Assignment zum Modul WIN03

Thema: Aufgabengebiet und Einsatz der Computer-Forensik im betrieblichen Umfeld

[redacted]

Inhaltsverzeichnis

1 Einleitung

1.1 Problemstellung

Einen Tag ohne digitale Unterstützungen, sei es privat oder beruflich, kann man sich kaum noch vorstellen. Mittels Smartphone, Tablet oder PC tauchen wir täglich in die digitale Welt ein und hinterlassen dort unsere Spuren. Die wenigsten machen sich dabei Gedanken über die Sicherheit oder die Publikation ihrer privaten Daten.

Aufgrund dessen stellt die Sicherheit der Informationstechnik ein wachsendes Problem dar. Organisationen wie Industriezweige, Banken, Krankenhäuser, Polizei, Öffentliche Einrichtungen und viele mehr, nutzen solche digitalen Dienste für den reibungslosen Ablauf von Geschäfts- und Arbeitsprozessen.[1] Angewiesen auf die Informationstechnologie, werden die oben genannten Organisationen zu einem idealen Ziel für Angreifer. Im Jahr 2015 wurde auf 58% der Unternehmensrechner mindestens ein Malware-Infizierungsversuch verzeichnet.

Angesichts der zahlreichen Angriffe auf Unternehmen, werden Forensiker mit der Ermittlung digitaler Spuren beauftragt, bevor die Polizei eingeschaltet wird.

Meist befinden sich die Täter in den eigenen Reihen, die sich berechtigterweise im selben Netzwerk befinden. Tatmotive reichen hierbei von Neid, Neugierde, Erpressung, Verkauf von Daten oder einfache Delikte wie Kollegen schlecht dastehen zu lassen.

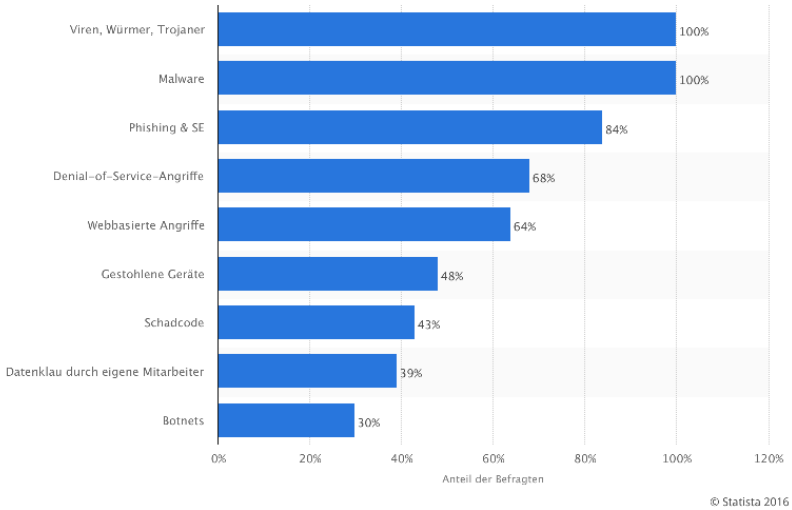


Abbildung 1: Cybercrime - Vorfälle 2015[2]

[1] URL: https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologiefrueherkennung/IT-Forensik/it_forensik.html

[2] URL: http://de.statista.com/statistik/daten/studie/186740/umfrage/datenklau-und-spionage-in-deutschen-unternehmen/

1.2 Ziel und Aufgabe der Arbeit

Ziel dieser Projektarbeit, ist das Aufgabengebiet und den Einsatz der Computerforensik im betrieblichen Umfeld darzustellen. Dazu werden die Grundlagen der Computerforensik, mit Hilfe der Definition, verschiedenen Vorgehensweisen und den Anforderungen der forensischen Untersuchung aufgeführt. Anhand eines ausgewählten Szenarios, wird gezeigt, wie man unter Anwendung des BSI Leitfaden und der Durchführung einer Post-mortem-Analyse, den mutmaßlichen Täter überführt. Des Weiteren werden die erfolgreich gesicherten Datenquellen aufgelistet, die im Falle eines Prozesses, als Beweismittel dienen. Eine Überarbeitung und Verbesserung des Sicherheitskonzeptes, wird für die Firma vorgeschlagen und teilweise durchgeführt, damit solch ein Vorfall in Zukunft nicht mehr auftritt.

2 Grundlagen

2.1 Computer-Forensik

Die klassische Forensik steht für wissenschaftliche und technische Arbeitsgebiete, bei denen meist kriminelle Handlungen systematisch untersucht werden.

„Der Begriff stammt vom lat. *forum:* Marktplatz, Forum (Plural: Foren). Im antiken Rom wurden Gerichtsverfahren, Untersuchungen, Urteilsverkündungen, sowie der Strafvollzug öffentlich auf dem Marktplatz durchgeführt. Unter Forensik werden heute jene Arbeitsgebiete zusammengefasst, in denen systematisch kriminelle Handlungen identifiziert, analysiert bzw. rekonstruiert werden.“[3]

Zu den Teilgebieten der klassischen Forensik zählt die Computer-Forensik, die auch als Digitale Forensik oder IT-Forensik bezeichnet wird. Diese Begriffe haben sich in den letzten Jahren bei den Ermittlungen im Bereich der Computerkriminalität durchgesetzt.

Eine Computer-Forensische Untersuchung, wird immer dann durchgeführt, wenn von einem kriminellen Vorfall im Bereich der IT ausgegangen wird. Mit Hilfe von Ermittlungs- und Analysetechniken, versucht der Forensiker eine Beweiskette zu dokumentieren, damit sich genau feststellen lässt, welche Vorgänge auf einem IT-System stattgefunden haben, sodass im Falle einer Gerichtsverhandlung diese Beweiskette auch verwertbar ist.[4]

[3] URL: http://wirtschaftslexikon.gabler.de/Definition/forensik.html
[4] Vgl. http://www.searchsecurity.de/definition/Computer-Forensik-IT-Forensik

2.2 Definition Computer-Forensik

Alexander Geschonneck beschreibt in seinem Buch „Computer Forensik“ den Begriff, mit folgender Definition: „Der Begriff Computer-Forensik oder auch Digitale Forensik hat sich in den letzten Jahren für den Nachweis und die Ermittlung von Straftaten im Bereich der Computerkriminalität durchgesetzt. In Anlehnung an die allgemeine Erklärung des lateinischen Worts Forensik ist die Computer-Forensik ein Teilgebiet, das sich mit dem Nachweis und der Aufklärung von strafbaren Handlungen z.B. durch Analyse von digitalen Spuren beschäftigt.“[5]

2.3 Arten forensischer Untersuchungen

Die Computer-Forensik lässt sich im Allgemeinen abhängig vom Zeitpunkt des Vorfalls in die Post-mortem-Analyse und die Live-Forensik unterteilen.

2.3.1 Post-mortem-Analyse

Mittels der Post-mortem-Analyse kann man nachträglich Vorfälle aufklären, aufgrund dessen wird das Verfahren auch als Offline-Forensik bezeichnet. Um das Verfahren anwenden zu können muss zuerst eine Datenträgerabbildung erstellt werden. Dies geschieht am sichersten mit Hilfe eines Write Blockers. Dieser verhindert, dass bei der Image-Erstellung versehentliches Schreiben und damit unsauberes Arbeiten entsteht. Dabei wird durch den Einsatz der speziellen Hardware und Software sichergestellt, dass die Kopie 1:1 identisch zum Original ist.

2.3.2 Live-Forensik

Bei der Live-Forensik richtet sich der Fokus auf die Gewinnung und Untersuchung gelöschter, umbenannter, versteckter oder verschlüsselter Dateien auf dem Datenträger.

Da bei der Offline-Forensik viele wertvolle Daten verloren gehen können, wenn der Computer vom Strom getrennt wird, gibt es eine weitere Methode welche als Live-Forensik bezeichnet wird. Mit der Live-Forensik oder auch Online-Forensik können sogenannte flüchtige Daten aufgespürt werden. Dabei werden zum Beispiel der Hauptspeicherinhalt, Informationen über anhaltende Netzwerkverbindungen und die aktiven Prozesse untersucht. [6]

---

[5] Geschonneck, A., S. 2

[6] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2011) S.13

2.4 Vorgehensweise bei einer forensischen Untersuchung

In diesem Abschnitt wird auf den forensischen Prozess laut BSI und das S-A-P Modell näher eingegangen.

2.4.1 S-A-P Modell

Das Secure-Analyse-Present-Modell (S-A-P) ist ein einfaches Modell, welches beschreibt, wie bei einer forensischen Untersuchung vorzugehen ist. Es richtet sich auf die anschließende Verfolgung von Straftaten aus.

- *Secure-Phase:* In dieser Phase wird die betroffene Datenquelle identifiziert und nach dem Vier-Augen-Prinzip gesichert. Dabei entsteht ein forensisches Abbild.
- *Analyse-Phase:* Diese Phase ist unterteilt in Vorbereitung, Durchführung und Interpretation. In der Vorbereitung wird zuerst die Master-Kopie dupliziert. Bei der Durchführung wird nach auffälligen Daten gesucht, die auf Zusammenhänge untersucht werden. Zuletzt gibt der Forensiker eine Bewertung in Bezug auf die Untersuchung ab.
- *Present-Phase:* Jetzt muss das vollständige Ergebnis zielgruppengerecht und glaubwürdig präsentiert werden.[7]

2.4.2 Der forensische Prozess laut BSI

Für die Anwendung einer forensischen Ermittlung, hat das BSI einen Leitfaden „IT-Forensik“, in dem ein erweitertes S-A-P Modell beschrieben ist. Das öffentliche Dokument der Bundesbehörde für IT-Sicherheit in Deutschland, dient als Wegweiser für forensische Untersuchungen. Der Prozess des BSI, wird in sechs Abschnitte unterteilt, wie in der Abbildung 2 zu sehen ist.[8]

[7] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2011) S.24
[8] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2011) S.13

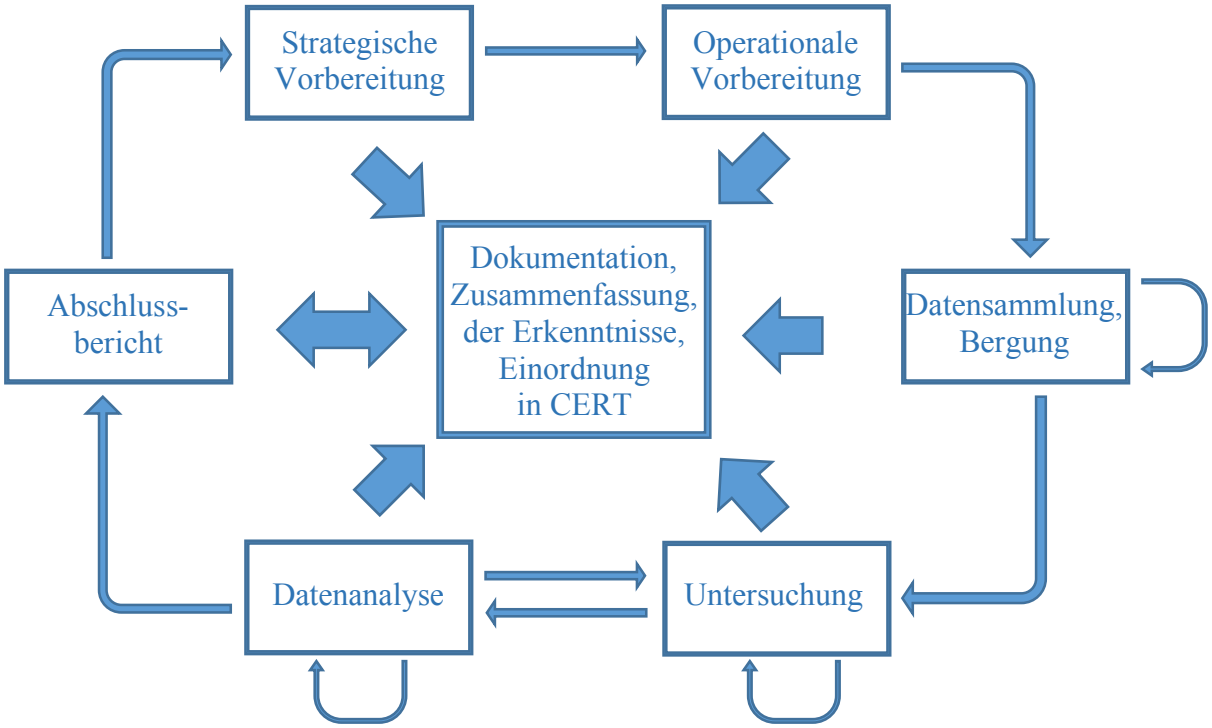


Abbildung 2: Abschnitte des forensischen Prozesses[9]

2.5 Anforderungen an den Ermittlungsprozess

Folgende Anforderungen werden an die Vorgehensweise der forensischen Untersuchung gestellt, damit die gewählten Methoden und Hilfsmittel, vor Gericht als glaubwürdig angesehen werden. Oftmals sitzen Dritte in einer Gerichtsverhandlung, die eventuell nicht das selbe technische Verständnis aufweisen. Daher ist es wichtig, die passenden Methoden und Hilfsmittel zu wählen:

- *Akzeptanz:* Angewandte Methoden müssen in der Fachwelt anerkannt sein. Neue Methoden müssen auf Korrektheit nachweisbar sein.
- *Glaubwürdigkeit:* Angewandte Methoden müssen robust und funktional sein.
- *Wiederholbarkeit:* Methoden müssen bei Anwendung Dritter gleiche Ergebnisse liefern.
- *Integrität:* Datensicherung muss auf Echtheit belegbar sein.
- *Ursache und Auswirkungen:* Ergebnisse der Methoden müssen logisch nachvollziehbar sein, um genaue Rückschlüsse ziehen zu können.
- *Dokumentation:* Angemessene Dokumentation aller Schritte.[10]

[9] URL: In Anlehnung an: https://www.maximiliankrieg.de/index.php/77-kosi/master/semester-1m/cofo/418-cofo-20150622
[10] Vgl. Geschonneck (2011) S.66

2.6 Ziele einer Ermittlung

Nach einem Systemeinbruch oder einem Sicherheitsvorfall, ergeben sich in der Regel folgende Ziele:

- Rekonstruktion der Vorgehensweise und entdecken der Lücke,
- Schadensermittlung,
- Überführung des Täters,
- Beweissicherung für gerichtliche Schritte.[11]

3 Anwendungsfall

3.1 Beschreibung

Das Szenario beschreibt ein mittelständisches Unternehmen, das Design Prototypen für einen namhaften Smartphone Hersteller entwickelt. Es gab einen ernstzunehmenden Vorfall, bei dem geheime Bilder eines Prototyps im Internet veröffentlicht wurden. Die Bilder sorgten für Schlagzeilen in den Medien und in der Presse, was für den Smartphone Hersteller einen immensen Schaden darstellte.

Der Firmenchef wandte sich zuerst an die interne IT, welche nach Auffälligkeiten im Netzwerk schauen sollte. Bei entdecken der Lücke, sollte diese von der IT geschlossen und zusätzlich der verantwortliche für das Leck gefunden werden.

Anhand der vorhandenen Logdateien erkannte der IT Mitarbeiter, dass jede Nacht um 3 Uhr, sensible Forschungsergebnisse von einem Computer mit der IP (192.168.0.123) aus der Entwicklungsabteilung an eine fremde IP-Adresse geschickt wurden. Um diese Uhrzeit befand sich jedoch keiner der Mitarbeiter physikalisch im Gebäude.

Um herauszufinden wie es zu diesem Datenklau kam, entschieden sich der IT Mitarbeiter und der Firmenchef einen IT-Forensiker zu beauftragen.

[11] Vgl. Geschonneck (2011) S.65

3.1.1 Gesamtübersicht

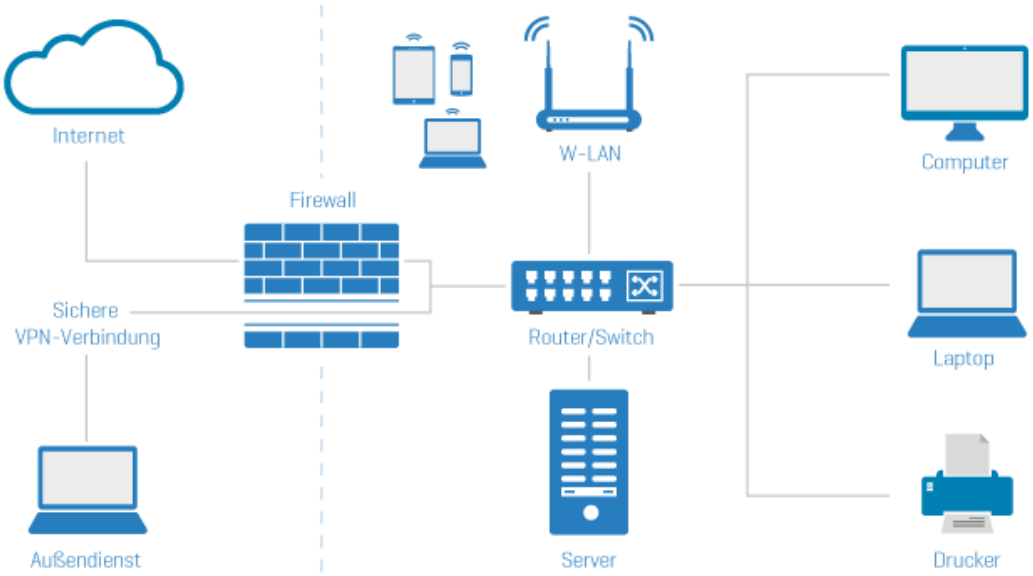


Abbildung 3: Firmeninfrastruktur[12]

3.1.2 Technische Details

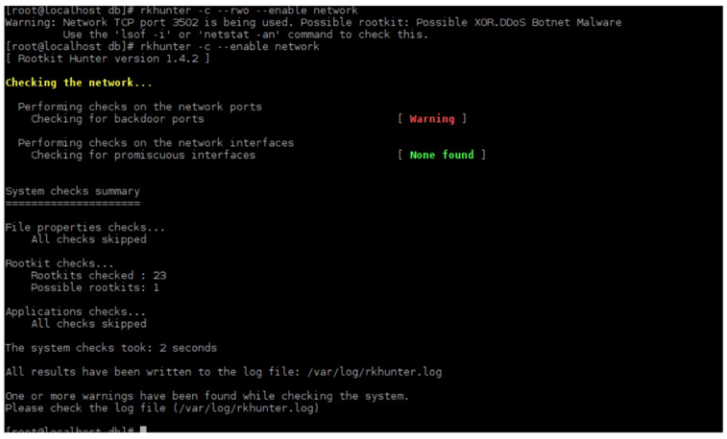
Auf den Firmencomputern befindet sich eine Standardinstallation von Microsoft Windows 7 Professional 64bit, die Windows-Firewall und Windows-Update sind deaktiviert. Die Computer sind über ein LAN-Kabel mit dem internen Firmennetz verbunden. Alle wichtigen Daten der Firma werden auf dem internen Server, in einer eigenen Datenbank gespeichert. Bilder und Spezifikationen sind zusätzlich auf den Firmen-Computern lokal gespeichert. Im ganzen Unternehmen wird keine Festplatten und Datenverschlüsselung verwendet. Die Datenbank ist mit einer eingebauten Verschlüsselung geschützt und verlangt beim Anmelden eine User-Identifikation mit User-Name und Passwort. Der Firmenserver und die Mitarbeiterterminals sind über einen Router mit dem Internet verbunden, welcher eine aktive Firewall besitzt. Außendienstmitarbeiter können über einen VPN-Verbindung auf das interne Netzwerk zugreifen. Die VPN-Verbindung wird auch über den Router appliziert. Im Firmen WLAN sind nur die von der Firma ausgegebenen Geräte zugelassen (MAC-Adressfilterung).

[12] URL: http://www.kosytec-portal.de/de/leistungen/it_infrastruktur/

3.2 Forensische Analyse

3.2.1 Vorgehensweise

Der IT-Forensiker richtet sein Vorgehen nach dem forensischen Prozess laut BSI aus. Er stellt nach Eintreffen fest, dass das Opfersystem sich im heruntergefahrenen Zustand befindet und physikalisch vom Netzwerk getrennt wurde, um einen weiteren Datendiebstal zu unterbinden. Er entscheidet sich erstrangig für das Post-mortem-Verfahren. Bei diesem Verfahren erstellt der Forensiker zuerst eine Kopie der Festplatte des Opfersystems, mit Hilfe eines Hardware-Writer-Blockers. Nachdem er ein weiteres Abbild der Master-Kopie erstellt hat, schließt er diese an seinem Arbeitscomputer an.[13] Diesen bootet er mit einer garantiert nicht infizierten Linux Live-CD (Knoppix). Unter Linux startet er das Terminal und überprüft die angeschlossene Festplatte mit den Programmen *chkrootkit* und *rkhunter* nach Viren und Trojaner. Nachdem *rkhunter* durchgelaufen war, konnte man anhand der Ausgabe erkennen, dass sich ein *rootkit* auf der Festplatte befindet, welches eine Malware verbirgt.



rkhunter checking network

Abbildung 4: Konsolenausgabe rkhunter[14]

Mit einer speziellen Linux Software spürt der IT Forensiker den versteckten Trojaner auf der Festplatte auf und entfernt diesen. Nach einem Neustart der Festplatte, lässt er diese noch ein weiteres Mal von seinen Forensik Tools überprüfen. Da alle weiteren Programme keinerlei Schadsoftware auf der Festplatte feststellen konnten, führt der Forensiker die selben Schritte an

[13] Vgl. Willer (2012) S.57
[14] URL: http://linoxide.com/security/xor-ddos-malware-rkhunter-centos-7/

der Originalen Festplatte durch. Anschließend baut er die originale Festplatte wieder in den Computer der Firma ein.
Nachdem das Opfersystem wieder vollständig funktioniert, erstellt der IT-Forensiker einen detaillierten Bericht, welcher im Falle einer Gerichtsverhandlung Personen überzeugen muss, die während der gesamten Ermittlung nicht dabei waren.

3.2.2 Sicherheitsmaßnamen

Als Sicherheitsmaßname aktiviert er die Firewall des Computers und führt die letzten Windows Sicherheitsupdates durch. Danach sperrt er die aus den Server Logdateien herausgefundene Täter IP-Adresse. Der Computer-Forensiker rät der internen IT auf einen anderen Virenscanner umzusteigen, dem schneller Updates für aktuelle Malware zur Verfügung stehen. Zusätzlich müssen alle Computer des Unternehmens mit Sicherheitsupdates auf den neuesten Stand gebracht werden. Des Weiteren schlägt er der Firma vor die gesamte Belegschaft zu sensibilisieren was das Thema Malware angeht und wie man sich gegenüber SPAM-Mails verhält.

3.2.3 Datenquellen

Potenzielle Datenquellen sind die Logdateien, die bei jedem nächtlichen Angriff aufgezeichnet worden sind. Aus den Logdateien kann die IP-Adresse des Angreifer Systems ermittelt werden.
Über die Konsolenausgabe *traceroute* kann man die IP-Adresse nachverfolgen, dadurch sieht man über welche Knoten diese im Datennetz läuft. Als nächster Schritt kann die IP-Adresse auf der Homepage *https://www.whatismyip.com/ip-whois-lookup/* eingegeben werden, welche einem meist eine Adresse des Computerbesitzers aufführt, wie in Abbildung 5 zu sehen ist. Die Adresse kann vor Gericht als Beweismittel aufgeführt werden, sowie der auf der Festplatte gefundene Trojaner.

```
NetRange:       215.0.0.0 - 215.255.255.255
CIDR:           215.0.0.0/8
NetName:        DNIC-NET-215
NetHandle:      NET-215-0-0-0-1
Parent:          ()
NetType:        Direct Assignment
OriginAS:
Organization:   DoD Network Information Center (DNIC)
RegDate:        1998-06-05
Updated:        2011-06-21
Ref:            https://whois.arin.net/rest/net/NET-215-0-0-0-1


OrgName:        DoD Network Information Center
OrgId:          DNIC
Address:        3990 E. Broad Street
City:           Columbus
StateProv:      OH
PostalCode:     43218
Country:        US
RegDate:
Updated:        2011-08-17
Ref:            https://whois.arin.net/rest/org/DNIC
```

Abbildung 5: Überprüfung der Täter IP : 215.66.132.87

4 Fazit und Ausblick

Das Thema Computer-Forensik wird in der heutigen Zeit immer wichtiger, aufgrund der tendenziellen Steigerung der Internetkriminalität. Wenn man sich die Statistiken der letzten Jahre näher anschaut, bemerkt man schnell, dass die Internetkriminalität an Zuwachs gewinnt.

Gerade die vielen verschiedenen Angriffsmöglichkeiten und der schnelle Fortschritt der Computertechnologien, macht es schwer diese Verstöße alle aufzudecken und zu ahnden.

Aufgrund dessen werden heutzutage als Beispiel komplette Studiengänge in dem Bereich IT-Security, sowie Digitale Forensik angeboten.

In dieser Projektarbeit wird daher nur auf einen kleinen Teil des Themas Computerforensik eingegangen, bezüglich der vorgeschriebenen Seitenanzahl.

Das BSI wendet sich mit seinem Leitfaden „Leitfaden Informationssicherheit“ an Administratoren und Fachverantwortliche in kleinen und mittelständischen Unternehmen sowie an Behörden. Der Leitfaden soll einen Überblick über die wichtigen organisatorischen, infrastrukturellen und technischen Informationssicherheitsmaßnahmen geben.

Wer die Empfehlungen aus dem BSI Leitfaden konsequent umsetzt oder sich bei der Zusammenarbeit mit IT-Dienstleistern daran orientiert, legt bereits ein solides Fundament für ein vertrauenswürdiges Informationssicherheitsniveau. [15]

Wie in dem Beispielszenario aufgelistet, suchen Firmen vermehrt Hilfe bei Unternehmen, die sich auf den Bereich der Computer-Forensik spezialisiert haben. Mit dem ausführlichen Wissen und den nötigen Hilfsmitteln, können diese den Fehler schnell beheben und die Sicherheitslücke schließen. Durch die speziell entwickelten Verfahren, kann in den meisten Firmen trotz der forensischen Untersuchung, die Arbeit weiter aufgenommen werden.

[15] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2012) S.8

Literaturverzeichnis

GESCHONNECK, A.
Computer Forensik: Computerstraftaten erkennen, ermitteln, aufklären, 5., aktualisierte und erweiterte Auflage 2011.

WILLER, C.
PC-Forensik: Daten suchen und wiederherstellen, 1. Auflage 2012.

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK - BSI.
Leitfaden IT-Forensik, Version 1.0.1 März 2011, online im Internet, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=2 (Zugriff am 15. August 2016).

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK – BSI.
Leitfaden Informationssicherheit: IT-Grundschutz kompakt, Februar 2012, online im Internet, http://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile (Zugriff am 15. August 2016).

SILLER, H.
Springer Gabler Verlag (Herausgeber), Gabler Wirtschaftslexikon, Stichwort: Forensik, online im Internet, http://wirtschaftslexikon.gabler.de/Archiv/1408495/forensik-v3.html

BUNDESKRIMINALAMT – BKA.
IT-Forensik: Spurensuchen in Bits und Bytes, März 2016, online im Internet, https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologiefrueherkennung/IT-Forensik/it_forensik.html (Zugriff am 15. August 2016).

Abbildungsverzeichnis

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]