Sicherheit von USB-Flashspeichern in Schweizer Unternehmen und Behörden

Kurzfassung

Im Auftrag von Kingston Technology

Vom Ponemon Institute LLC unabhängig durchgeführt

Datum der Veröffentlichung: November 2011

Zur Lage der USB-Speichersicherheit in der Schweiz

Ponemon Institute, November 2011

Einleitung

Das Ponemon Institute freut sich, die Ergebnisse der von Kingston Technology geförderten Untersuchung Zur Lage der USB-Speichersicherheit in der Schweiz vorzustellen. Im Fokus dieser Studie steht das bessere Verständnis für die Komplexität, mit der Unternehmen und staatliche Organisationen mit den Anforderungen an Sicherheit und Datenschutz bei der Erhebung und Speicherung von Daten auf USB-Speichern umgehen.

Wir glauben, dass wir aus dieser Studie lernen können, dass Organisationen sehr wohl wissen, dass sie wegen der Nachlässigkeit ihrer Mitarbeiter gefährdet sind; oftmals werden aber die nötigen Schritte versäumt, USB-Speicher zu schützen. Unsere Studie belegt auch, dass der Schaden durch Verstöße gegen die Datensicherheit durch verloren gegangene oder gestohlene USB-Speicher trotz ihrer geringen Größe erheblich ist. Etwa 59 Prozent der Befragten sagen, dass eine Verletzung der Datensicherheit durch sensible oder vertrauliche Daten verursacht wurde, die auf einem verloren gegangenen USB-Speicher gespeichert waren.

Im Folgenden nennen wir zehn USB-Sicherheitsmaßnahmen, die von vielen Organisationen laut dieser Studie nicht berücksichtigt werden:

1. Den Mitarbeitern werden für die Arbeit genehmigte, hochwertige USB-Speicher zur Verfügung gestellt.
2. Richtlinien und Schulungsprogramme klären, wie USB-Speicher genutzt werden sollen und nicht genutzt werden dürfen.
3. Mitarbeiter mit Zugang zu vertraulichen Daten dürfen ausschließlich sichere USB-Speicher verwenden.
4. Vor dem Kauf von USB-Speichern wird ihre Zuverlässigkeit und Integrität sichergestellt, indem sie auf die Einhaltung aktueller Sicherheitsstandards und das Vorhandensein von Malware geprüft werden.
5. Auf den Geräten wird eine Datenverschlüsselung eingerichtet.
6. Die USB-Speicher werden im Rahmen der Asset-Management-Prozesse überwacht und protokolliert.
7. Die Geräte werden regelmäßig auf Viren und Malware untersucht.
8. Die Geräte werden durch ein Kennwort oder Zugriffssperren gesichert.
9. Vertrauliche Daten auf den USB-Speichern werden grundsätzlich verschlüsselt.
10. Ein Verfahren für die Wiederbeschaffung verloren gegangener USB-Speicher wird eingerichtet.

Wir befragten 306 IT-Fachleute in der Schweiz mit durchschnittlich knapp 11 Jahren IT-Erfahrung oder IT-Sicherheitserfahung. Die meisten der Befragten (56 Prozent) berichten an den IT-Vorstand, 67 Prozent arbeiten in ihrer Organisation als Abteilungsleiter oder höher. 89 Prozent dieser Befragten bestätigen, dass es sehr wichtig oder wichtig ist, dass USB-Speicher hohe Sicherheitsstandards erfüllen.

Der nächste Abschnitt berichtet von den wichtigsten Ergebnissen unserer unabhängig durchgeführten Erhebung. Zusammengefasst bieten unsere Ergebnisse deutliche Hinweise darauf, dass Organisationen sich nicht mit den potenziellen Risiken bei Datenschutz und -sicherheit befassen, die durch unbesonnen eingesetzte, allgegenwärtige und unsichere USB-Speicher hervorgerufen werden und die in vielen Organisationen verbreitet sind. Beachten Sie bitte, dass bei vielen der Fragen mehr als eine Antwort möglich war. Deswegen kann die Antworthäufigkeit bei den wichtigsten Ergebnissen mehr als 100 Prozent betragen.

Die wichtigsten Ergebnisse

Viele Organisationen messen der Sicherheit von USB-Speichern eine hohe Priorität bei, die jedoch den Einsatz geeigneter Technik erfordert. 58 Prozent der Befragten stimmen darin überein, dass ihre Organisationen dem Schutz vertraulicher und sensibler Daten, die auf einem USB-Speicher erfasst und vorübergehend gespeichert werden, eine hohe Bedeutung beimessen.

Während 57 Prozent der Befragten darin übereinstimmen, dass ihre Organisationen angemessene Governance-Verfahren, Kontrollen und Richtlinien haben, um den Missbrauch von USB-Speichern durch Mitarbeiter zu unterbinden oder einzuschränken, sagen weniger als die Hälfte (41 Prozent), dass sie geeignete Technologien haben, um den Download vertraulicher Daten auf USB-Speicher durch nicht autorisierte Dritte zu verhindern oder zeitnah zu ermitteln. 40 Prozent geben an, dass ihre Organisation über geeignete Technologien verfügt, mit denen Viren und Malware, die sich auf USB-Speichern befinden, verhindert oder entdeckt werden, bevor Mitarbeiter damit arbeiten.

Mitarbeiter sind beim Einsatz von USB-Speichern nachlässig und das gefährdet sensible Unternehmensdaten. Mitarbeiter machen Folgendes immer oder sehr oft: Sie benutzen USB-Speicher, ohne zuvor die Erlaubnis dafür eingeholt zu haben (71 Prozent), oder sie verlieren USB-Speicher, ohne die zuständige Stelle davon in Kenntnis zu setzen (46 Prozent).

Eine sehr positive Erkenntnis ist, dass 58 Prozent der Befragten sagen, dass ihre Organisationen Mitarbeitern zugelassene USB-Speicher zum Gebrauch an ihrem Arbeitsplatz zur Verfügung stellen, und nur 21 Prozent gaben an, dass Mitarbeiter immer oder sehr oft gewöhnliche, kostenfreie USB-Speicher einsetzen, die sie auf Tagungen, Messen und anderen Veranstaltungen erhalten haben.

Viele Organisationen haben durchsetzbare Richtlinien, in denen der zulässige Gebrauch von USB-Speichern festgelegt ist, und setzen diese auch durch. 85 Prozent der Befragten sagen, dass ihre Organisationen USB-Sicherheitsrichtlinien haben. 65 Prozent der Befragten jener Organisationen, die USB-Sicherheitsrichtlinien haben, sagen, dass sie von Mitarbeitern, die Zugang zu sensiblen und vertraulichen Daten haben, verlangen, ausschließlich sichere USB-Speicher einzusetzen. 63 Prozent gaben an, dass sich ihre Organisationen zur Durchsetzung der Richtlinien auf Stichproben verlassen, und 40 Prozent sagen, dass sie Network Intelligence Tools einsetzen.

Organisationen setzen unterschiedliche Kriterien bei der Auswahl von USB- und anderen Speichertechnologien ein. Die beiden Hauptkriterien beim Kauf eines USB-Speichers sind: die Fähigkeit, Angriffe von Malware, Botnets und Viren zu verhindern sowie Sicherheitszertifizierung und -tests. Die Prioritäten beim Kauf anderer Speichergeräte sind: Sicherheitszertifizierung und -tests, Preis und Kompatibilität mit hohen Verschlüsselungsstandards.

Zur Bewertung der Zuverlässigkeit und Integrität von USB-Speichern bestätigen 62 Prozent der Organisationen die Übereinstimmung mit führenden Sicherheitsstandards vor dem Kauf, 43 Prozent kaufen nur von vertrauenswürdigen Anbietern und 40 Prozent prüfen, dass sich kein Malware auf den Geräten befindet. Am meisten verlassen sich Organisationen darauf, dass sie eine Richtlinie haben, um minderwertige USB-Speicher in den Händen ihrer Mitarbeiter zu unterbinden, und diese auch konsequent durchsetzen.

USB-Speicher sind in einer Organisation verbreitet und die meisten sind nicht sicher. Auf Basis dieser Erkenntnisse werden von den Mitarbeitern der in dieser Studie dargestellten Organisationen im Schnitt 39.004 USB-Speicher eingesetzt. Durchschnittlich glauben die Befragten, dass 60 Prozent der Geräte sicher sind. Die am weitesten verbreiteten sensiblen oder vertraulichen Daten auf einem USB-Speicher sind: Kundendaten und geistiges Eigentum.

Die Geräte sind zwar klein, aber der Schaden durch Datensicherheitsprobleme aufgrund eines verlorenen USB-Speichers kann verheerend sein. Die Mehrheit der Befragten in dieser Studie (59 Prozent) sagen, dass sie absolut sicher sind (34 Prozent) oder mit hoher Wahrscheinlichkeit annehmen (25 Prozent), dass ein Schaden durch ein Datensicherheitsproblem aufgrund sensibler oder vertraulicher Daten entstanden ist, die auf einem verloren gegangenen USB-Speicher gespeichert waren. In den letzten 24 Monaten kam es in den Organisationen dieser Studie durchschnittlich zu 3,8 separaten Vorfällen, bei denen sensible oder vertrauliche Daten abhanden gekommen sind, die auf einem USB-Speicher gespeichert waren. 34 Prozent der Befragten glauben mit absoluter Sicherheit oder hoher Wahrscheinlichkeit, dass diese Speicher Kunden-, Verbraucher- oder Mitarbeiterdaten enthielten.

In Abgrenzung zur Böswilligkeit ist die Nachlässigkeit des Endbenutzers die häufigste Ursache für verloren gegangene USB-Speicher. Durchschnittlich 56 Prozent aller verloren gegangenen USB-Speicher werden eher durch Nachlässigkeit als durch Betrug, Diebstahl oder andere böswillige Handlungen verursacht. Auf Basis dieser Erkenntnis sollten Schulung, Bewusstseinsschaffung sowie Richtlinien erste Schritte sein, um die USB-Sicherheit in Unternehmen zu verbessern.

Schlussfolgerung

USB-Speicher sind für Mitarbeiter in allen Organisationen zu einer unverzichtbaren Technologie geworden. Wie diese Studie zeigt, stellen jedoch verloren gegangene oder gestohlene USB-Speicher eine große Gefahr für die sensibelsten und vertraulichsten Daten eines Unternehmens dar. Während Organisationen allem Anschein nach den Bedarf begriffen haben, proaktiver gegen die Nachlässigkeit ihrer Mitarbeiter vorzugehen, scheinen USB-Sicherheitsvorkehrungen nicht Teil ihrer übergreifenden Datenschutzstrategie zu sein.

In der Einleitung zu diesem Bericht haben wir 10 USB-Sicherheitsvorkehrungen aufgelistet, die Organisationen umsetzen sollten, aber viele tun das nicht. Die gute Nachricht ist, dass 58 Prozent der Befragten sich darin einig sind, dass ihre Organisationen dem Schutz vertraulicher und sensibler Daten, die auf einem USB-Speicher erfasst und vorübergehend gespeichert werden, eine hohe Bedeutung beimessen.

Unser Anliegen bei der Vorstellung dieser Studie ist es zu zeigen, dass USB-Speicher zwar unscheinbar aussehen, aber die Folgen durch Datensicherheitsprobleme aufgrund verloren gegangener oder gestohlener USB-Speicher enorm sein können. 59 Prozent der Befragten dieser Studie gaben an, dass sie absolut sicher sind oder mit hoher Wahrscheinlichkeit annehmen, dass ein Schaden, der ihrem Unternehmen durch ein Datensicherheitsproblem entstanden ist, auf sensible oder vertrauliche Daten auf einem verloren gegangenen USB-Speicher zurückzuführen war.

Durchschnittlich haben Organisationen in unserer Studie während der letzten 24 Monate mehr als 76.738 Aufzeichnungen über Kunden, Verbraucher und Mitarbeiter verloren, die auf USB-Speichern gespeichert waren. Wie der Bericht „2010 Annual Study: Cost of a Data Breach“ des Ponemon Institute zeigt, können die finanziellen Konsequenzen durch Datenpannen aufgrund verloren gegangener oder gestohlener USB-Speicher bedeutend sein. Das belegt überzeugend den Bedarf, Richtlinien, Prozesse und Schulungsprogramme einzuführen, um mögliche Verletzungen der USB-Datensicherheit zu entschärfen.

Ponemon Institute

Förderung eines verantwortlichen Informationsmanagements

Das Ponemon Institute führt unabhängige Untersuchungen durch und bietet Fortbildungsmaßnahmen zur Förderung des Datenschutzes und des Schutzes personenbezogener Informationen in Organisationen des privaten und öffentlichen Sektors an. Unsere Tätigkeit umfasst qualitativ hochwertige empirische Studien zu kritischen Aspekten rund um das Management und die Sicherheit sensibler Personen- und Unternehmensdaten.

Als Mitglied des **Council of American Survey Research Organizations (CASRO)** setzen wir uns für strikte Geheimhaltungs-, Datenschutz- und ethische Forschungsstandards ein. Wir erheben grundsätzlich keine Daten, die Rückschlüsse auf die Identität von Personen (oder auf Organisationen in unseren Unternehmensumfragen) zulassen. Darüber hinaus gewährleisten wir bei unseren Umfragen die Einhaltung strenger Qualitätsstandards zum konsequenten Ausschluss belangloser, irrelevanter oder unangemessener Fragen.