

[1] Update on PlayStation Network and Qriocity `http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/` (Zugriff am 30.01.2014)

[2] Frequently asked questions about rsa securid, `http://www.emc.com/collateral/guide/11455-customer-faq.pdf` (Zugriff am 30.01.2014)

Systemen. Dies hat z.B. der Stuxnet-Wurm[3] eindrucksvoll gezeigt. Der bei einem solchen zielgerichteten Angriff entstehende Schaden kann dabei enorme und für manche Organisationen auch existenzbedrohende Ausmaße annehmen [BSJ10]. Dabei ist der direkt zu beziffernde Schaden oft nur die Spitze des Eisberges [ABB+12]. Neben rechtlichen Konsequenzen wie Schadensersatzforderungen oder Strafen kann der Ruf einer Organisation enorm leiden. Um schnell und zielgerichtet auf einen erfolgreichen Angriff reagieren zu können, bieten sich Methoden aus der digitalen Forensik an. Neben einer umfassenden Aufklärung eines IT-Sicherheitsvorfalls können im Rahmen von digitalen forensischen Untersuchungen auch Spuren bzw. Beweise zur Täterverfolgung gerichtsfest gesichert werden. In vielen Publikationen wird die Verwendung von digitaler Forensik zur Aufklärung von IT-Sicherheitsvorfällen in Organisationen propagiert und gilt teilweise auch bereits als gegeben [Row04, PIP10]. In anderen Arbeiten wird dagegen von einem erheblichen Nachholbedarf von Unternehmen gesprochen [MGL11]. Der tatsächliche Stand der Integration und Verwendung von digitaler Forensik in Organisationen wurde jedoch noch nicht umfassend untersucht. Ziel der in diesem Paper präsentierten Studie ist es deshalb den tatsächlichen Stand der Integration und Verwendung von digitaler Forensik in Organisationen zu klären. Weiter sollten auch Hinweise auf Forschungslücken im Bereich der digitalen Forensik in Organisationen gefunden werden.

Das Paper ist wie folgt aufgebaut: Im nächsten Abschnitt 2 werden verwandte Arbeiten bzw. Themengebiete aufgezeigt. In Abschnitt 3 werden das Design sowie die Ziele der Studie im Detail vorgestellt. Die Ergebnisse der Studie werden dann in Abschnitt 4 vorgestellt und in Abschnitt 5 diskutiert. Im letzten Abschnitt 6 folgt dann eine kurze Zusammenfassung des Papers und ein Ausblick auf weitere Themen im Gebiet der Unternehmensforensik.

2 Verwandte Arbeiten

Mit der Integration und Verwendung von digitaler Forensik in Organisationen beschäftigt sich insbesondere das Gebiet der *Forensic Readiness*. Die Ziele der *Forensic Readiness* sind zum einen den Nutzen der gesammelten digitalen Spuren zu erhöhen und zugleich die Kosten für Untersuchungen zu verringern [Tan01]. Um *Forensic Readiness* zu erreichen, wurden in der Literatur bereits verschiedene Maßnahmen vorgeschlagen. Ein umfassendes Werk mit Vorschlägen zur Implementierung von *Forensic Readiness* ist [Row04]. Rowlingson legt dabei in einer eher pragmatischen Sichtweise die benötigten Richtlinien und Vorgehensweisen für Unternehmen in seinen zehn Schritten zur *Forensic Readiness* dar. In [Row04] wird zudem gezeigt, dass digitale Forensik eine Ergänzung und Verbesserung zu bestehenden Aktivitäten wie dem Risikomanagement, dem Vorfallsmanagement, der IT-Sicherheitsüberwachung sowie der Aus- und Weiterbildung sein kann. Außerdem wird nach einem Vorfall ein explizites Lernen der Organisation von einem Vorfall gefordert [Row04]. Eine weitere Arbeit aus dem Bereich *Forensic Readiness* ist [YM01]. Yasinsac und Manzano schlagen Richtlinien zur Verbesserung digitaler foren-

[3] The Real Story of Stuxnet, `http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet` (Zugriff am 30.01.2014)

sischer Untersuchungen nach dem Eintreten von Vorfällen der Computerkriminalität vor. Weiter wird eine bessere Täterverfolgung gefordert, die nach Ansicht der Autoren durch Computer- und Netzwerkforensik ermöglicht wird [YM01]. Daneben ist auch ein Bewusstsein für IT-Sicherheitsrichtlinien, sowie insbesondere deren Einhaltung im Management nötig [WWW03]. Die Einbettung von digitaler Forensik in das IT-Sicherheitsmanagement und insbesondere das Vorfallsmanagement ist ein weiterer nötiger Aspekt [WWW03, PMB03, PK10]. Zudem muss verhindert werden, dass Geschäftsabläufe massiv gestört und unterbrochen werden [PMB03]. Um dies sicherzustellen muss digitale Forensik im und vom Unternehmen selbst betrieben werden und darf nicht komplett an Dritte ausgelagert werden [PMB03]. Mit dem Fokus auf kleine und mittlere Unternehmen stellen Barske et al. Maßnahmen zur Implementierung von *Forensic Readiness* vor [BSJ10]. Dabei bedienen sich Barske et al. größtenteils der Maßnahmen und Konzepte aus bereits vorhandenen Werken im Bereich *Forensic Readiness*, wie z.B. [Tan01] oder [Row04] und zeigen diese für den Kontext der kleinen und mittleren Unternehmen auf. Aufgrund der vielen unterschiedlichen Initiativen, sowohl in Organisationen wie auch bei öffentlichen Einrichtungen wird in [MGL11] eine Standardisierung innerhalb des Bereichs *Forensic Readiness* gefordert.

Um die Reife eines Unternehmens hinsichtlich der *Forensic Readiness* festzustellen, wird von Chryssanthou und Katos ein Reifegradmodell vorgestellt [CK12]. Je nachdem welche Maßnahmen zur Vorbereitung einer digitalen forensischen Untersuchung im Unternehmen implementiert sind, wird das Unternehmen auf einer Skala von 0 bis 5 eingeordnet. 0 bedeutet, dass nahezu keine Vorbereitungen getroffen wurden und 5 bedeutet, dass über alle notwendigen Maßnahmen hinaus Vorbereitungen getroffen wurden.

Für die konkrete Durchführung von digitalen forensischen Untersuchungen wird neben den vorbereitenden Maßnahmen vor allem ein Vorgehensmodell benötigt. In [Cas11, S. 187ff], [FS07] und [DF11, S. 57ff] finden sich verschiedene Vorgehensmodelle zur Durchführung von Untersuchungen. Grundsätzlich sind die Phasen Vorbereitung, Identifizierung, Konservierung, Untersuchung und Analyse sowie Präsentation in fast allen Modellen, jedoch teilweise in unterschiedlichen Ausprägungen enthalten [Cas11, S. 189f]. Eine allgemein akzeptierte und standardisierte Vorgehensweise gibt es jedoch bisher nicht, obwohl insbesondere von Dewald und Freiling auf die besondere Wichtigkeit eines Vorgehensmodells hingewiesen wird [DF11, S. 84].

Zusammenfassend bieten die vielen Veröffentlichungen ein breites Spektrum an Maßnahmen welche in Organisationen implementiert werden könnten. In manchen Publikationen wird deshalb auch bereits von der digitalen Forensik als zentrales Element der ITK-Infrastruktur gesprochen [PIP10]. Die tatsächliche Integration von Maßnahmen der digitalen Forensik in Organisationen wurde jedoch noch nicht genauer untersucht.

3 Studiendesign und Durchführung

Wie bereits in den vorangegangenen Abschnitten erwähnt soll diese Studie klären, ob sich Organisationen tatsächlich bereits aktiv mit dem Thema digitale Forensik beschäftigen.

Weiter sollte geklärt werden, ob und für welchen Zweck digitale Forensik in Organisationen verwendet wird, wenn es bereits eingesetzt wird.

Da die digitale Forensik in Organisationen oft mit IT-Sicherheitsvorfällen in Verbindung gebracht wird sollten auch Beziehungen zum Bereich IT-Sicherheit überprüft werden. Insbesondere die im Rahmen einer Zertifizierung des IT-Sicherheitsmanagements nach ISO 27001 oder BSI Grundschutz umgesetzten Maßnahmen gelten als Basisvoraussetzungen für digitale forensische Untersuchungen [Nel06], weshalb hier auch die Details etwaiger Beziehungen genauer mit untersucht werden sollten.

Sollte eine Organisation bisher noch keine forensischen Untersuchungen durchgeführt haben bzw. entsprechende Methoden zur *Forensic Readiness* noch nicht implementiert haben sollte geklärt werden, welche Gründe gegen den Einsatz von digitaler Forensik sprechen bzw. welche Probleme es bei der Implementierung vorbereitender Maßnahmen gibt.

Zusammenfassend lassen sich folgende Forschungsfragen ableiten, die mithilfe der Studie geklärt werden sollten:

1. Haben sich Organisationen bereits mit der Thematik digitale Forensik beschäftigt und entsprechende Maßnahmen und Ressourcen etabliert?
2. Zu welchem Zweck werden Methoden der digitalen Forensik verwendet?
3. Sehen die Organisationen Beziehungen zum IT-Sicherheitsmanagement?
4. Welche Gründe stehen dem Einsatz von digitaler Forensik in Organisationen entgegen?

Zur Durchführung der Studie wurde ein Fragebogen mit insgesamt 21 Fragen erstellt. Der Fragebogen war sowohl als „Offlineversion“ in Papierform verfügbar als auch online mithilfe des Systems SoSci Survey[4] modelliert. Potentielle Teilnehmer wurden entweder per E-Mail eingeladen den Onlinefragebogen auszufüllen oder auf Veranstaltungen mit dem Themenschwerpunkt IT-Sicherheit direkt akquiriert. Insgesamt konnten im Untersuchungszeitraum vom 15.05.2013 bis 24.06.2013 **69 Organisationen** erfolgreich befragt werden.

4 Ergebnisse

Da die Studie im deutschsprachigen Raum durchgeführt wurde ist es nicht überraschend, dass von den 69 befragten Organisationen 65 ihren Hauptsitz in Deutschland haben. Von den verbliebenen vier Organisationen hat je eine Organisation ihren Sitz in Frankreich, Japan, der Türkei und in den Vereinigten Staaten. Abbildung 1 zeigt die Größe der Unternehmen gemessen an deren Mitarbeiterzahl und der zugehörigen Branche. Deutlich zu sehen ist in Abbildung 1, dass es gelungen ist Organisationen aus verschiedenen Branchen und mit unterschiedlicher Größe zu akquirieren. Die Unternehmensgröße ist in Form der

[4] https://www.soscisurvey.de/

Mitarbeiterzahl angegeben, da manche Unternehmen die Frage nach dem Umsatz der Organisation nicht beantwortet haben. Im Folgenden und bei allen Hypothesentests wird deshalb als Kennzahl für die Unternehmensgröße immer die Anzahl der Mitarbeiter verwendet. Bei allen Hypothesentests gilt zudem eine Irrtumswahrscheinlichkeit von $\alpha = 0,05$. Das Hypothesenpaar ist dabei definiert als H_0: Die Merkmale sind unabhängig. H_1: Die Merkmale sind abhängig.

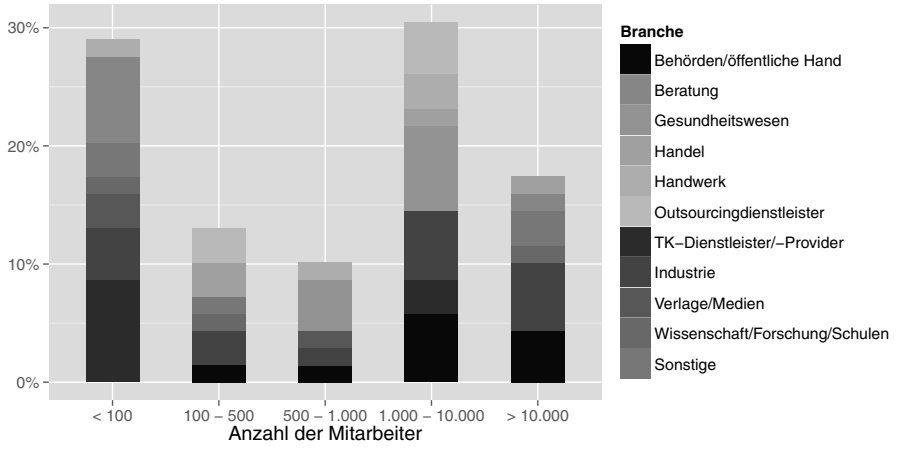


Abbildung 1: Teilnehmer nach Anzahl der Mitarbeiter und Branche

Neben der Mitarbeiterzahl wurde das jährliche Budget für IT-Sicherheit abgefragt. Dabei sind die Ausgaben für IT-Sicherheit höher, je größer ein Unternehmen ist (Spearmans Rangkorrelationskoeffizient (r_s) = 0,82). Dieser Zusammenhang ist auch statistisch signifikant bei einem p-Wert von 0,00. Zwischen der Branche und den Ausgaben für IT-Sicherheit beträgt der Kontingenzkoeffizient (K) 0,77, jedoch muss aufgrund eines p-Wertes von 0,20 ein statistischer Zusammenhang abgelehnt werden.

Die zentrale Frage nach der Implementierung bzw. Verwendung von digitaler Forensik sollte zum einen über die Frage nach der bewussten Implementierung von Maßnahmen aus der *Forensic Readiness* beantwortet werden und außerdem über die Frage, ob im Unternehmen bereits digitale forensische Untersuchungen durchgeführt wurden bzw. dies zukünftig geplant ist. Abbildung 2 zeigt die Antworten auf die beiden Fragen in einer kombinierten Darstellung. Die Balken zeigen jeweils den Prozentsatz der Antworten auf die Frage nach der Implementierung von *Forensic Readiness*. Die Antwort auf die Frage, ob im Unternehmen bereits eine digitale forensische Untersuchung durchgeführt wurde wird über die Füllung der Balken in Abbildung 2 dargestellt. Abhängig von der Antwort auf die erste Frage wurde die Antwort auf die zweite Frage dem entsprechenden Balken zugeordnet. Lediglich 15,93 % der Organisationen haben demnach bereits Maßnahmen aus dem Bereich *Forensic Readiness* implementiert. 40,60 % der Organisationen planen zukünftig konkrete Maßnahmen zu implementieren und in 43,47 % der Organisationen spielt das Thema *Forensic Readiness* überhaupt keine Rolle. Digitale forensische Untersuchungen haben bereits 37,68 % der befragten Organisationen durchgeführt. In 62,32 % der

Organisationen wurden noch keine Untersuchungen durchgeführt und es sind auch keine digitalen forensischen Untersuchungen geplant.

Betrachtet man Abbildung 2 genauer, so lässt sich eine Korrelation zwischen der Durchführung von Untersuchungen und der Implementierung bzw. Planung von Maßnahmen der *Forensic Readiness* vermuten. Die Korrelation lässt sich mit einem r_s von 0,58 bestätigen und ist statistisch signifikant bei einem p-Wert von 0,00. Eine besondere Abhängigkeit zwischen einer Zertifizierung nach ISO 27001 bzw. BSI Grundschutz und der Durchführung digitaler forensischer Untersuchungen kann dagegen nicht nachgewiesen werden.

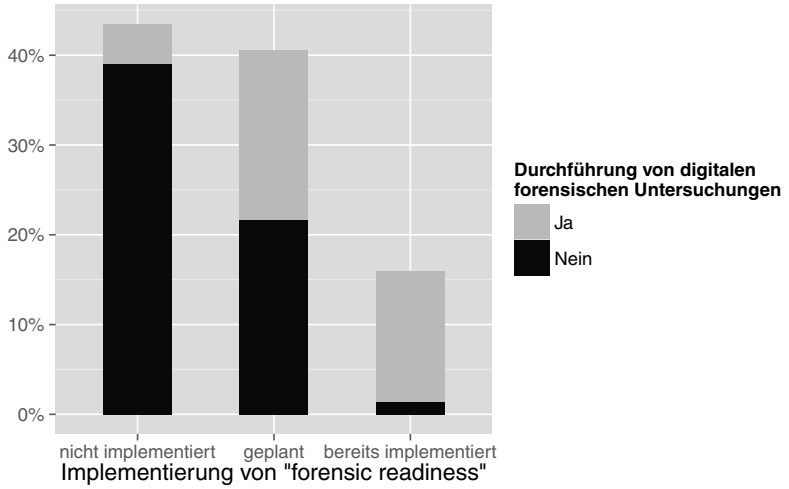
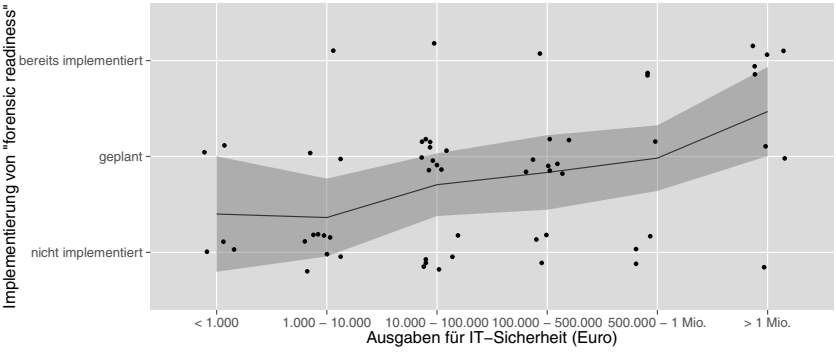


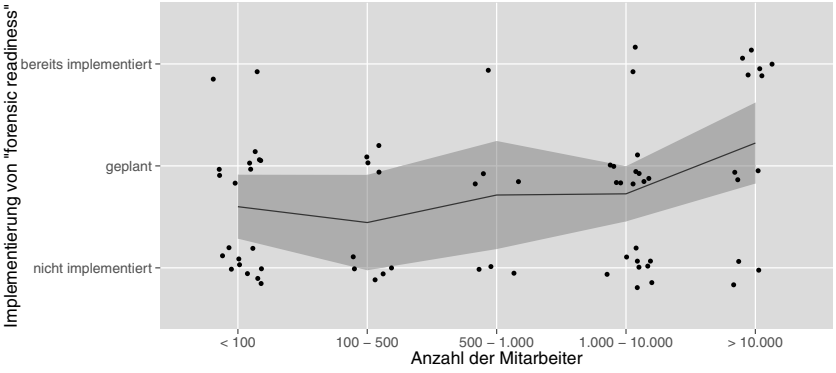
Abbildung 2: Implementierung von *Forensic Readiness* und Durchführung digitaler forensischer Untersuchungen

Hinsichtlich der Implementierung von *Forensic Readiness* kann weiter eine Korrelation zur Größe einer Organisation als auch zu den IT-Sicherheitsausgaben nachgewiesen werden. Abbildung 3(a) zeigt die Ausgaben für IT-Sicherheit in Relation zur Implementierung von *Forensic Readiness*. Die Korrelation ist bei r_s = 0,41 (p-Wert = 0,00) eher schwach. Dasselbe gilt für die Abhängig der *Forensic Readiness* von der Unternehmensgröße, dargestellt in Abbildung 3(b). Hier kann lediglich eine sehr schwache aber statistisch signifikante Korrelation von r_s = 0,24 (p-Wert = 0,02) nachgewiesen werden. Eine Abhängigkeit des Implementierungsgrades von der Branche muss jedoch abgelehnt werden (K = 0,63, p-Wert = 0,20). Weiter hat auch die Bedeutung von IT-Systemen für den Geschäftsbetrieb nur eine geringe (r_s = 0,30, p-Wert: 0,01) Auswirkung auf die Implementierung von Maßnahmen der *Forensic Readiness*. Eine Zertifizierung nach ISO 27001 bzw. BSI Grundschutz und die Implementierung bzw. geplante Implementierung von Maßnahmen der *Forensic Readiness* korrelieren dagegen mit einem r_s von 0,48 (p-Wert = 0,00).

Neben den präventiven Maßnahmen der IT-Sicherheit sollte auch geprüft werden, ob die befragten Organisationen tatsächlich bereits Opfer von Computerkriminalität bzw. digitalen Angriffen wurden. Eine Organisation hat bei dieser Frage keine Auskunft erteilt. Von



(a) *Forensic Readiness* und Ausgaben für IT-Sicherheit



(b) *Forensic Readiness* und Unternehmensgröße

Abbildung 3: Ausgaben für IT-Sicherheit bzw. Unternehmensgröße in Relation zur *Forensic Readiness*

den verbleibenden 68 Organisationen wurden 40,0 % bereits Opfer von Angriffen. Wenn eine Organisation bereits einem Angriff auf ihre IT-Systeme zum Opfer gefallen ist, so könnte man meinen, dass diese sich auf zukünftige Angriffe besser vorbereitet. Ein Zusammenhang zwischen der Implementierung von *Forensic Readiness* und der Opfer von Angriffen kann jedoch nicht nachgewiesen werden (r_s = 0,13, p-Wert = 0,15). Auch die Ausgaben für die IT-Sicherheit sind bei Organisationen die bereits angegriffen wurden nicht zwingend höher als bei den anderen 60 % der noch nicht wissentlich erfolgreich angegriffenen Organisationen (r_s = 0,24, p-Wert = 0,07). Die Gruppe der noch nicht erfolgreich angegriffenen Organisationen wurde zudem befragt, ob die Organisation in naher Zukunft mit einem Angriff rechnet. Dabei gaben 44,0 % der Organisationen an, dass sie nicht mit einem Angriff rechnen und 56,0 % der Organisationen rechnen mit einem Angriff. Die Organisationen, die mit einem Angriff rechnen bereiten sich jedoch nicht zwingend besser auf digitale forensische Untersuchungen vor als die Organisationen die nicht mit einem Angriff rechnen (r_s = 0,19, p-Wert = 0,12).

4.1 Einsatz von digitaler Forensik in Organisationen

Abbildung 4 zeigt im Detail zu welchen Zwecken Methoden der digitalen Forensik in Organisationen verwendet werden. Am häufigsten verwenden Organisationen demnach digitale Forensik tatsächlich zur Täteridentifikation nach einem IT-Sicherheitsvorfall gefolgt von einem expliziten Lernen von einem digitalen Angriff zur Verbesserung der IT-Sicherheit. Darauf folgend wird digitale Forensik zur Untersuchung von Verstößen gegen interne Richtlinien verwendet und danach zur Aufklärung von klassischen Verbrechen. Bei der Häufigkeit von digitalen forensischen Untersuchungen gibt es keinen Zusammenhang zwischen großen Organisationen und häufigeren Untersuchungen (r_s = 0,19, p-Wert = 0,23). Weiter haben Organisationen die regelmäßig forensische Untersuchungen durchführen nicht zwingend interne personelle Ressourcen um diese Untersuchungen durchzuführen (r_s = 0,32, p-Wert = 0,20).

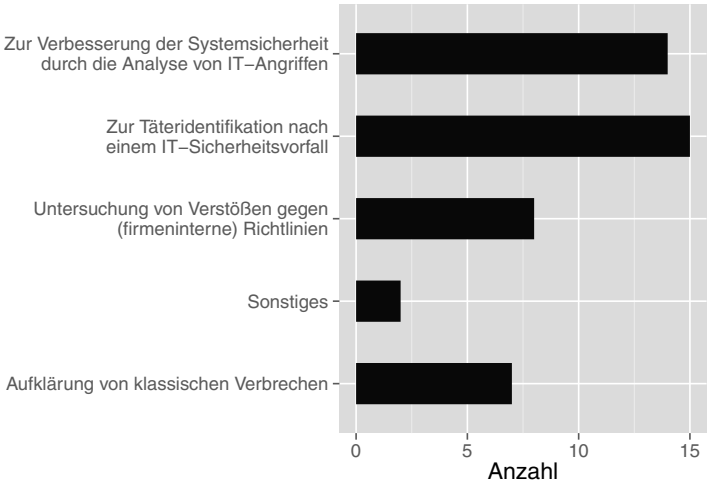


Abbildung 4: Verwendung von digitaler Forensik in Organisationen

Die Höhe der Ausgaben für IT-Sicherheit und die Höhe der Ausgaben für digitale Forensik korrelieren dagegen sehr stark bei einem r_s = 0,87 und einem p-Wert von 0,00.

4.2 Gründe für das Fehlen von digitalen forensischen Maßnahmen in Organisationen

Neben den im vorigen Abschnitt 4.1 beschriebenen konkreten Zielen von digitalen forensischen Untersuchungen wurde im Rahmen der Studie auch explizit nachgefragt wieso digitale Forensik gerade nicht eingesetzt wird. Abbildung 5 zeigt die Antworten auf diese Frage. Demnach wird digitale Forensik insbesondere aufgrund fehlender personeller und/oder finanzieller Mittel nicht eingesetzt gefolgt von fehlenden Best Practices für digi-

tale forensische Untersuchungen. In 15 Organisationen ist das Thema nicht einmal bekannt und vier Organisationen halten digitale Forensik sogar für nicht geeignet.

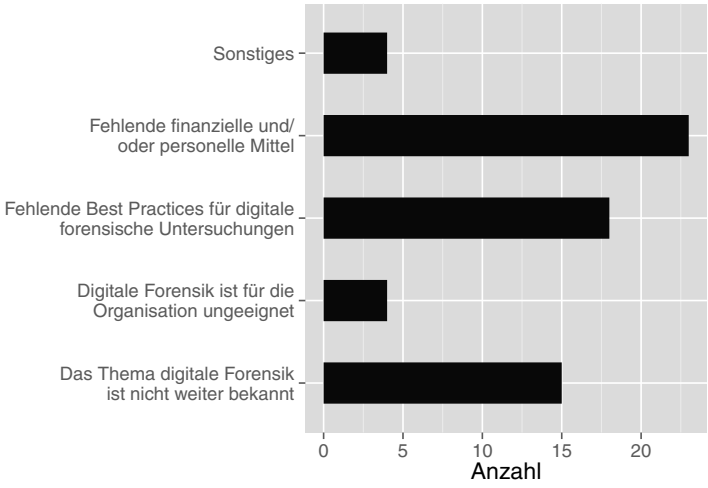


Abbildung 5: Gründe wieso digitale Forensik in Organisationen nicht zum Einsatz kommt

5 Bewertung der Ergebnisse

Im Folgenden sollen nun die in Abschnitt 3 aufgeworfenen Forschungsfragen mithilfe der Ergebnisse aus dem vorigen Abschnitt 4 diskutiert und beantwortet werden.

Frage 1: Haben sich Organisationen bereits mit der Thematik digitale Forensik beschäftigt und entsprechende Maßnahmen und Ressourcen etabliert?
Die Antwort auf diese Frage liefern die Ergebnisse aus der direkten Frage nach der Implementierung von Maßnahmen aus dem Bereich *Forensic Readiness* sowie der Nachfrage hinsichtlich der Durchführung von digitalen forensischen Untersuchungen. Die Antworten zeigen, dass manche, insbesondere große Organisationen sich bereits mit dem Thema auseinander gesetzt haben. Weiter wurden in 37,68 % der befragten Organisationen bereits digitale forensische Untersuchungen durchgeführt. Zusammenfassend lässt sich sagen, dass sich manche Organisationen bereits mit dem Thema digitale Forensik beschäftigt haben. In der Mehrzahl der Organisationen ist jedoch keine Forensikkompetenz vorhanden und das Thema digitale Forensik ist eher unwichtig.

Frage 2: Zu welchem Zweck werden Methoden der digitalen Forensik verwendet?
Forschungsfrage 2 lässt sich erschöpfend über Abbildung 4 beantworten. Es zeigt sich, dass digitale Forensik tatsächlich für die Täteridentifikation verwendet wird. Aber auch

die Kontrolle und Durchsetzung von internen Richtlinien mittels Methoden der digitalen Forensik zeigt, dass das breite Anwendungsspektrum zumindest in einigen wenigen Organisationen bereits ausgeschöpft wird.

Frage 3: Sehen die Organisationen Beziehungen zum IT-Sicherheitsmanagement?
Verbindungen zwischen der IT-Sicherheit und der digitalen Forensik können über das zur Verfügung stehende Budget für das jeweilige Thema nachgewiesen werden. So ist eine positive Korrelation zwischen der Höhe der Ausgaben für IT-Sicherheit und dem Budget für digitale Forensik nachweisbar. Was die Vorbereitung auf digitale forensische Untersuchungen mittels Methoden aus der *Forensic Readiness* angeht kann zumindest eine schwache positive Beziehung zu den Ausgaben für IT-Sicherheit festgestellt werden. Auch gibt es eine sehr schwache Korrelation zwischen einer vorhandenen Zertifizierung nach BSI Grundschutz bzw. ISO 27001 und der Implementierung von *Forensic Readiness*. Zusammenfassend können durchweg eher schwache bis mittelstarke Beziehungen zwischen den Gebieten nachgewiesen werden.

Frage 4: Welche Gründe stehen dem Einsatz von digitaler Forensik in Organisationen entgegen?
Neben den heute schon genutzten Möglichkeiten der digitalen Forensik hat die Studie insbesondere gezeigt wieso das Thema digitale Forensik gerade keine Rolle in der Mehrzahl der befragten Organisationen spielt. Abbildung 5 beantwortet diese Frage direkt. Neben fehlenden personellen wie auch finanziellen Mitteln sind insbesondere fehlende Best Practices Gründe wieso die digitale Forensik eine solch geringe Durchdringung erfährt. Auch ist es eher beunruhigend, dass manche Organisationen die digitale Forensik für ungeeignet halten bzw. das Thema noch gar nicht in der Organisation bekannt ist.

6 Fazit und Ausblick

Die Studie hat gezeigt, dass digitale Forensik in manchen Organisationen bereits in der vollen Breite genutzt wird. Viel wichtiger für die Wissenschaft ist jedoch die Erkenntnis, dass insbesondere Best Practices fehlen und auch die notwendigen personellen wie auch finanziellen Mittel zur Einführung und Nutzung von digitaler Forensik anscheinend noch zu hoch sind. Auch ist in vielen Organisationen ein Bewusstsein für die Thematik digitale Forensik nicht vorhanden. Deswegen besteht hier auch insbesondere in der Lehre und Ausbildung entsprechend Aufholbedarf, um das Wissen um die verfügbaren Mittel in die Organisationen hinein zu tragen.

Basierend auf den Ergebnissen der Studie sollten sich zukünftige Arbeiten auf dem Gebiet der digitalen Forensik in Organisationen insbesondere auf Methoden zur einfachen und möglichst kostengünstigen Implementierung von *Forensic Readiness* fokussieren. Bereits existierende Ansätze wie z.B. der Leitfaden „IT-Forensik“ [Bun11] sind teilweise sehr auf einzelne Implementierungen spezialisiert und nicht wissenschaftlich diskutiert. Gerade im Bereich der digitalen Forensik ist es jedoch nötig Methoden auch wissenschaft-

lich zu diskutieren, da zum einen die Beweiskraft durch die Verwendung anerkannter und überprüfter Best Practices gesteigert werden kann und zum Anderen auch Beschuldigte bzw. unabhängige Sachverständige die Möglichkeit haben die angewandten Verfahren transparent nachzuvollziehen.

Danksagung

Die Arbeit wurde unterstützt von "Regionale Wettbewerbsfähigkeit und Beschäftigung", Bayern, 2007-2013 (EFRE) als Teil des SECBIT Projekts (`http://www.secbit.de`).

Literatur

[ABB+12] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michael van Eeten, Michael Levi, Tyler Moore und Stefan Savage. Measuring the Cost of Cybercrime. In *11th Annual Workshop on the Economics of Information Security, WEIS 2012, Berlin, Germany, 25-26 June, 2012*, 2012.

[BSJ10] David Barske, Adrie Stander und Jason Jordaan. A Digital Forensic Readiness Framework for South African SME's. In *Information Security South Africa Conference 2010, Sandton Convention Centre, Sandton, South Africa, August 2-4, 2010. Proceedings ISSA 2010*. ISSA, Pretoria, South Africa, 2010.

[Bun11] Bundesamt für Sicherheit in der Informationstechnik. Leitfaden IT-Forensik, 2011.

[Cas11] Eoghan Casey. *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Academic Press, 3. Auflage, 2011.

[CK12] Anargyros Chryssanthou und Vasilios Katos. Assessing Forensic Readiness. In *Proceedings of the Seventh International Workshop on Digital Forensics & Incident Analysis (WDFIA 2012)*, 2012.

[DF11] Andreas Dewald und Felix Freiling. *Forensische Informatik*. Books on Demand, 1. Auflage, 2011.

[FS07] Felix C. Freiling und Bastian Schwittay. A Common Process Model for Incident Response and Computer Forensics. In *IT-Incidents Management & IT-Forensics - IMF 2007, Conference Proceedings, September 11-13, 2007, Stuttgart, Germany*, Jgg. 114 of *LNI*, Seiten 19–40. GI, 2007.

[MGL11] Antonis Mouhtaropoulos, Marthie Grobler und Chang-Tsun Li. Digital Forensic Readiness: An Insight into Governmental and Academic Initiatives. In *Proceedings of the 2011 European Intelligence and Security Informatics Conference*, EISIC '11, Seiten 191–196. IEEE Computer Society, 2011.

[Nel06] Anthony Nelson. ISO 27001 as a Support to Digital Forensics. *J. Digital Forensic Practice*, 1(1):43–46, 2006.

[PIP10] George Pangalos, Christos Ilioudis und I. Pagkalos. The Importance of Corporate Forensic Readiness in the Information Security Framework. In *Proceedings of the 2010*

19th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE 2010), WETICE '10, Seiten 12–16. IEEE Computer Society, 2010.

[PK10] Georgios Pangalos und Vasilios Katos. Information Assurance and Forensic Readiness. In *Next Generation Society. Technological and Legal Issues*, Jgg. 26 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Seiten 181–188. Springer Berlin Heidelberg, 2010.

[PMB03] John Patzakis, Scott Mann und Melisa Bleasdale. Computer Forensics in the Global Enterprise. In *1st Australian Computer, Network & Information Forensics Conference, 25 November 2003, Perth, Western Australia*. School of Computer and Information Science, Edith Cowan University, Western Australia, 2003.

[Row04] Robert Rowlingson. A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence (IJDE)*, 2(3), 2004.

[Tan01] John Tan. Forensic Readiness, 2001.

[WWW03] Jeni Wolfe-Wilson und Henry B. Wolfe. Management strategies for implementing forensic security measures. *Information Security Technical Report*, 8(2):55–64, 2003.

[YM01] Alec Yasinsac und Yanet Manzano. Policies to Enhance Computer and Network Forensics. In *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*. 2001.