



Den vollen Nutzen sicherer USB-Sticks aus zentralem Management schöpfen

Ein sicheres USB-Flash Laufwerk verschlüsselt ausnahmslos alle darauf abgelegten Daten hardwarebasiert und sichert sie mit einem obligatorischen Passwort. Der Grund, warum Organisationen sich für die Einführung einer solchen Technologie interessieren, ist eindeutig:

Nie wieder sensible Daten auf einem USB-Stick verlieren!

Es gibt eine Fülle von Faktoren, die zu berücksichtigen sind, wenn Sie sich vor der Beschaffung von sicheren USB-Sticks befinden, vor allem wenn es um die zentrale Verwaltung dieser Technologie geht.



EXECUTIVE SUMMARY

Es gibt eine Fülle von Faktoren, die zu berücksichtigen sind, wenn Sie sich vor der Beschaffung von sicheren USB-Sticks befinden, vor allem wenn es um die zentrale Verwaltung dieser Technologie geht.

- 1.** Zuerst sollte berücksichtigt werden, wie schnell und einfach diese Technologie einzuführen ist. Wie kommen die USB-Sticks zu den Anwendern? Denken Sie auch daran, dass die Bereitstellung und Delegation von Berechtigungen so wenig Aufwand und Kosten wie möglich verursachen sollte.
- 2.** Ein zweiter Faktor hierbei ist der Grad der Kontrolle, den Sie über Anwender und deren USB-Sticks haben wollen oder dürfen. Nur autorisierte Inhalte oder erlaubte Software sollten auf USB-Sticks installiert werden können und außerdem muss zurück gemeldet werden, dass die Daten oder Applikationen auch tatsächlich installiert wurden. Besonders hervorzuheben ist die Notwendigkeit eines stets aktuellen und effektiven Schutzes vor Viren und Malware auf den USB-Sticks.
- 3.** Beachten Sie auch den Schutz der Privatsphäre des Anwenders. Die Lösung darf niemals Passwörter zentral speichern! Gleichzeitig müssen sowohl gesetzliche Vorschriften als auch interne Richtlinien hinsichtlich Datenschutz eingehalten werden: können/dürfen Sie ein Auditing von Benutzern und Inhalten durchführen?
- 4.** Entscheidend ist, dass Sie die Kontrolle über alle einzelnen administrativen Aufgaben haben. Wie können Sie Offline-Anwendern helfen, die Ihr Passwort vergessen haben, ohne dabei deren Passwort zu erfahren oder gar ein Master-Passwort zu besitzen? Können Daten eines verlorenen USB-Sticks schnell und einfach auf einem neuen USB-Stick des Anwenders wiederhergestellt werden? Ist es möglich, verlorene USB-Sticks aufzuspüren, aus der Ferne zu sperren, zu löschen oder komplett zurückzusetzen?
- 5.** Fünftens ist zu berücksichtigen wie die Lösung sich in Ihre bestehende Infrastruktur integriert. Ist die Lösung kompatibel zu anderen Sicherheitslösungen? Existieren Schnittstellen und APIs dazu? Ist es möglich Daten auf andere Systeme zu exportieren?
- 6.** Schließlich ist noch der allgemeine Zugriff der Lösung auf das System entscheidend. Anwender und Administratoren, die das Unternehmen verlassen haben, sollte der Zugang zur Managementlösung möglichst einfach gesperrt werden können. Anstatt die Anwender einzeln verwalten zu müssen, sollte die Möglichkeit bestehen, dies über das zentrale Anwenderverzeichnis durchzuführen.



EINFÜHRUNG - EIN BLICK HINTER VERSCHLÜSSELTE USB-STICKS

USB-Sticks sind ein elementarer Bestandteil unseres täglichen Arbeitslebens geworden. Seite an Seite mit Notebooks und Smartphones spielen USB-Sticks eine absolut entscheidende Rolle bei der Realisierung von flexiblen mobilen Arbeitsplätzen. Noch wichtiger ist dabei die Tatsache, dass uns USB-Sticks mobilen Zugriff auf all die sensiblen und großen Dateien geben, die nicht über ein öffentliches Netzwerk bereitgestellt oder heruntergeladen werden können.

Schwerwiegende Datenpannen und Malware Attacken durch unsichere USB-Sticks sind schon in allen Branchen vorgekommen. In Manchester beispielsweise verseuchte ein einzelner USB-Stick mit dem Conficker Virus das ganze IT-System einer Polizeistation, was dazu führte, dass die Dienststelle für mehrere Tage geschlossen werden musste¹. Die Zürich Versicherung wurde in Großbritannien mit einer Strafe von 2,27 Millionen Pfund belegt, weil sie sensible Daten auf mobilen Speichergeräten verloren hat². Ähnliche Fälle gibt es auch in Deutschland, einige davon dokumentiert das Projekt Datenschutz³, viele werden jedoch nie bekannt. Alle diese Vorfälle können jedoch mit hardwareverschlüsselten USB-Flash-Laufwerken verhindert werden.

Wenn Sie sich mit der Anschaffung von hardwareverschlüsselten USB-Sticks befassen, dann

Fragen Sie sich – Wie sicher ist der USB-Stick und wie zukunftssicher meine Investition?

- Welche Verschlüsselungsstärke und Methode (ECB/CBC) verwendet der sichere USB-Stick?
- Erfolgt die Passwortverifizierung auf dem USB-Stick oder lokal auf dem Computer⁴?
- Ist der Hersteller in der Vergangenheit bereits wegen Unlock-Codes oder BackDoors in der Presse aufgefallen⁴?
- Welche Sicherheitsbestimmungen gelten in dem Land des Herstellers?
- Ist der sichere USB-Stick ausreichend gegen Brute-Force Attacken gesichert?

- Gibt es Kompatibilitäts- oder Performanceprobleme?
- Können Sie die Software/Firmware auf den USB-Sticks remote updaten, um auf zukünftige Änderungen reagieren zu können?
- Ist dazu die Interaktion des Anwenders erforderlich oder kann das Update zentral verteilt werden?

SICHERE USB-STICKS SIND ABER NUR EIN TEIL EINER GESAMTLÖSUNG!

Die Auswahl von passenden und sicheren USB-Sticks an sich ist schon eine komplexe Aufgabe, die Evaluierung von entsprechenden Managementlösungen muss aber auch mit Ihren Vorgaben verglichen werden. Unter einer Managementlösung für sichere USB-Sticks verstehen wir eine zentrale Softwarelösung die es Ihnen ermöglicht USB-Sticks einem Anwender zuzuordnen, diese zu konfigurieren und zu verwalten.

Zusätzliche Funktionen, die dem mobilen Anwender noch dazu erweiterten Nutzen bringen, erhöhen die Akzeptanz. Dieses Whitepaper ist eine allgemeine Diskussionsgrundlage über einige der wichtigsten Probleme, bei denen Sie eine USB-Managementlösung unterstützen muss, und stellt gleichzeitig sicher, dass Sie den größten Nutzen aus der Gesamtlösung erhalten.



Ein Device-Management sollte den Wert Ihrer Investition erhöhen

Durch die Ergänzung von Management-Funktionen für sichere USB-Sticks erzielen Sie weitere entscheidende Vorteile, die für jede Organisation auf dem Weg zu mehr USB-Sicherheit extrem wichtig sind. Mit der richtigen Lösung gewinnen Sie die volle Kontrolle und Transparenz über sicherheitsrelevante USB-Stick Aktivitäten, gleichzeitig verbessern Sie durch die Verwaltungs- und Management-Funktionen den Alltagsnutzen Ihrer Investition. Gerade bei den Device-Managementlösungen gibt es gravierende Unterschiede, die Auswahl der falschen Lösung schadet mehr als sie nützt. Hier besteht das Risiko, sich zu sehr auf Einzelheiten zu konzentrieren und dabei das Gesamtkonzept zu vernachlässigen - die falsche Lösung kann im Verwaltungschaos enden und die Produktivität der Anwender stören. Einfach ausgedrückt: Es bedarf einer genauen Überprüfung, um die richtige Wahl zu treffen!

„Verwaltete, sichere USB-Sticks können ein produktives Multifunktions-Tool sein, das die gemeinsame Nutzung, den Transport sowie die Verteilung von Daten und die Zusammenarbeit vereinfacht...“

Verwaltete, sichere USB-Sticks können ein produktives Multifunktions-Tool sein, das die gemeinsame Nutzung, den Transport sowie die Verteilung von Daten und die Zusammenarbeit vereinfacht, zusätzlich wird die Arbeit mit virtuellen Arbeitsumgebungen direkt vom USB-Stick ermöglicht.

Fragen Sie sich – Wie kann ich die USB-Sticks mit dem Server verbinden und unter die Kontrolle des Managementtools bekommen?

- Wie kommen die verwalteten USB-Sticks zum Anwender?
- Ist dieser Prozess flexibel? Können die Sticks auch versandt und von überall aktiviert werden?

- Muss jeder Stick bereits vorab registriert sein?
- Wie können sich Administratoren an der Managementlösung anmelden?
- Müssen neue Benutzerstrukturen angelegt werden, um die Konfiguration einzurichten und Berechtigungen sowohl für Administratoren als auch für User zuzuweisen?
- Kann der USB-Stick einfach mit dem Server verbunden werden, ohne Emails, zusätzliche Codes oder andere Wege, die vom Anwender Interaktion verlangen und ihn ggf. verwirren?
- Wie sicher und einfach kann ein USB-Stick mit dem Server verbunden werden?

Sichere USB-Sticks müssen unter der Kontrolle des Administrators sein

Um ein gewisses Maß an Sicherheit zu erreichen, dürfen administrative Berechtigungen niemals an Anwender übertragen werden. Mit der richtigen USB-Stick-Managementlösung und der richtigen Person in der Rolle des Administrators sind Sie in der Lage, Benutzern den alltäglichen Umgang mit USB-Sticks zu ermöglichen, ohne die Kontrolle darüber zu verlieren. Letztlich muss der Administrator definieren können, welche Dateien auf USB-Sticks gespeichert werden dürfen, welche Applikationen autorisiert sind, benötigte Software installieren und Dateien und Dokumente an ausgewählte USB-Sticks on-demand senden können, auch ohne selbst vor Ort zu sein.

Doch wie sieht häufig die Praxis aus? Unsichere USB-Sticks dürfen unkontrolliert benutzt werden, was Datenpannen und Malware-Attacken zur Folge hat. Viele aktuelle Sicherheitsvorfälle sind genau auf dieses unvorsichtige Handeln zurückzuführen! Jedoch können selbst sichere USB-Flash-Laufwerke von Malware, Phishing und Social Engineering Attacken betroffen sein, wenn der Anwender solchen Gefahren ohne zentrale Unterstützung oder Konfiguration ausgesetzt wird.

Laut Reports führender Antivirensoftware-Herstellern sind genau diese Viren, die speziell für die Verbreitung über USB-Flash Laufwerke entwickelt wurden, bereits zum wiederholten Mal auf Platz 1 der Bedrohungsranglisten zu finden. Wenn Sie also



Anwendern die Admin-Berechtigung entziehen, dann geht die Wahrscheinlichkeit einer Malware-Infektion beinahe gegen Null.

Ein intelligentes USB-Geräte-Management kann also die Produktivität beim Einsatz hardwareverschlüsselter USB-Sticks steigern, ohne die Datensicherheit zu beeinträchtigen, indem es sowohl den kontrollierten Datenaustausch zwischen vertrauenswürdigen als auch unbekannt Systemen erlaubt und damit die Zusammenarbeit dieser beiden an sich unverträglichen Systeme ermöglicht.

„Das zentrale Speichern von Passwörtern, egal in welcher Form, verletzt grundlegende Sicherheitsprinzipien und hebt die hohe Sicherheit von hardwareverschlüsselten USB-Sticks geradezu wieder aus.“

Fragen Sie sich – Wer ist bei Ihnen für USB-Sticks verantwortlich?

- Wie können wir sicherstellen, dass nur vorab autorisierte Software oder erlaubte Dateitypen auf den USB-Sticks unserer Organisation genutzt werden können?
- Sind wir in der Lage, Dokumente und portable Applikationen komplett ohne Interaktion oder Unterstützung des Anwenders auf USB-Sticks zu verteilen?
- Schützt unsere Managementlösung gegen noch unbekannt USB-Viren (Zero-Day-Attacks)?
- Ist es dem Anwender trotz Malware-Schutz möglich, problemlos mit USB-Sticks zu arbeiten?

STELLEN SIE SICHER, DASS PRIVATSPHÄRE UND COMPLIANCE GEWÄHRLEISTET SIND

Eine Organisation sollte bei Bedarf immer die Möglichkeit eines kompletten Compliance-Audits haben, um sicherzustellen, dass die Vorgaben geltender Gesetze (z.B. BDSG) und Regularien erfüllt werden.

Häufig haben zentrale Device-Managementlösungen hier vielfältige Möglichkeiten, die durch unterschiedliche Datenschutzbestimmungen in verschiedenen Ländern (Safe Harbor Abkommen⁵) jedoch auch problematisch sein können. Deshalb ist es wichtig, eine entsprechende Lösung zu wählen, die niemals die Grenzen der Privatsphäre und der Compliance-Vorgaben überschreitet. Wenn sich beispielsweise eine Organisation für den Einsatz von sicheren USB-Sticks entschieden hat, ist es in punkto IT-Sicherheit unerlässlich, dass keine Passwörter von USB-Sticks zentral oder in der Cloud⁶ gespeichert werden und damit rekonstruierbar sind. Das zentrale Speichern von Passwörtern, egal in welcher Form, verletzt grundlegende Sicherheitsprinzipien und hebt die hohe Sicherheit von hardwareverschlüsselten USB-Sticks geradezu wieder aus.

USB-Stick-Managementlösungen sammeln und speichern zur besseren Übersicht im Normalfall sowohl Informationen über die dem Anwender zugeordneten USB-Sticks als auch die damit durchgeführten Aktivitäten. In einigen Organisationen oder Ländern kann dies wichtig sein, in vielen europäischen Ländern verletzt dies jedoch die Privatsphäre und gültige Datenschutzbestimmungen, wenn der Administrator z.B. auf einer Landkarte verfolgen kann, wo ein Anwender mit seinem USB-Stick war oder sich gerade befindet. Deshalb ist es unerlässlich, dass alle oder einzelne Audit-Funktionen in der mit dem Datenschutzbeauftragten vereinbarten Konfiguration auch deaktiviert werden können.

Bei der Entscheidung für eine USB-Stick-Managementlösung ist es notwendig, sowohl die Integrität und Sicherheit der Managementlösung auf dem Server als auch die Kommunikation zwischen Server und USB-Device sicherzustellen. Im besten Fall wird die komplette Kommunikation ausschließlich über private Zertifikate gesteuert; damit werden Lauschangriffe der Kommunikation und Angriffe auf den Server wirkungsvoll verhindert.

Auch sollte sorgfältig geprüft werden, wie neue Systeme und Benutzer eingebunden werden. Wenn Mitarbeiter die Organisation verlassen, wie kann gewährleistet werden, dass diese keine sensiblen Informationen auf geschützten USB-Sticks abrufen oder sich Zugriff auf das Managementsystem



verschaffen können, was ernsthaften Datenverlust bedeuten könnte? Idealerweise werden alle Zugriffsversuche mit Ihrem zentralen Anwenderverzeichnis synchronisiert, so dass dort gesperrte Benutzer auch im USB-Stick-Management blockiert werden.

Fragen Sie sich – Ist die gewählte Managementlösung konform mit internen und externen Sicherheits- und Datenschutzbestimmungen?

- Ist sichergestellt, dass USB-Passwörter niemals zentral gespeichert werden?
- Können einzelne oder alle Audit-Funktionen in der Voreinstellung deaktiviert werden?
- Ist es möglich einzelne Funktionen, die die Privatsphäre der Anwender beeinträchtigen, zu deaktivieren?
- Ist der Datenschutz auch für alle Daten sichergestellt, die auf dem Server gespeichert werden?
- Können eigene Zertifikate zur Kommunikationsverschlüsselung verwendet werden?
- Ist es gewährleistet, dass nicht-autorisierte Personen niemals auf die Server- und Kommunikationsdaten zugreifen können?

„Hier ist die richtige Antwort sicher nicht: Fliegen Sie zurück und wir bekommen das schon wieder hin!“

DAS DEVICE-MANAGEMENT IM ALLTAG

Mit dem richtigen USB-Stick-Management profitieren Sie also von allen Vorteilen der USB-Sticks wie Mobilität und Flexibilität, ohne deren Nachteile in Kauf zu nehmen. Anwender müssen Ihre Aufgaben durchführen können, ohne durch Sicherheitsbestimmungen ausgebremst zu werden.

Deshalb sollten durch eine Managementlösung alle Ansätze genutzt werden, die einen möglichst hohen Grad der Automatisierung und gleichzeitig maximale Transparenz für den Anwender erlauben. Dadurch erleichtern Sie die Akzeptanz bei den Anwendern, die die sicheren USB-Sticks dann als nützliches Tool schnell in Ihrem Arbeitsalltag integrieren.

Ein sicherer USB-Stick ist ein handliches Gerät, das unfreiwillig unter eine tägliche Bewährungsprobe gestellt wird. Es wird fallen gelassen, vergessen, in Hosentaschen mit gewaschen und vielleicht wird auch einmal darauf getreten. Diese externen Einflüsse müssen zusammen mit den internen Sicherheitsrisiken unter einen Hut gebracht werden.

Für letztere muss eine Managementlösung in der Lage sein, vergessene USB-Passwörter ohne Datenverlust wiederherzustellen, die Daten von zuvor verlorenen USB-Sticks wiederherzustellen oder die vorgegebene Passwortstärke und Sicherheitsbestimmungen der Organisation nahtlos auch bei USB-Sticks durchzusetzen.

Hier ist die richtige Antwort sicher nicht: Fliegen Sie zurück und wir bekommen das schon wieder hin!

Da aber USB-Sticks mit dem Anwender unterwegs sind, ist es unbedingt erforderlich, dass diese Aktionen auch remote durch einen Administrator durchgeführt werden können, ohne dass die Sicherheit dabei leidet. Unter diesen Umständen muss der Administrator in der Lage sein, den USB-Stick zurückzusetzen, zu löschen, zu blockieren, USB-Sticks neuen Anwendern zuzuordnen oder den ursprünglichen Datenbestand wiederherzustellen, ohne selbst vor-Ort sein zu müssen - egal wo sich die USB-Sticks gerade befinden!

Ein Beispiel mag dies verdeutlichen: Eine Führungskraft hat sein USB-Passwort vergessen und die wichtige Bilanz-Präsentation, die er auf dem USB-Stick gespeichert hat, soll in wenigen Minuten starten. Hier ist die richtige Antwort des Administrators sicher nicht: Fliegen Sie zurück und wir bekommen das schon wieder hin! Eine Managementlösung sollte in der Lage sein, das Passwort über interne Mechanismen in wenigen Schritten zurückzusetzen, um die Präsentation pünktlich beginnen zu können.

Fragen Sie sich – Ist meine Sicherheitslösung wirklich für die tägliche Praxis entwickelt?

- Wie können wir Anwendern helfen, die Ihr Passwort vergessen haben?
- Funktioniert die Lösung auch im Zusammenhang mit anderen Endpoint-Security-Lösungen?
- Wie kann ein wiedergefundener USB-Stick



ohne Beeinträchtigung des Anwenders wiederhergestellt werden?

- Ist es möglich Backups aller USB-Sticks zu erstellen?
- Ist das Backup automatisiert, transparent und inkrementell?
- Kann durch den Administrator ein Klon eines verlorenen USB-Stick auf einem neuen Stick erstellt werden?
- Ist es möglich eine „Verloren“-Nachricht anzuzeigen, wenn der USB-Stick eines Anwenders als verloren gemeldet wurde und von einem Kollegen gefunden wurde?
- Kann ein Administrator auch dann noch USB-Sticks verwalten oder einem Anwender helfen, wenn er nicht vor-Ort ist?
- Kann er Benutzern dabei helfen, ihr Passwort ohne Datenverlust zurückzusetzen, ohne dabei dessen Passwort zu erfahren oder gar ein Masterpasswort zu besitzen? Letzteres bedeutet ein massives Sicherheitsrisiko für die gesamte Struktur!
- Bietet die Lösung ein sicheres Self-Service Passwort-Rücksetzungsverfahren via Challenge-Response?

„...ein Masterpasswort...bedeutet ein massives Sicherheitsrisiko für die gesamte Struktur!“

LANGFRISTIG AUF SICHERE LÖSUNGEN SETZEN!

USB-Sticks gibt es bereits seit über 10 Jahren! Die Vorteile einer zentralen Verwaltung von sicheren USB-Sticks werden weltweit von den führenden Unternehmen und Organisationen anerkannt. Hardwareverschlüsselte USB-Sticks sind eine bewährte Technologie zum Schutz mobiler Daten, die aufstrebende Branche zeigt ein schnelles Wachstum. Neue technologische Durchbrüche umfassen u.a. virtuelle Desktops oder Funktionen zum Ausbau als 2-Faktor-Authentifizierung. Wie sich gezeigt hat, ist aber dennoch kein Unternehmen vor unvermeidbaren Branchenrisiken geschützt, die sich am Ende ungünstig auf Ihre Investition auswirken könnten.

Fragen Sie sich – Welche technologischen und branchenspezifischen Neuerungen wird es geben?

- Habe ich zur Not Zugriff auf den hinterlegten Quellcode (Escrow⁷)?
- Gibt es eine dokumentierte Geräte-API?
- Gibt es eine dokumentierte Management-API?
- Kann die Software auf dem USB-Stick über eine signierte Update-Funktion aktualisiert werden?

USB-STICK VERWALTUNG KANN AUCH EINFACH UND SCHNELL FUNKTIONIEREN

Es wird immer dringlicher, aktuelle Probleme mit USB-Sticks zu lösen, weg von Datenverlust und Malware-Attacken. Eine zentrale Managementlösung gibt Ihnen die verlorene Kontrolle über mobile Daten auf USB-Sticks zurück und kann ohne viel Aufwand eingeführt werden.

Sichere USB-Sticks setzen sich durch. Sie wurden erfunden um Daten von A nach B zu bewegen. Und zwar sicher!

Die Wahl der richtigen Managementlösung macht die Verwaltung von sicheren USB-Sticks über Internetverbindungen möglich, verknüpft Anwender mit „Ihrem“ USB-Stick und erhöht den Wert Ihrer Investition in diese intelligenten Geräte.

Mit nur einem Klick wird aus einer sicheren Einzelplatzlösung für USB-Sticks eine unternehmensweit einsetzbare Security-Lösung mit vielen Vorteilen, die die Einhaltung aktueller und zukünftiger Sicherheitsbestimmungen garantiert und dabei den Aufwand für Administratoren, Helpdesk-Mitarbeiter und Anwender minimiert.

Anders Pettersson

Chief Security Officer, BlockMaster AB



QUELLENANGABEN

- 1) <http://www.scmagazineuk.com/greater-manchester-police-hit-by-conficker-from-infected-usb-that-leaves-it-unconnected-from-its-network-for-three-days/article/162904/>
- 2) <http://www.scmagazineuk.com/zurich-insurances-fsa-fine-should-act-as-a-warning-on-the-importance-of-protecting-sensitive-information/article/177482/>
- 3) <http://www.projekt-datenschutz.de/>
- 4) http://www.sys.de/fileadmin/ressources/040_veroeffentlichungen/dokumente/SySS_knackt_SanDisk_USB-Stick.pdf
- 5) http://de.wikipedia.org/wiki/Safe_Harbor
- 6) <http://blog.zeit.de/kulturkampf/2010/08/24/wenn-daten-in-der-cloud-verschwinden>
- 7) <http://de.wikipedia.org/wiki/Escrow>

WWW.SAFECONSOLE.COM

WWW.SAFESTICK.DE

UNITED KINGDOM
+44 (0)2033 554 188

sales@blockmastersecurity.com

UNITED STATES
1 - 888 - 432 - 4957

sales@blockmastersecurity.com

MAIN OFFICE (SWEDEN)
+46 (0)46 - 276 51 00

sales@blockmaster.se

VERTRIEBSPARTNER IN DEUTSCHLAND
ProSoft Software Vertriebs GmbH
Bürgermeister-Graf-Ring 10, 82538 Geretsried

+49 (0) 8171/405-0 | www.prosoft.de