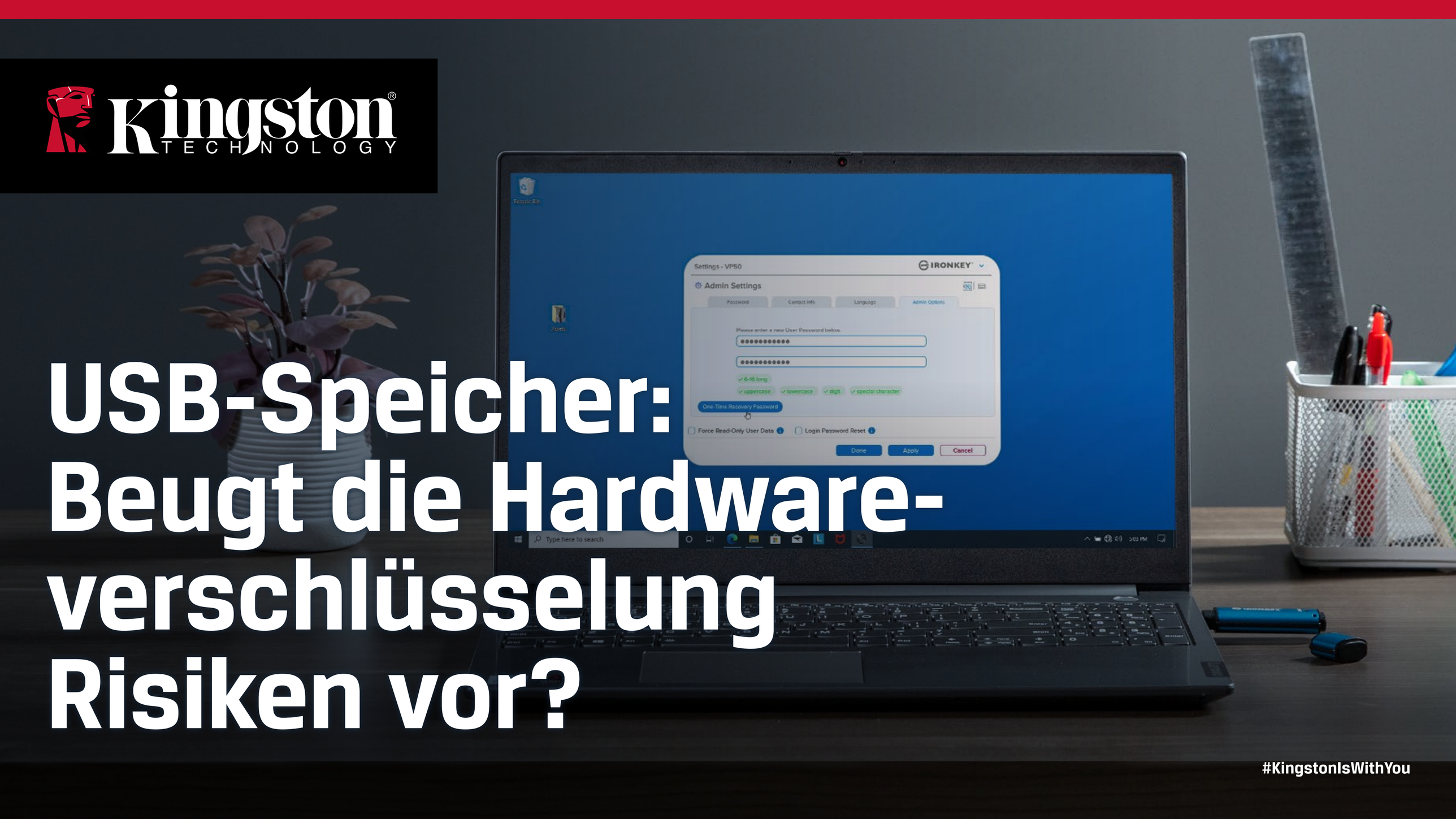
USB-Speicher: Beugt die Hardware-verschlüsselung Risiken vor?



#KingstonIsWithYou

USB-Speicher: Beugt die Hardwareverschlüsselung Risiken vor?

Vorwort und Inhalt

Cybersicherheit ist für Unternehmen wichtiger denn je, aber zu viele Unternehmen sind nicht über die Gefahren der Cybersicherheit informiert und nicht ausreichend auf sie vorbereitet. In den USA Staaten verfügen nur 50 % der Unternehmen über einen Cybersicherheitsplan. Von diesen 50 % haben 32 % ihre Cybersicherheitspläne seit dem Beginn der COVID-19-Pandemie nicht mehr aktualisiert, obwohl laut UpCity die Pandemie dazu führte, dass viele Unternehmen auf Remote- oder Hybrid-Arbeitsmodelle umstellten. Außerdem nimmt die Häufigkeit von Cyberangriffen weiter zu – weltweit steigt die Zahl der Unternehmen, die von Ransomware-Angriffen betroffen sind, von 37 % im Jahr 2020 auf 66 % im Jahr 2021[1].

Eine kompromittierte Cybersicherheit kann verheerende Auswirkungen auf ein Unternehmen haben – abgesehen von den finanziellen Kosten von Cyberangriffen kann sich der Verlust von Daten, Sicherheit und Reputation in vielerlei Hinsicht sowohl kurz- als auch langfristig negativ auf Unternehmen auswirken.

Ein gängiges Mittel für Cyberangriffe sind USB-Sticks. Sie sind in vielen Unternehmen aufgrund ihrer Einfachheit allgegenwärtig geworden – man schließt sie einfach an ein Gerät an und schon sind sie einsatzbereit. Doch gerade diese Einfachheit macht USB-Sticks so anfällig für Angriffe: Es genügt ein einziger verlegter oder gestohlener Stick, damit ein böswilliger Angreifer auf potenziell sensible Daten zugreifen kann. Hier kann die Verschlüsselung eine wichtige Rolle spielen, um USB-Sticks sicher zu machen und gleichzeitig die damit verbundenen Risiken für den Einzelnen und das Unternehmen zu minimieren. In diesem eBook geben wir Antworten auf die folgenden Schlüsselfragen:

- Warum sind verschlüsselte USB-Sticks so wichtig für den Schutz vor Cyberangriffen?
- Wo und wie machen sich Organisationen angreifbar?
- Was können sie unternehmen, um sich zu schützen?

Inhaltsverzeichnis	Seiten

USB-Speicher: Beugt die Hardwareverschlüsselung Risiken vor?

Mitwirkende

Dieses eBook wurde in Zusammenarbeit mit führenden Personen der IT-Branche und neuen Technologien sowie mit unserem eigenen technischen Experten erstellt.

David Clarke

David gilt als einer der Top-10-Influencer nach Thompson Reuters „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.

Pasi Siukonen

Pasi Siukonen ist verantwortlich für die Leitung eines Expertenteams, das die Kingston Abteilungen wie PR, Marketing, Außendienst, technischer Support und Kundendienst für Kingston Produkte unterstützt. Sein Hauptproduktfokus liegt auf Flashspeicher- und SSD-Produktlinien.

Der Unterschied zwischen handelsüblichen und verschlüsselten Sticks

Während herkömmliche (unverschlüsselte) Sticks extrem einfach zugänglich und nutzbar sind, bietet die Hardware-Verschlüsselung mehrere Sicherheitsstufen, sowohl physisch als auch digital, wodurch der USB-Speicher wesentlich sicherer wird. Die leichte Verfügbarkeit, die niedrigen Kosten und die Mobilität von unverschlüsselten Standard-Sticks bedeutet, dass sie zwar für den Benutzer sehr bequem sind, aber auch für böswillige Akteure, die darauf abzielen, sensible Daten zu stehlen, Malware oder Ransomware in ein Unternehmensnetzwerk einzuschleusen, und vieles mehr. Da USB-Sticks so häufig verwendet werden, gibt es viele Möglichkeiten für Cyberangriffe. Es gibt zwei Hauptrisiken im Zusammenhang mit herkömmlichen USB-Speichersticks:

- **Ransomware-Angriffe:** Bei diesen USB-basierten Angriffen wird Malware in Unternehmensnetzwerke eingeschleust und Unternehmensdaten und/oder -systeme durch Verschlüsselung erpresst. Diese werden häufig von BadUSBs verursacht und haben sich zur bekanntesten Art von Malware entwickelt.
- **Gestohlene Daten:** Es genügt ein verlorener, gestohlener oder unbeaufsichtigter Speicherstick ohne entsprechende Sicherheitsvorkehrungen, damit ein böswilliger Angreifer einfach auf die auf dem Stick gespeicherten Daten zugreifen kann – egal ob es sich um Kundeninformationen, Quellcode oder sensible Finanz- und Leistungsdaten handelt.

BadUSB – ist ein Angriff, der die Schwachstelle von USB-Sticks mit ungeschützter Firmware ausnutzen kann, die dann mit bösartiger Software programmiert werden können. Diese bösartigen Tools sind weit verbreitet und für Cyberkriminelle leicht erhältlich, doch viele sind sich der Gefahren durch diese Tools nach wie vor nicht bewusst. Deshalb kann diese Art von Angriffen nur allzu leicht durchgeführt werden, indem die Firmware eines handelsüblichen USB-Sticks durch eine gehackte Firmware ersetzt wird, bei der sich der USB-Stick als Tastatur ausgeben und im Grunde Skripte ausführen kann, um die Firewall anzugreifen. Da so viele Cyberangriffe von ahnungslosen Insidern mit oder ohne böswillige Absichten ausgeführt werden, ist es unglaublich wichtig, dass Unternehmen verschlüsselte Sticks mit geschützter, digital signierter Firmware verwenden, um diese Angriffe zu verhindern, was die Erfolgschancen von Cyberkriminellen senken kann.

> **Die Kosten für den Wiederaufbau der Infrastruktur und möglicherweise die Zahlung eines Lösegelds und anderer Erpressungen sind im Vergleich zu den Kosten für verwaltete USB-Sticks enorm. - David Clarke**

Warum sollten verschlüsselte USB-Sticks verwendt werden?

Verschlüsselte Sticks sind speziell dafür ausgelegt, die darauf gespeicherten Daten sowie alle Geräte, an die der Stick angeschlossen wird, zu schützen, was sie zu einem wertvollen Instrument im IT-Arsenal aller Unternehmen macht. Da die Bedrohungen für die Cybersicherheit immer fortschrittlicher werden, haben sich auch die Funktionen der verschlüsselten Sticks weiterentwickelt, damit die Sticks Cyberkriminellen, die diese Geräte ausnutzen wollen, einen Schritt voraus sind. Wie bei der hardwareverschlüsselten Produktlinie Kingston IronKey™ zu sehen ist, wurden im Laufe der Jahre Funktionen wie AES 256-Bit-Verschlüsselung im stärksten XTS-Modus, ein robustes und manipulationssicheres Gehäuse, digital signierte Firmware, virtuelle Tastaturen, komplexe oder Passphrase-Modi und vieles mehr entwickelt und hinzugefügt, um sicherzustellen, dass Benutzer wirklich vor allen Arten von Angriffen geschützt sind.

Da Cyberrisiken oft nur unzureichend bekannt sind, entscheiden sich viele Unternehmen für den Einsatz von Standard-Speichersticks, obwohl diese eine Reihe von Schwachstellen mit sich bringen. Die leichte Verfügbarkeit, die niedrigen Kosten und die Verwendung von Softwareverschlüsselung spielen hier eine Rolle, ebenso wie das Fehlen eines Genehmigungsverfahrens für Speichersticks im Unternehmen. Zu häufig gibt es keine organisatorischen Richtlinien oder Prozesse für bewährte Praktiken zur Einhaltung verschiedener IT- und Cybersicherheitsstandards wie ISO27001, DSGVO, SOC2 und WISP-Best-Practices. Dies bedeutet, dass Risiken oft auf der Grundlage von Meinungen und nicht von tatsächlichen Beweisen bewertet werden, weshalb viele Organisationen für Angriffe anfällig sind.

Manche verwenden zwar handelsübliche Sticks mit vorhandenen Software-Verschlüsselungsprogrammen, doch gibt dies nur ein trügerisches Sicherheitsgefühl, da viele softwareverschlüsselte Sticks mit kostenlosen oder kostenpflichtigen Tools gehackt werden können, die im Internet für jedermann erhältlich sind. Die Softwareverschlüsselung kann auch durch eine einfache Neuformatierung des Laufwerks durch den Benutzer entfernt werden, damit die Benutzung einfacher wird oder die Sticks werden auf nicht unterstützten Betriebssystem-Plattformen zu verwenden. Hardwareverschlüsselte USB-Sticks haben eine ständig aktive Verschlüsselung, die nicht deaktiviert werden kann, und sind speziell für den Datenschutz entwickelt. Deshalb werden sie so gebaut, dass sie manipulationssicher sind und digital signierte Firmware verwenden, um die Authentizität und Integrität des Laufwerks zu gewährleisten. Die Begrenzung von Passwortversuchen (Schutz vor Brute-Force-Angriffen) und virtuelle Tastaturen (Schutz vor Keylogging und Screenlogging) sind zwei weitere Merkmale von verschlüsselten Sticks wie IronKey VP50. Diese Funktionen erfüllen die branchenüblichen Best Practices zum Schutz vor böswilligen Akteuren, die darauf abzielen, Passwörter von ahnungslosen Benutzern zu erhalten.

> Wenn der IronKey Stick erkennt, dass die Firmware manipuliert wurde, wird das Laufwerk gebrickt und kann nicht mehr hochgefahren werden, was die Cybersicherheit erhöht. - Pasi Siukonen

Wer ist gefährdet?

Jedes Unternehmen, das nicht in der Lage ist, seinen USB-Zugang zu kontrollieren, ist einem Risiko ausgesetzt – und oft sind sich die Unternehmen gar nicht bewusst, worin diese Risiken bestehen. Es gibt jedoch Faktoren, die bestimmte Unternehmen zu attraktiven und anfälligen Zielen für Cyberangriffe machen können.

Unternehmen im Gesundheits- und Finanzwesen verfügen über Daten, die nicht nur viel attraktiver für Cyberkriminelle sind, sondern sie haben auch schwerwiegendere Auswirkungen auf die Organisationen und ihre Kunden. Im Vereinigten Königreich führte ein Cyberangriff auf den NHS (nationaler Gesundheitsdienst) im Jahr 2017 dazu, dass mehr als 19.000 Termine abgesagt werden mussten, was den NHS 92 Mio. Pfund (106 Mio. Euro) an Produktionsausfällen sowie Aufwendungen für die Wiederherstellung von Daten und Systemen kostete. Dadurch wurde nicht nur die medizinische Versorgung der betroffenen Patienten verhindert, sondern der NHS wurde auch heftig dafür kritisiert, dass er auf frühere Warnungen vor Cyberbedrohungen nicht schnell und umfassend genug reagierte. Zwar sollten alle Organisationen in Bezug auf die Cybersicherheit auf dem neuesten Stand und gut informiert sein, aber diejenigen, die mit sensiblen Informationen – insbesondere mit Daten besonderer Kategorien – umgehen, sollten in Bezug auf Cyberrisiken doppelt wachsam sein.

Je höher der Wert des Unternehmens, gemessen am Umsatz, desto größer ist die Belohnung für böswillige Akteure – und damit auch das Risiko für das Unternehmen, das ihnen durch Cyberbedrohungen entstehen kann. Das bedeutet jedoch nicht, dass sich kleinere Unternehmen keine Gedanken über die Cybersicherheit machen sollten. Größere Unternehmen sind zwar ein attraktiveres Ziel für Angriffe, verfügen aber oft auch über die Ressourcen und Spezialisten, um Cyberbedrohungen zu bekämpfen. Auf der anderen Seite verfügen viele KMU nicht über spezielle Cybersicherheitsteams und machen Ausnahmen für leitende Angestellte, damit sie das USB-Management umgehen können, was sie besonders anfällig für verheerende Folgen macht. Aus einigen Studien geht hervor, dass kleine und mittlere Unternehmen häufiger Ziel von Cyberangriffen sind.

Das Risiko ist sogar noch größer für Mitarbeiter in leitenden Positionen; diese Personen sind leicht auffindbar und verfügen häufig über die Privilegien, Sicherheitsvorkehrungen in Bezug auf USB-Sticks umgehen zu können, was bedeutet, dass Kontrollen zur Cybersicherheit – wie z. B. USB-Management-Verfahren – nicht von ihnen verlangt werden, was sie zu lukrativen Zielen für Cyberkriminelle macht. Hier können Sticks mit immer aktiver Hardwareverschlüsselung zusammen mit einem guten Wissen über Cybersicherheit und der Einhaltung bewährter Verfahren und Prozesse einen großen Beitrag zur Risikominderung und zum Schutz vor Angriffen leisten.

> Viele der jüngsten Sicherheitsverletzungen wurden von böswilligen Akteuren begangen, die sich auf die Hilfe von Insidern spezialisiert haben, die die Insider bewusst oder unbewusst bieten - David Clarke

Wer ist gefährdet?

> **Organisationen unternehmen nicht genug, um Bedrohungen der Cybersicherheit zu begegnen.**
> **- David Clarke**

Die Lieferkette ist ein weiterer potenzieller Schwachpunkt für Unternehmen, und Angriffe auf die Lieferkette sind nur allzu häufig. Im Jahr 2013 wurde das US-Einzelhandelsunternehmen Target von einer der größten Datenschutzverletzungen in der Geschichte des Einzelhandels betroffen, bei der die Debit- und Kreditkartendaten von über 40 Mio. Kunden offengelegt wurden. Obwohl Target selbst sehr auf die Cybersicherheit bedacht war und erst sechs Monate vor dem Angriff ein umfassendes Cybersicherheitssystem installiert hatte, waren die Angreifer bei einem der Drittanbieter von Target eingedrungen und hatten sich über diesen Zugang zum Hauptdatennetz von Target verschafft. Insgesamt wurden 90 Klagen gegen Target eingereicht, und das Unternehmen verlor 61 Mio. Dollar zur Behebung der Sicherheitsverletzung. Auch wenn Target nicht direkt für den Angriff verantwortlich war, reichte diese Schwachstelle in der Cybersicherheit der Lieferkette aus, um Schaden sowohl in finanzieller Hinsicht als auch für den Ruf zu verursachen.

Auch die Umgehung von Sicherheitsmaßnahmen durch der Mitarbeiter können eine Schwachstelle darstellen. Während diese Umgehung von Sicherheitsmaßnahmen es den Mitarbeitern ermöglichen, bei ihrer täglichen Arbeit effektiver zu sein, werden viel zu oft grundlegende Sicherheitsprozesse und bewährte Verfahren übersehen, wie z. B. die Passwortverwaltung. Obwohl die Leitlinien des NCSC und des CISA recht einfach sind, ist es oft schwierig, sie in der Praxis umzusetzen, vor allem für Mitarbeiter, die mit IT und Cybersicherheit nicht vertraut sind. Ein engagiertes Cybersicherheitsteam kann sicherlich hilfreich sein, aber auch die Bereitstellung der richtigen Tools für die Mitarbeiter – wie z. B. hardwareverschlüsselte Sticks – kann die Risiken durch die Umgehung von Sicherheitsmaßnahmen durch Mitarbeiter erheblich verringern.

> **Hardwareverschlüsselte USB-Sticks lassen sich heute leicht einführen und in bestehende Cyber-Sicherheitsrichtlinien integrieren. Von der Vielfalt der Schnittstellen (grafisch, Tastatur, Touchscreen) bis hin zur breiten Unterstützung von Betriebssystemen und mit Kapazitäten, die den Anforderungen jeder Organisation gerecht werden. - Pasi Siukonen**

Wie können Unternehmen das Risiko von Cyberangriffen verringern?

Aus organisatorischer Sicht kann eine Reihe von Maßnahmen ergriffen werden, um Endgeräte zu sichern und Daten zu schützen. Ohne Governance, Risk, Compliance (GRC) ist die Cybersicherheit zum Scheitern verurteilt – daher ist es für Unternehmen unglaublich wichtig, die Prozesse zu kennen und zu befolgen, um sich zu schützen. Eine robuste Sicherheitssoftware für die Endgeräte kann auch eine Reihe von Cyberbedrohungen neutralisieren, und bei der Behebung von Sicherheitslücken muss so schnell wie möglich reagiert werden.

> **Die Frage, ob Sie Verschlüsselungsrichtlinien einführen sollen oder nicht, ist für das Risikomanagement ebenso wichtig, wenn nicht sogar wichtiger als die Frage, ob Sie Ihre Daten sichern sollen oder nicht....**
> **- Pasi Siukonen**

Auf individueller Ebene kann verschlüsselte Hardware jedoch die Anfälligkeit für Bedrohungen der Cybersicherheit drastisch verringern. Mit der Zunahme – und dem Fortbestehen – von Remote- und Hybridarbeit, insbesondere in Verbindung mit der Zunahme von Cyberangriffen im letzten Jahr, ist es wichtiger denn je, sicherzustellen, dass Mitarbeiter auf jeder Ebene des Unternehmens Unternehmensdaten sicher bearbeiten, übertragen und lesen können. Hardwareverschlüsselte USB-Sticks ermöglichen es den Benutzern, weiterhin von der Mobilität und Benutzerfreundlichkeit von USB-Sticks zu profitieren und gleichzeitig das mit ihnen verbundene Risiko erheblich zu verringern. Während ein verlegter oder gestohlener Standard-Stick den Verlust von Daten, Geld, Ansehen und mehr bedeuten kann, sind hardwareverschlüsselte Sticks so konzipiert, dass sie sensible Daten vor einer Vielzahl von Angriffen schützen. Und da Cyberkriminelle neue Angriffsmethoden entwickeln, werden sich verschlüsselte Sticks weiterentwickeln, um auch diesen neuen Herausforderungen zu begegnen.

Alles in allem können die Kosten für die Bewältigung eines Cyberangriffs enorm sein. Die Einführung und Verwendung verschlüsselter Sticks auf Unternehmensebene erfordert zwar eine aufwändigere Genehmigung und Einrichtung, kann dem Unternehmen aber auf lange Sicht viel Geld sparen – sowohl in Form von Erpressungskosten als auch in Form von Umsatzeinbußen aufgrund eines beschädigten Rufs. Allein die Rechtskosten im Falle eines Verstoßes gegen die Datenschutzbestimmungen können die zusätzlichen Kosten für hardwareverschlüsselte USB-Sticks leicht ausgleichen.

> **Durch sein langjähriges Engagement für hervorragende verschlüsselte USB-Lösungen ermöglicht Kingstons Portfolio allen Unternehmen, seine Anforderungen an die Cybersicherheit zu erfüllen – durch erzwungene Hardware-Verschlüsselung auf Industriestandard , richtlinienkonforme Designs für Endgeräte und Geräteverwaltungsfunktionen. - Pasi Siukonen**

Fazit

Wir bei Kingston haben die Entwicklungen im Bereich der Cybersicherheit stets im Blick und stellen sicher, dass unsere verschlüsselten IronKey Sticks den neuesten Anforderungen entsprechen und die Cybersicherheitsanforderungen von großen und kleinen Unternehmen erfüllen. Wir sind davon überzeugt, dass Unternehmen mit den richtigen Tools und Kenntnissen gut gerüstet sind, um diese Herausforderungen zu meistern und sich selbst, ihre Mitarbeiter und ihre Kunden zu schützen, denn die Cybersicherheit wird weltweit immer wichtiger.

1. https://www.techtarget.com/searchsecurity/news/252516423/Sophos-66-of-organizations-hit-by-ransomware-in-2021

Über Kingston

Mit über 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.

#KingstonIsWithYou