Marketingmitteilung

FIPS 140-2-Standard und Selbstverschlüsselung

Häufig gestellte Fragen (FAQ)

Was ist FIPS 140-2?

FIPS (Federal Information Processing Standard) 140-2 ist ein Standard der US-Regierung und beschreibt die Verschlüsselung und die zugehörigen Sicherheitsanforderungen, die IT-Produkte zur *vertraulichen*, aber nicht klassifizierten Nutzung erfüllen sollten.

Was legt FIPS 140-2 fest?

Der Standard gewährleistet, dass ein Produkt solide Sicherheitspraktiken wie etwa zugelassene, starke Verschlüsselungsalgorithmen und -verfahren einsetzt. Zudem legt er fest, wie Einzelpersonen oder andere Prozesse zur Nutzung des Produkts autorisiert werden müssen und wie Module oder Komponenten zur sicheren Interaktion mit anderen Systemen entwickelt werden müssen.

Warum ist eine Verschlüsselung erforderlich?

Festplatten werden ständig außer Betrieb genommen (innerhalb der Garantie, zur Reparatur und wegen abgelaufener Leasingverträge eingeschickt, für andere Speicheraufgaben eingesetzt oder verkauft), gehen verloren oder werden gestohlen. Wenn ungeschützte Daten nicht mehr kontrolliert werden können und gefährdet sind, läuft ein Unternehmen Gefahr, Einnahmen, Marktanteile und das Vertrauen seiner Kunden zu verlieren. Dies kann als Verstoß gegen Datenschutzauflagen sogar zivilrechtliche Strafen nach sich ziehen. Die Folgen sind für jedes Unternehmen, insbesondere aber für kleine und mittelständische Unternehmen, katastrophal.

- Seagate schätzt, dass 50.000 Festplatten mit mehreren Terabyte von Daten *jeden Tag Rechenzentren verlassen.*
- IBM schätzt, dass 90 Prozent aller als Garantiefall zurückgegebenen Festplatten lesbare Daten enthalten.

Laut Branchenexperten wie dem Ponemon Institute nehmen die durchschnittlichen Kosten für jeden Datenmissbrauch jährlich zu und beliefen sich 2008 auf 6,6 Millionen US-Dollar, das sind 202 US-Dollar pro gefährdetem Datensatz.[1]

Weiterhin schätzt das Ponemon Institute, dass 81 Prozent aller Laptops vertrauliche Daten enthalten und 10 Prozent aller Laptops während ihrer Lebensdauer verloren gehen oder gestohlen werden. Zusätzlich werden Schätzungen zufolge allein an US-Flughäfen jede

[1] Ponemon Institute, *Jährliche Studie 2008: U.S. Cost of a Data Breach,* Februar 2009, www.ponemon.org, zitiert in *Data-breach costs rising, study finds* von Ellen Messmer, Network World, 02.02.09.

FIPS 140-2-Standard und Selbstverschlüsselung

Häufig gestellte Fragen (FAQ)

Woche 12.000 Laptops gestohlen oder gehen verloren. Die durchschnittlichen Kosten für ein Unternehmen bei einem verschwundenen Laptop mit vertraulichen, aber unverschlüsselten Daten betragen fast 50.000 US-Dollar. In extremen Fällen können sich die Kosten sogar auf fast 1 Million US-Dollar belaufen.[2]

Was sind die verschiedenenn Stufen von FIPS 140-2?

FIPS 140-2 arbeitet mit insgesamt vier Sicherheitsstufen. Durch die Validierung gemäß FIPS 140-2 wird die Sicherheitsstufe festgelegt, die das Produkt erfüllt.

- **Stufe 1** hat nur sehr geringe Sicherheitsanforderungen und wird gewöhnlich für Produkte verwendet, die lediglich über eine Software-Verschlüsselung verfügen. Alle Komponenten müssen einen hohen *Fertigungsgrad* und dürfen keinerlei Sicherheitslücken aufweisen.
- **Stufe 2** erfordert *funktionsbasierte* Authentifizierung. (Eine individuelle Benutzerauthentifizierung ist nicht erforderlich.) Außerdem muss die Möglichkeit bestehen, durch den Einsatz physikalischer Sperren oder manipulationssicherer Siegel physischen Missbrauch *zu erkennen*.
- **Stufe 3** fügt dazu noch *Immunität* gegen physische Manipulation und Schutz vor Demontage oder Modifizierung hinzu, wodurch das Produkt äußerst gut vor Eindringversuchen geschützt ist. Wenn ein Manipulationsversuch erkannt wird, muss das Gerät in der Lage sein, kritische Sicherheitsparameter zu löschen. Stufe 3 enthält robusten Verschlüsselungsschutz und Schlüsselmanagement, *identitätsbasierte* Authentifizierung sowie physische und logische Trennung zwischen den Schnittstellen, die von *kritischen Sicherheitsparametern* verwendet werden.
- **Stufe 4** enthält erweiterten Manipulationsschutz und ist für Produkte geeignet, die in physisch ungeschützten Umgebungen verwendet werden.

Welche Validierungsstufe von FIPS 140-2 hat Seagate?

Sich selbst verschlüsselnde Festplatten (SEDs) von Seagate® besitzen die Validierungsstufe 2 gemäß FIPS 140-2.

Warum hat Seagate die Validierungsstufe 2 von FIPS 140-2 erworben?

Unternehmen unterschiedlichster Art fordern zunehmend, ruhende Daten zum Schutz vor Verlust oder Diebstahl zu verschlüsseln. Die Validierungsstufe 2 von FIPS 140-2 gilt als Zeichen für Sicherheit und Qualität und zertifiziert allen Käufern, dass die SEDs mit FIPS von Seagate die Voraussetzungen für Sicherheitsprodukte der US-Bundesregierung erfüllen.

Für welche Produktarten ist FIPS 140-2 relevant?

FIPS 140-2 gilt für jedes Produkt, das vertrauliche Daten speichern oder übertragen kann. Dazu gehören Hardware-Produkte wie Link-Verschlüsselungsgeräte, Festplatten, Flash-Festplatten oder andere mobile Speichermedien. Der Standard gilt ebenfalls für Software-Produkte, die Daten bei der Übertragung oder bei der Speicherung verschlüsseln.

Benötige ich wirklich so viel Sicherheit? Reicht ein Passwort in meinem Betriebssystem nicht aus?

Die Sicherheit des Betriebssystems, etwa ein Passwort, lässt sich leicht umgehen, indem man die Festplatte aus- und in einen anderen Computer einbaut. Sogar ATA-Festplatten mit BIOS-Passwort sind ungeschützt, wenn Sie nicht zum Beispiel mit einer SED von Seagate verwendet werden. Die Verschlüsselung der Daten auf der Festplatte oder dem Speichermedium ist ein bewährtes Schutzmittel.

Für welche Organisationen oder Unternehmen ist die Einhaltung von FIPS 140-2 erforderlich?

In den USA verlangt das National Institute of Standards and Technology von allen Bundesbehörden, Produkte mit der Validierungsstufe 2 von FIPS 140-2 zu verwenden, um als *vertraulich, aber nicht klassifiziert* eingestufte Daten auf Computer- und Telekommunikationssystemen (einschließlich Sprachsystemen) zu schützen.[3] In Kanada verlangt das Communications Security Establishment (CSE) von Bundesbehörden, Verschlüsselungsmodule mit der Validierungsstufe 2 von FIPS 140-2 zu verwenden, um als *geschützte Informationen* (A oder B) eingestufte Daten auf Computer- und Telekommunikationssystemen (einschließlich Sprachsystemen) zu schützen. Die FIPS 140-Validierung

[2] Intel-Studie: Stolen Laptops Cost to Business; eWeek, 23. April 2009; Studie des Ponemon Institute, April 2009.

[3] http://csrc.nist.gov/groups/STM/cmvp/index.html

FIPS 140-2-Standard und Selbstverschlüsselung

Häufig gestellte Fragen (FAQ)

Zertifizierung gemäß FIPS 140-2 Validated

ist zudem eine notwendige Vorstufe, damit ein Verschlüsselungsprodukt in die ITS-Liste für vorqualifizierte Produkte der kanadischen Regierung aufgenommen wird.[3] In Großbritannien empfiehlt die Communications-Electronics Security Group die Nutzung von Verschlüsselungsmodulen mit FIPS 140-Validierung.[4]

Weltweite Zivilunternehmen, die einen Vertrag mit Organisationen der US-, kanadischen oder britischen Regierung abschließen, von denen eine Verschlüsselung gemäß FIPS 140-2 verlangt wird, müssen diese Vorgaben ebenfalls erfüllen. Des Weiteren verlangen kommerzielle Unternehmen – besonders im Finanzsektor, Gesundheitswesen, Bildungswesen und in der Infrastruktur (nationale Sicherheit) – zunehmend die Einhaltung von FIPS 140-2 auf der ganzen Welt. Diese Unternehmen wollen unbednqt den höchsten Datenschutzstandard bieten. Sie wissen um die strengen Kriterien einer Zertifizierung gemäß FIPS-140, halten ihn für den bevorzugten Sicherheitsstandard und verlassen sich in Bezug auf ihre eigenen Verschlüsselungsanforderungen auf diesen Standard.

Was ist eine FIPS 140-2-Validierung?

Eine FIPS 140-2-Validierung ist ein Test- und Zertifizierungsprogramm, das verifiziert, dass ein Produkt den Standard FIPS 140-2 erfüllt. Das NIST hat dazu das Validierungsprogramm für Verschlüsselungsmodule (Cryptographic Module Validation Program, CMVP) entwickelt.

Was ist für eine Zertifizierung gemäß FIPS 140-2 erforderlich?

Damit ein Produkt dem Standard FIPS 140-2 Validated entspricht, muss es die Vorgaben zu Design und Umsetzung erfüllen und von einem von 13 unabhängigen und von dem NIST akkreditierten Laboren getestet und genehmigt werden.

Welcher ist der aktuelle Standard für FIPS 140-2 Validated?

Die 140 nummerierten FIPS-Veröffentlichungen stellen eine Reihe von Sicherheitsstandards dar, die bestimmte Vorgaben für Verschlüsselungsmodule festlegen. FIPS 140-1 wurde 1994 festgelegt, jedoch durch FIPS 140-2 ersetzt. Dieser heute aktuelle Standard wurde 2001 festgelegt. FIPS 140-3 ist eine neue Version des Standards und wird seit 2005 entwickelt. Im Dezember 2009 wurde ein Entwurf dazu veröffentlicht, es wird allerdings wahrscheinlich noch mindestens ein Jahr dauern, bevor dieser Entwurf als Nachfolger von FIPS 140-2 in Kraft tritt.

Gibt es eine Liste von Produkten, die FIPS 140-2 Validated entsprechen?

Das NIST führt eine Liste aller handelsüblichen Produkte, die dem Standard FIPS 140-2 Validated entsprechen. Sie können diese Liste auf der Website http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm sehen.

Warum ist FIPS 140-2 für Vertriebspartner von Seagate wichtig?

Vertriebspartner von Seagate können FIPS 140-2 Validated als wirksames Marketing-Tool einsetzen, um die Qualität und die wichtigen Sicherheitsfunktionen ihrer Produkte zu demonstrieren, die andere Produkte nicht aufweisen. Es dient den sicherheitsbewussten Käufern von heute als wichtiges Unterscheidungsmerkmal.

[3] http://csrc.nist.gov/groups/STM/cmvp/index.html

[4] www.cesg.gov.uk/

www.seagate.com
Gebührenfrei: 00 8004 SEAGATE (732 4283)
(gebührenpflichtig: 001 405 324 4714)
Kunden in Österreich wählen bitte zunächst die Hauptzugangsnummer 0-800-200-288 und dann die 888-212-1077.

NORD- UND SÜDAMERIKA Seagate Technology LLC 920 Disc Drive, Scotts Valley, California 95066, United States, +1 831-438-6550
ASIEN/PAZIFIK Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapore 569877, +65 6485 3888
EUROPA, NAHER OSTEN UND AFRIKA Seagate Technology SAS 16-18 rue de Dôme, 92100 Boulogne-Billancourt, France, +33 1 41 86 10 00