SOFTWARE-VERSCHLÜSSELUNG UND EINHALTUNG GESETZLICHER VORSCHRIFTEN: PREISGÜNSTIGERE LÖSUNG MIT GROSSEN SICHERHEITSRISIKEN

GESETZLICHE UND COMPLIANCE-ANFORDERUNGEN

Früher war die Datensicherheit nur den IT-Abteilungen vorbehalten, aber aufgrund der ständigen Verstöße gegen den Schutz der Kundendaten wurden von Regierungen weltweit immer mehr Anforderungen an Unternehmen gestellt, alle personenbezogenen Daten zu verschlüsseln und zu schützen.

Von HIPAA im Gesundheitswesen über die DSGVO im EMEA-Raum bis hin zu CCPA in Kalifornien wird die Verschlüsselung von geschützten Datenklassen durch Vorschriften geregelt. Die Zahl der Compliance-Organisationen hat sich in den letzten drei Jahren exponentiell erhöht, da diese Vorschriften und die damit verbundenen Bußgelder und rechtlichen Risiken in die Höhe geschnellt sind.

Angesichts dieser Veränderungen haben die IT-Abteilungen Mühe, mit der Sicherheit und den steigenden Kosten Schritt zu halten. Während der Coronapandemie werden die Budgets für Investitionen in zusätzliche Hardware und Firewall eingesetzt, während die Konzentration auf die Datenverschlüsselung vernachlässigt wird.

Die Softwareverschlüsselung mit Microsoft BitLocker® oder Endpoint Management Software von Unternehmen wie Symantec, McAfee und anderen ist tatsächlich auf dem Vormarsch. Einige Unternehmen und Verbraucher verwenden auch Standard-USB-Sticks mit „Tresor"-Software, wie sie von einigen Anbietern angeboten werden.

VERSCHLÜSSELUNG UND DATENÜBERTRAGUNG

Arbeitnehmern und Endkunden wollen ihre Daten unterwegs mitnehmen. Ihnen stehen folgende Optionen zur Verfügung:

1. Cloud-Dienste: Diese sind großartig, da sie von jedem Gerät aus zugänglich sind, das mit dem Internet verbunden werden kann. Diese Flexibilität hat jedoch ihren Preis. Die Datenspeicherung in Clouds entzieht dem Nutzer oder dem Unternehmen die Kontrolle über die Daten und birgt ein potenzielles Risiko, denn es ist schon vorgekommen, dass Cloud-Server offen zugänglich gelassen wurden oder auf sie zugegriffen wurde.
2. Standard USB-Sticks: Wenn ein USB-Stick dagegen mitgenommen wird, scheint dies im ersten Moment sicherer zu sein, aber das Risiko, dass Daten durch den Verlust des USB-Sticks gefährdet werden, kann sehr groß sein. Es gibt viele Geschichten über verlorene USB-Sticks, auf denen geheime Informationen gefunden wurden, oder über Wäschereien mit Schubladen voller verlorener USB-Sticks.
3. Hardwareverschlüsselte USB-Sticks: Diese USB-Sticks verfügen über eine angepasste Architektur, die einen integrierten Verschlüsselungs-Controller und eine Zugriffskontrolle einschließt. Die Daten werden im XTS-Modus generell mit der stärksten AES-256-Bit-Verschlüsselung verschlüsselt, zusammen mit anderen möglichen Sicherheitsvorkehrungen, um physische und Firmware-basierte Angriffe abzuwehren. Diese USB-Sticks werden von Unternehmen hergestellt, die sich auf Sicherheitsgeräte spezialisiert haben, und sind zwar teurer als herkömmliche USB-Sticks, bieten aber eine höhere Datensicherheit. FIPS 197- oder FIPS 140-2 Level 3 USB-Sticks können einen höheren Grad an Schutz und Sicherheit bieten.
4. Standard-USB-Sticks mit Softwareverschlüsselung: Für die gesetzlich vorgeschriebene Sicherheit kann eine Softwareverschlüsselung mit BitLocker oder anderen Tools verwendet werden. Sie sind eine gute Option, da sie relativ kostengünstig sind und die gleiche AES-256 XTS-Verschlüsselung bieten.

Es überrascht nicht, dass Unternehmen und Branchen in den meisten Fällen zu Option 4 tendieren, d. h. zur Verwendung von Standard-USB-Sticks mit Softwareverschlüsselung, vor allem, weil Softwareverschlüsselung wie BitLocker oder andere Datentresor Software „kostenlos" sind.

SOFTWAREVERSCHLÜSSELUNG IST NICHT REGELKONFORM

Für Sicherheitsexperten in Unternehmen kann die Softwareverschlüsselung genau dieselben Verschlüsselungsfunktionen bieten wie teurere hardwareverschlüsselte USB-Sticks. Aber ist das der richtige Weg? Die Budgets sind knapp, weshalb Unternehmen aus Gründen der Einhaltung von Vorschriften auf Softwareverschlüsselung umsteigen, ohne sich der Schattenseiten der softwarebasierten Verschlüsselung bewusst zu sein.

Was ist das Problem bei softwareverschlüsselten USB-Sticks? Sind gespeicherte Daten und Daten während der Übertragung nicht mit AES-256 XTS verschlüsselt? Im Allgemeinen schon. Das Problem besteht in Folgendem: Softwareverschlüsselung gilt als „entfernbare Verschlüsselung".

Moment – entfernbar? Bedeutet das, dass die Verschlüsselung eines softwareverschlüsselten USB-Sticks von einem Benutzer deaktiviert werden kann?

Die Antwort lautet: Ja. Benutzer können die Softwareverschlüsselung von ihren USB-Sticks entfernen. Warum sollten sie das tun, fragen Sie sich? Weil sie es können – und weil sie einfach auf die Dateien zugreifen wollen, ohne ein Passwort zu verwenden, oder weil sie einfach das Passwort vergessen haben, aber den USB-Stick verwenden müssen.

ENTFERNEN DER SOFTWAREVERSCHLÜSSELUNG VON EINEM VERSCHLÜSSELTEN USB-STICK

Für einen Benutzer, der sich nicht mit der Eingabe komplexer oder anderer Passwörter befassen möchte, um auf seine Daten zuzugreifen, ist das Verfahren einfach:

1. Der softwareverschlüsselte USB-Stick wird an einen Computer angeschlossen
2. Der USB-Stick wird formatiert
3. Nach dem Formatieren des USB-Sticks ist die gesamte Verschlüsselung entfernt
4. Dateien mit geheimen oder vertraulichen Informationen werden auf den USB-Stick kopiert, um den Zugriff zu erleichtern

IT-Abteilungen haben die Verwendung von Formatierungsbefehlen auf Firmencomputern eingeschränkt, aber dies kann auf jedem anderen, nicht firmeneigenen Computer durchgeführt werden.

Für Compliance-Zwecke bedeutet die einfache Entfernung der Datenverschlüsselung, dass der vom Unternehmen bereitgestellte USB-Stick nun unverschlüsselt ist, obwohl die auf dem USB-Stick verschlüsselten Daten als für immer verloren gelten, sobald die Verschlüsselung mit der oben beschriebenen Methode entfernt wird (Verschlüsselungsschlüssel sind an Daten gebunden). Alle Daten, die nach Aufhebung der Verschlüsselung auf das Gerät kopiert werden, gelten als ungesichert und sind möglicherweise nicht mehr konform, was zu einem Verstoß gegen die Vorschriften von HIPAA, DSGVO, GDPR, CCPA und vielen anderen führen kann.

FOLGEN DES VERLUSTS EINES UNVERSCHLÜSSELTEN USB-STICKS

Wenn ein für das Unternehmen bestimmter USB-Stick verloren geht und gefunden wird, selbst wenn das Unternehmen zunächst nichts davon weiß und erst später über die sozialen Medien davon erfährt, gelten für das Unternehmen besondere Compliance-Anforderungen, die es möglicherweise zu erfüllen hat:

1. Durchführung einer forensischen Untersuchung, um festzustellen, welche Daten verloren gegangen sind
2. In Absprache mit der Rechtsabteilung feststellen, ob ein Rechtsverstoß vorliegt
3. Feststellen, ob Kunden benachrichtigt werden müssen

Hier kann der Verlust eines einzigen USB-Sticks sehr teuer werden. Bei Rechtskosten von mehreren Hundert Dollar pro Stunde kann dieser Compliance-Prozess Tausende und Abertausende von Dollar an Kosten verursachen, zusätzlich zu potenziellen Bußgeldern, kundenseitigen und anderen Klagen und der peinlichen Offenlegung von Daten.

Bei der kostengünstigen Implementierung von Softwareverschlüsselung werden diese Risiken und ihre enormen finanziellen Auswirkungen nicht berücksichtigt.

Die Verwendung von unverschlüsselten USB-Sticks in einem Unternehmensnetzwerk birgt noch eine weitere Gefahr. Diese wird allgemein als „BadUSB" bezeichnet. BadUSB ist eine Klasse von Malware, die von böswilligen Akteuren eingesetzt wird, um die Firewall eines Unternehmens zu durchbrechen und Malware über USB-Sticks in die Cyberabwehrsysteme eines Unternehmens einzuschleusen.

BadUSB

Wenn ein USB-Stick in einen Computer eingesteckt wird, startet der Chipset-Controller des Computers über die Firmware einen Handshake mit dem USB-Stick-Controller. Dieser Austausch findet statt, bevor das Betriebssystem (z. B. Microsoft/macOS/Linux) überhaupt darüber informiert ist, dass ein USB-Stick angeschlossen wurde. Jeder USB-Stick verfügt über eine Firmware, die ausgeführt wird, wenn der USB-Stick an einen USB-Anschluss angeschlossen wird.

Böswillige Akteure haben gelernt, dass sie über diesen Handshake-Mechanismus Malware einschleusen können, indem sie die Firmware, die auf dem USB-Stick läuft, durch eine andere, bösartige Firmware ersetzen, die bei der Kommunikation mit dem USB-Stick Malware in das Zielcomputersystem einschleust. Ein Standard-USB-Stick hat keine Sicherheit für seine interne Firmware, die von seinem Controller ausgeführt wird, also wurde BadUSB geboren, als gute USB-Laufwerke bewaffnet wurden, um Firewalls zu durchdringen und Cyberabwehr zu durchbrechen.

Viele Unternehmen versuchen, die Verwendung von USB-Sticks in ihren Systemen zu verbieten, oder gehen sogar so weit, USB-Anschlüsse mit Epoxid zu füllen. Aber es wurde festgestellt, dass viele Arbeitnehmer ihre Daten auf USB-Sticks mit sich nehmen müssen. Führungskräfte möchten beispielsweise Daten mitnehmen, um sie zu bearbeiten oder externen Rechts- oder Finanzberatern zur Verfügung zu stellen, die nicht in der Unternehmens-Cloud sind. Auftragnehmer des Unternehmens benötigen Daten für ihre Arbeit, haben aber nur eingeschränkten Zugang zu den Unternehmensdatenbanken. Finanzanalysten, die es eilig haben, nutzen USB-Sticks, um die Monatsberichte abzuschließen und zu Hause an Tabellenkalkulationen zu arbeiten.

Wie die vorangegangene Analyse zeigt, birgt die Verwendung dieser Standardlösung aus USB-Stick und Softwareverschlüsselung ein erhebliches Risiko. Was auf den ersten Blick preisgünstiger aussieht, entpuppt sich als potenziell sehr schädlich und sehr viel teurer. Allein die Kosten für 2 bis 3 Stunden Beratung mit einem Anwalt wegen einer möglichen Datenverletzung machen alle Einsparungen durch die Verwendung der preisgünstigeren Lösung zunichte.

HARDWAREVERSCHLÜSSELTE USB-STICKS SIND DIE BESTE OPTION FÜR DIE EINHALTUNG GESETZLICHER VORSCHRIFTEN

Deshalb sind hardwareverschlüsselte USB-Sticks die beste Wahl für die folgenden gesetzlich vorgeschriebenen Anwendungen:

1. Bei hardwareverschlüsselten USB-Sticks ist die Verschlüsselung immer aktiv: Es gibt keine Möglichkeit für Benutzer, die Verschlüsselung zu deaktivieren, die Passwortregeln (Mindestlänge, Komplexität) zurückzusetzen und die automatischen Passwortwiederholungen zu deaktivieren. Im Gegensatz zur Softwareverschlüsselung, die das wiederholte Erraten von Passwörtern durch Software-Wörterbuchangriffe nicht verhindert, beschränken die Hardwareversionen die Wiederholung von Passwörtern – und sperren die Daten, wenn die falschen Passwörter 10 Mal oder manchmal sogar weniger häufig eingegeben werden. Dies ist im Zeitalter der Supercomputer sehr sicher.
2. Hardwareverschlüsselte USB-Sticks verwenden hochwertige Verschlüsselungs-Controller und verfügen über zahlreiche Sicherheitsfunktionen: Obwohl wir nicht immer alle Sicherheitsmaßnahmen offenlegen, gibt es eine Gegenmaßnahme zum Schutz vor BadUSB. Wenn die Firmware nur auf hardwareverschlüsselte USB-Sticks geladen wird, wird die Firmware werkseitig digital signiert und geladen. Das bedeutet, dass der Verschlüsselungs-Controller beim Einstecken dieser verschlüsselten USB-Sticks zunächst die Integrität der Firmware anhand der digitalen Signatur prüft und sie nur dann lädt, wenn sie diese Prüfung besteht. Jeder Versuch, die Firmware zu ersetzen, führt dazu, dass der USB-Stick nicht mehr funktioniert – und daher keine Gefahr mehr darstellt.
3. Für hardwareverschlüsselte USB-Sticks können individuelle Produkt-IDs (PIDs) für ein bestimmtes Unternehmen eingerichtet werden: In diese Premium-USB-Sticks kann eine digitale Kennung einprogrammiert werden, dann wird der USB-Stick, wenn er an die innere oder äußere Firewall des Unternehmens angeschlossen wird, als ein vom Unternehmen ausgegebener USB-Stick identifiziert. Wenn zum Beispiel ein Mitarbeiter einen Firmen-USB-Stick verliert und das gleiche Modell im Einzelhandel kauft, wird der neu gekaufte Stick im Firmennetz nicht zugelassen. Diese Personalisierung fügt der Nutzung von USB-Sticks eine weitere Sicherheitsebene hinzu.
4. Hardwareverschlüsselte Sticks sparen sehr schnell Geld: Allein durch die Verringerung und Beseitigung von Risiken wird die Amortisation sehr schnell erreicht.

Kingston ist der weltweit größte Hersteller von verschlüsselten USB-Sticks und bietet USB-Stick-Serien mit verschiedenen Funktionen und Preisklassen an. Setzen Sie sich direkt mit Kingston in Verbindung, um zu besprechen, wie wir Ihnen mit verschlüsselten USB-Lösungen für Führungskräfte, Mitarbeiter, Auftragnehmer und andere helfen können, die geltenden Richtlinien einzuhalten.