log der Landesregierung Rheinland-Pfalz zum Thema „Mobile Payment" gestartet. In zwei Arbeitsgruppen haben sich Expertinnen und Experten aus Verbraucher- und Datenschutz, Wirtschaft, Forschung und Verwaltung schwerpunktmäßig mit Zahlungssicherheit und Datenschutz bei mobilen Bezahlverfahren befasst. Teilgenommen haben rund 20 Verbände, Unternehmen, Organisationen und Einrichtungen, darunter marktführende Akteure.

In beiden Arbeitsgruppen ist es gelungen, einstimmig Empfehlungen zur verbrauchergerechten Angebotsgestaltung zu verabschieden, die seit dem 04. November 2013 vorliegen. Die Empfehlungen zur Zahlungssicherheit und zum Datenschutz richten sich an Anbieter von Mobile Payment-Verfahren und dienen insbesondere der Verbrauchersicherheit, den Verbraucherrechten sowie der Verbraucherinformation. Sie definieren Anforderungen an einen verbraucherfreundlichen Einsatz von Mobile Payment und enthalten grundlegende Kriterien u.a. zur Datenverarbeitung, Nutzerregistrierung und -authentifizierung, Zahlungsautorisierung, Transparenz und Kostenkontrolle sowie zu technisch-organisatorischen Sicherheitsvorkehrungen. Sie sollen im Sinne eines präventiven Verbraucher- und Datenschutzes dazu beitragen, dass Mobile Bezahlverfahren von Anfang an sicher und verbrauchergerecht auf dem deutschen Markt eingeführt werden.

Der Verbraucherdialog ist eine Veranstaltung des MJV in Kooperation mit der Verbraucherzentrale Rheinland-Pfalz e.V. und dem rheinland-pfälzischen Landesbeauftragten für den Datenschutz und die Informationsfreiheit.

Auch Experten des Bundesamts für Sicherheit in der Informationstechnik (BSI) waren intensiv an diesem Verbraucherdialog beteiligt. Sie empfahlen unter anderem die Nutzung des neuen Personalausweises für die Kundenidentifizierung bei mobilen Bezahlverfahren als technische Lösung und formulierten zentrale Sicherheitsanforderungen an das kontaktlose mobile Bezahlen.

Zum Abschluss des Verbraucherdialogs wurden die Arbeitsergebnisse in zwei Papieren zusammengefasst. Zur technischen Absicherung kontaktloser Bezahlverfahren wird demnach insbesondere empfohlen

- eine gegenseitige Authentisierung der Kommunikationspartner zu verwenden,
- Nutzinformationen, die kontaktlos ausgetauscht oder gespeichert werden, zu verschlüsseln,
- Vertrauensanker („Secure Elements") zu nutzen, um potenziell unsichere Smartphones für sicheres kontaktloses Bezahlen nutzbar zu machen.

Beide Ergebnispapiere sind auf der Website *http://www.mjv.rlp.de/Startseite/broker.jsp?uMen=1fb6ec57-083e-e310-caca-fc377fe9e30b* verfügbar.

Mindeststandard TLS 1.2 und Web-Seiten des BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat am 8. Oktober 2013 einen Mindeststandard für den Einsatz einer Transportverschlüsselung mittels des TLS-Protokolls veröffentlicht[1]. Ein Mindeststandard des BSI beschreibt die zu erfüllenden sicherheitstechnischen Anforderungen an eine Produkt- bzw. Dienstleistungskategorie oder Methoden, um einen angemessenen Mindestschutz gegen IT-Sicherheitsbedrohungen zu erreichen. Mit der Veröffentlichung des Mindeststandards zu TLS 1.2 hat das BSI im Sinne der Internetnutzer in Deutschland eine Zielvorgabe formuliert, auf die die Einrichtungen der Bundesverwaltung, zu denen auch das BSI gehört, nun hinarbeiten können.

Es liegt dabei in der Natur der Sache einer Zielvorgabe, dass diese in der Zukunft liegt. Ein Ziel vorzugeben, das man bereits erreicht hat, ist aus Sicht des BSI wenig sinnvoll. Am 13.11.2013 hat das B SI seine eigene Migrationsstrategie publiziert.

Da eine Migration zu TLS 1.2 in der Regel nicht nur Software-, sondern auch Hardware-Produkte umfasst, kann dies ein zeitintensiver Prozess sein, bei dem neben technischen auch organisatorische Aspekte zu berücksichtigen sind. Insofern ist auch nach der Setzung eines konkreten Zieles eine Übergangszeit durchaus üblich und sinnvoll. Das BSI begleitet diese Übergangszeit und steht den Behörden bei der Migration beratend zur Seite. Auch im BSI selbst erfolgt die Migration in einem strukturierten und sorgfältig vorbereiteten Prozess. Dieser Prozess hat bereits begonnen. Gemeinsam mit seinem Hosting-Dienstleister arbeitet das BSI derzeit mit Nachdruck an der Umstellung der Webserver, auf denen die BSI-eigenen Webseiten gehostet werden. Zunächst geht es dabei um die Beendigung des exklusiven Einsatzes des Verschlüsselungsalgoritmus RC4. Dies konnte bereits kurzfristig realisiert werden. Die Migration zu TLS 1.2 ist bereits eingeleitet.

B-W: Öffentliche Einrichtungen verzichten auf den Like-Button von Facebook

Im August dieses Jahres hatten Mitarbeiter des Landesbeauftragen für den Datenschutz Baden-Württemberg über 4.300 Internetseiten von öffentlichen Stellen mit einem speziellen Prüfprogramm auf die Verwendung des Facebook-Like-Buttons untersucht und dabei in 47 Fällen Abhilfe gefordert. Das Fazit der Untersuchung ist positiv: Am 19.11.2013 konnte der LfD mitteilen, dass alle angeschriebenen Behörden auf die Aufforderung reagiert und den Like-Button gänzlich von ihrem Internetauftritt entfernt oder durch die sogenannte Zwei-Klick-Lösung ersetzt haben.

Hintergrund der Überprüfung war, dass Facebook mit dem Like-Button Daten über die Vorlieben seiner Nutzer nicht nur auf der eigenen Webseite, sondern auch auf den beanstandeten Webseiten sammeln kann. Dabei kann es sich um personenbezogene Daten handeln, wenn der Nutzer gleichzeitig in Facebook eingeloggt und dadurch eindeutig identifizierbar ist. Die Nutzerdaten können aber auch bis zu zwei Jahre rückwirkend zugeordnet werden, wenn sich jemand später bei Facebook anmeldet.

„Der Aufwand hat sich gelohnt!" so der Landesbeauftragte Jörg Klingbeil. „Der Schutz der personenbezogenen Daten von Bürgerinnen und Bürger muss Vorrang haben. Deshalb soll es auch in Zukunft weitere Prüfungen von Internetauftritten – nicht nur im öffentlichen Bereich – geben. Für das nächste Jahr ist bereits eine weitere Überprüfung geplant."

BSI: Zertifikate für IT-Sicherheitsdienstleister

Am 08.11.2013 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) der secuvera GmbH ein Zertifikat überreicht, das das Unternehmen als ein vom BSI zertifizierter IT-Sicherheitsdienstleister im Bereich Penetrationstests bestätigt. Die secuvera GmbH ist somit befähigt, Sicherheitsuntersuchungen, Schwachstellen-

1 DuD 12-2013, S. 817