in CBC-Modus und Zwei-Faktor-Authentifizierung mittels Smartcard und PIN nach erfolgreicher Zertifizierung beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein das ULD-Datenschutzsiegel und European Privacy Seal (EuroPriSe). Mit diesen Siegeln wird bestätigt, dass die HS256S die Anforderungen des BDSG und der EG-Datenschutz-Richtlinie erfüllt und zur Speicherung personenbezogener Daten als erste und derzeit einzige externe Festplatte zugelassen ist.

4 Fazit

Oft befinden sich auf externen Speichermedien vertrauliche und wertvolle Daten. Gelangen diese in falsche Hände, birgt dies die Gefahr großer finanzieller Schäden und Reputationsverlusten. Sinnvoller und kostengünstiger ist es daher, solchen Fällen vorzubeugen, indem die verwendeten Speichermedien ein ausreichend hohes Sicherheitsniveau gewährleisten.

Auch der Zeitfaktor spielt bei der Implementierung innovativer Sicherheitsspeichermedien in Unternehmen eine Rolle: Die Verwendung eines im Speichermedium integrierten Hardwareverschlüsselungsmoduls ist deutlich schneller als eine Softwarelösung. Kann der Anwender den kryptografischen Schlüssel zudem selbst verwalten, macht ein Schlüsseltausch das Speichermedium schnell und unkompliziert einsatzfähig für den nächsten Nutzer – ohne dass dabei ein Nutzer auf die Daten des anderen zugreifen kann.

Greifen die vier Hauptkriterien – Datenverschlüsselung, Zugriffskontrolle, Speicherort des kryptografischen Schlüssels sowie dessen Verwaltung durch den Anwender – in geeigneter Weise ineinander, ist auch die umfassende Sicherheit hochsensibler Daten gewährleistet. Das „Tür-Schloss-Schlüssel"-Bild ist geeignet, das Zusammenwirken der relevanten Elemente der Sicherheitskette deutlich zu machen.

Durch die Zertifizierung entsprechender Produkte brauchen sich Anwender nicht länger auf die bloßen Behauptungen von Herstellern über die Sicherheitsstufe der von ihnen produzierten Speichermedien verlassen. Sie sollten vielmehr jegliche Lösungen für ihre Datensicherheit anhand der genannten Hauptkriterien selbst bewerten und dabei auch die Ergebnisse von Zertifzierungsprozessen mit einbeziehen.

ULD: Datenschutz-Zertifizierung

Als Datenschutzaufsichtsbehörde des Landes Schleswig-Holstein vergibt das Unabhängige Landeszentrum für Datenschutz (ULD) für Produkte, die datenschutzgerecht gestaltet sind, ein gesetzlich geregeltes Gütesiegel. Die Prüfkriterien leiten sich aus den datenschutzrechtlichen Vorschriften für die öffentlichen Behörden des Landes, in erster Linie den Vorschriften des Landesdatenschutzgesetztes (LDSG), her. Obwohl es eine konkrete Rechtswirkung in Form einer Beschaffungsempfehlung nur in Schleswig-Holstein entfalten kann, wird es in der Praxis bundesweit werbewirksam eingesetzt. Zertifizierungsfähig sind Hardware, Software und automatisierte Verfahren, die zur Nutzung durch öffentliche Stellen geeignet sind.

Das ULD ist auch Zertifizierungsstelle für das Europäische Datenschutz-Gütesiegel EuroPriSe, das 2009 aus einem EU-Projekt hervorgegangen ist. Die EuroPrise-Kriterien basieren auf den europarechtlichen Vorgaben, in erster Linie der Datenschutzrichtlinie der EU, sowie auf der Rechtsprechung der europäischen Gerichte und den Empfehlungen der Artikel 29-Datenschutzgruppe.

Beiden Verfahren ist gemein, dass der Hersteller oder die Vertriebsfirma eines Produktes oder Verfahrens vom ULD anerkannte Sachverständige mit der Begutachtung des Produktes beauftragt. Diese müssen von ihrer Fachkunde her die Bereiche Recht und Technik abdecken. Das Ergebnis der Begutachtung wird im Rahmen der Zertifizierung vom ULD durch eine Validierung der Prüfergebnisse auf Vollständigkeit und Plausibilität und zusätzlich hinsichtlich der Konsistenz und Prüftiefe qualitätsgesichert. Gegenstand der Zertifizierung ist in beiden Fällen die Aussage, dass ein Anwender das zertifizierte Produkt bzw. Verfahren datenschutzkonform nutzen kann. Die Gutachter prüfen, ob sich mit der vorhandenen Ausgestaltung des Produktes oder Verfahrens einschließlich der Dokumentation personenbezogene Daten rechtskonform verarbeiten lassen. Dies bezieht sich nicht nur auf die Produktfunktionalitäten, sondern zum Beispiel auch auf Protokollierungen, Backup-Verfahren und Vertragsgestaltungen im Rahmen einer Auftragsdatenverarbeitung. Ob ein Anwender als verantwortlicher Stelle das Produkt bzw. Verfahren tatsächlich datenschutzkonform einsetzt, kann der Hersteller in der Regel nicht beeinflussen, so dass dieses auch nicht zertifiziert werden kann. Er kann aber durch geeignete Produktgestaltung, Dokumentation sowie Hinweise darauf hinwirken.

Bei typischen Zertifizierungsverfahren stehen datenschutzrechtliche Fragen im Vordergrund, insbesondere Fragen zu Umfang, Zweck und Zulässigkeit der Datenverarbeitung. Daneben spielen technische Fragen zum Datenschutz und zur Datensicherheit sowie deren Maßnahmen bzw. notwendigen Funktionalitäten (etwa Verschlüsselungen, Protokollierungen, Zugriffskontrollmechanismen) eine Rolle. Zentrales Element ist auch, die Prüfergebnisse transparent und vergleichbar zu gestalten. Daher muss im Rahmen der Zertifizierung stets auch ein Kurzgutachten auf den Webseiten des ULD bzw. von EuroPriSe veröffentlicht werden.

Bei dem Zertifizierungsverfahren von Digittrade handelte es sich um ein kombiniertes Verfahren von EuroPriSe und dem Datenschutz-Gütesiegel Schleswig-Holstein. Das hier betrachtete Produkt einer Verschlüsselungshardware kann prinzipiell zur Verarbeitung verschiedenster Daten eingesetzt werden. Ob diese Daten personenbezogen sind und ob die Datenverarbeitung rechtmäßig ist, liegt vollständig in der Hand des Anwenders und kann durch den Hersteller nicht beeinflusst werden. Der Schwerpunkt der Prüfung lag daher bei diesem Verfahren in der Handhabung der Verschlüsselung, dem Schlüsselmanagement sowie der Dokumentation: Die Speicherung der Schlüssel erfolgt auf Smartcards, die zur Verwendung eine Benutzerauthentisierung mittels einer PIN erfordern. Ebenso werden die einzelnen Smartcards durch eine Initialisierung an die Festplatten gebunden; es gibt Möglichkeiten einer Schlüsselkopie sowie eine Schlüsselrevokation. Dadurch ergeben sich deutlich komplexere Möglichkeiten für das Schlüsselmanagement als beispielsweise bei einer passwortbasierten Containerverschlüsselung in einem Dateisystem. Zu prüfen war daher insbesondere, ob dies dem Anwender hinreichend transparent dargestellt wird und ob notwendige Schritte, etwa bei der Schlüsselrevokation oder der Vernichtung von Schlüsselmaterial hinreichend klar beschrieben wurde.

Die Prüfung der korrekten Implementierung des zugrundeliegenden Verschlüsselungsverfahrens war im Rahmen dieser Datenschutzzertifizierung hingegen nicht zu leisten. Hierzu wurde die Zertifizierung der Hardware sowie der verwendeten Smartcards herangezogen.

Rechtlich war vor allem darauf zu achten, dass die einsetzende Stelle in der Dokumentation auf ihre eigenen Prüfpflichten zur Einsatzmöglichkeit des Produkts hingewiesen wird und einige allgemeine Hinweise zum Datenschutzrecht an die Hand bekommt.

Weitere Informationen zu EuroPriSe: *www.european-privay-seal.eu*

Weitere Informationen zum Datenschutz-Gütesiegel Schleswig-Holstein: *www.datenschutzzentrum.de/guetesiegel*

Henry Krasemann, Unabhängiges Landeszeutrum für Datenschutz Schleswig-Holstein