Digitale Forensik

Dipl.-Ing. Thomas Käfer, M.Sc.

Dipl.-Ing. M.Sc.
Thomas Käfer
EDV Sachverständiger



www.KaeferLive.de

IT-Sicherheit - Datenschutz - Pen-Testing

oder: Was Entwickler von Hackern lernen können...

Vortrag IT-Sicherheit – Datenschutz – Pen-Testing oder: Was wir von Hackern lernen können…

Motivation: Die IT und die Vernetzung von unterschiedlichsten Systemen untereinander – das Internet of Things – ist das zentrale Thema nicht nur aus Entwicklersicht, sondern auch in Hinblick auf die IT-Sicherheit und den Datenschutz. Und so ist es nicht verwunderlich, dass neben den vielen positiven Meldungen über neue Errungenschaften auch die Kehrseiten deutlich werden. Ob es angegriffene Fahrzeuge, groß angelegte Hacker-Attacken auf Telekommunikationsnetze oder Web-Server, Datenschutzpannen und vielleicht demnächst ein Angriff auf die Strom- und Wasserversorgung sind: IT-Sicherheit ist ein ernstzunehmendes Thema. Und dies mehr als bisher, als man sich rein im Internet der Dienste „nur“ mit Nutzerdaten beschäftigt hat.

Beispiel Vernetzte Autos: Die zunehmende Vernetzung von Fahrzeugen untereinander, mit Smartphones und zentralen Infrastrukturen (Car2X) sowie Erweiterungen wie Unfalldatenschreiber und das System „eCall“ wurden bisher in Bezug auf IT-Sicherheitsaspekte und Datenschutzbetrachtungen in der Automobilindustrie im Gegensatz zu Fragen der Functional- und Road-Safety niedriger priorisiert. Das Bewusstsein über die Gefahren, die durch mangelhafte IT-Sicherheit im Automotive-Umfeld ausgehen, hat sich durch die zahlreichen Incidents und Veröffentlichungen in 2015 spürbar verändert. Die Speicherung und der Austausch von Fahrzeug- und Bewegungsdaten wecken Begehrlichkeiten bei Industrie, Polizei und Justiz, Versicherungen und Dienstleistern aber auch bei Kriminellen. Und die Automobilindustrie und deren IT-Produkte sind ein gutes Beispiel, wie man es nicht machen sollte. An Beispielen von Apps und IT-Services u.a. von BMW ConnectedDrive, Ford Car-Sharing und myAudi wird gezeigt, wie leicht der Hacker System angreifen kann.

Beispiel SmartMeter: Das gleiche gilt für die geplante flächendeckende Einführung von intelligenten Stromzählern – sogenannten SmartMetern. Diese besitzen auch einen Internetanschluss und vielfach die Möglichkeit, den Strom via Fernzugriff abzuschalten. Ein massenhafter Angriff auf solch ein System würde die Stromversorgung in die Knie zwingen und in letzter Konsequenz zur flächendeckenden Notabschaltung von Kraftwerken führen. Der Roman „Blackout“ ist nicht weit hergeholt.

Beispiel Verschlüsselung: Und selbst wenn die Entwickler meinen, Sie hätten alles richtig gemacht und ihre Daten und die Kommunikation verschlüsselt, heißt das nicht, dass das wirklich sicher und dem aktuellen Stand der Technik entsprechend erfolgt ist. Das Mitlesen selbst verschlüsselter Verbindungen gelingt dem Hacker nämlich in vielen Fällen trotzdem. Wie das geht, wird im Seminar gezeigt.

Beispiel Phishing und Schad-Software:
Es vergeht praktisch kein Tag, an dem sich im E-Mail-Postfach nicht mindestens eine E-Mail findet, in der mit mehr oder weniger perfiden Tricks versucht wird, an Zugangsdaten zu gelangen (Phishing) oder Schad-Software zu verbreiten (Ransom-Ware). An konkreten Beispielen wird gezeigt, wie man diese Attacken erkennen und wie man sich dagegen schützen kann.

Elchenrather Weide 20 – D-52146 Würselen
Tel. 02405/47949-0 – E-Mail: Kaefer@Kaeferlive.de – www.Car-Forensics.de

Beispiel Künstliche Intelligenz (KI): Die Verbreitung von künstlicher Intelligenz, oder kurz KI, ist in aller Munde und es stellt sich nicht nur die Frage, ob KI zum Angriff auf IT-Systeme, sondern auch zur Abwehr eingesetzt werden kann. Und wie so oft: Wo viel Licht ist, ist auch viel Schatten. KI bringt neue Sicherheitslücken, neue Angriffsformen, aber auch die Möglichkeit, sich mit KI-Hilfe besser gegen Attacken der bösen Buben zu wehren oder die eigenen Systeme systematisch auch nach Schwachstellen zu untersuchen und zu härten.

Beispiel Incident Response: Und wenn es dann doch passiert ist und das Unternehmen erfolgreich angegriffen worden ist, die EDV in Scherben auf dem Boden liegt und die IT-Mannschaft nur noch wie ein aufgescheuchter Haufen Hühner durch die Gegend läuft, dann ist irgendwas schiefgelaufen. Aber auch dann gilt es, mit einem kühlen Kopf und Fachverstand den Schaden einzugrenzen und mit einem Plan auf die Attacke zu reagieren und den Wiederaufbau systematisch zu orchestrieren. Einfach die Systeme wieder hochzufahren, liefert möglicherweise den nächsten Schaden oder vergrößert ihn nur unnötig. Auch auf solche Szenarien kann man sich vorbereiten und man sollte es auch.

Vortragskonzept: Der Vortrag „IT-Sicherheit – Datenschutz – Pen-Testing“ basiert auf und orientiert sich an den praktischen Erfahrungen des Teams um Thomas Käfer, der mit forensischen Analysen und Penetration-Tests bereits zahlreiche Systeme untersucht und deren Schwachstellen aufgedeckt hat. In seiner Forschungsarbeit „Car-Forensics“ wurde u.a. gezeigt, was technisch im Bereich der digitalen forensischen Auswertung der in den Kfz verbauten bzw. extern mit den Fahrzeugen gekoppelten IT-Systemen derzeit bereits möglich und zukünftig denkbar ist. U.a. wurde thematisiert und geprüft, welche Schnittstellen die verschiedenen Systeme besitzen, die forensisch angesprochen bzw. ausgewertet werden können.

Mittels Vorgehensweisen der digitalen Forensik und typischer Angreifer wird an konkreten Beispielen aus dem Automotive-Umfeld, dem Internet der Dinge sowie dem Internet der Dienste gezeigt, inwieweit technische und organisatorische Sicherungsmaßnahmen umgangen werden können, um Zugangssicherungen auszuhebeln bzw. wie welche Daten kompromittiert, verändert und abgegriffen werden können. Das können sowohl Web-Services als auch Smartphone-Apps sein, die bevorzugt als Einfallstor in ein IT-System genutzt werden.

Viele Entwickler kennen die zahlreichen Möglichkeiten gar nicht, die man forensisch und auch für dunkle Zwecke missbrauchen kann. Der Entwickler hat nämlich eine ganz andere Sichtweise als der Hacker. Während der Entwickler – bildlich gesprochen – versucht, einen besonders schönen und hohen Bauklötzchen-Turm aufzubauen, sucht der Hacker nach der Schwachstelle, wie er den Turm möglichst effektiv zum Einsturz bringen kann. Es wird somit nicht allein das Bewusstsein für die Schwächen und Angriffsvektoren geschärft, sondern ganz konkrete Empfehlungen für die Verhinderung eines Security-Incidents gegeben.

Zielgruppe: Das Seminar richtet sich an Versicherungskaufleute, die sich in diesem Bereich fortbilden möchten. Anhand der typischen Aufgabenstellung der Zielgruppe, nämlich der Beratung von Versicherungsnehmer hinsichtlich der Gefahren, deren Abwehr und nachfolgend einer Absicherung des Restrisikos durch eine Cyberversicherung wird eine konkreter Bezug hergestellt.

Elchenrather Weide 20 – D-52146 Würselen
Tel. 02405/47949-0 – E-Mail: Kaefer@Kaeferlive.de – www.Car-Forensics.de

Vorstellung Referent Dipl.-Ing Thomas Käfer, M.Sc.



Dipl.-Ing. Thomas Käfer, M.Sc. ist mit seinem IT-Systemhaus seit 1990 selbstständig in der IT tätig. Das Tätigkeitsfeld der Firma Käfer umfasst Consulting-Leistungen im Bereich der IT-Sicherheit incl. Penetration-Testing u. a. im Automotive-Umfeld sowie die Entwicklung und der Vertrieb von Full-Motion-Simulatoren für Racing und Flight. Thomas Käfer arbeitet seit 2002 als Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung (seit 2006 öffentlich bestellt), als IT-Consultant, Fachautor und beschäftigt sich vor allem mit Fragen der IT-Sicherheit, dem Datenschutz und dem Gebiet der Digitalen Forensik. Ehrenämter als Handelsrichter am Landgericht Aachen sowie als Mitglied der Vollversammlung der IHK Aachen (Ausschüsse Industrie und Technologie, Außenhandel sowie Berufsbildung) komplettierten in der Vergangenheit seine Tätigkeiten. Er hat 2015 erfolgreich den berufsbegleitenden Masterstudiengang „Digitale Forensik“ an der Hochschule Albstadt-Sigmaringen in Kooperation mit der LMU München und der FAU Erlangen abgeschlossen und in diesem Rahmen eine umfangreiche Forschungsarbeit zum Thema Digitale Kfz-Forensik (Car-Forensics) erstellt. Er ist Speaker auf Veranstaltungen zum Thema IT-Sicherheit und Datenschutz und hält Schulungen und Workshops zu diesem Thema für Automobilindustrie, Industrie, Zulieferern, Behörden und Verbände.

Beispiele für öffentliche Vorträge und Workshops (ohne Firmenbeauftragung):

- 17.11.2021: Vortrag Sicherheit Autonomes Fahren beim AKEUR in Köln
- 18.06.2020: Moderator des Kolloquiums „Cyber Security von Anlagen und Maschinen“ der weyer Gruppe Düren
- 02.04.2020: IT-Security: „Was wir von Hackern lernen können“ beim IHK-Versicherungstag in Vallendar
- 20.03.2020: Vortrag: „Digitalisierung aber sicher“ bei der 1.IDA-Tagung der FH Aachen
- 05.02.2020: Vortrag zu IT-Security bei der Jahrestagung des Bundesverbands Deutscher Versicherungskaufleute e.V. in Maria Laach
- 30.01.2020: Tages-Workshop: IT-Sicherheit in Industriesteuerungsanlagen

- Okt. 2015/2016 und 2018 Car Forensics - 27. Aachener Fahrzeug- und Motorenkolloquium von FKA und IKA der RWTH Aachen
- Car-Forensics beim Science-Link: Networking 4.0 "Datensicherheit bei autonomem Fahren" am 19.03.2018 in Aachen
- 18.11.2016: Berater Fachtagung VDE/VDI Frankfurt/Main
- 02.11.2016: Speaker Leetcon IT Sicherheits-Convention – Hannover
- 11.12.2015: Speaker auf dem Aachener Interdisziplinären Verkehrssymposium
- 02.12.2015: Speaker IT Sicherheit Industrie 4.0 auf dem Sicherheitstag NRW
- 06.11.2015: Speaker Car-Forensics beim IT Security Breakfast Bonn
- 21.-22.10.2015: Poster Car-Forensics auf der Automotive Security 31. VDI/VW-Gemeinschaftstagung in Wolfsburg
- 06.10.2015: Hausmesse Wolfsburg - Vortrag zur IT Sicherheit im Kfz
- 16.09.2015: Speaker Digitalisierung bei der IHK Aachen
- 12.05.2015: Speaker IT-Forensik-Workshop an der FH-Aachen
- 16.03.2015 - 20.03.2015: CeBIT – Speaker Car-Forensics
- 03.12.2014: Speaker IT Sicherheit Hagen - IT-Sicherheitstag NRW 2014
- 24.11.2014: Speaker Digitale KFZ-Forensik - Köln - cologne IT summit
- 16.09.2014: Speaker Car-Forensics 9. Dortmunder Autotag
- Speaker Digitale KFZ-Forensik - Köln - cologne IT summit 2014
- Speaker Car-Forensics 9. Dortmunder Autotag 2014

Presseberichterstattung über IT-Forensik, Datensicherheit und Car-Forensics:

- WDR Lokalzeit Aachen vom 08.01.2019 zu Hacker-Angriffen auf Prominente
- Car-Forensics in den Wirtschaftlichen Nachrichten 11/2016 der IHK Aachen
- Berufsporträt Digitaler Forensiker in den VDI Nachrichten vom 09.10.2015
- ARD Tagesschau und WDR Aktuelle Stunde Stellungnahme zur VW-Abgassoftware (22.09.15 und 25.09.2015)
- ARD Plusminus extra Stellungnahme zur VW-Abgassoftware (21.09.2015)
- MDR Fakt ist…! BMW Hack (21.09.2015)
- Selbst ist das Auto in der FAZ vom 06.09.2015
- ARD tagesthemen vom 23.07.2015 mit Stellungnahme zum Jeep-Hack / BMW-Hack
- Berufsbild Digitale Forensik in der Südwest Presse und Stuttgarter Zeitung
- Car-Forensics in den Aachener Nachrichten vom 21.07.2015 und 15.09.2015
- Digitale Forensik im Innovationsmagazin „Technology Review“ 07/201
- Wo die Autoentwickler der Zukunft herkommen in „Die Welt“ vom 23.06.2015
- WDR-Fernsehen Lokalzeit Aachen vom 08.05.2015
- Car-Forensics in der Zeitschrift Mobile Business 03-2015

Beispiele für Veröffentlichungen:

- Zahnmedizin up2date - Datenschutz und Datensicherheit (Juli 2016)
- Forschungsbericht Car-Forensics (2015 bis 2019)
- Fachartikelreihe DigiFor Inside (2014)
- Computer-Forensik: Analyse von Angriffen (TecChannel Compact 04/2004)
- EDV in der Zahnarztpraxis (Quintessenz Team-Journal - Ausgabe 01-2005)
- Datenschutz und Datensicherheit (Quintessenz Team-Journal - 05-2005)