21.11.2014

EPR16/2014

http://www.enisa.europa.eu/me

Schutz persönlicher Daten: ENISA-Leitlinien zu kryptografischen Lösungen

Die ENISA veröffentlicht heute zwei Berichte. Der Bericht „Algorithms, key size and parameters“ (Algorithmen, Schlüsselgrößen und Parameter) von 2014 ist ein Referenzdokument mit Leitlinien für Entscheidungsträger. Er richtet sich insbesondere an Experten, die kryptografische Lösungen zum Schutz persönlicher Daten in Unternehmen oder Behörden entwerfen und implementieren. Der Bericht „Study on cryptographic protocols“ (Studie über kryptografische Protokolle) bietet eine Umsetzungsperspektive und beinhaltet Leitlinien zu den Protokollen, die für den Schutz der Online-Kommunikation von Unternehmen und der darin enthaltenen persönlichen Daten benötigt werden.

„Algorithms, key size and parameters“

Dieser Bericht enthält eine Reihe von Empfehlungen in einem handlichen Format. Der Schwerpunkt liegt auf Online-Diensten von Unternehmen, in deren Rahmen persönliche Daten von EU-Bürgern gesammelt, gespeichert und verarbeitet werden. Es handelt sich um eine Aktualisierung des Berichts zu kryptografischen Leitlinien von 2013 über Sicherheitsmaßnahmen zum Schutz persönlicher Daten in Online-Systemen. Der Bericht ergänzt die Fassung von 2013 um einen Abschnitt über Hardware- und Software-Seitenkanäle, Zufallszahlengenerierung und die Verwaltung des Lebenszyklus von Schlüsseln. Der Abschnitt über Protokolle ist im Bericht von 2014 umfassender und stellt eine eigene Studie zu kryptografischen Protokollen dar.

In dem Bericht werden zwei Aspekte kryptografischer Mechanismen erläutert:

- ob die Verwendung eines bereits im Einsatz befindlichen Primitivs oder Verfahrens heute in Betracht gezogen werden kann
- ob die Verwendung eines Primitivs oder Verfahrens für den Einsatz in neuen oder künftigen Systemen geeignet ist.

Neben Fragen zur langfristigen Datenspeicherung werden auch eine Reihe allgemeiner Fragen zur Entwicklung kryptografischer Primitive und Verfahren untersucht. Alle im Rahmen des Berichts behandelten Mechanismen wurden in gewissem Umfang standardisiert und ihr Einsatz in bestehenden Systemen ist entweder bereits erfolgt oder für die Zukunft geplant.

„Study on cryptographic protocols“

Schwerpunkt des zweiten Berichts ist der aktuelle Stand bei kryptografischen Protokollen. Die weitere Erforschung der Materie wird empfohlen. Er enthält eine kurze Übersicht über Protokolle, die in relativ eingeschränkten Anwendungsbereichen verwendet werden, darunter Drahtlostechnologien, Mobilfunk und Bankgeschäfte (Bluetooth, WPA/WEP, UMTS/LTE, ZigBee, EMV), sowie Umgebungen, die eigens für die Cloud konzipiert wurden.

Der Bericht soll in erster Linie Wissenschaftlern und Organisationen, die auf diesem Gebiet tätig sind, Leitlinien an die Hand geben, unter anderem:

- Kryptografische und Sicherheitsprotokolle sind von Experten für kryptografische Protokolle zu erstellen statt wie bislang von Netzwerk- und Protokollexperten. Zudem sollten die Wissenschaftler die Analyse vereinfachen und sicherstellen, dass die automatisierten Tools zuverlässige rechnerbasierte Garantien liefern.

- Die automatische Überprüfung ist stärker zu berücksichtigen, damit die Implementierung eines Protokolls die Sicherheitsziele erfüllen kann. Es sollte untersucht werden, wie automatisierte Tools die fehlerfreie Protokollimplementierung sicherstellen können.
- Geringfügige Änderungen der Protokolle können die Garantiebeweise ungültig machen.
- Künftige Protokolle sollten auf der Grundlage solider und bewährter technischer Prinzipien im Hinblick auf eine einfache formale Sicherheitsanalyse und in Verbindung mit der Entwicklung formaler Sicherheitsbeweise nach der Kryptoanalyse ihrer jeweiligen Primitive entwickelt werden.
- Künftige Protokolle sollten nicht komplexer sein als nötig.
- An der Überprüfung von APIs für Anwendungsprotokolle muss noch weiter gearbeitet werden.

Udo Helmbrecht kommentierte die Berichte folgendermaßen: *„Besonders hervorgehoben wird die Notwendigkeit von Zertifizierungsprogrammen in allen Phasen des technischen Lebenszyklus. ‚Security by Design or by Default', d. h. die Berücksichtigung von Sicherheitsfragen bereits in der Entwicklung von Prozessen und Produkten, ist eine grundlegende Voraussetzung für Vertrauen. Die Standardisierung des Prozesses trägt wesentlich dazu bei, dass eine korrekte Umsetzung der Datenschutzreform im Dienste der EU-Bürger und des Binnenmarkts erfolgt. Die Leitlinien der ENISA sollen dabei einen richtungsweisenden Rahmen für den Schutz von Online-Systemen bilden."*

In der EG-Verordnung Nr. 611/2013 wird die ENISA als beratendes Organ genannt, das eine Liste angemessener kryptografischer Schutzmaßnahmen für den Schutz persönlicher Daten erstellt. Die kryptografischen Leitlinien der ENISA sollen als Referenzdokument dienen. In diesem Rahmen sind die Grundsätze als relativ konservative Richtschnur zu betrachten, die auf dem aktuellen Stand der Wissenschaft beruht und die Entwicklung neuer kommerzieller Systeme mit einem langen Lebenszyklus betrifft.

Die vollständigen Berichte (in englischer Sprache) sind hier abrufbar: „Algorithms, key size and parameters" und „Study on cryptographic protocols"

Interviews und weitere Informationen: press[at]enisa.europa.eu