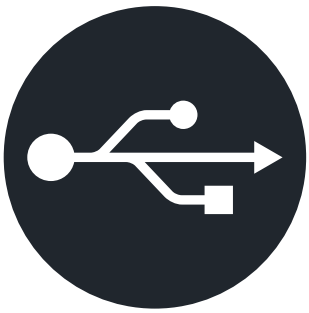
So erlauben Sie den Zugriff von USB-Sticks

ohne Beeinträchtigung der Endpoint Security

#KingstonIsWithYou #KingstonIronkey

Einführung

Im Januar 1996 läutete die offizielle USB 1.0-Spezifikation bei ihrer Veröffentlichung eine neue Ära der Einheitlichkeit, des Komforts und der Vielseitigkeit für Anbieter von Peripheriegeräten und Endbenutzer ein. 27 Jahre später wird die Abwärtskompatibilität mit jeder Revision beibehalten, und USB ist nach wie vor ein Eckpfeiler der Computer-Hardware-Schnittstelle von Servern bis zu Smartphones.



Die Einfachheit von USB durch Plug-and-Play und die immer höheren Geschwindigkeiten haben dazu geführt, dass sich der tragbare USB-Speicher zu einem der großen Gewinner entwickelt hat. Doch dieser Komfort hat einen Nachteil, wenn es um die Datensicherheit geht. In der heutigen Welt, ohne den Einsatz geeigneter Instrumente wie Endpoint Protection auf Host-Computern und ordnungsgemäße Datensicherheitspraktiken, setzen Benutzer im unvorsichtigem Umgang mit tragbaren USB-Sticks sich selbst und andere möglichen Datenverletzungen aus, die für den Endbenutzer kostspielig sein und sogar eine ganze Organisation oder Regierung gefährden können.

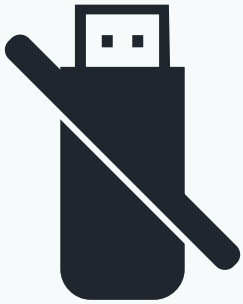
Zusätzlich zum Schutz der Host-Umgebung sollte der USB-Stick mit einem Passwortschutz und einer geräteinternen Hardware-Verschlüsselung gesichert werden. Dies bietet den robustesten Schutz gegen ungewollte Zugriffe. Wir werden einige bewährte Praktiken zur sicheren Verwendung von USB-Sticks durchgehen sowie einen tieferen Einblick in USB-Sticks im Allgemeinen geben.

Während ein kombinierter Ansatz ideal ist, sind die Robustheit der Verschlüsselung und die Hardwarekomponenten des USB-Sticks selbst von größter Bedeutung. Davon profitieren Branchen wie das Finanzwesen über das Gesundheitswesen bis hin zur Fertigung und dem Militär. Sie spielen auch eine Rolle bei der Fernarbeit, wenn der Netzwerkzugang entweder nicht verfügbar, anfällig oder unpraktisch ist.

Hardwareverschlüsselte USB-Sticks sind mit unterschiedlichen Zertifizierungseinstufungen erhältlich und bieten gleichzeitig eine Reihe von Sicherheitsfunktionen. Durch die Untersuchung ihrer Eigenschaften und Anpassungsmöglichkeiten wird auch ihre Eignung als Einzellösung verdeutlicht, indem sie ihren Platz in allen möglichen sensiblen Umgebungen sichern.

Port-Administration: USB-Stick trifft auf Endpoint Management Software zum Schutz vor Datenverlust

Seit Jahrzehnten bieten Antiviren- und Anti-Malware-Anwendungen Schutz auf der grundlegendsten Ebene. Sie scannen automatisch Downloads und angeschlossene Geräte und melden oder reagieren auf verdächtige Inhalte. Der Schutz durch NGAV-Software, Antivirenschutz der nächsten Generation, geht noch einen Schritt weiter. Anstatt sich ausschließlich auf eine ständig aktualisierte Datenbank mit Virensignaturen zu verlassen, fügt NGAV Funktionen für maschinelles Lernen und Verhaltenserkennung hinzu, die unbekannte Bedrohungen identifizieren und abwehren können.



Dies ist jedoch nicht die einzige Waffe in der Waffenkammer, und für diejenigen, die einen kugelsicheren Schutz von Benutzerperipheriegeräten und mehr wünschen, bietet die Endpoint Management Software zur Verhinderung von Datenverlusten (DLP) die Mittel, um jede Art von Zugriff auf USB-Ports und andere Zugangspunkte zu verweigern.

Die Vorgehensweise alle Ports zur Sicherheit zu blockieren kann gewiss Risiken beseitigen und ist unter bestimmten Umständen auch wünschenswert, aber eine solche Politik kann sich oft als sehr stumpfes Instrument mit unerwünschten Folgen erweisen.

Dennoch ziehen es einige IT-Administratoren vor, Anfragen zum Öffnen von USB-Ports auf Benutzerrechnern abzulehnen, da dies auf diesen Endgeräten einen direkten Zugriff durch die Firewall des Unternehmens ermöglichen würde. Solche Vorsicht ist verständlich, aber wenn es um die Freigabe des Zugriffs für USB-Sticks geht, muss die Bereitstellung dieser Berechtigung kein massives Sicherheitsproblem darstellen, wenn bestimmte Voraussetzungen beachtet werden.

Eine wesentliche Anforderung ist eine Endpoint Management Suite, die sowohl Scans zur Erkennung von Bedrohungen durch Antiviren-/Antimalware-Lösungen als auch eine zentrale Überwachung und Verwaltung aller Benutzerendpunkte bietet.

In der Regel findet sich dieser einfache Ansatz in verschiedenen Ausprägungen in vereinheitlichten Lösungen bekannter Hersteller wie McAfee MVision, Sophos Intercept X, Symantec Endpoint Security, Trend Micro Smart Protection und WinMagic SecureDoc, um nur einige zu nennen.

Verfeinerungen im Whitelisting

Wenn es um die Absicherung von USB-Sticks geht, hängt die eingesetzte Methode vom erforderlichen Schutzgrad ab. Ein einfacher, aber effektiver Ansatz ist das Whitelisting von USB-Sticks unter Verwendung ihrer jeweiligen VID- (Vendor Identifier) und PID-Werte (Product Identifier). Eine Sache bei allen USB-Peripheriegeräten ist, dass die Hersteller jeweils eine eindeutige VID haben, aber die PID ändert sich bei jedem auf den Markt gebrachten neuen Produkt.

Für das Whitelisting wäre die Verwendung der VID eines Herstellers allein für eine Absicherung zu weit gefasst, da jedes USB-Gerät, das dieser Hersteller jemals produziert hat, zugelassen wäre. Die PID bietet mehr Feineinstellmöglichkeiten und verlangt, dass nur einem bestimmten Modell der Zugriff auf das Host-System gewährt wird.

Dies ist zwar eine Verbesserung, aber immer noch nicht ideal. USB-Sticks erfreuen sich großer Beliebtheit, da Anwender eigene Geräte erwerben können, die den zugelassenen Modellen entsprechen. Unter Berücksichtigung dieser Aspekte bietet Kingston Technology eine maßgeschneiderte Lösung, um die Sicherheit von USB-Sticks zu erhöhen.

Über das Personalisierungsprogramm können unternehmensspezifische PID-Profile erstellt und auf eine Reihe von verschlüsselten USB-Sticks von Kingston angewendet werden. Unternehmen, die Geräte mit einer maßgeschneiderten Produktkennung einsetzen, profitieren nicht nur von einem vereinfachten Whitelisting, sondern auch von einer deutlich erhöhten Sicherheit. Ohne passende benutzerdefinierte PID wird selbst scheinbar identischen Geräten, die von Mitarbeitern unabhängig vom Unternehmen gekauft wurden, der Zugriff verweigert.

Während die Verwendung von benutzerdefinierten PIDs es IT-Administratoren ermöglicht, neue USB-Sticks schnell und

einfach in Betrieb zu nehmen, ist eine granularere Alternative die Verwendung von individuellen Geräteseriennummern, die auf den meisten verschlüsselten USB-Sticks von Kingston zu finden sind. Diese Anordnung erfordert, dass jede eindeutige Geräteseriennummer bei der Endpoint Management Suite registriert wird. Zunächst wird dies von den IT-Mitarbeitern bearbeitet. Kingston kann bei jeder Bestellung eine Liste mit Seriennummern zur Verfügung stellen, diese sind immer alphanumerisch und nicht fortlaufend. Die Wahl dieser Methode ermöglicht weitaus flexiblere Richtlinien, die auf dem Eigentum des einzelnen Laufwerks basieren, mit dem Bonus einer präzisen Rückverfolgung der Herkunft der Geräte, was in forensischen IT-Szenarien von unschätzbarem Wert sein kann. Einige Kingston Sticks verfügen über eine Seriennummer und einen Barcode auf dem Gehäuse für die elektronische Abtastung. Andere Sticks lassen sich so anpassen, dass sie einen Barcode und eine Seriennummer auf dem Gehäuse für Unternehmen enthalten. Diese Elemente können zur Verfolgung von USB-Sticks verwendet werden.

Standardmäßig bieten Endpoint Management Systeme Zugriff auf VID/PID für Portsperrung und Whitelisting. Was Kingston anbietet, ist ein vielseitigerer Weg bei der Nutzung dieser Funktionen, der kulantere und einfallsreichere Richtlinien ermöglicht, die wiederum die Nutzung von USB-Sticks erleichtern. Durch die Festlegung einer geeigneten Identifizierungsmethode ist eine pauschale 'Blockierung aller Ports nicht nur zu simpel, sondern auch unnötig.

Sichere, konforme Lösungen für Fernanwender

Wenn es um Sicherheit geht, ist das Whitelisting von Geräten nur die Hälfte des Problems, oder anders ausgedrückt, die Hälfte der Lösung.

Die Bequemlichkeit und Einfachheit von USB-Sticks macht sie in vielen Unternehmen und Institutionen unentbehrlich, wo Portabilität der Schlüssel zu reibungslosen Datentransfers ist. In den meisten Umgebungen ist es aus Gründen der Compliance und guter IT-Hygiene notwendig, die Mitarbeiter für solche Aufgaben mit verschlüsselten USB-Sticks auszustatten. Durch die Verwendung einer Kombination aus Passwortschutz und Geräteverschlüsselung wird der tragbare Speicher mit Sicherheitsvorkehrungen versehen, die den Zugriff auf sensible Daten verhindern, falls ein Gerät verloren geht, gestohlen wird oder in einer potenziell gefährdeten Situation zurückgelassen wird.

Es handelt sich nicht um eine Einheitslösung, da die Verschlüsselungstechniken variieren und die größten Unterschiede beim Vergleich von Software- und Hardware-Verschlüsselungslösungen zu Tage treten. Was ist also besser? Es hängt von Ihren Bedürfnissen ab, aber eine grundlegendere Frage wäre: „Was ist sicherer?"

Die Software-Verschlüsselung ist im Wesentlichen eine preisgünstige Wahl, die für einige Branchen mit kleineren Betrieben zufriedenstellend sein wird. Sie würde auch zu Unternehmen passen, deren Datentransfers nicht als sensibel gelten und deren Bedenken eher mit der Einhaltung von Richtlinien zu tun haben.

Der Modus Operandi der Software-Verschlüsselung ist jedoch auch ihre Achillesferse, da sie Client-Anwendungen erfordert, die sich auf einen Computer verlassen, um dort die Verschlüsselungsaufgaben zu erfüllen. Daher ist ein softwareverschlüsseltes Speichergerät nur so sicher wie der Host-Computer.

Die Anfälligkeit für Exploits wird ebenfalls erhöht, da Hacker mit Zugriff auf den Speicher des Computers die Verschlüsselungs-/Entschlüsselungsschlüssel „erschnüffeln" können. Die Daten auf dem Laufwerk können auch Brute-Force-Angriffen ausgesetzt sein, da der Passwort-Zugriffsschutz nicht benötigt wird, wenn auf die verschlüsselten Dateien zugegriffen und diese kopiert werden können.

Denken Sie daran, dass softwarebasierte Verschlüsselung wahrscheinlich von Zeit zu Zeit Software-Updates benötigt, was deren Implementierung durch die zusätzliche Belastung des IT-Personals erschweren kann. Das Schlimmste aber ist, dass die Softwareverschlüsselung von frustrierten Mitarbeitern, die Probleme mit der plattformübergreifenden Portabilität des Laufwerks haben, komplett entfernt werden kann. Benutzer des Laufwerks können die Daten des verschlüsselten Laufwerks auf einen Computer kopieren, das Laufwerk als ein unverschlüsseltes Laufwerk neu formatieren und dann die Daten erneut auf das Laufwerk kopieren. Dann wären die Daten ungesichert und völlig anfällig für einen Angriff. Aus Gründen der Einhaltung von Datenschutzgesetzen und -vorschriften ist dies nicht akzeptabel, da die Sicherheit des USB-Sticks effektiv deaktiviert werden kann.

On-Chip-Verschlüsselung: die harte und schnelle Lösung

Im Gegensatz dazu funktioniert ein hardwareverschlüsselter USB-Stick unabhängig vom Computer, da er über einen speziellen Prozessor verfügt, der in das eigentliche Laufwerk integriert ist und die Verschlüsselung verwaltet. Er verfügt über einen immer aktiven Verschlüsselungsprozess mit Schutz gegen Brute-Force-Passwortangriffe. Die verschlüsselte Daten sind nicht zugänglich und können nicht kopiert werden.

Kingstons hardwareverschlüsselte USB-Sticks für Unternehmen und das Militär nutzen eine AES 256-Bit-Verschlüsselung im XTS-Modus. Die weltweit anerkannte Verschlüsselungstechnik AES 256-Bit bietet strenge Datensicherheiten. Durch die Verwendung von zwei separaten Schlüsseln in verschiedenen Phasen des Verschlüsselungs-/Entschlüsselungsprozesses hat der XTS-Modus einen ähnlichen Effekt wie die doppelte Verschlüsselung der Daten.

Im Einsatz wird der Chiffrierschlüssel aus dem Zufallszahlengenerator des Stick-Controllers abgerufen, den das Passwort des Benutzers freischaltet. Da die Authentifizierung innerhalb der Krypto-Hardware des Geräts stattfindet, sind Verschlüsselungsschlüssel und andere kritische Sicherheitsfunktionen gegen gängige Exploits wie BadUSB, Cold-Boot-Angriffe, bösartigen Code und Brute-Force-Angriffe geschützt.

Einer der unmittelbarsten Vorteile der Hardware-Verschlüsselung ist, dass die Leistung des Laufwerks deutlich besser ist als bei einem softwareverschlüsselten Laufwerk, da die Verschlüsselungsaufgaben nicht auf den Host-Computer ausgelagert werden. Alles findet innerhalb des Sticks statt.

Hardwareverschlüsselte USB-Sticks wie der Kingston IronKey D500S sind passwortgeschützte Geräte, die bereits im Auslieferungszustand verschlüsselt sind. Bei der Verwendung ist zunächst nur das schreibgeschützte Start-Laufwerk sichtbar, da dieses die Anwendung enthält, die zur Authentifizierung des Passworts und zum Entsperren des verschlüsselten Hauptspeicher-Laufwerks verwendet wird. Mit diesem Verfahren wird die Installation aller Arten von Treibern oder Software auf dem Host-PC vermieden.

Darüber hinaus verfügen Kingstons hardwareverschlüsselte USB-Sticks über digital signierte Firmware, die jegliche Manipulation der Firmware im Gerät verhindern. Diese zusätzliche Sicherheitsebene bietet Schutz vor Angriffen wie BadUSB, die eine inhärente Schwachstelle in der Firmware von USB-Geräten ausnutzen. Diese Schwachstelle kann dazu führen, dass verdeckt ausgeführte Befehle oder bösartiger Code auf dem Host-Computer ausgeführt werden.

Natürlich würde der Ansatz, einfach alle Ports zu blockieren das Risiko von BadUSB-Exploits einschränken, aber warum sollte man die Produktivität mit solch veralteten Praktiken opfern? Wie oben hervorgehoben, kann eine sichere Umgebung in Verbindung mit der Verwendung von tragbaren Speichergeräten aufrechterhalten werden, wenn einfache Beschaffungs- und Bereitstellungsverfahren zur Einführung von hardwareverschlüsselten USB-Sticks vorhanden sind.

Sicheres und vorschriftenkonformes Arbeiten aus der Ferne

Für Remote-Mitarbeiter erfordert die Arbeit, z. B. im Home-Office, also nicht in der sicheren Umgebung eines Unternehmens, eine überarbeitete Strategie und einen neuen Blick auf die Prioritäten.

Wenn es um einen Remote-Sicherheitsplan geht, ist es dann sinnvoll, die USB-Anschlüsse am Laptop Ihres Mitarbeiters zu sperren, nur damit dieser über das Internet auf einen Server zugreifen kann, um Dokumente hochzuladen oder abzurufen? Unterwegs kann eine offene Internetverbindung, wie z. B. ein unsicherer oder nicht vertrauenswürdiger WLAN-Zugangspunkt, alles sein, was zur Verfügung steht, und dies führt zu einer Vielzahl von Gefahren, die die Möglichkeit eines Angriffs oder Datenverlusts stark erhöhen. Bedrohungen wie das Abfangen

und Überwachen von Daten durch Spoofing, Man-In-the-Middle (MitM)-Angriffe und das Abhören von Netzwerken sind nur einige der immer ausgefeilteren Hacking-Methoden, die Cyberkriminellen zur Verfügung stehen. Sogar VPNs wurden kompromittiert.

Die Netzwerkverbindung eines Unternehmens mit dem Internet ist nur ein weiterer Endpunkt, der durch seine inhärente Gefährdung einen extrem anfälligen und häufig genutzten Einstiegspunkt darstellt. Die Öffnung für den Fernzugriff birgt eigene Sicherheitsrisiken, insbesondere wenn es um sensible Daten geht.

Wenn Sie Ihren Außendienstmitarbeitern oder Mitarbeitern im Home-Office passwortgeschützte und hardwareverschlüsselte USB-Sticks anvertrauen, werden potenzielle Schwachstellen im Netzwerk effektiv beseitigt. Um solche Vorkehrungen zu treffen, muss man jedoch die verfügbaren USB-Sticks genauer unter die Lupe nehmen und prüfen, wie sie den Anforderungen der jeweiligen Remote-Arbeitsumgebung gerecht werden. Dabei geht es nicht einfach darum, eine Entscheidung über die Kapazität des Laufwerks zu treffen oder ob die Seriennummer protokolliert werden soll. Dies betrifft die physikalische Konstruktion des Gerätes selbst.

Manipulationssichere Schutzvorrichtungen: Die soliden Optionen

Die Hauptfrage ist hier, ob ein hardwareverschlüsselter USB-Stick manipulationssicher ist oder nicht. Wie sicher ein Gerät gegen solche Angriffe ist, spiegelt sich in Standards wie FIPS 140-3 wider, der über mehrere Klassen verfügt, die die Widerstandsfähigkeit der physikalischen Konstruktion eines Laufwerks ohne kryptografische Methoden prüfen.

Die zugehörige FIPS-197-Zertifizierung bezieht sich nur auf die Hardware-Verschlüsselungsattribute und Geräte wie die Baureihe Kingston IronKey Vault Privacy 50 und Vault Privacy 80 Externe SSD, bei denen es sich um unternehmensorientierte Modelle handelt, die keine Anforderungen an die Datensicherheit auf Militärstandard erfüllen müssen. Diese Sticks sind preiswerter, haben aber keinen Schutz gegen Manipulationen am Stick selbst.

Mit der FIPS 140-3 Level 3-Zertifizierung (ausstehend) werden die eingesetzten Methoden zur Aufdeckung von Gerätemanipulationen als Militärstandard eingestuft. Kingston liefert diese FIPS 140-3 Level 3 Sticks an Unternehmen, Regierungen und das Militär auf der ganzen Welt.

Die Verwendung von Epoxidharz zur internen Beschichtung aller für die Sicherheit erforderlichen Schaltkreise im Stick und das Verkleben der internen Komponenten mit dem Gehäuse schaffen einen weiteren Schutzwall. Jeder Versuch, das Metallgehäuse zu öffnen, wäre extrem schwierig und würde dazu führen, dass die internen Chips und andere Komponenten zerstört werden und der Stick schließlich nicht mehr funktionsfähig ist. Mit diesem harten und undurchsichtigen Epoxidharz wird die Manipulation wichtiger Komponenten nahezu unmöglich. Geräte wie der Kingston IronKey D500S und S1000 enthalten diese zusätzliche Sicherheitsmaßnahme.

Dieser Geräteschutz beschränkt sich nicht nur auf physikalische Maßnahmen. Der Kingston IronKey S1000 erhöht den Manipulationsschutz um eine weitere Ebene. Der interne Kryptochip des IronKey S1000 kann jede physische Manipulation erkennen und macht das Laufwerk unbrauchbar, sobald das Gerät eingeschaltet wird. Der Einsatz von hardwareverschlüsselten USB-Speichergeräten für den Zugriff auf und die Übertragung von sensiblen Dateien ist ein pragmatischer Schritt, der reibungslose Remote-Vorgänge ermöglicht und die Sicherheit außerhalb des Unternehmens effektiv gewährleistet.

Stellen Sie sicher, dass Sie die Hardware und die Sicherheitsfunktionen des USB-Sticks recherchieren, um zu sehen, ob es für Ihre speziellen Anforderungen und Ihren Anwendungsfall geeignet ist. Jeder USB-Stick sollte von Fall zu Fall geprüft werden, wobei vertrauenswürdige Akkreditierungen bei diesen Entscheidungen helfen können. Unabhängig von den Prioritäten bietet Kingston eine Reihe von hardwareverschlüsselten USB-Sticklösungen und Personalisierungsoptionen zu erschwinglichen Preisen, die alle Arten von Umgebungen abdecken: von allgemeiner Compliance bis hin zu den härtesten militärischen Spezifikationen.

Sicherheit an erster Stelle: Keine Netzwerke, keine Probleme

Heutzutage kennt das Büro keine Grenzen mehr, und da die Arbeit von zu Hause aus immer mehr zunimmt, rückt die Problematik des Fernzugriffs für viele Unternehmen in den Mittelpunkt. Viele sehen sich zum ersten Mal mit diesen Herausforderungen konfrontiert und suchen nach sicheren Wegen, um diesem wachsenden Trend gerecht zu werden.

Um diese Anforderungen in einer Vielzahl von Branchen zu erfüllen, sind hardwareverschlüsselte USB-Speichergeräte bereits gut etabliert und bieten eine sichere Lösung, wenn die Übertragung von Daten über Netzwerke aus verschiedenen Gründen unpraktisch oder unerwünscht ist.

Im Finanzbereich fordern die Aufsichtsbehörden häufig Daten an, um das Verhalten und die Compliance eines Unternehmens zu überprüfen. Das Risiko einer Exposition ist viel zu groß, als dass man in Erwägung ziehen könnte, ein Netzwerk für die Übertragung sensibler Dokumente zu nutzen, die genaue Details zu Investitionen, Börsenhandel und anderen vertraulichen Bankaktivitäten enthalten. Die einfache und effektive Lösung besteht darin, diese Informationen auf einem hardwareverschlüsselten USB-Stick bereitzustellen.

Die Verwendung von sicheren USB-Sticks zur Übertragung von Dateien im Gesundheitswesen ist an der Tagesordnung. Dies dient auch der Bequemlichkeit von Ärzten oder Fachärzten, die Akten analysieren, zu Forschungszwecken heranziehen oder Medizinstudenten Fallbeispiele präsentieren möchten. Es gibt auch praktischere Anforderungen, wenn es um proprietäre Systeme geht, wie z. B. medizinische Bildgebungsgeräte, bei denen der Netzwerkzugang nicht vorhanden oder unsicher ist. Durch die Verwendung von konformen, hardwareverschlüsselten USB-Sticks können Dateien einfach zur Verwendung an anderer Stelle übertragen werden.

Was man tun und nicht tun sollte

✓ **Verwenden Sie konforme, sichere Sticks** und überprüfen Sie die Spezifikationen, damit Sticks beschafft werden, die den Anforderungen des jeweiligen Einsatzes entsprechen.

✗ **Autorisieren Sie keine willkürliche oder persönliche BYOD-Richtlinie (Bring Your Own Device) für ein Unternehmen,** denn der Verlust unverschlüsselter Sticks ein zu hoher Preis in Form von finanziellen Verlusten und Reputationsschäden.

✓ **Setzen Sie eine Endpunkt-Managementsuite** ein und verwenden Sie hardwareverschlüsselte USB-Sticks, die spezielle Whitelisting-Funktionen bieten.

✗ **Überlassen Sie nichts dem Zufall.** Anforderungen für Vor-Ort- und Remote-Arbeitsumgebungen richtig einschätzen.

✓ **Schulen Sie die Mitarbeiter** in Sicherheitsfragen. Es liegt in ihrem eigenen Interesse, dass das Unternehmen vor Sicherheitsverletzungen geschützt bleibt.

✗ **Gestalten Sie die Sicherheit nicht so schwierig,** dass Anwender nach Wegen für deren Umgehung suchen, die dazu führen könnten, dass inoffizielle IT-Lösungen genutzt werden. Nur weil eine pauschale Richtlinie schon immer angewendet wurde, bedeutet das nicht, dass sie für alle Szenarien geeignet ist. Der Arbeitsplatz verändert sich und durch die Wahl der richtigen Lösungen können neue Richtlinien entwickelt und durchgesetzt werden.

In diesem Szenario spielt der Kingston IronKey Keypad 200 (KP200) seine Stärken aus. Da es sich um ein betriebssystemunabhängiges Laufwerk handelt, gibt es kein Start-Laufwerk zur Eingabe des Passworts, sondern eine alphanumerische Tastatur, mit der das Gerät für die Verwendung auf jeder Plattform entsperrt wird. Wie ein Schweizer Taschenmesser erstreckt sich der Einsatz von hardwareverschlüsselten USB-Sticks auf die Fertigung; die sichere Übertragung von Anwendungen, die in der IT-Forschungs- und Entwicklungswelt erstellt wurden, sowie auf Maschinen, die von Plattformen der Betriebstechnologie (OT) gesteuert werden. Für den Betrieb auf gemischten Plattformen, bei denen auch Linux zum Einsatz kommt, stellt der KP200 eine der einfachsten und sichersten Lösungen dar.

Hardwareverschlüsselte USB-Speichergeräte spielen auch in der Strafverfolgung eine wichtige Rolle. Sie schützen und übertragen Falldateien, Bilder und andere Beweismittel sicher an Außendienstmitarbeiter, Ermittlungsgruppen und forensische Teams. Kingston bietet einen zusätzlichen Vorteil, da es Sticks mit der internen Seriennummer liefern kann, die neben einem Barcode auf das äußere Gehäuse gedruckt ist. Das Ausgeben und Katalogisieren von Sticks wird einfach und leicht nachvollziehbar. Es ist so einfach wie das manuelle Erfassen einer Seriennummer oder so schnell wie das Scannen eines Barcodes. Das Auditing und Bestandsmanagement könnten nicht einfacher sein. Diese Funktion ist standardmäßig in den Kingston IronKey-Sticks D500S, D500SM und S1000B/E enthalten, ist aber auch für andere hardwareverschlüsselte Modelle im Rahmen des Kingston Personalisierungsprogramms verfügbar.

Sicherheit und Speichermobilität: Der Stand der Technik

Passwortschutz, Hardware-Verschlüsselung, manipulationssichere Schutzmechanismen, granulare Endpunkt-Whitelists, militärische FIPS 140-3 Level 3-Zertifizierung (ausstehend) und At-a-Glance-Protokollierung sind Standardfunktionen von Kingston USB-Sticks, die ohne jegliche Verzögerung eingesetzt werden können.

Diese robusten Sicherheitsvorkehrungen gewährleisten, dass der USB-Stick und seine Daten in der Host-Umgebung sicher bleiben. Obwohl die Spezifikationen auf dem Papier beeindruckend sind, wird die zufällige Auswahl eines Modells ohne jegliche Recherche nicht unbedingt die ideale Lösung für einige Organisationen mit anspruchsvolleren Anforderungen ergeben.

Als unabhängiger Hersteller bietet Kingston eine breite Palette von Optionen, um die Bedürfnisse der Kunden zu erfüllen. Durch das Kingston Personalisierungsprogramm sind fortschrittliche Lösungen verfügbar, die eine nahtlose Benutzererfahrung ermöglichen.

Die sichere Personalisierung geht darüber hinaus, einer Organisation eine eigene USB-PID für das Whitelisting zur Verfügung zu stellen. Das Sicherheitsprofil der Launcher-Anwendung kann ebenfalls mit fünfzehn verschiedenen Einstellungen angepasst werden, von Kontakt- und Firmendaten bis hin zur Aktivierung von Passwort-Hinweisen und der Festlegung der maximalen Anzahl von Passwortversuchen. Äußerlich ist ein Firmenbranding (Co-Logo) sowie eine Farbpalette für bestimmte Sticks möglich. Bei einer Mindestbestellmenge von fünfzig Sticks bieten all diese Funktionen einen mühelosen Integrationspfad für den Geräteeinsatz.

Wenn noch keine Endpunkt-Managementanwendung, die für sichere USB-Speicher geeignet ist, vorhanden ist, gibt es eine Managementlösung für Unternehmen, die ihre Flotte von Kingston-Sticks verwalten möchten, einschließlich der Option, Passwörter aus der Ferne zurückzusetzen.

Die Allgegenwärtigkeit und Bequemlichkeit von USB-Sticks hat dazu geführt, dass es eine Reihe von vielversprechenden Technologien überlebt hat und für viele Aufgaben bleibt die Unmittelbarkeit und Bequemlichkeit von USB-Speichern bestehen. Leicht verfügbar und immer sicher, bieten geschützte USB-Sticks eine einfache Lösung, die man schnell zu schätzen weiß.

Warum sollte man sich Sorgen um Netzwerkdatenverletzungen in Remote-Umgebungen machen? Mit den hardwareverschlüsselten Kingston IronKey USB-Speichergeräten liegt die Antwort in Ihrer Hand.

Wenn Sie mehr darüber erfahren möchten, wie Kingston Ihnen helfen kann, besuchen Sie kingston.com/ironkey. Bei speziellen Fragen wenden Sie sich bitte an einen unserer Experten für verschlüsselte USB-Sticks.

#KingstonIsWithYou #KingstonIronkey