Wie Blancco Unternehmen und öffentlichen Einrichtungen bei der Einhaltung des NIST SP 800-88 Standards unterstützt

Was ist NIST SP 800-88?

Die Veröffentlichungsreihe NIST Special Publication (SP) 800 enthält „Leitlinien, Empfehlungen, technische Spezifikationen und Jahresberichte über die Cybersicherheitsaktivitäten des NIST."

Diese vom US-amerikanischen National Institute of Standards and Technology (NIST) herausgegebenen Veröffentlichungen sind auf die Bedürfnisse von US-Bundesbehörden ausgerichtet, werden aber auch von Organisationen in vielen anderen Branchen und Regionen auf der ganzen Welt herangezogen. Insbesondere der Standard NIST SP 800-88, gilt mittlerweile in vielen Branchen und Ländern weltweit als Referenz. Besonders zu erwähnen ist die Veröffentlichung NIST SP 800-88, mit der das NIST seiner im Federal Information Security Management Act (FISMA) von 2002 verankerten gesetzlichen Aufgabe nachgekommen ist, Standards und Leitlinien zur Informationssicherheit und zur Datenvernichtung/Datenlöschung zu erarbeiten.

Die 2014 aktualisierte Ausgabe – NIST SP 800-88 Rev. 1 – wurde zwar für die Bundesbehörden in den USA verfasst, wird aber auch international genutzt, und zwar nicht nur von öffentlichen Einrichtungen, sondern auch von Unternehmen und privaten Einrichtungen.

Blancco unterstützt Unternehmen zahlreicher Branchen und öffentliche Einrichtungen bei der Compliance mit NIST SP 800-88, Rev 1. Die Tabelle unten enthält konkrete Anwendungsbeispiele für die Umsetzung der NIST SP 800-88, Rev 1 und wie Blancco dabei helfen kann.

AUSZÜGE AUS DER VERÖFFENTLICHUNG	WIE BLANCCO HILFT
Clear, Purge und Destroy sind Methoden zur Datenvernichtung. Diese unterscheiden sich wie folgt: **Clear** basiert auf der Anwendung logischer Techniken zur Vernichtung von Daten in allen vom Nutzer adressierbaren Speicherorten. Dies bietet Schutz vor einfachen, nicht invasiven Verfahren zur Wiederherstellung von Daten. Die Anwendung von Clear erfolgt in der Regel über Standard-Lese- und Schreibbefehle auf dem Speichermedium. Dabei wird der Speicher entweder mit einem neuen Wert überschrieben oder das Gerät wird über das Menü auf die Werkseinstellungen zurückgesetzt (wenn ein Überschreiben nicht unterstützt wird). **Purge** basiert auf der Anwendung physischer oder logischer Techniken, um eine Wiederherstellung der Zieldaten auch mit modernsten Labortechniken unmöglich zu machen. **Destroy** vernichtet die Zieldaten so, dass eine Wiederherstellung auch mit modernsten Labortechniken nicht möglich ist, und führt dazu, dass das Speichermedium anschließend nicht länger zum Speichern von Daten genutzt werden kann. Nutzern dieses Leitfadens wird empfohlen, die Informationen zu kategorisieren, die Art des Speichermediums zu bewerten, auf dem die Informationen gespeichert sind, das Risiko für die Vertraulichkeit abzuschätzen und festzulegen, was künftig mit dem Speichermedium geschehen soll. Anschließend kann das Unternehmen bzw. die Einrichtung das oder die geeignete(n) Datenvernichtungsverfahren wählen. Die Auswahl der Vernichtungsart(en) sollte u. a. Kosten, Umweltbilanz usw. berücksichtigen. Die Entscheidung, die getroffen wird, sollte das Risiko für die Vertraulichkeit bestmöglich minimieren und allen anderen Vorgaben bestmöglich gerecht werden.	Blancco unterstützt mit seinen softwarebasierten Lösungen zur Datenlöschung die Datenvernichtung gemäß NIST Clear und NIST Purge. Blancco Drive Eraser ermöglicht die Purge- und Clear-Datenvernichtung sowohl für SSDs, einschließlich NVMes, als auch für HDDs in SANs, Servern, Laptops und Desktop-Rechnern. Darüber hinaus erfüllt Blancco LUN Eraser die Anforderungen von NIST Clear für die Datenvernichtung in LUNs. Macs mit T2-Chips und Chromebooks lassen sich ebenfalls gemäß NIST-Spezifikationen löschen. Jede Datenlöschung mit Blancco wird verifiziert und in Form eines auditfähigen und manipulationssicheren Löschzertifikats reportiert. Darüber hinaus bietet die softwarebasierte Datenlöschung von Blancco folgende weitere Vorteile: effizientere Abläufe, bei gleichzeitiger Kostensenkung und sciherung durch einen Datenlösch-Konzept Steuerung. geringere Kosten und verbesserte Steuerung der Datenvernichtung.
(in Bezug auf das kryptografische Löschen): Da es bei der partiellen Datenvernichtung schwierig ist, sicherzustellen, dass tatsächlich alle sensiblen Daten gelöscht werden, ist die vollständige Löschung eines Speichermediums gegenüber der partiellen Datenlöschung vorzuziehen.	Blancco Drive Eraser greift bei der Datenlöschung auf alle Bereiche einer Festplatte zu, auch auf neu zugeordnete Sektoren und versteckte Bereiche. Um den Anforderungen an die Datenlöschung beim Wear-Levelling gerecht zu werden, bietet Blancco Drive Eraser sowohl bei magnetischen Festplatten als auch bei SSDs die Möglichkeit des Over-Provisioning. Dies sorgt für eine vollständige Datenvernichtung, was durch einen manipulationssicheren Löschbericht bestätigt wird.
Die Datenlöschverfahren Purge (und Clear, sofern zutreffend) bieten Vorteile gegenüber der Vernichtung von Speichermedien, vor allem unter Berücksichtigung von Umweltaspekten, wenn Speichermedien wiederverwendet werden sollen (sei es innerhalb des Unternehmens/der Einrichtung oder um diese zu verkaufen oder zu spenden), wenn die Kosten für Speichermedien oder Speichergeräte berücksichtigt werden oder wenn die physische Vernichtung bestimmter Arten von Speichermedien Probleme bereitet.	Die Datenlöschlösungen von Blancco vernichten Daten unwiderruflich von einer Vielzahl unterschiedlicher Geräte an deren Lebensende, um diese anschließend ohne Angst vor Datenpannen wiederzuverwenden, einem neuen Nutzer zuzuweisen oder als Gebrauchtgeräte zu verkaufen. Dies ist nicht nur gut für die Umwelt, sondern spart auch Kosten. Darüber hinaus hat sich dies als Best Practice etabliert. So werden aktuell weltweit mehrere Hunderte Millionen IT-Assets sicher wiederverwendet.

blancco

AUSZÜGE AUS DER VERÖFFENTLICHUNG	WIE BLANCCO HILFT
Die Überprüfung der Durchführung des ausgewählten Datenlösch- und Vernichtungsverfahrens ist von entscheidender Bedeutung, um die Vertraulichkeit von Daten sicherzustellen. Dabei sollten zwei Arten der Überprüfung in Betracht gezogen werden. Bei der ersten wird nach jeder Datenlöschung eine Überprüfung durchgeführt … Im Anschluss an die Datenvernichtung sollte für jedes elektronische Speichermedium ein entsprechendes Zertifikat erstellt werden, das die Datenlöschung bescheinigt. Ein solches Zertifikat sollte in jedem Fall folgende Angaben enthalten: • Hersteller • Modell • Seriennummer • Intern zugewiesene Speichermedien- oder Gerätenummer (falls zutreffend) • Art des Speichermediums (d. h. magnetisch, Flash-Speicher, Hybrid usw.) • Herkunft des Speichermediums (d. h. Nutzer oder Computer von dem das Speichermedium stammt) • Vertraulichkeitsstufe vor der Datenvernichtung (optional) • Datenlöschverfahren (d. h. Clear, Purge, Destroy) • Methode (d. h. Entmagnetisieren, Überschreiben, blockweises Löschen, kryptografisches Löschen usw.) • Verwendetes Tool (einschließlich Version) • Überprüfungsmethode (d. h. vollständige Überprüfung, stichprobenartige Überprüfung usw.) • Vertraulichkeitsstufe nach der Datenlöschung (optional) • Verbleib des Speichermediums nach der Datenvernichtung (falls bekannt) • Für Datenvernichtung und Überprüfung: • Name der Person • Funktion der Person • Datum • Ort • Telefonnummer oder andere Kontaktinformationen • Unterschrift	Die Software von Blancco führt nach jedem Löschvorgang eine Überprüfung durch und erstellt anschließend ein manipulationssicheres und auditfähiges Löschzertifikat, das belegt, dass die Datenlöschung erfolgreich war. Die Löschzertifikate können um benutzerdefinierte Felder ergänzt werden und enthalten wichtige Angaben zum IT-Asset, zum verwendeten Löschstandard sowie eine sichere digitale Signatur, die die Anforderungen des NIST vollständig erfüllt. Die Berichte können jederzeit im Blancco Management Portal oder dem Vorgänger, der Blancco Management Console, gespeichert, verwaltet und abgerufen werden.
USB-Wechseldatenträger – einschließlich Pen-Drives, Thumb-Drives, Flash-Memory-Drives, Speichersticks usw. **Clear:** Überschreiben Sie das Speichermedium mittels intern zugelassener und getesteter Überschreibungstechnologien, -methoden oder -tools. Bei Clear sollten mindestens zwei Überschreibungsvorgänge durchgeführt werden – der erste Überschreibungsvorgang für das Muster und der zweite für das Komplement. Es können auch weitere Überschreibungsvorgänge durchgeführt werden.	Die Lösung Blancco Removable Media Eraser, die speziell für das sichere und unwiderrufliche Löschen von Daten von unterschiedlichen Arten von Wechseldatenträgern, einschließlich SD-Karten, Thumb-Drives, Flash-Memory-Drives usw., entwickelt wurde, erfüllt und übertrifft die Anforderungen der NIST SP 800-88, Rev. 1 und anderen Datenlöschstandards. Nach Überprüfung der Datenlöschung wird ein entsprechendes Löschzertifikat erstellt.

AUSZÜGE AUS DER VERÖFFENTLICHUNG	WIE BLANCCO HILFT
Mobilgeräte (wenn ein Gerät über Wechseldatenträger verfügt, sollten Sie – nachdem Sie diese auf Verschlüsselung überprüft und gegebenenfalls entschlüsselt haben – vor der Datenlöschung aus dem mobilen Gerät entfernen). Die Sonderveröffentlichung NIST SP 800-88, Rev 1 beschreibt im Weiteren die spezifischen Datenlöschsverfahren für alle großen Mobilgerätemarken bzw. die verwendeten Betriebssysteme, einschließlich Apple, Android, Windows und Blackberry. Die Datenlöschung auf Mobilgeräten sollte entweder mittels Zurücksetzen auf die Werkseinstellungen, Überschreiben oder kryptografischem Löschen erfolgen, um den Anforderungen an die Datenvernichtung nach Clear oder Purge gerecht zu werden. Alternativ (oder zusätzlich) können diese Geräte physisch vernichtet werden, wenn sie nicht wiederverwendet, recycelt oder verkauft werden können. Nach Möglichkeit sollte ein entsprechender Löschnachweis erbracht werden.	Blancco Mobile Diagnostics & Erasure löscht die Betriebssysteme iOS, Android, Windows Phone und BlackBerry sicher von Mobilgeräten und übertrifft dabei sogar die in der NIST SP 800-88, Rev 1 enthaltenen Anforderungen. **Blancco Mobile Diagnostics & Erasure bietet folgende Vorteile:** • Unterstützung verschiedener Löschstandards, einschließlich NIST SP 800-88, Rev. 1, kryptografisches Löschen, verifiziertes Zurücksetzen auf die Werkseinstellungen und andere Löschstandards für Mobilgeräte • Überprüfung, dass die Überschreibung erfolgreich war und tatsächlich alle Sektoren des Geräts beschrieben wurden • Garantie der unwiderruflichen Datenlöschung in Form eines manipulationssicheren Audit-Trails • Vollständige Automatisierung und Löschen hoher Stückzahlen Darüber hinaus bietet Blancco Mobile Diagnostics & Erasure Funktionen zum Löschen von SD-Karten und anderen Speichermedien in mobilen Geräten.
Kopierer, Drucker und Faxgeräte **Clear:** Führen Sie einen vollständigen Hersteller-Reset durch, um das IT-Gerät auf die Werkseinstellungen zurückzusetzen. **Purge:** Siehe Destroy. Die meisten IT-Geräte unterstützen lediglich die Datenlöschung nach der Clear-Methode (und nicht Purge). Einige IT-Geräte können über Funktionen zur Unterstützung der Purge-Methode verfügen, allerdings sind diese häufig auf die Hardware und die Firmware des Geräts beschränkt, weshalb das Purge-Verfahren mit Vorsicht angewendet werden sollte. Wenden Sie sich an den Gerätehersteller, um sich zu erkundigen, ob das Gerät Purge-fähig ist und datenspeicherspezifische Datenlöschverfahren (wie Überschreiben oder blockweises Löschen) oder kryptografisches Löschen unterstützt, um sicherzustellen, dass die Daten tatsächlich unwiderruflich vernichtet und nicht bloß die Dateiverweise gelöscht werden. IT-Geräte können über Wechseldatenträger verfügen. In dem Fall müssen bei dem Speichermedium unter Umständen datenträgerspezifische Datenlöschverfahren angewendet werden. **Destroy:** Zerkleinern, zermahlen, pulverisieren oder verbrennen Sie das Gerät in einer zugelassenen Verbrennungsanlage.	Blancco Drive Eraser unterstützt das Löschen von HDDs in Druckern, Faxgeräten und Kopierern gemäß NIST Purge, wenn dieser Löschstandard ausgewählt wird. Nach Überprüfung der erfolgreichen Datenlöschung wird ein entsprechendes Löschzertifikat erstellt. Blancco Removable Media Eraser wurde zum Löschen einer Vielzahl unterschiedlicher Wechseldatenträger entwickelt, darunter SD-Karten und andere Speichermedien in Druckern, Faxgeräten usw. Nach Überprüfung der erfolgreichen Datenlöschung wird ein entsprechendes Löschzertifikat erstellt.

blancco

AUSZÜGE AUS DER VERÖFFENTLICHUNG	WIE BLANCCO HILFT
ATA-Festplatten – einschließlich PATA, SATA, eSATA usw. **Clear:** Überschreiben Sie das Speichermedium mittels intern zugelassener und geprüfter Überschreibungstechnologien, -methoden oder -tools. Bei Clear sollte mindestens ein Überschreibungsvorgang mit einem festgelegten Datenwert erfolgen, z. B. alles Nullen. Optional können mehrere Überschreibungsvorgänge durchgeführt oder komplexere Datenwerte verwendet werden. Im Text werden vier Optionen zur Datenlöschung vorgestellt: der ATA-Befehlssatz „Sanitize Device" (für ein bis drei Überschreibungsvorgänge), der Befehl „SECURE ERASE UNIT", kryptografisches Löschen über die Opal-SSC- oder Enterprise-SSC-Schnittstelle (SSC = Security Subsystem Class) der Trusted Computing Group (TCG) oder die Entmagnetisierung.	Die Software Blanco Drive Eraser löscht sowohl lose Festplatten als auch HDDs in Laptops, PCs, Servern und anderen IT-Assets und unterstützt die automatisierte Datenvernichtung gemäß den Anforderungen von NIST Clear für alle Arten von Festplatten, einschließlich PATA, SATA, eSATA. **Wichtigste Vorteile von Blancco Drive Eraser** • Löschen von Daten von mehreren HDD-Festplatten gleichzeitig und unwiderruflich • Automatisiertes Löschen von Festplatten und Aufhebung von BIOS Freeze Locks • Lokale und Remote-Bereitstellung • Auflösung des RAID-Verbunds und Pass Through • Erkennung von False Positives bei internen Löschprozessen • Erstellung eines digital signierten Zertifikats als Nachweis der Datenlöschung für Audit- und Compliance-Zwecke • Erfüllt alle US-amerikanischen sowie internationale Datenschutzvorschriften und -richtlinien Blancco Drive Eraser unterstützt die Löschstandards NIST Purge und NIST Clear. Jeder Löschvorgang wird anschließend verifiziert und zertifiziert.
SCSI Solid State Drives (SSSDs) — einschließlich Parallel SCSI, Serial Attached SCSI (SAS), Fibre Channel, USB-Speicher (USB Attached Storage – UAS) und SCSI Express. *HINWEIS VON BLANCCO: Die NIST SP 800-88, Rev. 1 schlägt drei Methoden zur Datenvernichtung vor. Die erste ist Clear, bei der der Nutzer „das Speichermedium mittels intern zugelassener und getesteter Überschreibungstechnologien, -methoden oder -tools überschreibt. Das Clear-Verfahren sollte auf mindestens einem Überschreibungsvorgang mit einem festgelegten Datenwert basieren, z. B. alles Nullen. Alternativ können mehrere Überschreibungsvorgänge oder komplexere Datenwerte verwendet werden."* *Die zweite ist Purge mit den Löschbefehlen SCSI-Bereinigung, blockweises Löschen oder kryptografisches Löschen.* *Die dritte ist die physische Vernichtung.* *Ähnliche Optionen werden auch für NVMe-SSDs vorgestellt, wobei zum Erreichen des Purge-Standards NVM-spezifische Befehle erforderlich sind, wie unten aufgeführt:* "Jede Datenlöschung zum Erreichen des Clear- und des Purge-Standards muss überprüft werden. Beim kryptografischen Löschen muss die Überprüfung vor Anwendung möglicher zusätzlicher Datenvernichtungsverfahren, wie z. B. Clear oder Purge, erfolgen, um sicherzustellen, dass das kryptografische Löschen erfolgreich durchgeführt wurde... Das kryptografische Löschen bietet nicht für alle Verschlüsselungen die gemäß den Anforderungen von Purge erforderliche Sicherheit. Die Entscheidung, ob kryptografisches Löschen infrage kommt, hängt von der Überprüfung zuvor in diesem Leitfaden genannter Attribute ab. Die Entmagnetisierung eignet sich bei flashbasierten Speichermedien nicht zur Datenvernichtung."	Die Software Blanco Drive Eraser löscht sowohl lose Festplatten als auch SSDs in Laptops, PCs, Servern und anderen IT-Assets und nutzt dafür unser patentiertes Verfahren zum Löschen von SSDs. **Vorteile des patentierten Verfahrens von Blancco zum Löschen von SSDs** • Löschen auf Firmware-Ebene: Nutzung interner Löschbefehle zur Bereinigung von SSDs, einschließlich Block Erase (blockweises Löschen) und Cryptographic Erasure (kryptografisches Löschen) • Mehrfaches Überschreiben mit zufälligen Daten, Aufhebung von Freeze Locks und vollständige Überprüfung • Nutzung aller Sicherheitsprotokolle, die von SSDs unterstützt werden • Automatisiertes Verfahren zur Sicherstellung, dass alle Schritte in der richtigen Reihenfolge durchgeführt und beendet werden • Verhinderung von Kompression oder Deduplizierung durch den SSD-Controller • Überschreiben der vollständigen logischen Kapazität der SSD mit Zufallsdaten • Überschreiben mit absolut zufälligen/nicht komprimierbaren Daten anstatt mit sich wiederholenden Bitmustern • Mehrfachüberschreibung stellt sicher, dass die vollständige logische (nicht bloß die komprimierte) Kapazität der SSD überschrieben wird • Schnittstellenunabhängig und dadurch einsetzbar für alle gängigen SSD-Schnittstellen (einschließlich SATA, SAS, eMMC und NVMe) • Zugriff auf zentrale Sicherheitsfunktionen von SSDs, um eine vollständige und unumkehrbare Datenlöschung zu ermöglichen • Sicherstellung der Betriebsfähigkeit der Festplatte • Erkennung von Anomalien beim Löschvorgang • Eliminierung von False Positives • Absolut manipulationssicherer Audit-Trail durch digital signierten Löschnachweis

Bei der Entwicklung von Richtlinien zur Datenvernichtung, die den Best Practices für eine Vielzahl unterschiedlicher IT-Assets entsprechen, sollten Sie die oben genannten Empfehlungen berücksichtigen. Gleichzeitig sollten Sie unter der Prämisse eines bestmöglichen Schutzes von Branchen-, Kunden- und Mitarbeiter die Risiken und Chancen für Ihr Unternehmen sorgfältig abwägen.

Blancco gewährleistet nicht nur die Compliance mit den NIST-Standards, sondern unterstützt auch das Intelligent Business Routing (IBR), das die Einrichtung automatisierter und benutzerdefinierter Workflows ermöglicht. Die Vorteile sind mehr Effizienz und höhere Datensicherheit. Mit dem IBR können Sie intelligente Aktionen durchführen und die Löschstandards für verschiedene Gerätearten und Sicherheitsniveaus festlegen. Dadurch ist sichergestellt, dass Sie die Compliance-Anforderungen für alle Ihre IT-Assets nicht nur erfüllen, sondern übertreffen.

Warum Blancco?

Die Blancco Technology Group bietet Unternehmen sichere, datenschutzkonforme und automatisierte Lösungen zur Unterstützung des Übergangs zur Kreislaufwirtschaft. Wir unterstützen mit unseren Lösungen zur Datenlöschung Unternehmen und Einrichtungen in streng regulierten Branchen dabei, branchenspezifische Standards und gesetzliche Anforderungen an die Datenlöschung zu erfüllen (und häufig zu übertreffen). Bestätigt wird dies durch mehr als 13 Zulassungen und Zertifizierungen von Branchenverbänden, staatlichen Stellen und internationalen Organisationen, darunter die NATO, Common Criteria und ADISA.

Dank der vollständigen Datenvernichtung sind Unternehmen und öffentliche Einrichtungen in der Lage, ihre IT-Assets ohne Sorge vor Datenpannen sicher wiederzuverwenden und das Erreichen ihrer ökologischen Nachhaltigkeitsziele voranzutreiben. Mehr erfahren Sie unter Über uns.

Überzeugen Sie sich selbst, wie Sie mit der Datenvernichtungssoftware von Blancco Ihre IT-Assets gemäß den Vorgaben der NIST SP 800-88 löschen können, und fordern Sie Ihre kostenlose und individuelle Testversion an.

Kostenlose Testversion für Unternehmen

Kostenlose Testversion für ITADs