
PRESSEMELDUNG von OPTIMAL System-Beratung

In Deutschland keine hardwareverschlüsselten USB-Sticks mit Sicherheitslücken im Umlauf

SafeStick von OPTIMAL System-Beratung ist immun gegen Hackerangriffe

Aachen, 19. Januar 2010.- Der hardwareverschlüsselte USB-Stick SafeStick ist gegen Hackerangriffe immun. Der in Deutschland von OPTIMAL System-Beratung vertriebene SafeStick ist nicht von der Sicherheitslücke betroffen, die kürzlich für einen Skandal sorgte. Die Prüfung des Nutzerpasswortes auf der Hardware selbst und der individuelle Antwortcode gewährleisten, dass die Daten nur von Befugten entschlüsselt werden können.

„Diese Sicherheitslücke ist so eklatant, dass es unbegreiflich ist, dass die Zertifizierungsstelle sie nicht entdeckt hat!“ erklärt Bert Rheinbach, Geschäftsführer von OPTIMAL System-Beratung. „SafeStick kann weder auf diese noch auf eine andere Weise geknackt werden.“ Als deutscher Vertriebspartner von Blockmaster sei er natürlich erleichtert, aber nicht erstaunt darüber, denn sein Testlabor habe den Stick auf Herz und Nieren geprüft.

Der hardwareverschlüsselte USB-Stick des schwedischen Herstellers Blockmaster funktioniert folgendermaßen: Bei richtiger Passworteingabe generiert SafeStick ein Einmal-Passwort, das den Zugang zu den gespeicherten Daten erlaubt. Anders als bei den geknackten USB-Sticks wird dieses Passwort auf der Hardware selbst generiert, und zwar jedes Mal ein neues. SafeStick verschlüsselt alle gespeicherten Daten via Hardware mit dem hohen Verschlüsselungsverfahren 256-Bit-AES (Advanced Encryption Standard) mit CBC.

Sicherheitslücke in amerikanischen USB-Sticks

Zwar haben auch die in Verruf geratenen USB-Sticks diesen anerkannt hohen Verschlüsselungsstandard. Aber deren Passwort wird nicht auf dem Stick, sondern in der Software am PC verifiziert. Bei einem erfolgreichen Anmeldevorgang sandte diese eine Zeichenfolge zur Bestätigung an den Stick, und zwar immer die gleiche Folge für alle Sticks dieses Typs. Die Tester schrieben also einfach ein Programm, das im Arbeitsspeicher des laufenden Passwort-Eingabeprogramms dafür sorgte, dass der passende String an den Stick gesandt wurde -

PRESSEMELDUNG von OPTIMAL System-Beratung

unabhängig vom eingegebenen Passwort. So erhielten sie Zugang zu allen Daten auf dem Speicherstift.

So funktioniert SafeStick

Safestick dagegen prüft das Passwort und generiert den Schlüssel auf der Hardware selbst: Das vom Anwender eingegebene Passwort wird von der Software auf dem Computer mit einem Hashwert versehen. Auf diese Weise wird ein einmaliger Passwortstring erzeugt, der dem SafeStick Hardware Controller durch einen privaten Kanal über USB mitgeteilt wird. Dieser Passwortstring wird auf dem SafeStick erneut mit einem Hashwert „gestempelt“. Das auf diese Weise doppelt gekennzeichnete Passwort wird genutzt, um mit einem Zufallszahlen-generator auf der Hardware (dem USB-Stick) den Schlüssel zu erzeugen, der alle vom Anwender gespeicherten Daten mit 256-Bit-AES verschlüsselt. Die Hardware ist komplett epoxidgehärtet.

Dieses Verfahren garantiert, dass SafeStick wirklich den hohen Sicherheitsanforderungen genügt, die die US-amerikanischen Hersteller der betroffenen USB-Sticks für sich lediglich beansprucht hatten. Nach Angaben der Hersteller wurden bisher keine betroffenen Sticks in Europa verkauft.

In Deutschland nutzen Unternehmen und Behörden SafeStick zur sicheren Speicherung sensibler Daten auf USB-Sticks. Mit der zusätzlichen Administrationssoftware SafeConsole können sie alle SafeSticks einer Organisation zentral verwalten und konfigurieren.

www.optimal.de

Weiterführende Links:

http://www.optimal.de/safestick_safeconsole_usb_management.html

<http://www.blockmastersecurity.com/security/competing-products-contain-serious-flaw-safestick-not-affected/>

<http://www.heise.de/newsticker/meldung/NIST-zertifizierte-USB-Sticks-mit-Hardware-Verschlüsselung-geknackt-894962.html>

<http://www.networkcomputing.de/loechrige-hardware-verschluesselung-macht-usb-sticks-zum-sicherheitsrisiko/?cid=IWKnewsletter-weekly-html>

PRESSEMELDUNG von OPTIMAL System-Beratung

459 Worte, 3520 Zeichen

Kurzprofil

OPTIMAL System-Beratung ist seit 1992 auf die Bereiche Client-Management- und Sicherheitslösungen spezialisiert. Von der Beratung und Programmierung über den Vertrieb bis hin zur Installation: Ständig sucht das IT-Systemhaus nach einfachen Softwarelösungen für komplizierte Anforderungen in IT-Management und Systemadministration, die Anwendern die Arbeit erleichtern. Dabei entwickelt OPTIMAL System-Beratung eigene Produkte oder erweitert und verbessert vorhandene Lösungen.

In Deutschland und Österreich sowie den deutschsprachigen Bereichen der Schweiz und Italiens beliefert OPTIMAL die Anwender entweder direkt oder mit Hilfe des ausgedehnten Partnernetzwerkes. OPTIMAL System-Beratung ist Mitglied im Bundesverband mittelständische Wirtschaft (BVMW) und dessen Kompetenzkreis IT. www.optimal.de