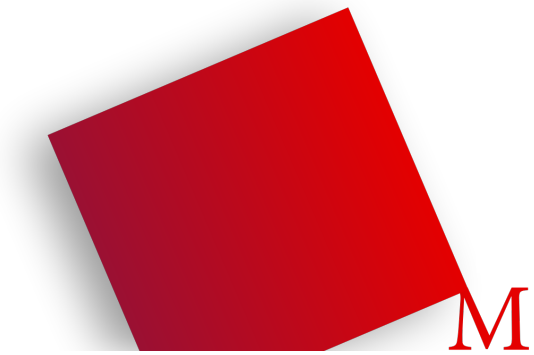
Fachbereich 07 Informatik/Mathematik



Praktikum Datenschutz und Datensicherheit
Sommersemester 2016

Prof. Dr. Rainer W. Gerling
Heidi Schuster

Man-in-the-Middle

Fabian Uhlmann
IF6

Diana Irmscher
IF7

15. Juli 2016

Abstract

Im Rahmen des Studiums Bachelor Informatik absolvieren wir (Fabian Uhlmann und Diana Irmscher) die zusätzliche Ausbildung zum betrieblichen Datenschutz an der Hochschule München.
Das Thema Datenschutz und IT-Sicherheit ist in den letzten Jahren immer mehr in den Vordergrund getreten. Meldungen über Angriff wie z.B. auf Bundestag im Mai 2015 und ganz aktuell auch der Krypto-Trojaner Locky sind fast täglich in den Nachrichten vertreten.
Wir haben das Thema "Man-in-the-Middle" gewählt, weil dieses Thema sehr spannend ausgearbeitet werden kann. Dabei werden wir erst darauf eingehen, wie sich der Angriff zusammensetzt, wo genau die rechtlichen Verstöße liegen und wie man sich vor solche Angriffen schützen kann.
Das Thema haben wir aufgeteilt in zwei Unterthemen. Herr Uhlmann wird darauf eingehen, wie man die Sicherheit eines Systems mit einem MITM-Angriff sehr effizient aushebeln kann. Frau Irmscher beschäftigt sich mit dem gezielten Angriff in TLS/SSL und in gesnifften Netzwerken.

München, 15. Juli 2016

Inhaltsverzeichnis

Aufgabenstellung **3**

1 Zusammenhang HTTP(s) und Zertifikate **3**

2 Bedeutung einer Man-in-the-Middle Attacke **4**

3 Sicherheitslücken bei bekannten Computer Herstellern **4**

3.1 Lenovo 5

3.1.1 Allgemeiner Ablauf 5

3.1.2 Der Angriff und die benötigten Mittel 5

3.2 DELL 6

4 Schutzmöglichkeiten **7**

5 Zwischenfazit **9**

6 Man-in-the-Middle-Angriffe im geswitchten Netz **10**

Literatur **11**

Aufgabenstellung

Dell und Lenovo haben demonstriert, dass man mit Man-in-the-Middle Angriffen die Sicherheit eines Systems sehr effizient aushebeln kann. Wie funktioniert ein derartiger Angriff und was kann man tun, um sich zu schützen.

1 Zusammenhang HTTP(s) und Zertifikate

Der Nutzer besucht z. B. eine Onlinebanking Webseite, die durch das Kürzel HTTPS signalisiert, dass es sich um eine verschlüsselte Verbindung handelt. Bei jeder HTTPS-Kommunikation muss sich der Webserver, auf dem die Internetseite gehostet wird, authentifizieren. Die Authentifizierung des Webservers gegenüber des Clients erfolgt durch ein für den Webserver ausgestelltes Zertifikat. Das Zertifikat enthält unter anderem den öffentlichen Schlüssel (Public Key), einen eindeutigen Fingerabdruck und Angaben über den Zertifikatsinhaber. Ein Zertifikat verbindet somit einen Inhaber mit einem öffentlichen Schlüssel. Mit dem Public Key verschlüsselt der Client die Daten, die er zum Webserver schickt. Anhand des Fingerabdrucks, welcher auch als digitale Signatur des Zertifikats bezeichnet wird, überprüft der Client, ob er mit dem richtigen Webserver kommuniziert. Der Fingerabdruck wird durch einen Hashalgorithmus wie z. B. SHA-2 erzeugt. Bei der Erzeugung gehen diverse Daten wie z. B. Zertifikatsaussteller, öffentlicher Schlüssel und Identifizierungsdaten über den Webserver mit ein. Wenn das Zertifikat von einer Zertifizierungsstelle (Certification Authority = CA) ausgestellt wurde, deren eigenes Zertifikat (= Root-Zertifikat oder Wurzelzertifikat) bereits im Browser installiert ist, dann wird dem ausgestellten Zertifikat automatisch vertraut. In den bekanntesten Webbrowsern wie z. B. Firefox, Chrome oder der Internet Explorer sind bereits viele Root-Zertifikate von den weltweit verschiedenen Zertifizierungsstellen vorinstalliert.

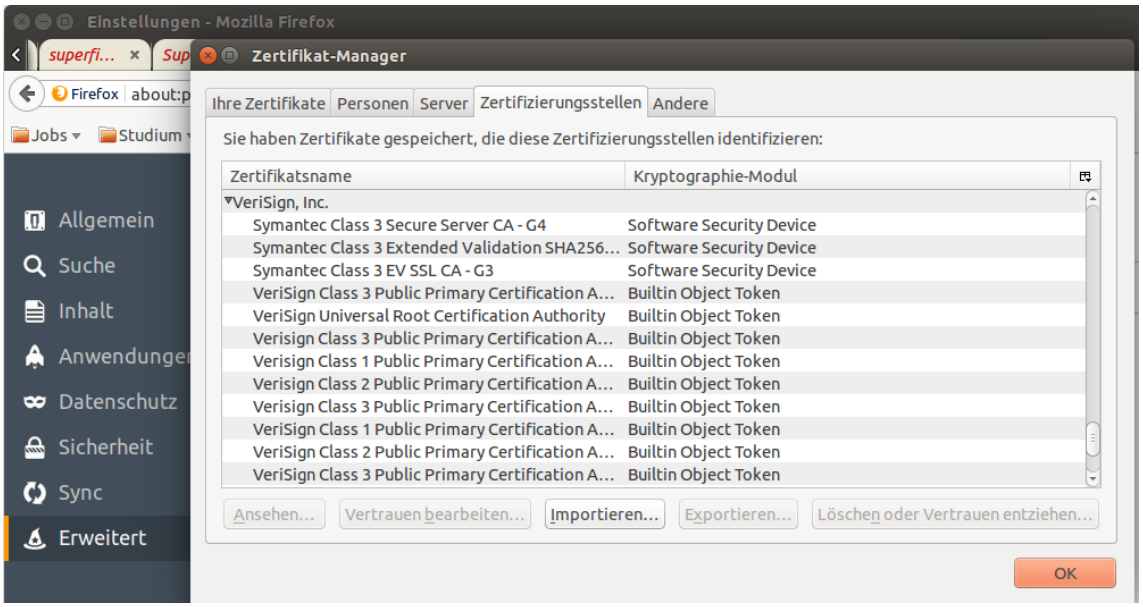


Abbildung 1: Ausschnitt vorinstallierter Zertifikate im Firefox Browser

Nutzt der Webservers jedoch ein selbst ausgestelltes (selbst signiertes) Zertifikat zur Authentifizierung, dann wird beim Verbindungsaufbau dem Nutzer eine Warnung angezeigt (siehe Bild ...). Der Nutzer kann anschließend selbst entscheiden ob er dem Zertifikat vertraut oder nicht. Außerdem entscheidet er ob er nur ein einziges Mal, d. h. nur für diese Verbindungssession, dem Zertifikat vertraut oder ob er eine dauerhafte Ausnahme macht. Ist letzteres der Fall, dann wird das Zertifikat im Browser installiert. Es wird dann bei den schon vorinstallierten Zertifikaten mit abgelegt. Eine dauerhafte Ausnahme hat zu Folge, dass der Benutzer beim Verbindungsaufbau zu der zugehörigen Webseite vom Webbrowser nicht mehr gewarnt wird.

2 Bedeutung einer Man-in-the-Middle Attacke

Man in the Middle (MITM) ist ein Angriffsszenario bei der ein unberechtigter Dritter versucht in eine zwischen zwei Kommunikationspartnern geführte, sichere (verschlüsselte) oder auch unsichere (unverschlüsselte) Kommunikation einzudringen. Ziel des Angreifers ist es, die zu übertragenen, vertraulichen Informationen unbemerkt mitzulesen und/oder zu manipulieren. Um unerkannt im Hintergrund an die Daten/Informationen zu gelangen, täuscht der Angreifer vor, der jeweilige, andere Kommunikationspartner zu sein.

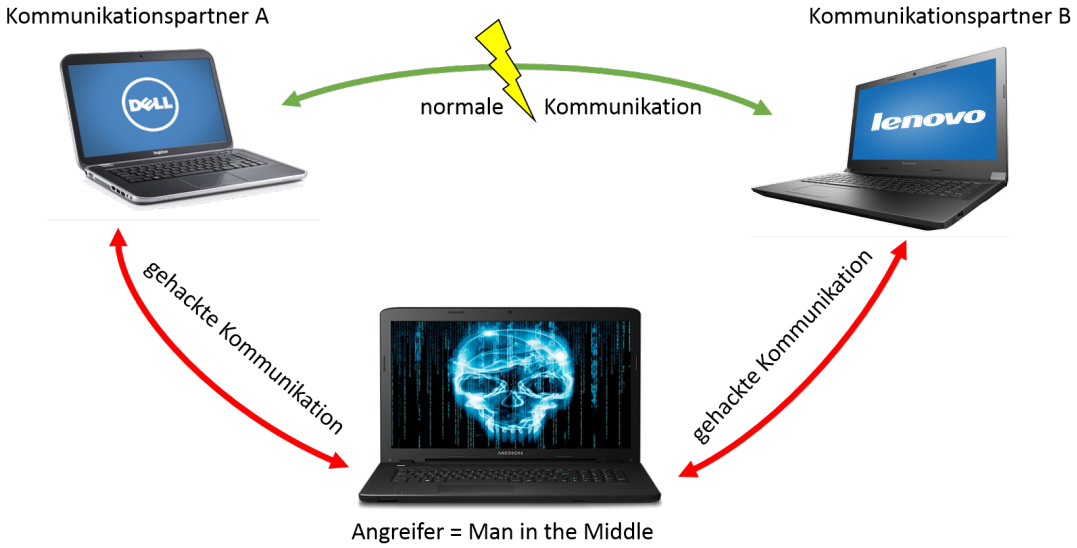


Abbildung 2: Man in the Middle Angriff

3 Sicherheitslücken bei bekannten Computer Herstellern

Man sollte davon ausgehen können, dass die großen PC Hersteller selbst am besten wissen müssten, wie hart der Markt in der Computer Branche umkämpft ist. Neben einer hohen Hardware-Qualität und ist Kundenvertrauen immens wichtig. Zwei

der weltweit bekanntesten und erfolgreichsten Computerhersteller [1, vgl.] haben anscheinend den Faktor Vertrauen etwas missverstanden. Denn sowohl Lenovo als auch DELL haben das Vertrauen ihrer Kunden stark missbraucht.

3.1 Lenovo

3.1.1 Allgemeiner Ablauf

Durch eine bereits vorinstallierte Software der Firma Superfish hat Lenovo versehentlich eine gravierende Sicherheitslücke auf einigen von ihren verschiedenen Notebookmodellen eingebaut. Dadurch wurde der Kunde einer zusätzlichen Gefahr eines leichteren Hackerangriffes ausgesetzt. Mit der Superfish-Software beabsichtigte Lenovo dem Nutzer gezielt personalisierte Werbung während des Surfens im Internet anzuzeigen. Um dies auch bei verschlüsselten Internetverbindungen (https) zu ermöglichen, wurde bei der Softwareinstallation auf den neuen Notebooks ein von Superfish selbst erstelltes Root-Zertifikat mit installiert. Der Kunde kaufte somit unwissentlich ein neues Notebook, auf dem kein neues, sondern ein bereits vor der Auslieferung manipuliertes Windows-Betriebssystem läuft. Mit dem selbst signierten Root-Zertifikat wurden sichere (verschlüsselte) HTTPS-Verbindungen in Form einer Man-in-the-Middle Attacke aufgebrochen. Dadurch konnte

3.1.2 Der Angriff und die benötigten Mittel

Die Internetseite golem.de beschreibt die Idee und den Ablauf von den benutzerspezifischen Werbeeinblendungungen auf den Lenovo-Rechnern wie folgt: „Grundsätzlich ist die Idee von Superfish, dass das Programm Bilder auf Webseiten durchsucht und anhand von Algorithmen versucht zu erkennen, was sich darauf befindet. Auf Basis dessen werden dem Nutzer passende Shopping-Angebote als Werbebanner angezeigt. Geradezu zynisch wirkt die Beschreibung des Lenovo-Angestellten im Forum: Die Funktion diene dazu, Nutzern zu helfen, visuell Angebote für Produkte zu finden, bei denen sie Schwierigkeiten haben, sie mittels einer textbasierten Suchmaschine zu finden.“[1] Für die Umsetzung der Idee reichte es nicht, dass nur ein Programm von Superfish auf den Lenovo-Rechnern installiert wird. Zusätzlich benötigte Superfish unbedingt ein eigen signiertes Root-Zertifikat auf dem System. Ohne dieses Zertifikat wäre es nicht möglich gewesen auch in verschlüsselten Internetverbindungen den Suchalgorithmus anzuwenden, um anschließend personalisierte Werbung einzublenden. Mit dem eigenem Root-Zertifikat war Superfish in der Lage für jede Verbindung, die zu einer HTTPS-Webseite aufgebaut wurde, ein eigenes, gefälschtes Zertifikat dynamisch zur Laufzeit zu erzeugen. Diesem Zertifikat wurde automatisch vertraut, da bereits dem zugehörigen Wurzelzertifikat vertraut wurde. Dem Root-Zertifikat von Superfish wurde wiederum vertraut, da dieses von Superfish direkt im Windows-Zertifikatsspeicher abgelegt wurde. Der Anwender bekam dadurch nicht mit, dass keine direkte verschlüsselte Kommunikation zu dem Server, der die Webseite hostet, aufgebaut wurde. (siehe Bilder ...) Weiterhin kam erschwerend hinzu, dass das Programm von Superfish für die Man-in-the-Middel Attacken ein schwaches Zertifikat nutzte. Das Root-Zertifikat verwendet für die digitale Signatur einen

SHA-1 Hashalsgorithmus und für die asymmetrische Verschlüsselung ein 1024 Bit RSA-Verschlüsselungsverfahren. Sowohl der SHA-1 Hashalgorithmus als auch das RSA-Verschlüsselungsverfahren mit einer Schlüssellänge von 1024 Bit sind bereits erfolgreich geknackt und daher als unsicher einzustufen. Doch noch fataler als der Einsatz des unsicheren Hashalgorithmus und des zu schwachen Verschlüsselungsfahren, ist die Leichtigkeit der Entschlüsselung des privaten, geheimen Schlüssels. Robert Graham beschreibt in seinem Blog auf Errata Security eindrucksvoll, wie mit simplen Mitteln der Private Key exportiert und anschließend mit einer einfachen Wörterbuch-Attacke entschlüsselt werden konnte. [2] Durch den privaten Schlüssel, welcher für alle betroffenen Geräte identisch ist, ist jeder Angreifer in der Lage, genau wie das Superfish-Programm, eigene „vertrauenswürdige“ Zertifikate für bösartige Verwendungen zu erstellen. Dadurch das den Angreifer-Zertifikaten ebenfalls automatisch vertraut wird, bekommen Anwender nicht mit, dass sie z. B. auf einer gefälschten Webseite serven und ihre Daten ausspioniert werden. Da das Superfish Root-Zeritifikat im Windows-Zertifikatsspeicher abgelegt wurde, können Angreifer mit Zertifikaten, die durch dieses Root-Zertifikat signiert wurden, nicht nur bösartige Webseiten, sondern auch kriminelle Software (z. B. Malware) dem Nutzer problemlos als gutartig erscheinen lassen.

3.2 DELL

Der Computerhersteller DELL leistete sich einen ähnlich gravierenden Sicherheitsfehler wie sein Konkurrent Lenovo zuvor. Genau wie Lenovo hat DELL auch selbst signierte Root-Zertifikate auf einigen seiner Laptops installiert. Bei dem US-amerikanischen Hersteller sind es sogar gleich zwei Root-Zertifikate. Sowohl das eDellRoot, als auch das DSDTestProvider Zertifikat, wurde genau wie das Superfish-Zertifikat im Windows-Zertifikatsspeicher abgelegt. Beim Aufruf der allgemeinen Eigenschaften des eDellRoot Zertifikats wird sogar ein Hinweis angezeigt, dass ein passender private key vorhanden ist. Joe Nord wendet in seinem Online-Blog die gleichen Vorgehensweisen zum Export und zur Entschlüsselung des DELL private keys an, wie Robert Graham beim Superfish private key. (siehe Bild ...). Angreifer mit dem privaten DELL Schlüssel haben die gleichen Angriffsmöglichkeiten auf infizierte DELL Geräte, wie Angreifer mit dem Superfish private key auf infizierte Lenovo Geräte. (siehe Abschnitt 3.1.) Beide DELL Zertifikate wurden durch Software installiert. Das eDellRoot Zertifikat mit dem Dell Foundation Services Programm und das DSDTestProvider Zertifikat mit der Dell System Detect Software. Sie sollen laut DELL für einfacheren Support dienen. DELL hat auf seiner online Webseite folgende Stellungnahme geäußert: „Das eDellRoot Zertifikat wurde durch eine Dell Foundation Services Anwendung auf Ihrem Dell PC installiert und wird vom Support verwendet, um einen besseren, schnelleren und einfacheren Support für unsere Kunden bereitzustellen. Das Zertifikat ist keine Malware oder Adware. Das Auslesen der Service-Tag-Nummer des Systems im online Support von Dell, ermöglicht uns, schnell das Computermodell zu erfassen. Dies macht es leichter und schneller den Service unserer Kunden zu identifizieren. Dieses Zertifikat wird nicht zum Sammeln von persönlichen Kundendaten verwendet. Es ist auch wichtig zu beachten, dass das Zertifikat sich nicht selbst wieder installiert, sobald es mit dem, von Dell empfohlenen, Prozess

ordnungsgemäß entfernt wurde. Wir haben alle unsere Anwendungen geprüft und können bestätigen, dass keine anderen Stammzertifikate werksseitig installiert sind. Wir haben herausgefunden, dass das Dell System Detect und sein DSDTestProvider Root-Zertifikat ähnliche Eigenschaften wie das eDellRoot haben. Im Falle vom Dell System Detect wird die Software vom Kunden heruntergeladen, um proaktiv mit der Dell Support-Website zu arbeiten. Wie schon eDellRoot, wurde dieses Zertifikat entwickelt, um einen schnelleren, personalisierten und einfacheren Support für unsere Kunden zu liefern. Das Problem der Zertifikate betrifft nur Kunden, welche die Software Funktionalität auf unserer Support-Website zwischen dem 20. Oktober und dem 24. November genutzt haben. Die Anwendung wurde umgehend von der Website entfernt und eine neue Version, ohne Zertifikat, ist nun verfügbar. Wir arbeiten an einem Software Update, um das Problem zu beheben und zeigen Ihnen nachfolgend, wie Sie das Zertifikat entfernen können."[2] DELL hat mit seiner Aussage offiziell bestätigt eigene Zertifikate auf Nutzer-Systemen zu installieren. Das eDellRoot wurde augenscheinlich bereits vor Auslieferung auf Geräten installiert und das DSDTestProvider erst nachträglich bei dem Besuch der DELL Support-Webseite. Es fällt auf, dass das eDellRoot Zertifikat sich anscheinend erneut installiert, wenn es nicht mit spezieller DELL Software ordnungsgemäß entfernt wurde.

4 Schutzmöglichkeiten

Bedauerlicher weiße haben Betroffene nicht all zu viele Möglichkeiten sich gegen eben beschriebene Sicherheitslücken zu schützen. Eine Option wäre der Kauf von neuen Systemen ohne vorinstalliertes Betriebssystem. Wenn der Anwender selbst ein Betriebssystem nach dem Kauf installiert, kann er mit großer Sicherheit davon ausgehen, dass sich keine ungewollte, vorinstallierte Software und/oder kein selbst signiertes Zertifikat auf dem neu angeschafften Gerät befindet. Jedoch schützt diese Option nicht für solchen Zertifikaten, die sich erst nachträglich installieren. Ein Beispiel ist das DSDTestProvider Zertifikat, welches sich beim Besuch der Support-Webseite von DELL installiert. Vorstellbar sind auch Szenarien, wo sich Zertifikate bei der Installation von Software mit einschleusen. Eine andere Variante des Schutzes ist die regelmäßige Kontrolle der auf dem System installierten Zertifikate. Durch diese Maßnahme können auch nachträglich installierte Zertifikate entdeckt werden. Zugegeben, bei der heutigen Masse an vorhanden, vertrauenswürdigen Zertifizierungsstellen und zugehörigen Zertifikaten, ist es nicht leicht den Überblick zu behalten. Erschwerend kommt hinzu, dass viele Programme zusätzlich einen eigenen Zertifikatsspeicher besitzen. Dabei kann nicht immer davon ausgegangen werden, dass diese Speicher sich auf den Zertifikatsspeicher des Betriebssystems beziehen bzw. die gleichen Zertifikate beinhalten. Um sicherzustellen, dass mit dem richtigen Server kommuniziert wird, d. h. es besteht keine Verbindung zu einer gefälschten Webseite, sollte man das Zertifikat prüfen, welches für die aktuelle Kommunikation verwendet wird. Jeder Browser zeigt neben der HTTPS-Adresse ein Schlosssymbol. Über dieses Symbol werden die Eigenschaften, des aktuell für diese verschlüsselte Verbindung verwendete Zertifikat, erreicht. Verschiedene Webseiten, z. B. https://globalsign.ssllabs.com, bieten eine Überprüfung der gewünschten Webseite an.

Als Ergebnis zeigen sie unter anderem an, welches originale Zertifikat diese Webseite wirklich verwendet. Mittels dieser Information und der Zertifikats-Eigenschaften durch den Browser, ist jeder in der Lage zu vergleichen, ob die verschlüsselte Verbindung das richtige Zertifikat nutzt. Handelt es sich nicht um das korrekte, originale Zertifikat und gab es keine Fehlermeldung, so muss davon ausgegangen werden, dass keine direkte Verbindung zu der gewünschten Webseite besteht. Dies bedeutet, die verschlüsselte Verbindung wurde durch eine MITM Attacke aufgebrochen und die Daten werden mitgelesen oder sogar manipuliert. Nach Aufdeckung einer solchen Attacke, muss das gefälschte Zertifikat im System gesucht und anschließend gelöscht werden. Dabei ist zu beachten, dass es nicht immer ausreicht nur das entdeckte Zertifikat selbst zu löschen. Da Zertifikate auf der Basis einer Public Key Infrastruktur erstellt sind, können noch weitere Zertifikate für solch eine Attacke verantwortlich sein. Es sollten neben dem aufgespürten, gefälschten Zertifikat zusätzlich alle anderen Zertifikate, die sich in der hierarchischen Kette befinden, überprüft und ggf. entfernt werden. Im Lenovo Beispiel konnten mittels des gehackten, selbst signierten Root-Zertifikats weitere Zertifikate erstellt werden. Mit jedem dieser Zertifiakte war anschließend eine MITM Attacke möglich. Das Sicherheitsproblem war mit der Eliminierung des für die MITM Attacke verwendeten Zertifikats nicht gelöst. Erst nach erfolgreichem Entfernen des selbst signierten Root-Zertifikats konnten keine weiteren gefälschten Zertifikate erzeugt werden. Beim DELL Vorfall schrieb Liam Tung auf der ZDNET-Webseite: „[...] das einfache Entfernen des eDELLRoot-Zertifikats aus dem Administrator und persönlichen Zertifikatsspeicher ist nicht genug, um den Nutzer zu schützen. Einige Nutzer haben in der Tat berichtet, dass das Zertifikat nach einem Neustart wieder aufgetaucht ist.“[3] Ursache für die Neuinstallation ist das DELL-Programm „Dell Foundation Services“, das dieses Zertifikat verwendet. Erst mit der Deinstallation des Programms bzw. eines Plugins des Programms und der manuellen Löschung des DELL Zertifikats, ist das selbst signierte Zertifikat dauerhaft vom System erfolgreich entfernt und die Sicherheitslücke geschlossen. Liam Tung schrieb zur korrekten Entfernung folgendes: „Um es dauerhaft zu entfernen und um zu verhindern, dass es sich erneut installiert, müssen Nutzer das eDELL Plugin entfernen.“ Für die detaillierte Information um welches Plugin es sich genau handelt, nutzt er die Ergebnisse von den Duo Security Forschern Darren Kemp, Michail Davidov und Kyle Lady. „‘Dies kann vollbracht werden mit Hilfe der Löschung des Dell.Foundation.Agent.Plugins.eDell.dll Moduls vom System. Geschieht dies nicht, so kann es weiterhin zur Aussetzung dieser Sicherheitslücke kommen.‘, sagte Duo Security.“ [3] Er fügte noch einen wichtigen Hinweis von Duo Security hinzu: „‘Beachte, immer wenn sie ein Werksreset auf ihrem DELL System durchführen, wird dieses Zertifikat und das eDell Plugin auf dem System wieder hergestellt und sie müssen es erneut manuell entfernen‘ [...] "[3] Die beiden Beispiele zeigen, dass es nicht ausreicht nur die Zertifikatsspeicher auf ungewöhnliche Eintragungen zu durchsuchen, sondern ebenfalls die Programmliste des Systems auf unerwartete oder ggf. unnötig installierte Programme zu kontrollieren.

5 Zwischenfazit

Beide Systemhersteller nutzten ihre Position in der Marktwirtschaft und das Vertrauen gegenüber dem Kunden schamlos aus. Sie ließen dem Käufer in dem Glauben, dass er ein solides Gerät mit sicherer Software gekauft hätte. Doch ohne selbständige Gegenmaßnahmen des Kunden, war dieser mittels der von Lenovo und DELL selbst signierten Zertifikate potentiellen Angreifern hilflos ausgesetzt. Die Käufer müssen auf der einen Seite für die Zukunft hoffen, dass die Gerätehersteller aus ihren Fehlern gelernt haben und wieder sichere Systeme herstellen bzw. verkaufen. Auf der anderen kann und sollte er selbständige Kontrollen und Überprüfungen durchführen. Außerdem ist es Ratsam sich ein wenig mit den Systemen zu befassen, mit denen man Tag täglich umgeht und wichtige Tätigkeiten, wie z. B. Online Banking, durchführt. Darunter zählt auch das regelmäßige Abrufen von Informationen über Sicherheitsneuigkeiten in bekannten Sicherheitsforen, z. B. `https://www.heise.de/security`

Gemäß dem Sprichwort „Vertrauen ist gut, Kontrolle ist besser.“, sollte jeder Benutzer, mit den verfügbaren Möglichkeiten, die verwendeten Systeme und Dienste immer wieder überprüfen.

6 Man-in-the-Middle-Angriffe im geswitchten Netz

Es gibt Man-in-the-Middle-Angriffe nicht nur gegen SSL/TLS Verbindungen sondern auch gegen "normale"Netzwerkverbindungen. Sie werden von Angreifern eingesetzt, um in einem geswitchten Netz zu sniffen.

Literatur

[1] STAMFORD, Conn. Gartner Says Worldwide PC Shipments Declined 9.6 Percent in First Quarter of 2016, 11. April 2016. http://www.gartner.com/newsroom/id/3280626
Abrufdatum: 15.07.2016.