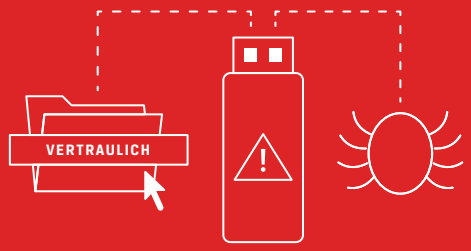
Warnung zu USB-Sticks:
Verschlüsseln Sie Ihre Daten



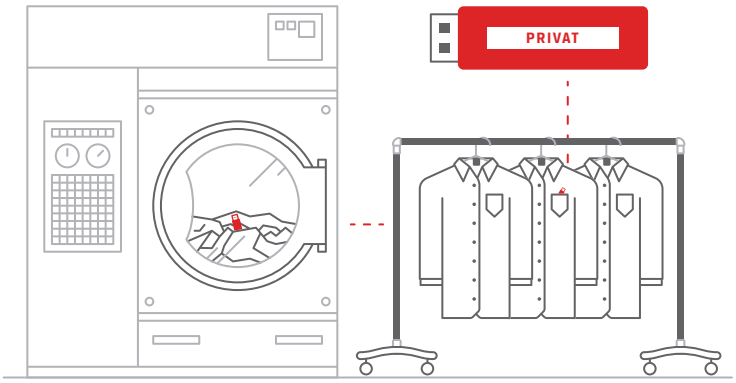
USB-Sticks haben nicht nur die Datenübertragung revolutioniert, durch sie entstanden auch schwere Sicherheitsrisiken. Aufgrund ihrer extremen Mobilität können USB-Sticks nicht nur überallhin mitgenommen werden, sondern auch überall abhanden kommen. Egal, ob sie in Jackentaschen vergessen oder auf Parkplätzen verloren werden – sie stellen immer ein Risiko für die Sicherheit Ihrer Daten dar. Wie kann eine IT-Abteilung diese Risiken ausschließen, ohne die Verwendung von USB-Sticks (mit allen daraus resultierenden Vorteilen) komplett zu verbieten?

Was kann schlimmstenfalls passieren?

USB-Sticks bergen vielfältige Risiken:

VERLOREN

Jedes Jahr landen **22.000 USB-Sticks** in Reinigungen[1]



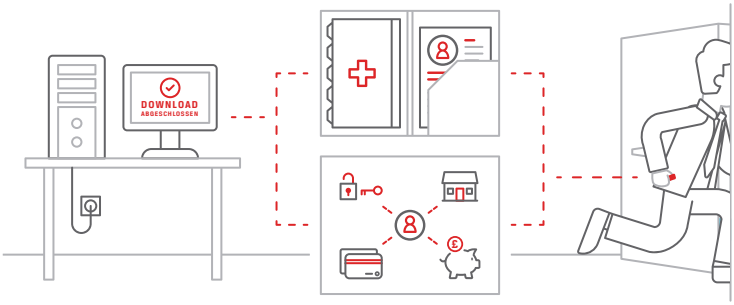
GEFUNDEN

48 % der Personen, die einen USB-Sticks finden, schließen ihn an und klicken auf zumindest eine Datei.[4]

GESTOHLEN

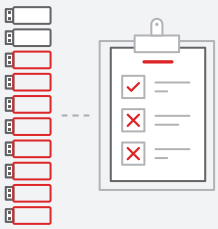
Aus der Notaufnahme eines Krankenhauses verschwand ein USB-Stick mit vertraulichen **Patientendaten.**[2]

Ein verärgerter Mitarbeiter stahl mit einem USB-Stick Bankdaten von **ca. 30.000 Personen.**[3]



Wie handhaben IT-Profis die Sicherheit von USB-Sticks?

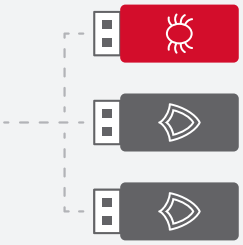
Eine Spiceworks Umfrage unter IT-Profis ergab, dass die Sicherheit von USB-Sticks in den meisten Unternehmen zwar ernst genommen wird, sie jedoch oftmals nicht ausreichend festgelegt ist.[5]



In 80% der Unternehmen gibt es USB-Richtlinien.

Die am häufigsten verwendete Richtlinie ist, die Verwendung von USB-Sticks auf bestimmte Mitarbeiter oder Abteilungen zu beschränken.

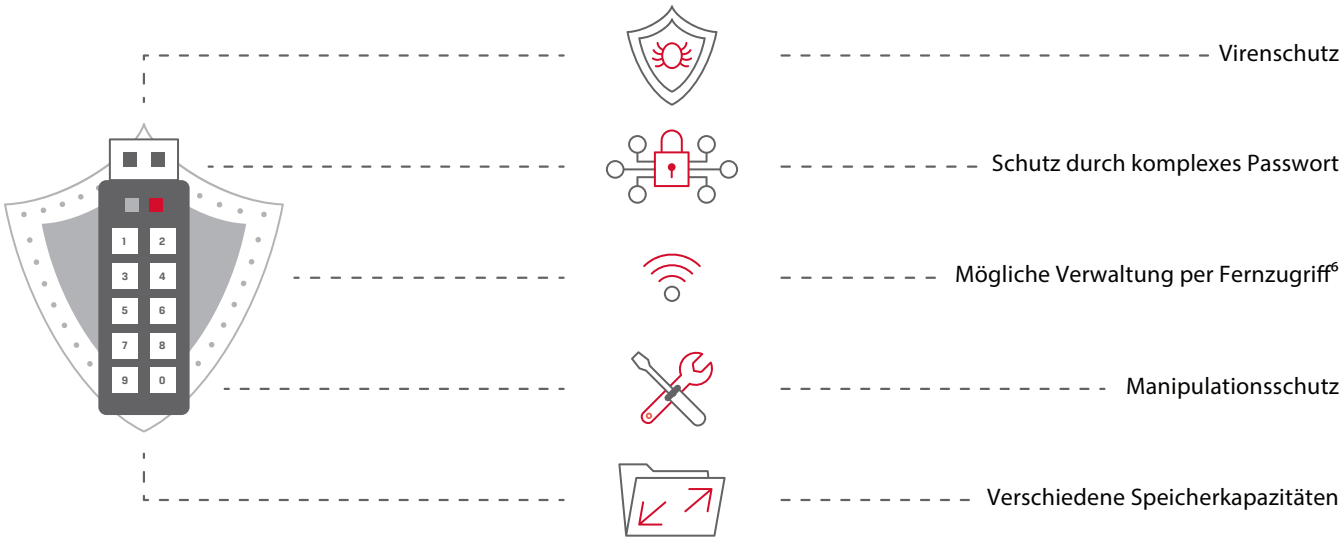
< 20 % der Unternehmen mit USB-Richtlinien schreiben die Verwendung verschlüsselter USB-Sticks vor.



Nichtsdestoweniger verzeichneten **1/3** der Befragten letztes Jahr eine Bedrohung oder Verletzung der Sicherheit von USB-Sticks.

Verschlüsselte USB-Sticks geben ihre Geheimnisse niemals Preis.

Verschlüsselte USB-Sticks können leistungsstarke Werkzeuge zum Schließen dieser allzu häufigen Sicherheitslücke sein. Mit den folgenden Merkmalen tragen sie dazu bei, dass sowohl die Sicherheit als auch die Erfüllung von Sicherheitsrichtlinien gewährleistet sind:



Sichern Sie sich mit Kingston ab!

In Kingstons mit IronKey Technologie verschlüsselten USB-Sticks sind auch hochsensible Daten gut geschützt. Sie wurden zur Einhaltung der striktesten Sicherheitsverordnungen und Protokolle von Regierungsbehörden, medizinischen Dienstleistern und Finanzinstitutionen konzipiert.

Quellen:
1 Steve Bush, „22,000 USB sticks go to the dry cleaners," ElectronicsWeekly.com, January 14, 2016. www.electronicsweekly.com/news/business/information-technology/22000-usbs-sticks-go-to-the-dry-cleaners-2016-01/
2 Taya Flores, „IU Health Arnett reports missing patient info," JConline, January 5, 2016. www.jconline.com/story/news/2016/01/05/iu-health-arnett-reports-missing-patient-info/78300400/
3 Tom Brant, „Report: FDIC Employees Caused Repeated Security Breaches," PC Magazine, July 15, 2016. www.pcmag.com/news/346179/report-fdic-employees-caused-repeated-security-breaches
4 Elie Bursztein, „Concerns about USB security are real: 48% of people do plug-in USB drives found in parking lots," Elie.net, April 2016. www.elie.net/blog/security/concerns-about-usb-security-are-real-48-percent-of-people-do-plug-in-usb-drives-found-in-parking-lots
5 Spiceworks Umfrage im Auftrag von Kingston unter 300 IT-Entscheidungsträgern in den USA, Kanada und Europa, Februar 2017.
6 Kingston Technology ist für die Bereitstellung von Verwaltungslösungen für seine verschlüsselten USB-Sticks eine Partnerschaft mit DataLocker eingegangen. www.kingston.com/us/usb/encrypted_security/management-solutions