VERSION 20.11 (November 2020)

1. Bestandsaufnahme der zur Abholung angemeldeten Systeme

Die Erfassung der Geräte erfolgt beim Kunden vor Ort, mittels einer mobilen Datenerfassungsstation. Nach der vollständigen Erfassung werden die Systeme entweder in verschließbare Rollcontainer bzw. verplombbare Kisten verpackt oder auf einen verplombbaren LKW verladen.
Der Kunde erhält einen Nachweis mit allen erfassten Geräten incl. Bearbeitungsnummer, Seriennummer, Hersteller, Geräteklasse, Plombennummer.

Für weit entfernte Standorte mit einer geringen Anzahl an zurückzuführenden Geräten kann die CHG-MERIDIAN einen Paketdienstleister einbinden. Der Kunde erhält einen sicheren Transportbehälter (z.B. Rimova-Koffer), den er mit einem Schloss verschließen kann. Er übergibt den Behälter mit der Hardware dem Paketdienstleister. CHG-MERIDIAN erhält die Sendungsnummer und verfolgt den Transportweg des Behälters.

2. Transport der Geräte zum Technologie- und Servicezentrum

Die CHG-MERIDIAN AG setzt ausgewählte Spediteure (eine Auflistung findet sich unter https://www.chg-meridian.de/eraSURE_Subunternehmer) für den verplombten Transport mit GPS-Überwachung und den geschützten Transport der IT-Hardware in stoßsicheren Behältern und luftgefederten LKW. Die Geräte werden auf direktem Weg zum CHG Technologie- und Servicezentrum, Wasserweg 2, 64521 Groß-Gerau, Deutschland, transportiert.

3. Wareneingang und Erfassung der Geräte bei CHG-MERIDIAN

Nach Überprüfung der Plombennummer werden die Geräte direkt in den Security Bereich gebracht und mittels Soll/Ist-Vergleich als Lagereingang gebucht. Entpacken und erfassen der einzelnen Geräte auf Basis der Geräteseriennummer. Erfasste Geräte erhalten einen Barcode Label mit einer eindeutigen CHG Stock-ID und der Geräteseriennummer.

4. Vorbereitung des Löschvorgangs

Jeder Prüfplatz hat eine eigene Identifikationsnummer. Der Barcode des Gerätelabels und die Prüfplatznummer werden an einer Konsole per Barcodeleser eingelesen und angemeldet. Die Anmeldung erstellt einen Datenbankeintrag, der die Anmeldung autorisiert.

5. Optische Überprüfung der zu löschenden Geräte

Ein Mitarbeiter überprüft die Geräte, insoweit dies technisch möglich ist, öffnet er hierzu das Gehäuse. Dies erfolgt in Abhängigkeit der Gehäusebauart und dem üblichen Verwendungszweck. Verklebte, vernietete oder anderweitig verschlossene und/oder nicht für eine Öffnung vorgesehene, zugängliche Gehäuse bleiben ungeöffnet. Durch die Überprüfung wird soweit sichergestellt, dass sich keine nicht angeschlossenen, als Raid konfigurierte oder sonstige nicht erreichbare Datenträger im Gerät befinden.

Zudem werden CD- und Disketten-Laufwerke, Steckplätze für Sim und Speicherkarten auf entsprechende Medien überprüft.
Gefundene Medien werden, wenn nicht anders mit dem Auftraggeber vereinbart, sicher verwahrt und nach Ziffer 10 der Zerstörung zugeführt.

6. Booten und Netzwerkverbindung

Das zu bearbeitende Gerät (ausgenommen Drucksysteme) wird mittels eines geeigneten Bootmediums gestartet. Danach wird die Software gestartet, die den Verlauf des weiteren Prozesses steuert. Nur unter der Voraussetzung einer erfolgreichen Anmeldung wie in Ziffer 3 beschrieben, wird der Prozess fortgesetzt.
Andernfalls erfolgt eine detaillierte visuelle Fehlermeldung.

6.1. Vorqualifizierung von Drucksystemen

Bei Drucksystemen werden, sofern dies technisch möglich ist, die Statusseite(n) ausgedruckt und am Gerät für die weiteren Arbeitsschritte angebracht.
Das System überprüft das angemeldete Gerät und liest die (Kern-) Merkmale wie Hersteller, Modell, Seriennummer, Zählerstände aus. Zudem wird ermittelt, ob für dieses Gerät ein Zurücksetzen auf Werkseinstellungen möglich ist und ob dies bereits durchgeführt wurde.

6.2. Prüfung und Werksreset bei Drucksystemen

Das Gerät wird auf Werkseinstellungen zurückgesetzt und eventuell vorhandene Adressbücher oder Konfigurationen gelöscht. Dieser Vorgang wird überprüft und im System als Status festgehalten.
Ist dieses Zurücksetzen auf Werkseinstellungen und das dazugehörige Löschen von Adressbüchern und / oder Konfigurationen nicht erfolgreich möglich, muss der Löschvorgang als nicht erfolgreich angesehen werden und das System wird für die Zerstörung wie in Ziffer 10 beschrieben, vorgemerkt.

Sollte das Gerät über verbaute wechselbare / ausbaubare Speichermedien (mechanische Festplatte, Hybrid- oder SSD-Speicher) verfügen, werden diese ausgebaut. Diese erhalten ebenfalls einen Barcode Label mit einer eindeutigen CHG Stock-ID über die die Speichermedien und das Gerät eindeutig einander zugeordnet werden können. Das zu bearbeitende Speichermedium wird an einem speziellen Prüfcomputer angeschlossen. Danach wird die Software gestartet, die den Verlauf des weiteren Prozesses steuert. Nur unter der Voraussetzung einer erfolgreichen Anmeldung, wird der Prozess fortgesetzt; andernfalls erfolgt eine detaillierte visuelle Fehlermeldung.
Wurde die Festplatte durch den Hersteller oder Anwender mit einem gerätespezifischen Passwort versehen und ist dieses der CHG nicht bekannt bzw. ist nicht entfernbar, muss die Festplatte der Zerstörung, wie in Ziffer 10 aufgeführt, zugeführt werden.

7. Automatische Erkennung des Speichermedientyps

Eine Datenträgerprüfung ermittelt automatisch den Speichermedientyp. Die Datenträgerprüfung unterscheidet folgende Speichermedientypen: mechanische Festplatte, SSD-, Hybrid- und Flash-Speicher. Nach heutigem Stand der Technik sind Hybrid-Festplatten nicht sicher löschbar und werden der Zerstörung wie in Ziffer 10 aufgeführt zugeführt.

8. Löschmethodik

Der Auftraggeber entscheidet über den jeweiligen Schutzbedarf der Daten und somit der Form der Datenlöschung. Bei normalem und höherem Schutzbedarf können die Datenträger bzw. Geräte nach BSI IT-Grundschutz B1.15 einer Löschung unterzogen werden. Bei höchsten Schutzbedarf empfiehlt der BSI IT-Grundschutz die vollständige Zerstörung nach DIN 66399.

7.1 Normaler Schutzbedarf

Dem Steuerprogramm wird durch eine Datenbankabfrage mitgeteilt, welche Art der Löschung (mechanisch / SSD / Flash) durchgeführt werden muss und startet eine entsprechende Löschmethode.
Eine Konsole überwacht den Client während der Löschung. Alle Löschvorfälle (defekte Sektoren, Fortschrittsnachrichten, Löschprotokoll usw.) werden in einer Datenbank gespeichert.

7.2 Höherer Schutzbedarf

Der Löschvorgang erfolgt wie in Ziffer 7.1 aufgeführt, unter Berücksichtigung der nachfolgend beschriebenen Hinweise
Je nach Verschlüsselungsart und Implementierung von Löschbefehlen der SSD-, Hybrid oder Flash-Speicher durch die jeweiligen Hersteller bestehen nach erfolgter Löschung nachfolgend genannte Restrisiken einer Wiederherstellung von Daten oder Datenfragmenten:

- Wenn eine SSD keine Verschlüsselung aufweist, werden die an sie übergebenen Daten im Klartext in den Speichermodulen gespeichert. Löschbefehle in SSDs, die eine rückstandsfreie Löschung solcher Inhalte garantieren sollen, sind nicht immer ausreichend vertrauenswürdig. Somit muss damit gerechnet werden, dass SSDs auch nach Anwendung von ATA-Löschbefehlen noch Daten enthalten. Ein Angreifer könnte sich dies zunutze machen, indem er die Speichermodule aus dem Gerät entfernt und mit einer externen Elektronik ausliest.
- Bei der Hardwareverschlüsselung werden die Nutzdaten des Benutzers von der SSD selbst vor Ablage mit einem in der Hardware der SSD generierten und auf der SSD abgelegten privaten Schlüssel verschlüsselt. Die Löschung beginnt damit, dass der Schlüssel gelöscht wird. Daten, die nach einer Löschung auf der SSD verbleiben, sind dann für einen Angreifer wertlos, da er sie nur mit sehr hohem Aufwand entschlüsseln kann. Notwendig wäre ein Nachbau des Entschlüsselungsmechanismus der SSD und ein Brute-Force-Angriff zur Ermittlung des Schlüssels.
- Bei der Softwareverschlüsselung wird die Verschlüsselung von dem Gerät bewerkstelligt, in das das SSD eingebaut ist. Der Schlüssel wird vom Verschlüsselungsprogramm auf dem Gerät erzeugt und auch dort abgelegt. Daten, die nach einer Löschung auf der SSD verbleiben, könnten bei Kenntnis des Verschlüsselungsprogramms und des Schlüssels gelesen werden. Notwendig wäre hier, den Entschlüsselungsmechanismus des Geräteprogramms nachzubauen und den Schlüssel aus dem Rechnerspeicher zu lesen.

7.3 Höchster Schutzbedarf

Ist der höchste Schutzbedarf erforderlich ist in einer zusätzlichen Vereinbarung der Auftragnehmer mit der Zerstörung nach Ziffer 10 der entsprechenden Datenträger oder Systeme zu beauftragen.

9. Prüfung des Löschergebnisses

Nach der Löschung erfolgt eine automatische Überprüfung ob:

- ein Löschprotokoll vorhanden ist
- das Löschprotokoll fehlerfreie Löschvorgänge ausweist

Im Falle eines aufgetretenen Fehlers wird der Prozess nach Fehlerbehebung neu gestartet oder der Datenträger als „nicht sicher zu löschen“ aussortiert und gemäß Ziffer 10 weiter behandelt.

10. Dokumentation des Löschvorgangs

Das Löschprotokoll wird dem Auftraggeber nach erfolgreicher Löschung und Überprüfung gemäß Ziffer entsprechend Ziffer 11 zur Verfügung gestellt.
Es existiert mindestens ein Backup, das an einer anderen physikalischen Lokation vorgehalten wird.

11. Spezielle Behandlung nicht überschreibbarer Speichermedien und Drucksystemen

Speichermedien, die als „nicht sicher zu löschen“ aus dem Prozess hervorgehen oder im Prozess einen Fehler verursachen, werden von dem mit dem Gerät arbeitenden Mitarbeiter so behandelt (z.B. neu angeschlossen, formatiert, im Bios konfiguriert, in einen anderen PC eingebaut usw.), dass sie den Löschprozess, beginnend bei Ziffer 3, erfolgreich durchlaufen können.
Ist dies, z.B. aufgrund eines Hardwaredefektes oder sonstiger Zugriffsbeschränkungen, nicht möglich oder gemäß Vereinbarung so beauftragt wird das Speichermedium soweit möglich ausgebaut. Ist ein Ausbau nicht möglich, wird das komplette Gerät dem nachfolgenden Prozess unterzogen.

- Mechanischen Festplatten werden degaussert und im Nachgang nach Ablauf einer Wartefrist von 6 Wochen geschreddert.
- SSD, Hybrid und Flash Speichermedien werden in einer versiegelten Aluminiumbox verwahrt.
- Die so verwahrten Speichermedien werden in kurzen regelmäßigen Abständen von einem zertifizierten Entsorgungsfachbetrieb (nach DIN 66399 Schutzklasse 2, Sicherheitsstufe E4 geschreddert) und die Restpartikel thermisch vernichtet.
- Die Entsorgung erfolgt nach dem „Vier Augen“ Prinzip und wird von beiden Seiten mit Unterschrift bestätigt.

Eine Auflistung der derzeit eingesetzten Subunternehmer findet sich unter https://www.chg-meridian.de/eraSURE_Subunternehmer.
xxxxx
Auf Wunsch des Auftraggebers, können nicht löschbare Speichermedien auch zurückgegeben werden.

Alle physikalisch zu löschenden Speichermedien lagern im Security-Bereich. Sie werden nach dem Ausbauen im Lagersystem der CHG-MERIDIAN erfasst und erhalten ebenfalls eine Bearbeitungsnummer (Stock-ID). Diese wird mit der ursprünglichen Seriennummer des Gerätes verknüpft, so dass jederzeit eine Zuordnung möglich ist.

Sollte der Auftraggeber die Rücksendung „nicht sicher löschbarer Speichermedien wünschen, so werden die Speichermedien mit einer separaten Beauftragung in verplombten Transportbehältern an ihn zurückgeschickt. Der Auftraggeber erhält via eMail die Liste der zu retournierenden Speichermedien und die Plomben-Nummer. Der Versand zum Auftraggeber erfolgt mittels Paketdienst.

12. Abruf und Versand von Löschinformationen

Sofern der Auftragnehmer TESMA® nutzt, kann er die Löschinformationen jederzeit über TESMA® im „End of Life-Modul“ unter „Löschprotokollsuche“ abrufen, als PDF-Dokument anzeigen lassen und herunterladen. Sofern der Auftraggeber TESMA® nicht nutzt, wird CHG-MERIDIAN dem Auftragnehmer die Löschinformationen bzw. – Protokolle per eMail oder per Post mit CD zusenden. Der Dokumentenname ist grundsätzlich die Seriennummer des Gerätes, aus dem die Festplatte stammt.
Bei Bedarf kann ein Auftraggeber welcher TESMA® nutzt, in Einzelfällen auch nachträglich Protokolle via eMail oder CD anfordern. Die Daten werden auf dem File-Server der CHG-MERIDIAN gespeichert und sind jederzeit abrufbar. Die Löschberichte werden nach Durchführung der Löschungsroutine mindestens zwei Jahre aufbewahrt.