Sicherheitsrisiken von SSL und TLS

Sichere Kommunikation über nicht vertrauenswürdige Netzwerke wie das Internet ist heutzutage für nahezu alle Anwendungen wie Bankzugänge und Web-Shops unerlässlich. Standard dafür sind die SSL/TLS-Protokolle. Sie sorgen nicht nur dafür, dass Datenpakete der Anwender verschlüsselt werden, sie kümmern sich auch um die Aushandlung der verwendeten Verschlüsselungsverfahren, ihrer Betriebsarten und Schlüssellängen, sowie den Austausch und die periodische Erneuerung der verwendeten Schlüssel.

Weil das Brechen aktueller Verschlüsselungsalgorithmen mit roher Gewalt praktisch fast unmöglich ist, haben Kriminelle, Sicherheitsexperten, Hersteller und Behörden das Protokoll selbst und seine Implementierungen auf Schwachstellen hin untersucht. Über die Zeit wurden unterschiedliche Angriffe gegen verschiedene Aspekte des SSL/TLS-Protokolls entwickelt, die nach ihrem Bekanntwerden durch die Entwickler behoben wurden:

Fehlerhafte Implementierung des Handshake-Mechanismus (2009): Diese Schwachstelle ermöglicht es einem Angreifer nach einer erneuten Aushandlung der kryptographischen Parameter eine eigene Nachricht an den Server zu senden. Der Angreifer kann zwar keine Nachrichten entschlüsseln, jedoch kann er verschlüsselte Pakete des Clients, welche z. B. Login-Daten eines Twitter-Accounts beinhalten, abfangen und als Inhalt seines Tweets an den Twitter-Server weiterleiten. Der Server entschlüsselt die Nachricht und veröffentlicht die vertraulichen Information (z. B.: Benutzername/Passwort) anschließend als Nachricht des Angreifers.

BEAST (2011): BEAST („Browser Exploit Against SSL/TLS“) ermöglicht es, Informationen zu entschlüsseln, die zwischen einem Browser und dem Ziel-Server übertragen werden. Konkret hat es BEAST auf Session-Cookies abgesehen, welche bei jeder Anfrage automatisch an den Webserver geschickt werden. Indem nach und nach Klartext-Blöcke mit bekanntem Inhalt eingefügt werden, kann sukzessive jedes einzelne Zeichen des Cookies ermittelt werden. Dies ermöglicht es dem Angreifer eine fremde Session und den zugehörigen Account zu übernehmen.

CRIME (2012): Mit CRIME („Compression Ratio Info-leak Mass Exploitation“) kann ein Angreifer die Länge der übertragenen Anfragen beobachten und durch eine geschickte Manipulation der gesendeten Daten Teile daraus entschlüsseln. Wenn der vom Angreifer manipulierte Teil mit dem Anfang der Anfrage (z. B. einem Session Cookie) übereinstimmt, reduziert der für die Komprimierung verwendete Algorithmus die Länge der Anfrage um die Länge der korrekt erratenen Zeichen. Dies ermöglicht dem Angreifer, das Cookie Stück für Stück zu erraten.

Lucky13 (2013): Bei Lucky13 handelt es sich um einen Angriff, bei dem die Antwortzeit des Servers verwendet wird, um den Klartext einer Nachricht zu ermitteln. Dies ist möglich, da der Client die Pakete vor der Verschlüsselung bis zu einer bestimmten Länge auffüllt. Nach Entschlüsselung des Pakets weiß der Server, wo die Nachricht für die Berechnung der Prüfsumme endet und die Fülldaten anfangen. Verändert sich nun die Antwortzeit des Servers durch die Manipulation eines Pakets, lässt dies auf eine Manipulation der Fülldaten schließen, da der Server nicht weiß, welche Daten er in die Berechnung der Prüfsumme einbeziehen muss.

Angriff auf RC4 (2013): Seit BEAST setzen sehr viele Webseitenbetreiber die 1987 entstandene Verschlüsselungsmethode RC4 ein, da diese nicht für BEAST anfällig ist. RC4 generiert per Pseudozufallszahlengenerator quasi zufällige Zahlen und verknüpft den zu verschlüsselnden Text mit diesen Zufallszahlen. Minimale Abweichungen dieser Funktionsweise von einer statistisch idealen Verteilung werden ausgenutzt, um die ersten 220 Byte einer Verbindung zu entschlüsseln.

Anfälligkeit der SSL/TLS-Versionen für Schwachstellen

	SSL	TLS		
	3.0	1.0	1.1	1.2
Handshake	Anfällig	Geschützt*	Geschützt*	Geschützt*
BEAST	CBC: Anfällig RC4: Geschützt	CBC: Anfällig RC4: Geschützt	CBC: Geschützt RC4: Geschützt	CBC: Geschützt RC4: Geschützt GCM**: Geschützt
CRIME	Anfällig***	Anfällig***	Anfällig***	Anfällig***
Lucky13	CBC: Anfällig RC4: Geschützt	CBC: Anfällig RC4: Geschützt	CBC: Anfällig RC4: Geschützt	CBC: Anfällig RC4: Geschützt GCM**: Geschützt
RC4	CBC: Geschützt RC4: Anfällig	CBC: Geschützt RC4: Anfällig	CBC: Geschützt RC4: Anfällig	CBC: Geschützt RC4: Anfällig GCM**: Geschützt

* sofern RFC 5746 umgesetzt wird.
** Die Betriebsart Galois/Counter Mode (GCM) stellt gegenüber Cipher-Block-Chaining (CBC) einen verbesserten Integritätsschutz bereit.
*** bei Komprimierung mit DEFLATE und SPDY.

Obige Tabelle zeigt, dass der einzige vollständige Schutz derzeit mit TLS v1.2, AES-GCM und abgeschalteter Komprimierung gewährleistet ist. Serverbetreiber sollten daher schnellstmöglich diese Version anbieten, um sicherheitsbewussten Kunden sichere Verbindungen bereitzustellen. Allerdings unterstützen derzeit nicht alle Browser schon TLSv1.2; insbesondere Firefox kann unter Windows derzeit nur TLSv1.0 und soll TLSv1.2 erst ab Version 24 unterstützen. Sobald Updates der Browser (oder anderer Client-Anwendungen) verfügbar sind, sollte der Support veralteter Protokollversionen zeitnah abgekündigt werden.

IMPRESSUM
atsec information security GmbH
Steinstr. 70
81667 München
Deutschland
Telefon: +49-89-442-49-830
Telefax: +49-89-442-49-831
E-Mail: info@atsec.com

Vertretungsberechtigte Geschäftsführer:
Salvatore la Pietra
Staffan Persson
Registernummer: HRB 129439
Registergericht: Amtsgericht München
UST-ID-Nr. gemäß § 27a UStG:
DE205370914
Verantwortlich für den Inhalt:
Staffan Persson (Anschrift s.o.)

atsec the information security provider
NEWS 02/13

O'zapft is!

Über meinem Schreibtisch hängt seit vielen Jahren ein Plakat der RSA-Konferenz von 1997, auf dem NSA-Geheimdienstler die private Kommunikation einer Familie abhören. Titel: „Add Uncle Sam to your circle of friends and family!" Wenn jetzt also die Medien suggerieren, man habe nicht gewusst, dass Geheimdienste Personen systematisch und in großem Stil ausspähen, sagt das viel über die Medien selbst aus, denen das Thema in den letzten 16 Jahren offenbar nicht sexy genug war, und die sich nun quasi über die eigene Untätigkeit wundern. Profilbildung aus gesammelten Daten ist nichts Unbekanntes und ein großes Geschäft in der gesamten Internetwirtschaft für gezielte Werbung - und dies erzeugt (bisher) keinen öffentlichen Aufschrei. Wir erwarten sogar von der Finanzwirtschaft, dass sie Fraud Detection Software einsetzt und ungewöhnliche Verhaltensmuster in unserem Finanzgebaren erkennt - was ohne die Bildung von Profilen unseres Verhaltens nicht möglich ist. Ignorierten die Geheimdienste all diese Technologien, müsste man ihre Kompetenz stark anzweifeln. Schließlich gehört das Sammeln von Daten und die Bildung von Profilen aus diesen Daten zu ihren Hauptaufgaben. Was war da nicht bekannt?

Sicher sind die meisten von Ausmaß und Ziellosigkeit (Masse statt Klasse) der technischen Überwachung überrascht worden, und auch von der bereitwilligen Kooperation der Industrie mit ihren nationalen Schlapphüten, die damit die in großem Umfang betriebene Wirtschaftsspionage kaschieren. Die Empörung über Länder- und Parteigrenzen hinweg mag aber auch damit zu tun haben, dass sich viele jetzt darüber ärgern, mit ihren Accounts bei Google, Facebook, Twitter, Xing oder LinkedIn den Geheimdiensten das Dossier über sich akkurat und kostenfrei selbst geschrieben zu haben. Früher haben wir eine „googlesichere Weste" propagiert, aber die Entwicklung hat uns da schon lange überrollt. Wenigstens haben jetzt alle gelernt, dass die vermeintliche Trennung von privaten und geschäftlichen Daten höchstens noch von uns selbst vorgenommen wird, während andere diese Daten zu umfangreichen Profilen über uns zusammenführen. Wir alle müssen endlich auch verinnerlichen, dass veröffentlichte Daten im Netz nicht verschwinden und nicht in der Anonymität der Netze untergehen.

Was mich in diesem Zusammenhang zudem beschäftigt ist die Frage, wo *Transparenz, Kontrolle und Integrität* geblieben sind, ohne die das Vertrauen, auf dem unsere demokratische Gesellschaft basiert, nicht bestehen kann. Geheime, nicht kontrollierte Operationen haben die fatale Tendenz, aus dem Ruder zu laufen, weil ein äußeres Korrektiv fehlt, das diese Werte einfordert.

Für uns bei atsec sind Integrität, Kontrolle und Transparenz Grundlage unserer Arbeit und nicht verhandelbar. Informationen zurückzuhalten würde das Vertrauen in unsere Arbeit zerstören, unsere Integrität in Frage stellen und unseren Kunden keinen vollständigen Überblick über ihre Risiken geben. Wenn wir Produkte evaluieren, dürfen wir keine Hintertürchen verschweigen, das wäre Betrug an den Benutzern. Wir lassen unsere Arbeit auch unabhängig kontrollieren, damit unsere Kunden wissen, dass ihr Vertrauen in uns gerechtfertigt ist.

Wie wir müssen sich auch die in die Kritik geratenen Organisationen einer funktionierenden und unabhängigen gesellschaftlichen (und parlamentarischen) Kontrolle stellen, um ihre Integrität und Transparenz zu beweisen.

Hoffen wir mal, dass ihre Dossiers über die Kontrolleure das nicht verhindern 😉

Herzlichst,
Gerald Krummeck
Leiter Prüfstelle

Messen und Konferenzen 2013

Die atsec information security wird in diesem Jahr auf folgenden Messen und Konferenzen vertreten sein:

- **ICCC in USA (Orlando, FL): 10.-12.09.2013**
  Die Internationale Common Criteria Konferenz bietet Herstellern, Prüfstellen, Anwendern sowie Behörden und Zertifizierungsstellen eine Diskussionsplattform und Informationen zu aktuellen Entwicklungen der Common Criteria.

- **ICMC in USA (Gaithersburg, MD): 24.-26.09.2013**
  Die erste „International Cryptographic Module Conference – ICMC" ist eine Experten-Konferenz für kryptografische Module. Für Details siehe http://www.icmc-2013.org/.

- **it-sa in Nürnberg: 08-10.10.2013**
  Auf der größten IT-Sicherheitsmesse im deutschsprachigen Raum wird sich atsec wie im letzten Jahr wieder mit einem eigenen Stand präsentieren. Sie finden uns dieses Jahr an Stand 12.0-214.

atsec it security blog
Verfolgen Sie brandaktuell Diskussionen und Erlebnisse unserer Mitarbeiter auf http://atsec-information-security.blogspot.de

Datenschutz-Management-Systeme

In den letzten Jahren taucht beim Thema „Datenschutz“ immer mal wieder der Begriff „Datenschutz-Management-System“ (kurz: DSMS) auf. Daher haben wir diesen Newsletter zum Anlass genommen, ein DSMS näher zu beschreiben und mögliche Umsetzungen aufzuzeigen.
Das DSMS gehört zur Gruppe der Management-Systeme. Diese sind hinreichend bekannt, wenn man schon einmal Kontakt mit einem Informationssicherheits-Managementsystem (ISMS) oder einem Qualitätsmanagement-System (QMS) gehabt hat.

Sobald Anforderungen für mehr als ein Management System im Haus bestehen, stellt sich die Frage, wie man diese organisiert. Ein häufig gewählter Ansatz ist, gemeinsame Themen aller zu implementierender Management-Systeme in ein allgemeines Management-System (MS) auszugliedern und nur die spezifischen Themen im jeweiligen ISMS oder QMS zu behandeln. Hier kommt ein DSMS ins Spiel. Nahezu jede Firma und Behörde in Deutschland hat Berührung mit personenbezogenen Daten und müsste damit diverse Datenschutz-Prozesse implementiert haben. Da liegt der Gedanke nahe, diese in ein existierendes Management-System zu integrieren, da hier bereits regelmäßige Prozesse und Abläufe definiert und gelebt werden, die auch einem Datenschutzbeauftragten den Alltag erheblich erleichtern können.

Die praktische Umsetzung eines DSMS hängt davon ab, was an Management-Systemen bereits vorhanden ist. Gibt es noch gar nichts, dann zeigt die Praxis, dass es nicht unbedingt ratsam ist, mit einem DSMS zu beginnen. Im Gegensatz zu einem QMS oder ISMS unterliegt der Datenschutz in Deutschland keinem wohldefinierten Standard. Damit fehlt quasi eine gute, standardisierte Anleitung zur Implementierung.

Wurde bereits mindestens ein QMS oder ein ISMS implementiert, dann tut man sich deutlich leichter bei der Implementierung eines DSMS. In beiden Fällen sind bereits Regelprozesse implementiert, in die sich ein DSMS sehr gut einbetten lässt.

Gehen wir im Folgenden davon aus, dass bereits ein ISMS implementiert wurde. Ein ISMS nach ISO 27001 beinhaltet zwar das Thema Datenschutz durch die Anforderungen im Annex A15, enthält allerdings keine konkreten Vorschriften zur Umsetzung. Die notwendigen Prozesse und Tätigkeiten für den Datenschutz leiten sich (abhängig davon, ob man eine öffentliche oder eine nicht-öffentliche Stelle ist) aus dem Bundesdatenschutzgesetz, dem Landesdatenschutzgesetz und diversen spezielleren Gesetzen ab. Diese Anforderungen gilt es, in einem DSMS umzusetzen. Dazu muss entschieden werden, wie das DSMS implementiert werden soll:

- **Option 1:** Das DSMS wird als eigenständiges System implementiert. Gemeinsamkeiten mit dem ISMS werden in ein generisches Management-System ausgelagert, um Redundanzen (z. B. mehrfache Audits zum gleichen Thema), mehrfachen Pflegeaufwand und daraus resultierende Akzeptanzprobleme zu vermeiden.

- **Option 2:** Das DSMS wird direkt in das ISMS integriert.

Beide Optionen haben ihre Vor- und Nachteile: Option 1 findet ihre Befürworter bei Datenschützern, die argumentieren, dass ein DSMS letztendlich ein ISMS aus Datenschutz-Perspektive überwachen sollte, und man es daher auch abgrenzen sollte. Option 2 dagegen ist im Alltag meist erheblich einfacher zu implementieren und zu pflegen, da ISMS und DSMS sich sehr viele Prozesse sehr einfach teilen können. Letztendlich spielt bei dieser Entscheidung natürlich auch die eigene Datenschutz-Organisation eine Rolle. Wenn diese bereits jetzt sehr eng mit der Sicherheits-Organisation zusammenarbeitet, dann sollte Option 2 ins Auge gefasst werden. Option 1 ergibt i.d.R. nur Sinn, wenn man eine große Datenschutz-Organisation mit entsprechenden Ressourcen hat.

Welche Prozesse eines ISMS lassen sich denn nun sehr gut auch für Datenschutz-Themen nutzen? Dazu ein kurzer Überblick:

- **Risikomanagement:** Im ISMS wurde bereits eine Methode entwickelt, um Informationssicherheitsrisiken zu bewerten. Diese Methode lässt sich meist auch identisch zur Bewertung von Datenschutz-Zielen verwenden. Risikoanalysen können vom Datenschutzbeauftragten bzw. der Datenschutz-Organisation genutzt werden, um mit einer standardisierten Methodik Datenschutz-Ri-

siken bei Verfahren abzuwägen. Neben der reinen Betrachtung der klassischen Sicherheitsziele (Vertraulichkeit, Integrität und Verfügbarkeit) sollte man beim Datenschutz allerdings auch zusätzlich Datenschutzziele in die Risikoanalysen integrieren. Vom ULD (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein) wird hier beispielsweise empfohlen: Transparenz (Nachvollziehbarkeit, Überprüfbarkeit und Bewertbarkeit der Datenverarbeitung), Nicht-Verkettbarkeit (Vermeidung von Zweckentfremdung der Daten) und Intervenierbarkeit (Ausübung von Betroffenen-Rechten).

- **Management Review:** In einem Management Review wird der aktuelle Stand der Sicherheit mit dem zuständigen Management besprochen, geprüft und bei Bedarf angepasst. Durch eine geeignete Ergänzung von Datenschutz-Themen auf der Agenda für den Management Review lässt sich dies hervorragend mit einem DSMS integrieren. Da ein Management Review normalerweise direkt mit der Leitungsebene stattfindet, und der Datenschutzbeauftragte ebenfalls direkt der Leitungsebene unterstellt sein sollte, findet dieser Management Review im Idealfall mit dem selben Kreis an Verantwortlichen statt.

- **Integration in Kernprozesse:** Bei einem ISMS muss dafür Sorge getragen werden, dass das Thema Informationssicherheit in Kernprozesse (z. B. Entwicklung, Projekte oder Ausschreibungen) integriert wird. Auch für einen Datenschutzbeauftragten ist es notwendig, in diese Prozesse standardmäßig integriert zu werden, sofern dort personenbezogene Daten erhoben, gespeichert oder genutzt werden.

- **Audit-Prozess:** Für ein ISMS wird gewöhnlich eine Audit-Methodik definiert. Diese kann man relativ einfach um Datenschutz-Audits ergänzen. Dabei sollten sowohl interne Datenschutz-Audits als auch die Prüfung externer Auftragsdatenverarbeiter gem. §11 BDSG berücksichtigt werden.

- **Security Incidents:** Häufig werden Security Incidents über ein Ticket-System erfasst, dort bearbeitet und später ausgewertet. Die meisten Ticket-Systeme lassen sich problemlos um geeignete Kategorien für Datenschutz-Vorfälle ergänzen. Hier sollten allerdings unbedingt die Vertraulichkeits-Anforderungen an das Ticket-System geprüft werden, da der Zugriff auf Datenschutz-Vorfälle per Definition nur einem minimalen Personenkreis möglich sein sollte (der nicht zwingend identisch mit dem Personenkreis ist, der auf Sicherheitsvorfälle Zugriff haben muss, und meist den Systemverwalter nicht einschließt).

- **Metriken:** Informationssicherheit und Datenschutz müssen die Wirksamkeit von Maßnahmen aus ihrer Sicht beurteilen. Dafür lassen sich grundsätzlich dieselben Mechanismen zur Erhebung und Verwaltung von Kennzahlen (KPIs) nutzen.

Viele Schutzmaßnahmen, die zur Datensicherheit aus einer Informationssicherheits-Perspektive getroffen werden, sind auch gleichzeitig technische und organisatorische Maßnahmen (TOMs) gemäß §9 BDSG. Da es momentan aber für ein DSMS keine einheitlichen Maßnahmenpläne gibt, wie sie z. B. mit dem Standard ISO 27002 bzw. mit den BSI-Grundschutzkatalogen vorliegen, muss hier zwangsweise selbst Hand angelegt werden. Einen guten ersten Überblick für potentielle Datenschutz-Maßnahmen findet man im Baustein B 1.5 des BSI-Grundschutzkatalogs. Ergänzende, unternehmensspezifische Maßnahmen müssen dann allerdings zwangsweise selbst erarbeitet werden. Das muss aber mit oder ohne DSMS ohnehin geschehen. Einfacher wäre all das, wenn es mittelfristig wenigstens europaweit einheitliche Standard-Maßnahmenpläne für den Datenschutz gäbe.

Generell gilt, dass ein DSMS einem Datenschutzbeauftragten (und damit letztendlich direkt der Unternehmensleitung) im Alltag einen erheblichen Mehrwert liefern kann. Automatismen und Regelprozesse sorgen dafür, dass das Thema „Datenschutz“ viel stärker in den Alltag integriert wird. Wie das DSMS genau aussieht, bleibt jedem selbst überlassen, da es dafür bisher keine Formvorschriften in Deutschland gibt. Man sollte sich daher auch nicht von den zahlreichen Diskussionen diverser Fach-Theoretiker treiben lassen, die in Summe sehr unterschiedliche Meinungen haben. Das schönste DSMS hilft einem nichts, wenn es keiner verwendet, weil es zu komplex ist. Die einzigen wirklich relevanten Anforderungen sind daher, dass das DSMS dazu dient, den gesetzlichen Datenschutz-Anforderungen nachzukommen, und dass es für die eigene Firma oder Behörde im Alltag nutzbar ist.