Sachverständigen-büro
Dr.-Ing. Markus a Campo

Försterstr. 25
D-52072 Aachen

Tel. 0241 / 15 80 80
Fax 0241 / 15 80 89

mail@m-acampo.de
http://m-acampo.de

Forensik mobiler Geräte in der Praxis

Anwendertag IT-Forensik 18.9.2012

Forensik mobiler Geräte in der Praxis

Kurzvorstellung Markus a Campo

- Arbeitsschwerpunkte
  - Security-Audits
  - BSI-Grundschutz/ISO 27001
  - IT-Forensik
  - Smartphone-Sicherheit
  - Sicherheit von Web-Applikationen
- Öffentlich bestellter und vereidigter Sachverständiger: „Systeme und Anwendungen der Informationsverarbeitung, insbesondere im Bereich IT-Sicherheit“
- Infos unter http://m-acampo.de/

Forensik mobiler Geräte in der Praxis

Gliederung

- Themen für forensische Gutachten
- Beweissicherung
- Analyse der Daten
- Fallbeispiele
  - Spionage-Software auf Symbian-Telefon
  - Missbrauch eines iPads

Forensik mobiler Geräte in der Praxis

Themen für forensische Gutachten

- Arbeitsgerichtsprozesse
  - unerlaubte Nutzung von Systemen
  - unerlaubte Installation von Programmen
  - Diebstahl/Löschen von Daten
  - Ausspähung von Daten
- Zivil-/Strafprozesse
  - Befall eines IT-Systems mit Malware
  - Copyright-Verletzungen

Forensik mobiler Geräte in der Praxis

Elemente einer forensischen Analyse

- Trennung von Beweissicherung und Analyse
- Reproduzierbarkeit von Sicherung und Analyse
- Beweismittel über Hashes absichern
- Jeder Schritt bei der Sicherung und Auswertung von Beweisen muss ausreichend dokumentiert werden
- Nachvollziehbarkeit in der Methodik

Forensik mobiler Geräte in der Praxis

Beweissicherung

- SIM-Karte/SD-Karten
  - über Kartenleser sichern
- Telefonspeicher
  - nur eingeschränkter Zugriff möglich
  - in der Regel keine Forensik-Tools vorinstalliert
- Lesen des Telefonspeichers
  - Erstellen einer Datensicherung
  - Auslesen über externe Schnittstelle
  - Installation eines Agenten (Forensik-Tool) und Auslesen über externe Schnittstelle
  - Jailbreak/Rooten/Hacken (nicht empfehlenswert)

Forensik mobiler Geräte in der Praxis

Beweissicherung

- Software zur Beweissicherung
  - Backup-Software (iTunes, BB Desktop, etc.)
  - MobilEDIT! Forensic
  - Oxygen Forensic Suite
- Umfang gesicherter Daten variiert je nach Methode
  - Beweismittel werden nicht vollständig gesichert
- Auswirkungen von Agenten nicht dokumentiert
  - Beweismittel werden überschrieben
- Hashes nicht exportierbar

Analyse der Daten

- Daten liegen in der Regel in proprietären Formaten vor
  - nicht dokumentiert
  - Ansicht und Analyse nur mittels Forensik-Programmen
  - externe Viren-Scans nicht möglich oder kompliziert
  - ggf. Ausnahmen bei Datensicherung
- Nachvollziehbare und reproduzierbar Analyse
  - Kontaktliste, Gesprächsliste, SMS, Kalender, Fotos etc.
- Analyse des Dateisystems problematisch
  - Was wurde gesichert?
  - Was wurde überschrieben?

Forensik mobiler Geräte in der Praxis

Fallbeispiel 1

- Symbian-Smartphone
- Einsatz im Ausland
  - Schwierigkeiten beim Rufaufbau
  - mysteriöse Nummern erscheinen in Gesprächsliste
- SIM durch PIN gesichert
- Keine Geräte-PIN
- Verdacht auf Installation von Spionage-Software

Forensik mobiler Geräte in der Praxis

Vorgehensweise

- Sicherung der SIM-Karte mit MobilEDIT!
- Sicherung Telefonspeicher mit MobilEDIT!
  - ohne Agent
  - Dateisystem unvollständig
- Sicherung Telefonspeicher mit Oxygen
  - Installation eines Agenten
  - Dateisystem etwas weniger unvollständig
- Suche in Dateisystem/SIM nach Name, Telefonnr., Zeitstempeln
  - erfolglos
- Internet-Recherche nach installierten Apps
  - zwei Apps mit Spyware-Funktionen

Forensik mobiler Geräte in der Praxis

Vorgehensweise

- Internet-Recherche nach Spionageprogrammen
  - werden normal installiert
  - nach Installation z.T. unsichtbar
  - Kommunikation über SMS oder Internet
  - Deinstallation z.T. über SMS möglich

Forensik mobiler Geräte in der Praxis

Forensik mobiler Geräte in der Praxis

NEO-CALL.COM

v. 2.1

NEO-CALL™ Software Suite

Parental Control, Child's Phone Activity Monitoring, Robbery insurance, Survival Kit

Quick Start Guide

Forensik mobiler Geräte in der Praxis

Vorgehensweise

- Test der SMS-Funktionen
  - Versand und Empfang nicht möglich
  - Auswirkungen eines Providerwechsels?
- WLAN
  - Start von Apps und Sniffen des Netzwerkverkehrs
  - eine App „telefoniert nach Hause“ und übermittelt Daten aus Adressbuch

Forensik mobiler Geräte in der Praxis

Vorgehensweise

- Test mit internem Viren-Scanner
  - Scanner-Update möglich
  - keine Malware gefunden
- Fazit
  - keine Spionage-Software gefunden
  - wegen unvollständiger Datensicherung keine absolute Sicherheit
  - Verdachtsmomente bleiben

Forensik mobiler Geräte in der Praxis

Fallbeispiel 2

- Apple iPad
- private Nutzung eingeschränkt
  - Besuch dubioser Webseiten verboten
  - WLAN-Nutzung verboten
- Verdacht auf Missbrauch des Geräts

Forensik mobiler Geräte in der Praxis

Vorgehensweise

- iPad-Datensicherung
  - Konfigurations- und Nutzdaten des Betriebssystems
  - Benutzerkonfiguration
  - Konfigurations- und Nutzdaten aller mitgelieferten Apps sowie aller später installierten Apps
  - keine E-Mails, Logdaten, Apps, temporäre App-Daten
- Sicherung von Beweismitteln
  - Datensicherung mit iTunes
  - Umwandlung in Dateisystem mit JuicePhone
- Manuelle Analyse
  - SQLite-Viewer
  - Plist-Viewer
  - Viewer für binäres Cookie-Format

Forensik mobiler Geräte in der Praxis

Cookies

Exhibit	Domain	Name	Created Time	Expires Time	Recognised Type	Extractor
Safari	.thespanker.com	__utmz	06.10.2011 07:44:23	05.04.2012 19:44:23	Google Analytics	Apple Safari...
Safari	.free-bdsm-movies.net	clk	06.10.2011 07:44:35	08.10.2011 07:44:31		Apple Safari...
Safari	.free-bdsm-movies.net	xraip	06.10.2011 07:44:35	08.10.2011 07:44:31		Apple Safari...
Safari	.free-bdsm-movies.net	xrbip	06.10.2011 07:44:35	08.10.2011 07:44:31		Apple Safari...
Safari	.free-bdsm-movies.net	ip_test	06.10.2011 07:44:35	08.10.2011 07:44:31		Apple Safari...
Safari	www.bdsmmpegs.net	from	06.10.2011 07:44:35	07.10.2011 07:44:31		Apple Safari...
Safari	www.bdsmmpegs.net	idcheck	06.10.2011 07:44:35	07.10.2011 07:44:31		Apple Safari...
Safari	www.bdsmmpegs.net	index_page	06.10.2011 07:44:35	07.10.2011 07:44:31		Apple Safari...
Safari	www.bdsmmpegs.net	lfrom	06.10.2011 07:44:35	07.10.2011 07:44:31		Apple Safari...
Safari	.bdsmmpegs.net	__utma	06.10.2011 07:44:36	05.10.2013 07:44:36	Google Analytics	Apple Safari...
Safari	.bdsmmpegs.net	__utmb	06.10.2011 07:44:36	06.10.2011 08:14:36		Apple Safari...
Safari	.bdsmmpegs.net	__utmz	06.10.2011 07:44:36	05.04.2012 19:44:36	Google Analytics	Apple Safari...
Safari	www.bdsmmpegs.net	stclick	06.10.2011 07:48:06	07.10.2011 07:48:02		Apple Safari...
Safari	www.bdsmmpegs.net	stfirst	06.10.2011 07:48:06	07.10.2011 07:48:02		Apple Safari...
Safari	www.bdsmmpegs.net	last_url	06.10.2011 07:48:07	07.10.2011 07:48:02		Apple Safari...
Safari	www.bdsmmpegs.net	to	06.10.2011 07:48:07	07.10.2011 07:48:02		Apple Safari...
Safari	.bondage-club.net	__utma	07.10.2011 13:21:30	06.10.2013 13:21:29	Google Analytics	Apple Safari...
Safari	.bondage-club.net	__utmb	07.10.2011 13:21:30	07.10.2011 13:51:29		Apple Safari...
Safari	.bondage-club.net	__utmz	07.10.2011 13:21:30	07.04.2012 01:21:29	Google Analytics	Apple Safari...
Safari	www.xxxbondagevideo.com	ddeb45390...	07.10.2011 13:22:16	08.01.2019 13:22:19		Apple Safari...
Safari	www.xxxbondagevideo.com	__st_click_c...	07.10.2011 13:23:22	08.10.2011 13:16:34		Apple Safari...

Forensik mobiler Geräte in der Praxis

List of known networks	array	
	dict	
AGE	integer	0
AP_MODE	integer	2
ASSOC_FLAGS	integer	1
BEACON_INT	integer	10
BSSID	string	0:1d:7[redacted]
CAPABILITIES	integer	1057
CHANNEL	integer	1
CHANNEL_FLAGS	integer	8
CaptiveNetwork	boolean	false
NOISE	integer	0
ORIG_AGE	integer	0
RATES	array	
RSSI	integer	-58
SSID	data	...
SSID_STR	string	[redacted]
ScaledRSSI	real	0.83837652206420898
ScaledRate	real	1
Strength	real	0.83837652206420898
UserDirected	boolean	true
WEPKeyLen	integer	0
authMode	integer	0
enabled	boolean	true
isValid	boolean	true
isWPA	integer	0
lastAutoJoined	date	2011-11-04T18:33:14Z
lastJoined	date	2011-09-16T13:16:33Z

WLANs

Forensik mobiler Geräte in der Praxis

Fazit

- Mobile Forensik
  - starke Abhängigkeit von Forensik-Programmen
  - gesicherter Datenbestand unklar und nicht dokumentiert
  - Standard-Fragestellungen können bearbeitet werden
  - Negativ-Beweise nahezu unmöglich