Prozess zur Medien-bereinigung während des Produktrücksendeverfahrens

Verfahrungsweise

Ziel

Diese Erklärung gibt Kunden von Seagate einen Überblick darüber, was mit Produkten geschieht, die an Seagate zurückgeschickt werden. Löschen Sie zum Schutz Ihrer Privatsphäre sowie anderer datenbezogener Interessen alle bzw. so viele Daten wie möglich von Ihrem Produkt, bevor Sie es an Seagate zurücksenden. Seagate ist sich jedoch darüber im Klaren, dass Sie bestimmte Daten auf zurückgesendeten Produkten nicht löschen konnten. Obwohl Seagate keine Verantwortung für Datenverluste von Anwendern übernimmt, wird Seagate die in dieser Erklärung beschriebenen Vorkehrungen treffen, um die physische Sicherheit solcher Produkte zu gewährleisten, und gegebenenfalls Daten auf von Seagate neu zertifizierten Produkten so schnell wie möglich überschreiben.

Seagate hat durch Rücksprache mit der National Security Agency (NSA) und dem Center for Magnetic Recording Research (CMRR) sichergestellt, dass alle von Seagate reparierten Produkte den entsprechenden Bestimmungen der US-Regierung zur Laufwerksbereinigung genügen oder diese übertreffen. Das National Institute of Standards and Technology (NIST) stellt bestimmte Normen zur Laufwerksbereinigung auf. Die entsprechende Spezifikation in der im Dezember 2014 veröffentlichten Special Publication 800-88 Revision 1, *Guidelines for Media Sanitization* definiert, dass eine *sichere Löschung* von Daten auf dem Medium eine akzeptierte Laufwerksbereinigung bei magnetischen Medien darstellt.

Ebenso stellen die International Organization for Standardization (ISO) und die International Electrotechnical Commission (IEC) auch Normen zur Laufwerksbereinigung zur Verfügung, die in der im Juli 2014 veröffentlichten Publikation ISO/IEC 27040:2014, *Information technology—Security techniques—Storage security* enthalten sind.

NIST 800-88

NIST-Veröffentlichung 800-88, Abschnitt 2.5, Arten der Bereinigung:

„Beim Löschen werden physikalische oder logische Methoden angewendet, durch die mit Hilfe modernster Labortechniken eine Wiederherstellung der Zieldaten unmöglich gemacht wird“.

NIST-Veröffentlichung 800-88, Abschnitt 5, Zusammenfassung von Bereinigungsmethoden:

„Einige Methoden der Bereinigung (die je nach Medium variieren und mit weiter unten in diesem Dokument beschriebenen Gesichtspunkten angewendet werden müssen) beinhalten Überschreiben, Blocklöschen und kryptographisches Löschen durch die Verwendung von dedizierten, standardisierten Gerätebereinigungsbefehlen, die medienspezifische Techniken anwenden, um die den typischen Lese- und Schreibbefehlen inhärente Abstraktion zu umgehen“.

Prozess zur Medienbereinigung während des Produktrücksendeverfahrens

ISO/IEC 27040

ISO/IEC Publikation 27040, Abschnitt 3.35, Begriffe und Definitionen:

„Löschung – Bereinigung (3.38) unter Verwendung physikalischer Methoden, die eine Wiederherstellung auch mit modernsten Labortechniken unmöglich machen, die die Speichermedien (3.48) jedoch in einem potenziell wiederverwendbaren Zustand halten“.

ISO/IEC Publikation 27040, Abschnitt „Anhang“ A.1, Angewendete Verfahren zur Bereinigung von Medien:

„Löschen – Entmagnetisieren, kryptographisches Löschen (siehe A.3) und Ausführen der entsprechenden ATA/SCSI-Firmwarebefehle zur Verwendung von Blocklöschvorgängen sowohl auf logisch adressierbaren als auch auf logisch nicht adressierbaren physikalischen Medien sind akzeptable Verfahren zur Bereinigung. Die Entmagnetisierung ist nicht für Geräte anwendbar, die nichtmagnetische Medien enthalten (z. B. SSD oder SSHD).“

ATA Secure Erase

Das Dokument „AT Attachment 8 - ATA/ATAPI Command Set (ATA8-ACS)“ definiert den Befehl SECURITY ERASE UNIT:

„Wenn der Modus „Normal Erase“ angegeben ist, schreibt der Befehl SECURITY ERASE UNIT binäre Nullen in alle Benutzerdatenbereiche (bestimmt durch READ NATIVE MAX oder READ NATIVE MAX EXT).“

„Im Modus „Enhanced Erase“ schreibt das Gerät zuvor festgelegte Datenmuster in alle Benutzerdatenbereiche. In diesem Modus „Enhanced Erase“ werden alle zuvor geschriebenen Benutzerdaten überschrieben. Das schließt auch Sektoren mit ein, die aufgrund einer Neuzuordnung nicht mehr verwendet werden“.

Der Befehl „ATA Security Erase“ läuft nach seiner Einleitung vollständig innerhalb des Laufwerks ab und meldet „In Betrieb“, bis der Befehl (vollständige Löschung) abgeschlossen ist.

Seagate hat nachgewiesen, dass bei seinen Reparaturen nicht nur die vom Benutzer adressierbaren Speicherorte, sondern auch die nicht vom Benutzer adressierbaren Speicherorte überschrieben werden. Seagate verwendet zufällige Zeichen, Hochfrequenzmuster und digitale Nullmuster, um der Technik der Festplatte gerecht zu werden.

Welcher Prozess wird bei an Seagate zurückgesendeten Produkten verwendet?

Seagate unterhält mehrere Sammellager auf der ganzen Welt, an die im Rahmen der Garantie Produkte zurückgesendet werden können. Diese Standorte sind hoch automatisiert und optimiert, um die zurückgesendeten Produkte in zwei grundlegende Gruppen aufzuteilen. Ein beträchtlicher Prozentsatz der an Seagate zurückgeschickten Laufwerke wird als „Kein feststellbarer Fehler“ (No Trouble Found, NTF) eingestuft. Diese Laufwerke werden zur schnelleren Rezertifizierung vom Rest getrennt. Der Rest der Laufwerke wird zur Prüfung und Reparatur zurück an die Werke von Seagate geschickt.

Für NTF-Laufwerke mit SATA-Schnittstelle verwendet Seagate den ATA-Befehl ATA SECURITY ERASE UNIT und den Modus „Enhanced Erase“ gemäß Empfehlung von NIST 800-88 und ISO/IEC 27040. Nach der Medienbereinigung werden die Laufwerke umbenannt und als zertifiziert und repariert gekennzeichnet.

Die an das Werk zurückgeschickten Laufwerke werden *aufbereitet*. Bei der Fertigung von Laufwerken wird nach der physikalischen Montage der Teile *Folgendes* vorgenommen: Zuerst wird eine Low-Level-Formatierung durchgeführt, dann werden die Servos kalibriert und anschließend die Mediendefekte bewertet sowie eine Neuzuordnung vorgenommen. Auf neuen Laufwerken befinden sich grundsätzlich keine Daten. Für aufbereitete Laufwerke gilt dasselbe. Die Aufbereitung von Laufwerken hat eine vollständige Medienbereinigung zur Folge und übertrifft den ATA-Befehl SECURITY ERASE UNIT in Bezug auf Gründlichkeit und Umfang.

Alle von Seagate® neu zertifizierten Laufwerke weisen ein einzigartiges Etikett mit einem grünen Rand auf der Oberseite auf, um sie von neu gefertigten Produkten unterscheiden zu können. Sowohl Laufwerke der Kategorie „Kein feststellbarer Fehler“ als auch aufbereitete Laufwerke erhalten dieses Etikett.

Medienzerstörung bei ausgefallenen Laufwerken

Laufwerke, die als nicht reparierbar eingestuft werden oder bei denen keine Reparatur angefordert wurde, werden verschrottet und dem Recycling zugeführt. Das Verschrotten beginnt mit der Zerstörung der gesamten Head-Disc-Assembly, wodurch das gesamte Medium zerstört wird. Die Medienzerstörung ist die ultimative Form der Bereinigung. Diese Tätigkeiten werden effizient und sicher ausgeführt, bevor das Laufwerk der Rohstoffrückgewinnung zugeführt wird.

Seagate Laufwerke mit Selbstverschlüsselung (SED)

Viele Laufwerke von Seagate sind mit Selbstverschlüsselung erhältlich. Alle auf das Medium geschriebenen Daten werden unter Verwendung eines einzigartigen Verschlüsselungscodes mit AES-128 oder AES-256 verschlüsselt. Keine zwei Laufwerke verfügen über denselben Code, sodass keine zwei SED-Laufwerke für dieselben Daten dieselben Datenmuster auf das Medium schreiben. Bei SED-Laufwerken führt der Befehl SECURITY ERASE im Modus „Enhanced Erase“ dazu, dass der SED-Verschlüsselungscode geändert wird, wodurch alle zuvor auf dem Gerät gespeicherten Daten umgehend unlesbar und nutzlos sind. Dies schließt alle neu zugeordneten Sektoren ein und sollte den Anforderungen gemäß NIST 800-88 genügen. Manche SED-Laufwerke von Seagate bieten überdies eine Zertifizierung gemäß FIPS 140-2 Level 2, wobei es sich um einen Standard der US-Regierung handelt. SED- und FIPS-SED-Laufwerke von Seagate werden immer neu verarbeitet.

Prozess zur Medienbereinigung während des Produktrücksendeverfahrens

Außer SATA gibt es noch folgende Schnittstellen: Außer SATA gibt es noch folgende Schnittstellen: SAS, SCSI und Fibre Channel

Ein interner Befehl zum sicheren Löschen ist in den SCSI-Spezifikationen des ANSI definiert. Der Befehl *Security Initialize* entspricht in Bezug auf die Funktion den ATA-Spezifikationen des ANSI. Darüber hinaus ist der Befehlssatz „Sanitize“ für viele Produkte verfügbar. Dieser stellt einen einzigen Befehl zur Offline-Bereinigung (Löschen) bereit, der bis zum Ende läuft.

Externe USB-Laufwerke

USB-Laufwerke enthalten automatisch auch ein SATA-Laufwerk. Eine kleine Leiterplatte überbrückt und verbindet die SATA- und die USB-Schnittstelle. Manche USB-Überbrückungskarten unterbinden den ATA-Befehl SECURITY ERASE, andere hingegen nicht. Aktuellere USB-Produkte von Seagate bieten über den ATA-Befehl SECURITY ERASE eine vollständige Medienbereinigung. Produkte, die den Befehl nicht zulassen, ermöglichen das vollständige blockweise Überschreiben des Mediums durch Nullen. Da USB-Produkte von Seagate über die volle native Maximalkapazität verfügen, entspricht dieses vollständige blockweise Überschreiben dem Befehl SECURITY ERASE im Modus „Normal Erase“ und sollte von daher den Anforderungen gemäß NIST 800-88 and ISO/IEC 27040 zum Bereinigen genügen.

Weitere Hilfsprogramme von Seagate (Überschreiben von Blöcken) NIST 800-88 Clear

Die im Vergleich zu NIST 800-88 und ISO/IEC 27040 etwas weniger sichere Stufe wird als *Löschen (Clearing)* bezeichnet. Hierbei werden ebenfalls alle Sektoren auf einer Festplatte überschrieben, und zwar so, wie es durch die Schnittstellenkapazitätsbefehle definiert ist. Mit anderen Worten, ein Laufwerk kann mit einer geringeren Speicherkapazität definiert werden, wodurch die Blöcke oberhalb der neuen Kapazität durch softwarebasierte Hilfsprogramme zum blockweisen Überschreiben nicht mehr erkannt werden. Obwohl es selten vorkommt, kann ein Laufwerk mit angepasster Speicherkapazität die Ursache dafür sein, dass sich NIST 800-88 und ISO/IEC 27040. voneinander unterscheiden. Ein weiterer Unterschied kann darin liegen, wie die Medienbereinigung durchgeführt wird. Das Löschen gemäß NIST 800-88 Clear wird in der Software blockweise verwaltet. Die einzelnen Blöcke werden durchgezählt und üblicherweise zeigt die Software einen Fortschrittsbalken an. Diese Vorgehensweise ist anfällig für ein Abfangen durch Schadsoftware. Die Bereinigungssoftware besteht aus einem einzigen Befehl, der das Laufwerk an der Schnittstelle in den Offline-Zustand versetzt und ausgeführt wird, bis der Vorgang abgeschlossen ist.

Das Hilfsprogramm SeaTools™ von Seagate mit verschiedenen Optionen zur Medienbereinigung ist auf der Seagate-Website unter www.seagate.com/support/seatools verfügbar.

DNR-Laufwerke werden versendet (Laufwerk nicht betriebsbereit)

Von Seagate wurden Standardvertragsklauseln (Kommissionsbeschluss 2010/87/EU oder eine Nachfolgeversion) festgelegt, die für die Unternehmenseinheiten von Seagate gelten, darunter auch die Transportunternehmen, die Seagate für den Versand von zurückgesendeten DNR-Laufwerken (Laufwerk nicht betriebsbereit) verwendet. Standardklauseln sind ein rechtmäßiger Übertragungsmechanismus für die extraterritoriale Übertragung von personenbezogenen Daten aus der Europäischen Union (EU) in Länder mit nicht adäquaten Bestimmungen außerhalb der Europäischen Union (EU).

Bitte beachten: Einige Länder, die nicht zum Europäischen Wirtschaftsraum (EWR) gehören, werden von der Europäischen Kommission als Länder mit einem angemessenen Datenschutzniveau gemäß den EWR-Standards anerkannt. Für diese Länder sind keine Standardvertragsklauseln erforderlich. Eine vollständige Liste und können hier nachgeschlagen werden.

Zusammenfassung

Wenn Sie ein Laufwerk an Seagate zurücksenden und Wert auf Datensicherheit legen, sollten Sie in Erwägung ziehen, die auf dem Laufwerk gespeicherten Daten vor dem Versand zu löschen. Ihr Versanddienstleister bietet eventuell Zustellbestätigungen an, die von Bedeutung sein können, wenn es um die alten Daten auf der Festplatte geht. Seagate übernimmt keine Verantwortung für Datenverluste von Anwendern. Sobald ein Produkt an Seagate zurückgesendet worden ist, gewährleisten wir die physische Sicherheit des Laufwerks. Des Weiteren führen wir gemäß unserer Verfahrensweise schnellstmöglich eine Medienbereinigung durch, um die noch auf dem Gerät gespeicherten Daten zu löschen.

seagate.com

AMERIKA Seagate Technology LLC 10200 South De Anza Boulevard, Cupertino, California 95014, USA, +1-408-658-1000
ASIEN/PAZIFIK Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapur 569877, 65-6485-3888
EUROPA, NAHER OSTEN UND AFRIKA Seagate Technology SAS 16–18, rue du Dôme, 92100 Boulogne-Billancourt, Frankreich, +33 1 4186 10 00