
Kingston
TECHNOLOGY
Warum sind USB-Sticks heute noch relevant?
#KingstonIsWithYou

Warum sind USB-Sticks heute noch relevant?

Vorwort und Inhalt

Im heutigen digitalen Zeitalter, in dem 60 % aller globalen Unternehmensdaten in der Cloud[1] gespeichert werden, mag die Diskussion über die Relevanz einer fast dreißig Jahre alten Speichertechnologie etwas seltsam erscheinen. Seit ihrer Einführung hat sich diese Speicherform jedoch weiterentwickelt und wird es auch weiterhin tun.

Die Zeiten, in denen USB-Sticks lediglich für den Zugriff auf Dateien, Laufwerke und Anwendungen dienten, sind längst vorbei. Die heutigen Lösungen zeichnen sich nicht nur durch eine erheblich verbesserte Übertragungsgeschwindigkeit aus, sondern bieten auch zuverlässige und sichere tragbare Datenträger, die in vielen Situationen unerlässlich sind. Aber warum sind USB-Sticks immer noch relevant, wenn Cloud-Speicherlösungen scheinbar viele der gleichen Vorteile bieten können?

In diesem eBook erörtern wir, wo USB-Sticks inmitten einer von der Cloud dominierten Landschaft hingehören. Unterstützt von wichtigen Erkenntnissen einiger führender Branchenexperten werden wir untersuchen, wie Unternehmen heute USB-Sticks einsetzen, und ihren Stellenwert in Bezug auf softwarebasierte Verschlüsselung, unabhängige Speicherumgebungen und Datensicherheit an Endgeräten diskutieren.

Inhaltsverzeichnis	Seiten

Mitwirkende

Dieses eBook wurde von drei Branchenexperten für IT und neue Technologien geschrieben.

Rafael Bloom

Rafael Bloom hat in leitenden Positionen in den Bereichen Technologieprodukte, Marketingkommunikation und Geschäftsentwicklung Karriere gemacht. Seine Beratungspraxis konzentriert sich auf die neuen organisatorischen, produktbezogenen und kommunikativen Herausforderungen. Dieser sehr vielseitige Arbeitsbereich umfasst Fachwissen über Information Governance und Compliance by Design, Datenschutz und aufkommende Technologien, wie z. B. AdTech, Mobile & 5G, KI und maschinelles Lernen.

Tomasz Surdyk

Mit über 24 Jahren Erfahrung in der IT-Sicherheit in Regierungen ist Tomasz Surdyk eine führende Persönlichkeit, wenn es um Informationssicherheit, personenbezogene Daten und Cybersicherheit geht. In seiner Vergangenheit hat er IKT-Systeme und Netzwerke überprüft, die Verschlusssachen und personenbezogene Daten in Regierungsbehörden sowie bei der NATO und der EU verarbeiten. Seit mehreren Jahren ist er Inhaber eines Unternehmens, das sich auf die Implementierung von Sicherheitslösungen spezialisiert hat, die die Sicherheit von Geschäftsinformationen und personenbezogenen Daten erhöhen.

David Clarke

David gilt als einer der Top-10-Influencer nach Thompson Reuter's „Top 30 most influential thought-leaders and thinkers on social media, in risk management, compliance and reg-tech in the UK" (die Top 30 der einflussreichsten Vordenker und Denker im Bereich Social Media, Risikomanagement, Compliance und Reg-Tech in Großbritannien) und zählt zu den Top 50 der Global Experts von Kingston Technology. In der Vergangenheit hatte David mehrere Positionen im Sicherheitsmanagement inne, wie Globaler Leiter der Bereitstellung von Sicherheitsdiensten und Leiter der Sicherheitsinfrastruktur für globale FTSE 100 Unternehmen.

Der Aufstieg des USB-Sticks

Als vor über zwanzig Jahren der erste USB-Stick (Universal Serial Bus) auf den Markt kam, bedeutete seine umfassende Kompatibilität einen Umbruch in der Computertechnologie. Mit der Möglichkeit, die Nutzung mehrerer Geräte für die breite Masse zugänglich zu machen, entwickelte sich der Universal Serial Bus bald weiter und bot mit der Veröffentlichung des ersten USB-Sticks im Jahr 2000 eine deutlich schnellere Datenübertragung, einen USB 3.0-Anschluss und noch größere Möglichkeiten.

Seitdem hat sich die Technologie im Hinblick auf die mobile Datenspeicherung und die Sicherheitsanforderungen stark weiterentwickelt. Der Schwerpunkt liegt auf der heutigen Generation von USB-Sticks, die für ganz bestimmte Anwendungsfälle konzipiert sind. Aus Unternehmenssicht führen die zunehmende Fern- und Hybridarbeit, die Nutzung von Cloud-Diensten und Bedenken hinsichtlich der Cybersicherheit zu einem Bedarf an effektiveren Lösungen. Außerdem müssen die Daten aufgrund gesetzlicher Vorschriften vorschriftsmäßig gespeichert werden. Dieser Druck wird häufig durch verteilte und komplexe Systeme verstärkt, die sowohl vor Ort als auch in der Cloud laufen können.

Hinzu kommt das stetig wachsende Volumen an strukturierten und unstrukturierten Daten wie Dokumenten, E-Mails, Fotos, Videos und Metadaten, die die Komplexität des Speicherbedarfs von Unternehmen noch weiter erhöhen.

Aber wenn die Cloud-Speicherung viele dieser Herausforderungen lösen kann, welche Bedeutung haben dann USB-Sticks in der heutigen Unternehmenslandschaft?

> **Viele Menschen halten USB-Sticks für altmodisch oder unnütz, weil sie in der Vergangenheit mehr oder weniger als Wegwerfgeräte mit geringer Leistung und geringer Sicherheit verwendet wurden.**
>
> **- Rafael Bloom**

Mobiler Speicher, der dem wachsenden Bedarf gerecht wird

Während ältere Nutzungsweisen von USB-Sticks als tragbares Speichermedium in den Hintergrund getreten ist, hat sich die Verwendung von Hochleistungs-USB-Sticks für persönliche, sichere lokale Backups mit zusätzlichem Datenschutz und gesteigerter Vertraulichkeit entwickelt. Dies ist besonders wichtig für Daten, bei denen Vorschriften eingehalten werden müssen, z. B. Personalakten, Finanzdaten, Gesundheitsdaten, geistiges Eigentum (IP) und alle personenbezogenen identifizierbaren Informationen (PII). Außerdem verfügt diese Generation von Geräten über schnelle Datenübertragungs-, Speicher-, Back-Up- und Sicherheitsfunktionen, die für viele Zwecke genutzt werden können:

- Behördliche Informationen, die persönlich zugestellt werden müssen
- Rechtliche und Finanzdokumente, die vor Ort oder außer Haus zugestellt und ausgedruckt werden müssen
- Alle potenziell feindlichen Umgebungen, in der Ransomware eine Bedrohung darstellen könnten
- Übertragung auf Drucksysteme, bei denen der Netzzugang unzulässig ist

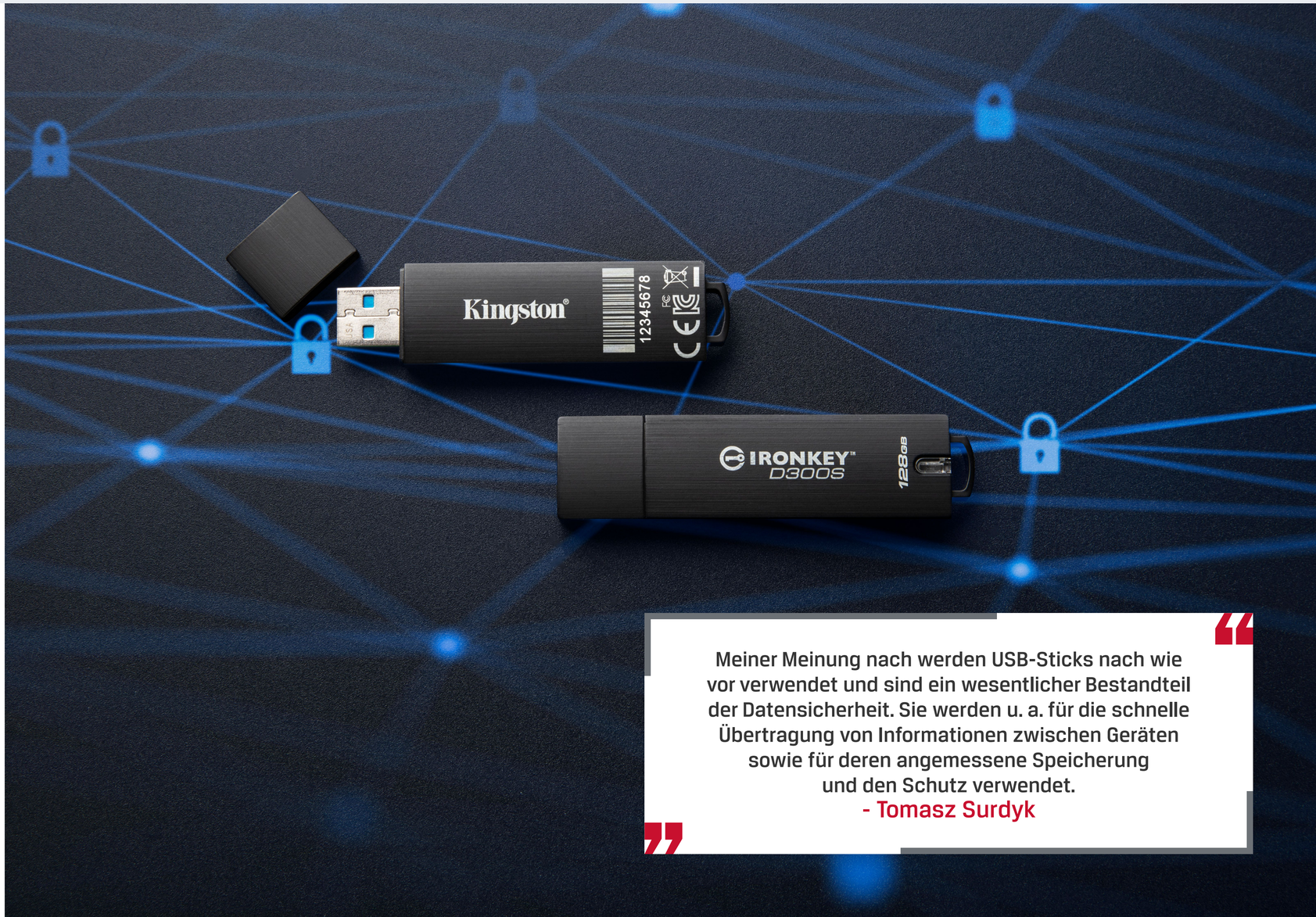
Als führender Anbieter von verschlüsselten USB-Geräten hat Kingston Technology mit der steigenden Nachfrage Schritt gehalten und Lösungen wie den Kingston IronKey™ S1000 auf den Markt gebracht. Dieser beste verschlüsselte USB-Stick seiner Klasse erfüllt die strengsten Standards und schützt vertrauliche Daten durch XTS-AES 256-Bit-Verschlüsselung und einen separaten Kryptochip mit starkem Schutz vor Manipulationen. Außerdem ist er nach FIPS 140-2 Level 3 zertifiziert. Das bedeutet, dass er von der US-Regierung offiziell für seine Wirksamkeit als kryptografische Hardware geprüft und bestätigt wurde, wodurch er ideal für Unternehmen ist, die in Hinsicht auf den Datenschutz zusätzliche Sicherheit benötigen.

Solche hardwareverschlüsselten USB-Sticks bieten zentralisierte Lösungen zur sicheren Geräteverwaltung, unabhängig davon, ob die Daten in der Cloud oder vor Ort gespeichert sind. Eine gesetzeskonforme verschlüsselte Datenspeicherung, die benutzerfreundlich ist und keine Software erfordert, spart wertvolle IT-Zeit und bietet Lösungen für eine schnelle und effiziente Bereitstellung.

Mobiler Speicher, der dem wachsenden Bedarf gerecht wird

Die Sicherung und Archivierung ist ein weiteres Beispiel dafür, dass USB-Sticks zum langfristigen Schutz digitaler Daten verwendet werden können, und zwar unabhängig von Cloud-Diensten von Drittanbietern. Es stimmt zwar, dass große Datenübertragungen problemlos in der Cloud abgewickelt werden können, doch kann geschütztes geistiges Eigentum immer noch so sensibel sein, dass es sich lohnt, es auf einem verschlüsselten, gesicherten USB-Stick zu speichern, der vom Internet getrennt und geschützt aufbewahrt werden kann.

Es wird immer Umstände geben, unter denen ein Unternehmen Daten logisch und physisch unter seiner Kontrolle haben muss, insbesondere bei der Verwendung verschlüsselter Laufwerke. Und es gibt Fälle, in denen der Speicher auf einer HDD/SSD nicht verschlüsselt werden kann. Die Verwendung externer verschlüsselter USB-Sticks löst dieses Problem, wie zum Beispiel der Kingston IronKey D300S. Dieses USB-Stick verfügt über die Hardware-Verschlüsselung XTS 256-Bit Advanced Encryption Standard (AES), eine Art Blockchiffre, die 128-Bit-Datenblöcke verschlüsseln kann. Wenn Daten dann noch weiter verschlüsselt werden müssen, verwendet AES den XTS-Blockchiffriermodus, der einen besseren und stärkeren Datenschutz bietet als die bisherigen Modi.



> Meiner Meinung nach werden USB-Sticks nach wie vor verwendet und sind ein wesentlicher Bestandteil der Datensicherheit. Sie werden u. a. für die schnelle Übertragung von Informationen zwischen Geräten sowie für deren angemessene Speicherung und den Schutz verwendet.
>
> - Tomasz Surdyk

Verschlüsselung: Hardware- oder softwarebasiert

Betrachtet man die Art und Weise, wie Daten verschlüsselt werden, kann man sagen, dass die Hardware-Verschlüsselung einfacher zu handhaben und sicherer ist als die Software-Verschlüsselung. Der Grund dafür ist, dass der Verschlüsselungsprozess vom Rest des Host-Systems getrennt ist, wodurch es viel schwieriger ist, ihn zu unterbrechen oder zu knacken. Mit der zentralen Verwaltung auf Geräteebene können Laufwerke über Intranet-LAN und Internetverbindungen kontrolliert werden und dies kann ein exzellentes Instrument für Folgendes sein:

- Festlegung und Durchsetzung von Richtlinien für die Nutzung verschlüsselter USB-Sticks durch Einzelpersonen und/oder Gruppen
- Überprüfen von Dateiaktivitäten für einen besseren Überblick über den Datenverkehr in oder aus Ihr/em Unternehmen
- Fern-Back-Up von Inhalten für den Transport wichtiger Daten
- Deaktivierung von Geräten aus der Ferne, wenn ein USB-Stick verloren geht oder beschädigt wird
- Zurücksetzen von vergessenen Passwörtern aus der Ferne

Wenn autorisierte Laufwerke auf diese Weise korrekt verwaltet werden, wird das Risiko minimiert, dass sensible Daten kopiert und weitergegeben werden. Außerdem bieten moderne hardwareverschlüsselte USB-Sticks eine Vielzahl zusätzlicher Sicherheitsfunktionen, die verhindern, dass Dateien und Nachrichten von anderen als den vorgesehenen Empfängern eingesehen oder gelesen werden können.

> **Ich glaube, dass Hardware-Verschlüsselung besser ist als Software-Verschlüsselung. Die Unterschiede zwischen den Methoden der Hardware- und der Software-Verschlüsselung sind im Hinblick auf die Anfälligkeit für Brute-Force-Angriffe erheblich. Denn Hardwareverschlüsselte Geräte erliegen solchen Angriffen nicht sehr leicht.**
>
> - Tomasz Surdyk

Verschlüsselung: Hardware- oder softwarebasiert

Auch wenn Unternehmen aus Kostengründen eine softwarebasierte Verschlüsselung in Betracht ziehen, ist dies möglicherweise etwas kurzsichtig. Softwarebasierte Lösungen teilen sich die Verschlüsselungsressourcen des Host-Geräts mit anderen Programmen, sodass sie nur so sicher sind wie der Computer selbst und oft Software-Updates erfordern, die Sie – wenn sie nicht gepflegt werden – angreifbar machen. Softwareverschlüsselte USB-Sticks können unbegrenzten Brute-Force-Angriffen ausgesetzt sein, um das Passwort zu erraten, und sie haben keine Möglichkeit, softwarebasierten Wörterbuchangriffen zu widerstehen – die Millionen von Zeichenkombinationen in kurzer Zeit testen können.

Außerdem ist die Software-Verschlüsselung auch eine entfernbare Verschlüsselung. Alle Mitarbeiter mit einem softwareverschlüsselten Laufwerk können die Daten kopieren, den USB-Stick formatieren, und schon ist die Verschlüsselung aufgehoben. Dann können die Dateien zurückkopiert werden und das Laufwerk kann ohne den mühevollen Weg der Authentifizierung auf verschiedenen Plattformen und Betriebssystemen verwendet werden.

Wie bereits erwähnt, erfolgt bei der hardwarebasierten Verschlüsselung die physische „Verschlüsselung" – und die anschließende Speicherung der Daten – unabhängig vom Host-System. Dies gewährleistet eine zusätzliche Verteidigungsebene, falls die Systeme jemals kompromittiert werden sollten.

Dies darf nicht übersehen werden, insbesondere in Branchen wie dem Finanzwesen, dem Gesundheitswesen und Regierungsbehörden. Dies liegt daran, dass Vorschriften wie der Health Insurance Portability and Accountability Act (HIPAA) (Arztgeheimnis) und der Payment Card Industry Data Security Standard (PCI DSS) oft strenge Anforderungen an die Verschlüsselung sensibler Daten stellen.

Die Einhaltung dieser Vorschriften durch die Verwendung stark hardwareverschlüsselter Geräte hilft Unternehmen letztlich, teure Geldstrafen, Gerichtsverfahren und potenziell erdrückende Rufschädigungen zu vermeiden. Hardwareverschlüsselte Laufwerke mögen zwar teurer sein als preiswertere USB-Sticks, aber die Rechtskosten bei einem Verstoß können leicht die Kosten für Hunderte von Sticks in nur wenigen Stunden Rechtsberatungsgebühren übersteigen.

Der wachsende Bedarf, sensible Daten zu schützen

> Verschlüsseln Sie alle Daten so schnell wie möglich, erstellen Sie Sicherungskopien nach der 321-Methode (USB-Sticks können eine Option sein, da sie leicht verfügbar sind) und implementieren Sie eine schnelle Mikro-Segmentierungsfunktion. - David Clarke

Wenn es darum geht, sensible Daten vor Verlust und Diebstahl zu schützen, sind alle Unternehmen verpflichtet, dafür zu sorgen, dass ihre Geräte über angemessene Sicherheitsfunktionen verfügen. Dabei muss auch unbedingt bedacht werden, dass es zwar eine Vielzahl von sich ständig weiterentwickelnden Cyber-Bedrohungen gibt, dass aber der Grad der digitalen Reife und die Fähigkeiten der Benutzer bei der Verwaltung ihrer Endpunktdaten ein wichtiger Risikofaktor bleiben, wenn diese nicht berücksichtigt werden. Insider-Bedrohungen wie der Verlust von Datenkontroll- oder USB-Speichergeräten, die Übertragung von Daten außerhalb einer sicheren Umgebung, die Verwendung unverschlüsselter USB-Sticks und die Weitergabe von Passwörtern können das Ergebnis mangelnder Sorgfaltspflicht der Endbenutzer sein. All dies lässt sich mit einer angemessenen Schulung, Fortbildung und den richtigen USB-Laufwerkslösungen vermeiden.

Die Vorplanung und eine gut eingespielte Kommunikationsstruktur sind ebenfalls ein Schlüsselfaktor für den Umgang mit einer potenziell existenziellen Bedrohung. Die heutigen Cyber-Bedrohungen zielen auf die Schwachstellen von Unternehmen ab.

Der beste Zeitpunkt für die Entwicklung eines Plans für verschlüsselte USB-Sticks ist, bevor er tatsächlich benötigt wird, indem verschlüsselte USB-Sticks und Richtlinien in die allgemeine Sicherheitsstrategie Ihres Unternehmens integriert werden. Wenn noch kein Plan für verschlüsselte USB-Sticks und keine Richtlinien vorhanden ist, können Sie nicht darauf aufbauen, und Ihr Unternehmen ist auf allen Ebenen Risiken ausgesetzt – einschließlich der Nichteinhaltung von Vorschriften wie der Datenschutzgrundverordnung (DSGVO), in deren Artikel 32 ausdrücklich festgelegt ist, dass sensible Daten verschlüsselt werden müssen.

> Das Unternehmen muss über eine übersichtliche Darstellung seiner Daten verfügen, die den Grad der Wichtigkeit und/oder Sensibilität aller Datensätze einschließt, wobei nach der Plan die wichtigsten Daten als Erstes abgearbeitet werden, indem entweder die Verbindung zu den Daten physisch unterbrochen oder die Datenquelle abgeschaltet wird. Die Fähigkeit, betroffene Systeme schnell zu isolieren, ist von entscheidender Bedeutung – und auch hier ist ein dokumentierter Plan, der praktisch geübt wird, absolut notwendig. - Rafael Bloom

> Benutzer verarbeiten sensible Daten. Der Verlust sensibler Daten erhöht die Verantwortung und wirkt sich erheblich auf das Image und die Sicherheit des Unternehmens aus. Zum Schutz sensibler Daten sollten verschiedene Sicherheitslösungen eingesetzt werden, darunter die Datenverschlüsselung. - Tomasz Surdyk

Schutz sensibler Finanzdaten

Neben den Sicherheitsaspekten gibt es auch Compliance-Standards, die von Datenspeicher- und Datensicherungslösungen eingehalten werden müssen. Einige dieser Praktiken, z. B. die Notwendigkeit der Verwaltung und Durchsetzung von Datenaufbewahrungsplänen, sind in allen Branchen gleich, während andere, beispielsweise die Migration von Unternehmensdaten in die Cloud, sehr unterschiedlich gehandhabt werden.

In vielen vertikalen Bereichen, z. B. bei den Finanzdienstleistungen, sind Vorschriften in Kraft getreten, die eine ordnungsgemäße Datenverwaltung zur Pflicht machen. Vor allem Banken waren anfangs sehr zurückhaltend, wenn es um die Nutzung von Drittanbietern für die Speicherung und Sicherung von Daten ging, und viele bestehen immer noch darauf, ihre gesamte Dateninfrastruktur selbst zu besitzen.

Finanzinstitute sind auch verpflichtet, eine wachsende Liste von Datensicherheitsvorschriften und -standards einzuhalten, wie z. B. den Sarbanes-Oxley Act (SOX) und die Datenschutzgrundverordnung (DSGVO). Mit der zunehmenden Zahl mobiler Mitarbeiter und Auftragnehmer steigt jedoch auch das Risiko von Datenverlusten und der Nichteinhaltung der durch diese Gesetze und Normen auferlegten Verpflichtungen.

Tatsächlich ist es so, dass die Bemühungen um die Einhaltung von Vorschriften mit verblüffender Leichtigkeit gefährdet werden können, wenn mobile Mitarbeiter ihre digitalen Identitäten, ihre mobilen Arbeitsbereiche, ihre Kundendaten und die von ihnen mitgeführten Finanzdaten nicht schützen. Deshalb setzen immer mehr Unternehmen auf mobile Sicherheitslösungen wie die verschlüsselten USB-Sticks von Kingston IronKey, um digitale Identitäten und Anwendungen zu schützen, egal wohin ihre Mitarbeiter sie mitnehmen.

> **“Wenn man den allgemeinen Trend zu einer dezentraleren IT-Ausstattung und die schiere Skalierbarkeit der Cloud-Infrastruktur bedenkt, ist es leicht zu verstehen, warum sich die meisten Branchen und ein Großteil der KMUs nicht mehr mit der Verwaltung gekühlter Serverräume beschäftigen. - Rafael Bloom”**

Sicherer Zugriff auf Gesundheitsdaten von Patienten

Das Gesundheitswesen ist eine weitere Branche, in der die Datensicherheit wichtiger denn je ist. Das Risiko, dass Patientendaten gestohlen werden, ist sogar noch größer: Im Jahr 2021 wurden 45,67 Millionen Patientendatensätze offengelegt –- die höchste jährliche Zahl seit 2015[2]. Bei der Datenspeicherung und -sicherung sind Patientendaten die entscheidenden und umfassenden medizinischen Informationen, die es Gesundheitsdienstleistern ermöglichen, ihre Patienten sicher zu behandeln.

Dies kann alles umfassen, von elektronischen Patientenakten (EHR) mit Krankengeschichten, Untersuchungen, Fotos und Röntgenbildern bis hin zu Verwaltungsdateien wie Gehaltsabrechnungen, Patientenversicherung und Kreditorenbuchhaltung. Angesichts einer wachsenden Anzahl mobiler Mitarbeiter und eines globalen Gesundheitsmarktes, der sich im Umbruch befindet, ist es nicht verwunderlich, dass sich die Gesundheitsdienstleister von heute Sorgen um die Datensicherheit machen.

> Da insbesondere Ransomware so etwas wie eine Wachstumsbranche ist, müssen alle Unternehmen, die mit sensiblen Daten umgehen, darüber nachdenken, wie sie unter extremem Zwang agieren können. - Rafael Bloom

Wenn es nicht gelingt, Risiken vorauszusehen und strenge Vorschriften wie den Health Insurance Portability and Accountability Act (HIPAA) (Arztgeheimnis) oder den Health Information Technology for Economic and Clinical Health Act (HITECH) einzuhalten, könnte dies zu einer kostspieligen Verletzung des Datenschutzes im Gesundheitswesen führen, wodurch das Vertrauen von Patienten, Partnern und Regulierungsbehörden weiter erschüttert werden kann.

Mit Lösungen wie den verschlüsselten Kingston USB-Sticks der IronKey-Reihe können Unternehmen im Gesundheitswesen von einer einzigen Konsole aus Richtlinien für Passwörter, die Nutzung von Anwendungen, die Wiederherstellung und vieles mehr festlegen – für eine Handvoll oder Tausende von Laufwerken. Mit benutzerfreundlichen Lösungen, die es den Mitarbeitern ersparen, für den sicheren Zugriff auf ihre gespeicherten Daten Treiber oder andere Software zu installieren können mobile Mitarbeiter und Mitarbeiter an der vordersten Front mehr Patienten betreuen. Benutzer und Administratoren können Daten einfach und schnell sperren, unabhängig davon, wo sie gespeichert sind.

Der USB-Stick in einer Zukunft der Cloud-Speicherung

> **Cloud-Datenspeicherung ist die Gegenwart und die Zukunft. Ich bin nach wie vor der Meinung, dass eine physische Sicherung der Daten, z. B. durch verschlüsselte USB-Sticks, am sichersten ist. Nutzer haben keine vollständige Kontrolle über das, was in der Cloud geschieht. Wir haben jedoch die Kontrolle über die Daten auf verschlüsselten USB-Sticks, die wir selbst schützen und aufbewahren. Denn außer uns hat niemand Zugang zu diesen Medien. - Tomasz Surdyk**

Da die Vorteile von USB-Sticks nun klar sind, stellt sich die Frage, welche Rolle sie in einer Zukunft der Cloud-Speicherung spielen werden.

Vor einem Jahrzehnt waren USB-Sticks als primäres Werkzeug zum bequemen Speichern und Übertragen von Daten sehr gefragt. Durch die Auswirkungen neuer hybrider Arbeitsmodelle und zunehmend verteilter Teams bietet die Cloud nun jedoch einen schnellen und einfachen Zugriff auf gespeicherte Informationen von vielen Geräten aus. Früher waren USB-Sticks wegen ihres einzigartigen Komforts beim Datentransport sehr beliebt. Heutzutage bieten Cloud-Speicherdienste eine einfachere Übertragbarkeit von Dateien.

Allerdings gibt es bei der Speicherung in der Cloud noch viele Einschränkungen. Es ist eine Netzwerkverbindung erforderlich, die nicht nur vorschreibt, wie und wann Dateien gesichert oder übertragen werden können, sondern auch ein zusätzliches Sicherheitsproblem darstellt. Wenn ein Unternehmen die Cloud-Nutzung vorschreibt, kann es nicht unbedingt kontrollieren, von wo aus auf die Daten zugegriffen wird. Schon der Zugriff auf ein VPN über eine persönliche oder öffentliche WLAN-Verbindung birgt daher das Risiko, gehackt zu werden. Außerdem sind Cloud-Dienste für Bedrohungsakteure sehr attraktiv, da die Mehrheit aller Schadprogramme (61 %) inzwischen über Cloud-Anwendungen verbreitet wird[3].

> **Es ist deshalb ratsam, sich Gedanken darüber zu machen, was passiert, wenn die Cloud nicht verfügbar ist, welche Szenarien es gibt, in denen Daten zu 100 % verfügbar sein müssen, und wo eine langfristige Speicherung eine Schwachstelle darstellen könnte. - David Clarke**

Der USB-Stick in einer Zukunft der Cloud-Speicherung

Auf der anderen Seite kann die USB-Verschlüsselung entweder über die Geräte-Hardware oder über die Software erfolgen. Hardwarezentrierte, softwarefreie Verschlüsselung ist das wirksamste Mittel zum Schutz vor Cyberangriffen. Es handelt sich um eine hervorragende, unkomplizierte Lösung zum Schutz vor Datenschutzverletzungen, die strenge Compliance-Standards erfüllen kann und Unternehmen dabei unterstützt, Bedrohungen zu bewältigen und Risiken zu reduzieren.

Da sie in sich geschlossen sind, benötigen hardwareverschlüsselte USB-Sticks kein Softwareelement auf dem Host. Da keine Software-Schwachstelle vorhanden ist, ist auch die Möglichkeit von Brute-Force-, Sniffing- und Memory-Hash-Angriffen ausgeschlossen. Bei softwareverschlüsselten USB-Sticks besteht außerdem das Risiko, dass jeder Benutzer die Verschlüsselung deaktivieren kann, indem er den USB-Stick auf einem beliebigen Computer formatiert und den Stick zur ungeschützten Speicherung sensibler Daten verwendet.

Hardwareverschlüsselte USB-Sticks bieten auch eine außergewöhnliche physische Methode zum Schutz von Daten. Sie ermöglichen die Festlegung von Kriterien für den Informationszugang durch einen Benutzer oder Administrator und können in bestehende lokale Endpunktlösungen integriert werden. Dies macht sie zu einer bequemen und kostengünstigen Lösung für viele Szenarien, in denen eine Speicherung in der Cloud nicht möglich oder nicht so effektiv wäre. Dies kann der Fall sein, wenn Daten von Geräten gespeichert werden müssen, die nicht vernetzt sind, die privat sein müssen oder auf die man zugreifen muss, wenn sie offline sind.

> **Wenn wir uns vorstellen, dass Daten entweder „hot" oder „cold" sind, je nachdem, wie nützlich sie täglich für ein Unternehmen sind, dann könnte es effizienter sein, „cold" oder kalte Daten in der Cloud zu speichern und sich mehr auf die lokale USB-Speicherung von „hot" oder heißen Daten zu stützen, wenn Betriebskontinuität und hohe Leistung für das Unternehmen, für eine bestimmte geschäftskritische Funktion oder einen Prozess wichtiger sind. - Rafael Bloom**

Fazit

Wir können zwar nicht vorhersagen, welche Innovationen in Zukunft auf uns zukommen, aber was wir anbieten können, ist ein preisgekröntes Portfolio von USB-Sticks, das eine dynamische Palette von verschlüsselten Lösungen für alle Anforderungen an den Schutz mobiler Daten bietet. Von USB-Sticks mit alphanumerischer Tastatur für einen benutzerfreundlichen PIN-Schutz über die FIPS 140-2-Level 3-Zertifizierung für die höchste Verschlüsselungsstufe und den Schutz vor Manipulationen bis hin zur SuperSpeed USB 3.1-Technologie, die keine Kompromisse bei der Sicherheit eingeht – die Kingston IronKey-Produkte sind darauf ausgelegt, Ihre Datenanforderungen zu erfüllen.

Unser spezialisiertes Expertenteam steht Ihnen bei jedem Schritt Ihrer Datenspeicherung zur Seite und hilft Ihnen, die richtige Speicherlösung für Ihre Anforderungen zu finden.

Wir verfügen über das Fachwissen und die technischen Möglichkeiten, um Sie dabei zu unterstützen, vertrauliche Informationen zu schützen und neue Vorschriften einzuhalten, ganz gleich, ob Sie einen Plan für verschlüsselte USB-Sticks erstellen, die besten USB-Sticks für Ihr Unternehmen suchen oder Sicherheitsrichtlinien festlegen und durchsetzen möchten. Wir bieten einen hochgradig personalisierten Service und sind bestrebt, Produkte zu liefern, die Ihre Prioritäten bei der Datenspeicherung unterstützen und es Ihnen ermöglichen, mit der beispiellosen Geschwindigkeit, mit der sich die Geschäftswelt entwickelt, Schritt zu halten.

Über Kingston

Mit 35 Jahren Erfahrung verfügt Kingston über das nötige Wissen, um Ihre Herausforderungen im Bereich der mobilen Daten zu erkennen und zu lösen – damit Ihre Mitarbeiter sicher arbeiten können, ohne Ihr Unternehmen zu gefährden.

1. Statista - https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data
2. SC Magazine - https://www.scmagazine.com/analysis/breach/breaches-exposed-45-67m-patient-records-in-2021-largest-annual-total-since-2015
3. Infosecurity Magazine - https://www.infosecurity-magazine.com/blogs/cloud-services-top-of-mind-phishers

#KingstonIsWithYou