SEP

The Data Protection Company

Mit Real Life Erfahrungen aus dem SEP Support

protectionnow.

SEP sesam - Cyber Security

Schutz vor Ransomware, Compliance und andere Datensicherheits-relevante Mehrwerte mit SEP sesam Backup & Recorery

1 Einführung

Cyberangriffe treffen nicht nur große Unternehmen, sondern in letzter Zeit immer mehr kleine und mittelständische Betriebe. Die Angreifer suchen dabei immer nach Schwachstellen und Einfallpunkte in Netzwerken und Servern, um Ransomware oder auch Malware in die Systeme einzuschleusen. Dabei werden oft auch Daten gestohlen oder auch die Infrastruktur verschlüsselt. Der Fokus bei einem Ransomware Angriffes liegt dabei auch immer auf den Datenbeständen des Backups. Denn ist auch dieser verschlüsselt, steigt der Wert der Verschlüsselung und die Forderung nach einem höheren Lösegeld (Ransom).

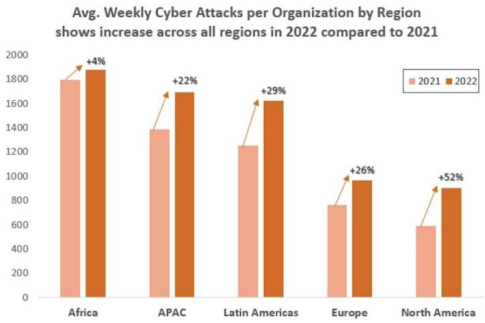
Den Daten der Security-Forscher von Check Point Research (CPR) zur Folge ist die Anzahl der Cyberangriffe in Deutschland 2022 im Vergleich zu 2021 um 27 Prozent angestiegen. Die Statistiken wurden zumeist von kleineren, agileren Cyberkriminellen und Ransomware-Banden vorangetrieben, die sich auf die Ausnutzung von Schwachstellen in Kollaborationstools konzentrierten, die in Arbeitsumgebungen von zu Hause ausgenutzt werden. In Deutschland zielten die Kriminellen zumeist auf

- Einzel-/Großhandelsunternehmen (+89 %)
- Einrichtungen der öffentlichen Verwaltung (+80 %)
- Bildungseinrichtungen (+60 %)

Die Forscher warnen zudem, dass der Reifegrad von KI-Technologien wie ChatGPT die Anzahl der Cyberangriffe im Jahr 2023 erhöhen könnte.

Die wichtigsten Statistiken zu den weltweiten Cyberangriffstrends 2022:

- Das weltweite Volumen von Cyberangriffen erreichte im 4. Quartal mit durchschnittlich 1168 wöchentlichen Angriffen pro Unternehmen ein Allzeithoch.
- Die Regionen Nordamerika (+52%), Lateinamerika (+29%) und Europa (+26%) verzeichneten 2022 den größten Anstieg an Cyberangriffen im Vergleich zu 2021.



[Steigerung der wöchentlich erfassten Cyberangriffe per Region in 2022 verglichen mit 2021, Quelle: Check Point", www.infopoint-security.de]

www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022

www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

2 Übersicht

Seit den 90er Jahren gibt es in der EU und Deutschland Bestrebungen, Schutz und Sicherheitsbestimmungen gesetzlich zu vereinheitlichen. Steigende und globale Angebote Daten in einer Cloud abzulegen oder vorzuhalten ist der Trend der Zeit. Cyberkriminalität allerdings auch!

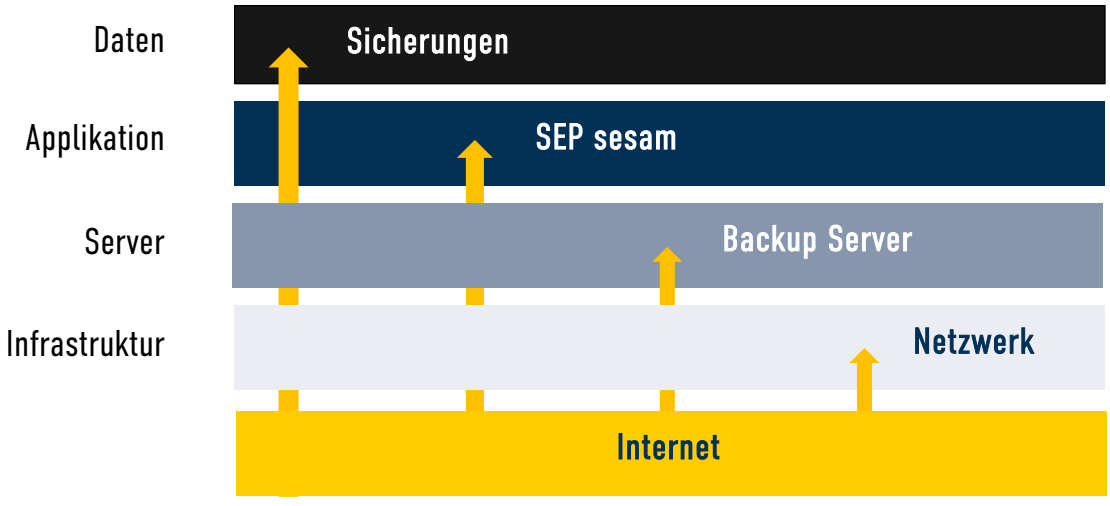
Es wurden seitdem eine Vielzahl von Datensicherheitsrelevanten Regularien entworfen, überarbeitet oder durch neue abgelöst.
Beispiele sind DSGVO, KRITIS, NIS2, PATRIOT Act und weitere.

SEP sesam bietet gute Möglichkeiten diesen Anforderungen gerecht zu werden und um die Sicherheit im Unternehmen enorm zu steigern. Auf diese Möglichkeiten wird in einem eigenen Kapitel detailliert eingegangen.

Hier die aufeinander aufsetzenden Schichten der Security, wie sie auch in der Kapitelstruktur dieses Dokuments zu finden sind:

Heutzutage in aller Munde sind Angriffe durch Ransomviren. Allerdings ist eine IT-Umgebung vielen verschiedenen Angriffsvektoren ausgesetzt, die auch auf unterschiedlichen Ebenen ansetzen. Ein Sicherheitskonzept eines Rechenzentrums gleicht einem Bollwerk aus verschiedensten nacheinander gestaffelten Fangnetzen. Ein schadhafter Angriff kann nur erfolgreich sein, wenn er alle Mauern überwindet.

Mögliche Schutzmechanismen der jeweiligen Ebenen sind z.B. eine Firewall auf Netzwerkebene, Linux als OS des Backup Servers, SEP sesam Credentials nicht im Active Directory halten und ein Immutability Storage für die Backupdaten.



Hier nur eine Auswahl der möglichen Angriffsvektoren:

- Ausführung oder Installation einer Malware über eine manipulierte Webseite (per E-Mail, Messenger oder SMS versendeter Link)
- Ausführung oder Installation einer Malware über einen manipulierten E-Mail-Anhang oder Internetdownload
- Unbefugte Verwendung von beispielsweise per Phishing beschafften Zugangsdaten
- Installation unerwünschter oder schädlicher Software über kompromittierte Software-Update-Verfahren (Supply-Chain-Angriff)
- Erzeugen von Speicherüberläufen und Ausführen von unberechtigtem Programmcode
- Unbefugter Zugang zu einem System über einen Zero-Day-Exploit (bisher unbekannte Schwachstelle)
- Massenhaftes Ausprobieren von Benutzernamen und Passwörtern (Brute-Force-Angriffe)
- Einschleusen von schädlicher oder unerwünschter Software über manipulierte Speichergeräte (zum Beispiel über USB-Sticks)
- Ausnutzen von Fehlern und Schwachstellen in Netzwerk- oder Authentifizierungsprotokollen für den unbefugten Zugang zu einem System
- Verschaffen von unbefugtem physischem Zugang zu einem IT-System
- Ausspähen von Zugangsdaten und anderen missbräuchlich nutzbaren Informationen per Social Engineering
- Umleiten von Webbrowser-Verkehr beispielsweise per Cross Site Scripting (XSS)

www.security-insider.de/was-ist-ein-angriffsvektor-a-1071184/

3 SEP sesam Funktionalitäten

3.1 Schutz der Backup Infrastruktur

Wie schon im Kapitel **Übersicht** angedeutet, findet der Schutz gegen Angreifer auf verschiedenen Ebenen statt.

Bzgl. der Infrastruktur müssen viele allgemeine Schutzmechanismen wie regelmäßige Updates, häufige Backups, Virenscanner, Firewall, sichere Passwörter und andere im Einsatz sein. Beispiel:

> **Netzwerksegmentierung**
>
> Eine generelle Unterteilung von produktiven und einem abgetrennten Backup Netzwerk stellt immer einen höheren Aufwand für Angreifer dar als eine einzige und flache Netzwerkstruktur.
>
> Wie eine Verkehrsampel den Straßenverkehr regelt, wird in einem segmentierten IT-Netzwerk auch den Verkehrstyp, die Quelle und das Ziel geregelt. Beispiele für eine Netzwerksegmentierung liefern VLAN, Software Defined Network (SDN) und auch Firewalls.

Aber auch die Vielzahl allgemeiner Schutzmechanismen können keinen 100%-igen Schutz bieten. Sind Viren z.B. zu aktuell, so gibt es dafür noch keine Erkennungsmuster und die Virenscanner greifen nicht.

Aus diesem Grund muss immer mit einem Durchbruch oder Direktangriff auf die nächste Ebene gerechnet werden. Dabei gilt es im nächsten Schritt den Backup Server abzusichern. Die Erfahrung zeigt, dass Ransomviren zunehmend versuchen zunächst den Backup Server zu infiltrieren (z.B. via Active Directory) und damit der Backupdaten habhaft zu werden. Ein Zerstören der Backupdaten verleiht dem Erpressungsversuch eine zusätzliche Wirksamkeit.

Für den Schutz des Backup Servers haben sich folgende Maßnahmen als wirkungsvoll erwiesen:

- Betriebssystem Linux statt Windows
- Betriebssystem des RDS unterschiedlich zum Backup Server
- Nur absolut notwendige Services aktivieren
- Services nur mit den notwendigen Rechten starten und root oder Administrator so gut es geht vermeiden
- Authentifizierung und Autorisierung nutzen
- Keine Integration mit Active Directory oder anderen Verzeichnisdiensten
- Den Backup Server, RDS und weitere Komponenten aus der Domäne nehmen
- Multi Factor Authorization (MFA), wo immer es möglich ist

wiki.sep.de/wiki/index.php/4_4_3_Beefalo:Ransomware_Protection_Best_Practices/de

3.2 Immutability

Auf den Schutz der Backupdaten wird in diesem Kapitel ausführlich eingegangen. In diesem Bereich bietet speziell SEP sesam eine Vielzahl sehr wirkungsvoller Maßnahmen, um Unveränderlichkeit (->Immutability) der Daten zu gewährleisten.

3.2.1 Bandtechnologie

Der wirksamste Schutz ist bekannterweise die schon sehr alte WORM-Technologie. Dadurch dass die Medien wie bei einer gebrannten CD/DVD aber immer nur einmal verwendbar sind, hat diese Technologie den nicht unerheblichen Nachteil eines erhöhten Medienbedarfs und damit verbundenen Kosten. WORM-Technologie ist damit nur zu Archivierungszwecke sinnvoll nutzbar, aber fürs tägliche Backup nicht zu gebrauchen.

Hierfür bietet sich als Lösung die ebenfalls schon alte Bandtechnologie an. Früher schon vielfach als Auslaufmodell deklariert, hat es gerade durch die stark zunehmenden Ransomviren wieder erheblich an Wert gewonnen. Das mit einer Auslagerung von Bändern leicht zu realisierende echte physikalische **Airgap**, war schon für viele attackierten SEP-Kunden die letzte Rettung.

Aufgrund unserer Erfahrung mit diesen Kundenszenarien empfehlen wir immer den Einsatz von Tape im Backupkonzept, d.h. um durch Migration mindestens eine weitere Kopie der Backupdaten zu erzeugen. In der Tat gibt es viele Kunden, die bisher ausschließlich auf Disk als Medium gesetzt haben, die nun wieder zur guten alten Bandbibliothek zurückkehren.

Bisher wurde noch kein Virus gefunden, der sich aufmacht, um ein ausgelagertes Band aus einer Bank oder einem Bunker zu holen.

SEP sesam hat viele Jahre Erfahrung mit der Bandtechnologie und unterstützt verschiedenste Hersteller, Laufwerkstypen und Bandformate. Auch Zusatzfunktionen wie Lesbarkeitstest, Sparepools, Umkopieren (z.B. LTO4 -> LTO8), Dateisuche, Laufwerksgruppen, Bibliotheks-Partitionierung, Laufwerks-Sharing, Anschlussprotokolle, Archivabgleich, Komprimierung, Verschlüsselung, Multiplexing, uvm. sind verfügbar. Dabei werden ausschließlich die im System vorhandenen Treiber verwendet.

wiki.sep.de/wiki/index.php/SEP_sesam_Storage_Hardware_Support_Matrix

wiki.sep.de/wiki/index.php/5_0_0:Tape_Management/de

3.2.2 SEP Immutable Storage

Um Angriffe auf Sicherungen zu verhindern, hat SEP den *SEP Immutable Storage (SiS)* eingeführt.

Die Idee hinter SiS ist, dass gespeicherte Daten während ihrer festgelegten Dauer (Lock Time) in ihrer ursprünglichen und unveränderten Form vollständig unverändert bleiben. Das bedeutet, dass Unternehmen sich schnell von einem Ransomware-Angriff erholen können, selbst wenn sie den Zugriff auf ihre Daten und Server verloren haben, indem sie gespeicherte unveränderte Datenkopien verwenden, um die gesamte Betriebsumgebung wiederherzustellen.

Der SiS ist im Grunde nicht nur eine Funktionalität, sondern beinhaltet ein gesamtes Konzept mit vielen Security-Empfehlungen mit dem Ziel maximale Sicherheit gegen Ransomware zu erreichen. Funktional setzt der SiS ein Linux voraus, wobei das Immutable Flag der erweiterten Dateiattribute verwendet wird.

Hierbei ist die Basis für den wirksamen Schutz gegen Ransomware das Zusammenspiel aus genau zwei Komponenten:

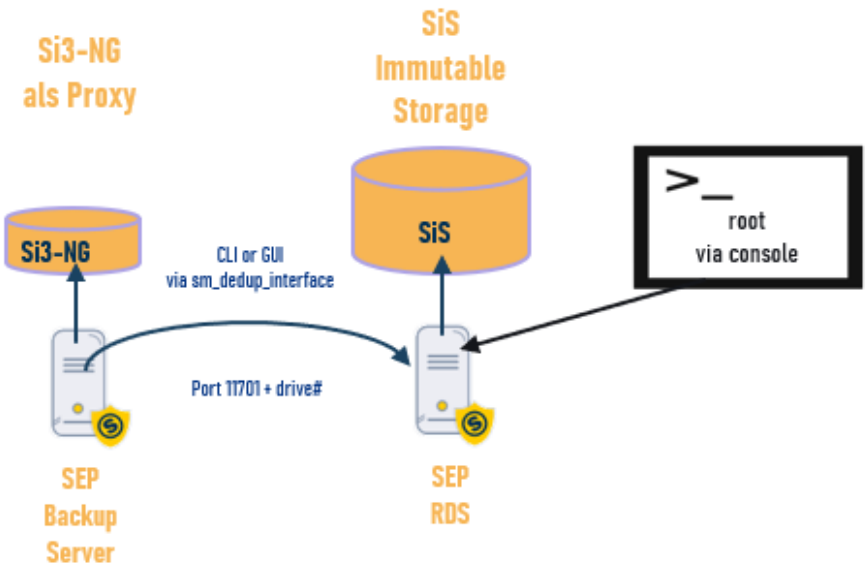
1. Die Administration und Konfiguration des Servers unter root erfolgt unter besonderem Zugangsschutz (nur Konsole)
2. Der Backup Server hat nur Zugriff über einen dedizierten Port mit sehr limitierten Berechtigungen. Solange die Lock Retention gültig ist, kann der Backup Server seine selbstgeschriebenen Daten weder löschen noch verändern. Das Schreiben neuer Daten oder Lesen vorhandener Daten zwecks Restore, Migration, Replikation, etc. ist jederzeit möglich

Damit schützt der SiS auch effektiv gegen eine feindliche Übernahme des Backup Servers selbst.

Folgende Voraussetzungen und Empfehlungen:

- Physikalischer Server
- Linux RDS: SLES15, RHEL8, Debian11
- ext4/XFS: Unterstützung des chattr Kommandos
- Gesicherter Server: kein ssh, Zugriff nur über lokale Konsole
- TCP/IP Verbindung
- Aufbewahrungszeiten: Mediapools > SiS Lock Time
- Korrekte Zeitsynchronisation (ntp)

Der SiS setzt die Verwendung der SEP sesam integrierten Software Deduplizierung Si3-NG voraus.



wiki.sep.de/wiki/index.php/5_0_0:SEP_Immutable_Storage_-_SiS/de

3.2.3 Blocky4sesam™

Backup ist ein Schlüsselbereich beim Schutz von Unternehmen vor Ransomware, da Cyber Attacken meist auch die Datensicherungen verschlüsseln oder zerstören. Mit Blocky4sesam™ besteht ein verlässlicher Schutz für die SEP sesam Backup Umgebung gegen Ransomware Attacken. Er ist sicher, vollständig integriert und ohne übertrieben hohen administrativen Aufwand für den Windows RDS (Remote Device Server) Server einzurichten.

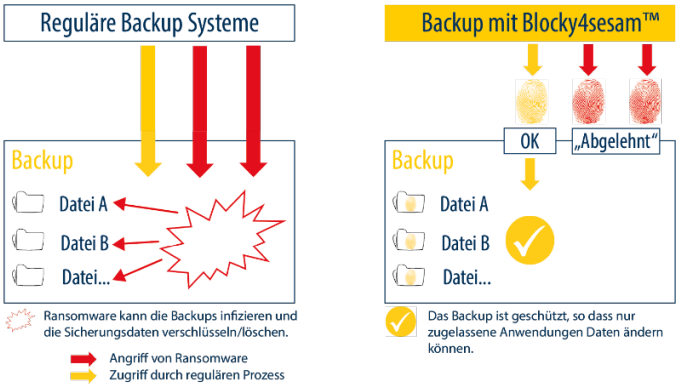
Der Ransomware Schutz der GRAU DATA ist eine bewährte Whitelisting-Technologie für Applikationen und wie sie auch vom BSI (Bundesamt für Sicherheit und Informationstechnologie) empfohlen wird.

Die Funktionalität ist dabei so ausgerichtet, dass es unmöglich ist, bereits abgespeicherte Sicherungsdaten durch fremde Prozesse zu verändern oder zu löschen. Um autorisierte Zugriffe zu identifizieren, verwendet Blocky4sesam™ den Fingerabdruck der Applikation. Unbefugte Zugriffe werden sofort protokolliert und dem Administrator gemeldet.

Nachdem der SEP sesam Prozess zur Whitelist hinzugefügt wurde, kann dieser jederzeit schreiben, lesen und löschen, wohingegen andere Applikationen bzw. Prozesse der Zugriff verweigert wird.

Eigenschaften von Blocky4sesam™:

- **Immutability für den SEP RDS**
  ⇨ Direct Attached Storage
- **Schützt komplette Windows Volumes/Partitions**
  ⇨ ReFS, NTFS
- **Applikations-Whitelist geschützter Zugriff**
  ⇨ Prüfen des Fingerabdrucks
- **Schreibzugriffe nur für den SEP sesam Prozess**
  ⇨ Schutz gegen fremde Applikationen
- **Setzt die integrierte SEP Software Deduplizierung voraus**
  ⇨ Si3-NG
- **Am Markt bekannt**
  ⇨ BlockyForVeeam, BlockyForTSM



Weitere Sicherheitsmaßnahmen des Schutzes der Komponenten wie bei SiS beschrieben, erhöhen auch hier die Sicherheit.

wiki.sep.de/wiki/index.php/5_0_0:Blocky4sesam_Configuration/de

3.2.4 S3 Object Lock

Beim Sichern von Daten im Cloud-Speicher S3 (Amazon Simple Storage Solution), Wasabi-Cloud-Speicher oder einer anderen S3-kompatiblen Cloud-Implementierung kann man die Objektsperrfunktion verwenden, um Daten vor Änderung oder Löschung zu schützen. Die Objektsperre ist eine Datenschutzfunktion, mit der die Unveränderlichkeit der Sicherungsobjekte anpasst werden kann. Die Aufbewahrungszeit kann auf einen festen Zeitraum oder auf unbestimmte Zeit eingestellt werden, und niemand kann ein Backup-Objekt ändern, löschen oder überschreiben, bis seine Aufbewahrungszeit abgelaufen ist.

SEP sesam verwendet die Objektaufbewahrung im Governance-Modus.
Im Governance-Modus kann der SEP sesam Backup-Benutzer die Aufbewahrungsfrist für ein Objekt hinzufügen oder verlängern, aber nicht verkürzen oder entfernen. Falls die Aufbewahrungsfrist falsch eingestellt ist (z. B. 100 Jahre), kann der Benutzer mit dem Benutzerrecht BypassGovernanceRetention diese Einstellung ändern.

wiki.sep.de/wiki/index.php/5_1_0:Configuring_Si3_NG_Deduplication_Store_with_Object_Lock/de

3.2.5 Andere Optionen der Immutability

Selbstverständlich gibt es nicht nur die in den bisherigen Kapiteln beschriebenen Möglichkeiten der Immutability. Die Bandbreite ist sehr groß, wobei nicht jede Option auch eine spezielle Implementierung der Backup Software erfordert.

Hier ein paar exemplarische Beispiele aus realen SEP-Kundenprojekten:

3.2.5.1 Safemode Snapshots

Viele Storagetypen bieten die Möglichkeit ReadOnly-Snapshots zu generieren. Diese können nicht verändert werden und die Lebensdauer kann ebenfalls vom Kunden festgelegt werden. Eine Backup Software wie SEP sesam kann diese Snapshots als zusätzliche Restorepunkte oder zur Migration nutzen.

Beispiele hierfür sind PureStorage FlashBlade oder Huawei OceanStor Dorado.

e.huawei.com/de/products/storage/ransomware

www.purestorage.com/solutions/data-protection/ransomware/safemode.html

3.2.5.2 HPE StoreOnce

Viele Dedup Appliances bieten die Möglichkeit ihre Daten mit einem Immutable Flag zu versehen. Auf der HPE StoreOnce liest SEP sesam dieses Flag mit dem Catalyst API aus und berücksichtigt den Status beim Zugriff auf die Daten.

support.hpe.com/hpesc/public/docDisplay?docId=sd00001027en_us&docLocale=en_US&page=catalyst_store_screens_properties.html

3.2.5.3 RDX

Eine weitere Möglichkeit mit dem SEP sesam ist nicht nur Bänder auszulagern, sondern eben auch mit Wechselplatten ein echtes Airgap zwecks Unveränderlichkeit für Disk Storage zu erzeugen. FAST LTA oder andere RDX-Hersteller sind hier am Markt mit dem Thema Cybersicherheit unterwegs.

wiki.sep.de/wiki/index.php/5_0_0:Configuring_Removable_Media/de

3.3 Virenscan

Es wird davon ausgegangen, dass die zu sichernden Daten bereits an der Quelle mit einem installierten aktuellen Virenscanner geprüft wurden.

Hinweis aus der Praxis:

Auf dem Backup Server kollidiert der Virenscanner oftmals mit der Backup Software und muss deaktiviert werden.

Mit der nächsten Version des SEP sesam wurde die Möglichkeit eines Viruschecks beim Restore integriert. Da der Zeitpunkt des Restores typischerweise einige Zeit nach dem Backup liegt, ist davon auszugehen, dass die dann anzuwendenden Virenpattern aktueller sind und damit auch bei mehr Virenarten greifen. Entdeckte infizierte Dateien werden gemeldet und können vom Restore exkludiert werden. Da der Scan erhebliche Performanceeinbußen mit sich bringt, ist er als optionale Funktion explizit zu aktivieren. Der Scan kann auf Linux und Windows Systemen gleichermaßen laufen.

Die Ikarus Scan Engine arbeitet mit hochentwickelter, leistungsstarker Scan-Technologie zur Analyse von bedrohlichen Inhalten aller Art. Das österreichische Produkt Ikarus dient als Algorithmus in vielen kommerziellen Virenscannern als Basis und ist somit als Quasi-Standard weit am Markt verbreitet.

www.ikarussecurity.com/

3.4 Verschlüsselung

SEP sesam bietet Datenverschlüsselungstypen auf verschiedenen Ebenen:

Sicherungsauftrag-Verschlüsselung für Sicherungssätze (im Sicherungsauftrag gesetzt), Si3-Verschlüsselung für den Si3 Deduplication Store und hardwarebasierte LTO-Verschlüsselung für LTO-Bandlaufwerke (Generation 4 und höher), die auf Medienpool-Ebene erfolgt. Für jede Verschlüsselung müssen Sie ein Verschlüsselungspasswort erstellen und speichern.

wiki.sep.de/wiki/index.php/4_4_3_Beefalo:Encryption_Support_Matrix/de

3.4.1 Allgemeine Hinweise

Ein Verschlüsslungsvirus verschlüsselt ALLE vorliegenden Daten, egal ob diese bereits verschlüsselt sind. Somit folgt:

Die Verschlüsselung von Backupdaten durch die Backup Software schützt zwar vor unbefugtem Zugriff, bietet aber keinerlei Schutz gegen die Erpressungsversuche der Ransomware.

SEP sesam hat zur eigenen Verwendung folgende Encryption-Technologien integriert. Die Versionen werden stetig aktualisiert, um die maximale Sicherheit der Verbindungen sicherzustellen:

- **openSSL 1.1.1**
- **TLS2**

3.4.2 Kommunikation

Zur Kommunikation des Backup Servers mit dem Client sind verschiedene auch verschlüsselte Protokolle verfügbar:

- **sm_ssh (SEP sesam** SSH **based control communication)**
- **ssh**

wiki.sep.de/wiki/index.php/5_0_0:Configuring_Clients/de

3.4.3 Transport

Zur Verschlüsselung der Datenübertragung bietet SEP sesam die Nutzung des https Protokolls als auch zertifikats-basierte Verbindungen an.

wiki.sep.de/wiki/index.php/Step_2:_Clients_4.4/de

wiki.sep.de/wiki/index.php/Configuring_SSL_Secured_Communication_for_SEP_sesam_Backup_Network/de

wiki.sep.de/wiki/index.php/5_0_0:How_to_Replace_the_REST_Server_HTTPS_Certificate_and_Private_Key/de

3.4.4 Data at rest (SW, HW, Cloud)

3.4.4.1 Software

SEP sesam kann Backupdaten mit modernen Algorithmen verschlüsseln (z.B. AES256).
Das Passwort wird auftragsspezifisch vergeben und kann entweder – ebenfalls verschlüsselt - in der Datenbank des SEP sesam oder extern gespeichert werden.

Zum Restore wird das Passwort entweder automatisch aus der Datenbank gelesen und angewendet oder es muss extern in eine Dialogbox eingegeben werden.

Das Passwort sollte möglichst sicher aufbewahrt und nicht vergessen werden, sonst kann nicht mehr auf die Daten zugegriffen. Wichtig ist zu wissen, dass auch die SEP als Hersteller die Daten nicht mehr lesen kann, da dies den eigentlichen Sicherheitszweck untergraben würde.

wiki.sep.de/wiki/index.php/4_4_3_Beefalo:Backup/de#Verschlüsselung

3.4.4.2 Si3 Deduplizierung

SEP sesam bietet Verschlüsselung für die Si3-Deduplizierung, um die Einhaltung der Datenschutzgesetze zu gewährleisten. Es kann einfach durch Angabe und Bestätigung des Verschlüsselungspassworts aktiviert werden. Hierbei wird jeder generierte Block nach erfolgter Komprimierung noch mit dem IDEA-Algorithmus verschlüsselt.

Wird ein falsches Passwort verwendet, beendet sich der Si3-Dienst (SDS) sofort nach Überprüfung des Passwortes.

Verschlüsselung bei der Si3 Replikation

Die Si3-Verschlüsselung ist im Lese-/Schreibverfahren des Dateisystems implementiert. Infolgedessen arbeitet die interne Verarbeitung mit den Rohdaten. Bei der Replikation eines verschlüsselten Datenspeichers werden die Daten nicht im verschlüsselten Zustand an den RDS übertragen. Die Daten werden zunächst auf dem Quell-Si3 entschlüsselt und dann auf dem Ziel-Si3 wieder verschlüsselt. Um eine absolute Sicherheit bei der Replikation von Quell-Si3 zum Ziel-Si3 zu gewährleisten, muss für die Kommunikation eine sichere VPN-Verbindung verwendet werden.

wiki.sep.de/wiki/index.php/Encrypting_Si3_NG_Deduplication_Store/de

3.4.4.3 Hardware

SEP sesam bietet native Unterstützung für die Verwaltung der hardwarebasierten LTO-Verschlüsselung, indem es die LTO-Verschlüsselung von Bandlaufwerken auf Medienpool-Ebene ermöglicht.

Bei der LTO-Verschlüsselung werden die Daten vom Server über den HBA-Controller zum Bandlaufwerk übertragen. Dann verschlüsselt und komprimiert das Bandlaufwerk die Daten, bevor es sie auf oder von Band schreibt (oder entschlüsselt, wenn es Daten liest).

Hierbei liegt der Vorteil in der Übertragung der Last vom Backup Server / RDS zum LTO-Laufwerk mit integriertem dediziertem Verschlüsselungschip, was einen erhebliche Performancegewinn ergibt. Insbesondere gilt das Äquivalent auch für die Komprimierung, die noch vor der Verschlüsselung auf dem Laufwerk erfolgen kann.

wiki.sep.de/wiki/index.php/LTO_Encryption/de

3.4.4.4 Cloud

Bei allen mit dem SEP sesam möglichen Cloudtypen als Backend Storage des Si3-NG Datenspeichers (S3, Azure Blob) wird automatisch immer eine verschlüsselte Verbindung aufgebaut. Dies ist insbesondere zur Übertragung über WAN essenziell. Die Daten selbst können gemäß Kapitel ‚Verschlüsselung' optional vor Übertragung verschlüsselt werden.

wiki.sep.de/wiki/index.php/5_0_0:Backup_to_S3_Cloud_Storage/de

3.5 Mandantenfähigkeit

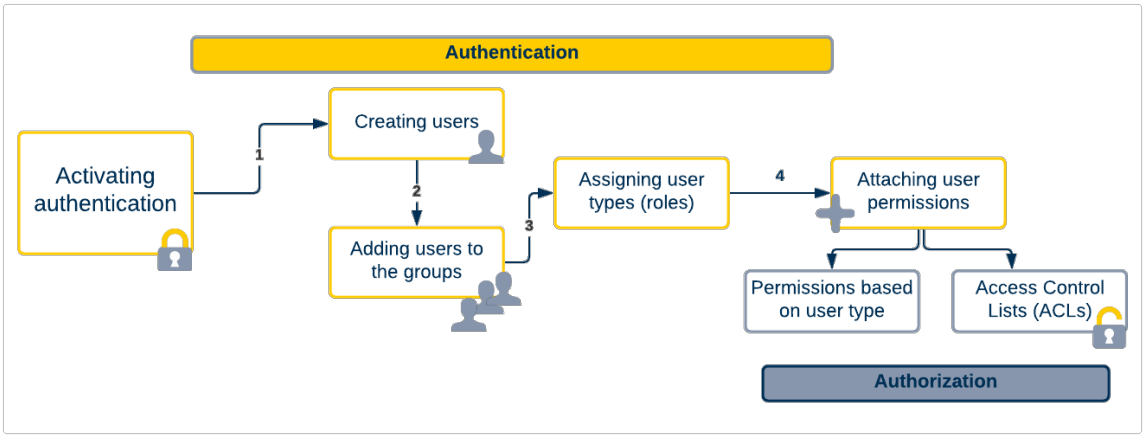
3.5.1 Authentifizierung

SEP sesam bietet verschiedene Methoden der Authentifizierung, um die funktionalen Nutzungsmöglichkeiten eines Benutzers einzuschränken:

- Policy-basierte Authentifizierung
- Datenbank-basierte Authentifizierung

Letztere kann in Kombination mit LDAP/AD Authentifizierung verwendet werden oder um die Zertifikat-basierten Authentifizierung zu ermöglichen.

Es kann jeweils nur eine Authentifizierungsmethode aktiv sein. Im Standardfall ist die Policy-basierte Authentifizierung aktiviert.



Die Policy-basierte Authentifizierung nutzt die Datei sm_java.policy zum Setzen der benötigten Benutzerrechte. Sie können dies entweder in der Policy-Datei editieren oder das GUI zum Setzen der Berechtigungen nutzen, indem sie Benutzertypen (Rollen) angeben.
SEP sesam bietet derzeit 5 Benutzertypen an. Die folgende Liste zeigt die verfügbaren Benutzertypen und ihre entsprechenden Rechte.

- **Superuser**
  Der einzige Benutzertyp mit voller Kontrolle über die SEP sesam Umgebung (früher Admin). Dieser Benutzertyp mit Superuser-Rechten wird automatisch ausschließlich dem Administrator-Benutzer zugewiesen, wenn die Datenbank-basierte Authentifizierung aktiviert ist. Wenn die Policy-basierte Authentifizierung aktiviert ist, wird dieser Benutzertyp mit Superuser-Rechten den Benutzern Administrator, root und sesam zugewiesen.
- **Administrator**
  Administratoren können das SEP sesam System administrieren und auf die GUI-Objekte zugreifen (außer Rechteverwaltung), wenn nicht eingeschränkt durch ACLs.

- **Operator**
  Operatoren können die gesamte Umgebung überwachen.
- **Backup**
  Sicherungsbenutzer können auf die GUI-Objekte zugreifen, die durch ACLs gewährt werden. Sie dürfen auch Sicherungen und Rücksicherungen starten.
- **Restore**
  Rücksicherungsbenutzer können auf die GUI-Objekte zugreifen, die durch ACLs gewährt werden. Sie dürfen nur Standard Rücksicherungen starten.

Beachten Sie, dass die angezeigten Komponenten und Funktionen in GUI und WebUI vom Benutzertyp abhängen.

3.5.2 Autorisierung

Zusätzlich zu den Standardberechtigungen (wie oben beschrieben), die auf dem ausgewählten Benutzertyp basieren, können Sie auch benutzerdefinierte Benutzerrollen festlegen, indem Sie ACLs konfigurieren, wenn Sie Superuser-Rechte haben.

ACLs ermöglichen Ihnen die Konfiguration von Berechtigungen für jeden Benutzer oder jede Gruppe mit fein abgestuften Zugriffsrechten für Standorte, Clients, Sicherungsaufträge (oder Gruppen), Medienpools und Zeitpläne. Wenn Sie beispielsweise einem bestimmten Sicherungsauftrag die Benutzerberechtigung Rücksichern zuweisen, kann dieser Benutzer die auftragsspezifische Sicherung starten.

wiki.sep.de/wiki/index.php/5_0_0:About_Authentication_and_Authorization/de

3.6 HPE Catalyst

Wenn die HPE StoreOnce DedupAppliance als Backupziel im Einsatz ist, gibt es verschiedene Möglichkeiten des Anschlusses, je nachdem ob SAN oder LAN. Im SAN ist der Anschluss als VTL möglich, was im SEP sesam als physikalische Band Library abgebildet wird. Im LAN kann es als nfs Storage oder via iSCSI gemountet werden. Dies sind alles offene Schnittstellen und bieten somit potenzielle Angriffsflächen.

Alternativ kann die StoreOnce sowohl im SAN als auch im LAN via dem Catalyst API angesprochen werden. Da es sich bei Catalyst um ein proprietäres Appliance-spezifisches API handelt, ist ein Angriff von außen erheblich schwieriger, was de facto ein zusätzlicher Schutz vor fremden Zugriffen darstellt.

https://www.hpe.com/psnow/doc/A00042003ENW.pdf?jumpid=in_lit-psnow-getpdf

3.7 Verifikation der Backupdaten

Eine Verifikation der Backupdaten wird von SEP sesam im Normalfall automatisch durchgeführt. Bei Backups (auch externe Backups), Restores und Migrationen wird eine Checksummenprüfung angewendet, um die einwandfreie Datenintegrität sicherzustellen.

Ebenso ist es möglich einen automatischen Verifikationsprozess zu aktivieren, der nach erfolgreichem Backup einen Restore in ein NULL Device startet. Sinnvollerweise wird dies als Follow-Up Event nach dem Backup konfiguriert.

https://wiki.sep.de/wiki/index.php/SBC_CLI/de

https://wiki.sep.de/wiki/index.php/Follow-up_Events/de#Sicherungssatz_nach_der_Sicherung_überprüfen

3.8 Reduktion der benötigten Ports

Anstatt für jeden Datenstrom einen eigenen Port zu öffnen (ftp Protokoll), kann durch Benutzung der Protokolle **http/https** die Datenübertragung auf einen einzigen Port beschränkt werden. Ihr Firewall Administrator wird glücklich sein, nur einzelne Ports statt ganze Portbereiche in seinem Heiligtum öffnen zu müssen. Offene Port Ranges untergraben den eigentlichen Zweck von Firewalls und erhöhen durch ihre Unbestimmtheit massiv die Unsicherheit. Aus diesem Grund ist bei SEP sesam der Default der Datenübertragung auf http gesetzt.

Default Ports (können für die Firewall angepasst werden):

http: **11000**
https: **11443**

wiki.sep.de/wiki/index.php/Topology_4.4/de

3.9 Remote Device Server (RDS)

SEP sesam Remote Device Server (RDS) ist eine Speicherverwaltungskomponente, die die Vorbereitung von Daten steuert, die für die Sicherung eines SEP sesam Client benötigt werden, und die die Sicherungsdaten auf die Sicherungsmedien schreibt. Während einer Rücksicherung findet der RDS die richtigen Sicherungssätze und sendet die Daten an den Client. So agiert der RDS in einer Backup-Infrastruktur als Media Server.

RDS besteht aus drei Komponenten: Sesam Transfer Protocol Server (STPD), Sesam Multiplex Stream Server (SMS) und SEP sesam Client (SBC) einschließlich Remote-Zugriff. Die Kontrolle über die Aufträge wird durch den SEP sesam Server gewährleistet. Für die Installation ist ein separates RDS-Installationspaket erhältlich.

Wenn das Netzwerk mehrere Standorte umfasst, kann man Speichergeräte standortübergreifend mit einem SEP sesam Server verwalten (z.B. weiter entfernt

stehende Bandbibliotheken oder SAN-Geräte). Wenn Ihre Infrastruktur jedoch mehrere Standorte umfasst, die eine schnelle Datenübertragung zum zentralen SEP sesam Server nicht ermöglichen, sollten ein Remote Device Server verwendet werden, um Daten auf lokal angeschlossenen Speicher an einem entfernten Standort zu sichern. RDS ermöglicht einen effizienten Datentransfer, entlastet den primären SEP sesam Server und nutzt die am Standort verfügbaren Speicherressourcen.

So fungiert der RDS an entfernten Standorten als Sicherungs-Server und kann entweder als Sicherungs-Proxy dienen, um Daten an den Hauptserver zu liefern oder Daten auf einem lokal angeschlossenen Storage zu speichern. Durch die Verwendung von RDS kann man viele entfernte Standorte einfach und bequem von einer zentralen Konsole aus verwalten.

In seiner Funktion ist der RDS damit eine wichtige Sicherheits-Komponente, um die Backup-Infrastruktur an vorgegebene Netzwerkstrukturen anzupassen und erhöht die Datensicherheit, wenn z.B. Backup Server und RDS durch eine Firewall getrennt und die Backupdaten nicht durch einen offenen Port in der Firewall geschleust werden müssen.

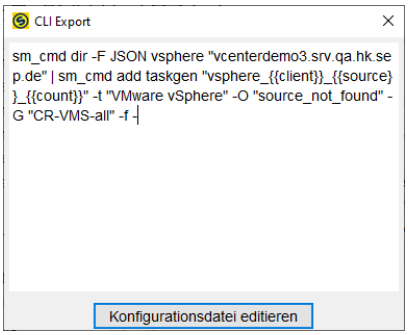
wiki.sep.de/wiki/index.php/5_0_0:How_to_create_a_Remote_Device_Server_(RDS)/de

3.10 Automatisches Erkennen von Sicherungsobjekten

Eine Erfahrung aus dem Support zeigt, dass in Krisensituation oftmals nicht der eigentliche Restore das Problem ist, sondern wichtige Daten einfach überhaupt nicht gesichert wurden. Änderungen der Dateninfrastruktur wurden versehentlich nicht im Backup nachgeführt. Und wo keine Sicherung vorhanden ist, kann auch nichts wiederhergestellt werden.

Genau für diese Situation kann SEP sesam Abhilfe schaffen.

Ein Algorithmus erkennt neue Sicherungsobjekte (VMs oder Datenbanken) und legt nach vordefinierten Regeln automatisch neue Sicherungsaufträge an, so dass die neuen Objekte sofort mitgesichert und nie wieder vergessen werden. Da die Regeln wie ein programmierbares Interface angelegt sind, bietet es vielfältige Definitionsmöglichkeiten. Neue VMs können z.B. nach Regular Expressions der VM-Namen oder Filtern der Metatags nach Produktiv- oder Test-VMs klassifiziert und automatisch Sicherungsaufträge in vordefinierten Auftragsgruppen oder Zeitplänen angelegt werden.



Dieses mächtige Werkzeug kann nicht nur auf alle vom SEP sesam unterstützte Hypervisor, sondern auch auf einige Datenbanken wie z.B. MS SQL angewendet werden.

Keine wichtige VM oder DB wird jemals mehr vergessen und die Vollständigkeit der Backups absolut sichergestellt.

wiki.sep.de/wiki/index.php/5_0_0:Automating_Backup_Process/de

3.11 Absichtliches Löschen von Backupdaten

Normalerweise ist das Löschen von Backupdaten über die in den Medienpools definierten Aufbewahrungsfristen geregelt und wird vom Backup Server automatisiert durchgeführt.

Ein absichtliches Löschen von Backupdaten hingegen kann in böser Absicht erfolgen, hier kann z.B. der Einsatz eines SEP Immutable Storage schützen. Es kann aber auch erforderlich sein, aufgrund von Regularien wie z.B. DSGVO bzgl. Löschen von Personendaten bei Ausscheiden eines Mitarbeiters. Dieser Vorgang ist als „Recht auf Vergessen“ (RTBF = Right to be forgotten) bekannt.

Beim Löschen von Backupdaten gilt es sehr genau auf die Granularität zu achten.

Für Bandsicherungen ist mit SEP sesam das Löschen eines kompletten Mediums möglich. Hier löscht SEP sesam ‚nur‘ die Einträge in der sesam Datenbank. Damit sind zwar die Daten selbst auf dem Band nicht gelöscht, aber ein Restore über die Backup Software nicht mehr möglich. Dies ist ausreichend, um den Vorgaben der DSGVO zu genügen.

Auf Disk Storage hingegen kann der Benutzer ein absichtliches Löschen auch von einzelnen Sicherungen herbeiführen, in dem er die EOL einer Sicherung z.B. auf ‚heute‘ setzt und die Bereinigung manuell anstößt.

wiki.sep.de/wiki/index.php/Tape_Management#expire

4 Konzeptelemente

4.1 Automatische Updates und Patches

Oftmals werden aktuelle Updates ignoriert oder verschoben. Für Angreifer ist das die beste Möglichkeit in ein System einzufallen, wenn Sicherheitsupdates entfallen. Die Systeme und Software auf dem neuesten Stand zu halten, stellt auch eine Wertgarantie dar.

SEP sesam bietet individuell konfigurierbare automatische Update Algorithmen, auch über das GUI.

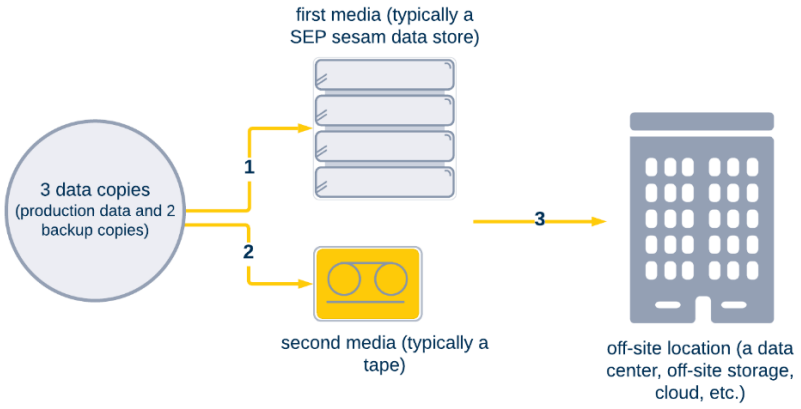
Ein automatisches Update aller Clients ist zwar sehr komfortabel, beinhaltet aber auch gewisse Risiken. So wäre ein Download der Updates oder Patches in ein Repository mit anschließendem isoliertem Test und geplantem Ausrollen in die Umgebung die sicherere Variante.

https://wiki.sep.de/wiki/index.php/4_4_3_Beefalo:Updating_SEP_sesam/de#mode

4.2 3-2-1 Backup Strategie

Ein Backupkonzept sollte mindestens
3 Kopien ihrer Daten gleichzeitig vorhalten (Original + Backup + Kopie), dabei
2 mindestens verschiedene Medientypen benutzen (z.B. Disk und Tape) und
1 Kopie an einem entfernten Ort ablegen.

Die 3-2-1 Regel ist die goldene Regel der Datensicherheit. Sie beschreibt die notwendigen Elemente eines Backupkonzepts, um ein Maximum an Sicherheit für Ihre Backupdaten zu erzeugen, denn auch diese sind vielfachen Angriffen von HW-Defekten über Ausfälle von ganzen Standorten bis hin zu Naturkatastrophen ausgesetzt.



wiki.sep.de/wiki/index.php/4_4_3_Beefalo:Backup_Strategy_Best_Practices/de

4.3 Disaster Recovery

Disaster Recovery ist ein wichtiges Thema, um das schnelle Wiederaufsetzen nach einem Totalausfall von einzelnen Clients, dem Backup Server, ganze Data Centers oder sogar ganzen Standorten nach Katastrophen sicherzustellen.

DR ist dabei nicht nur eine Funktionalität, sondern immer ein Konzept, d.h. eine ausgiebig zu testende Vorgangsbeschreibung. Nur durch intensives mehrmaliges Testen und Dokumentieren, kann ein reibungsloser Ablauf in der Krise garantiert werden. Beispiel: Man stockt im DR-Prozess, weil ein wichtiges Passwort für die benötigten Berechtigungen fehlt.

4.3.1 BSR für physikalische Server

4.3.1.1 Windows

SEP sesam BSR Pro ist eine schnelle und effiziente Desaster Recovery-Lösung für Windows-Systeme. Sie basiert auf O&O DiskImage. Diese Lösung ermöglicht es Ihnen, innerhalb kürzester Zeit ein voll funktionsfähiges Windows-System wiederherzustellen. Sie können Ihr System einfach über ein kleines GUI auf die gleiche oder eine andere (ungleiche) Hardware wiederherstellen. Dies gelingt, da zum Restore-Zeitpunkt fehlende Treiber nachinstalliert werden können.

wiki.sep.de/wiki/index.php/SEP_sesam_BSR_Pro_for_Windows

4.3.1.2 Linux

Das SEP Bare Metal Recovery Modul für Linux ist vollständig in die SEP sesam Client-Installation integriert, um eine schnelle und vollständige Systemwiederherstellung zu gewährleisten. Das Relax-and-Recover (ReaR) ist eine Linux BSR Wiederherstellungslösung (basierend auf GPL-Lizenz), die einfach einzurichten ist und keine Wartung benötigt. Im Falle einer Katastrophe kann das System entweder auf der gleichen Hardware oder auf kompatibler Ersatzhardware von einem externen Medium wie USB-Stick, DVD oder Netzboot des Image wiederhergestellt werden.

wiki.sep.de/wiki/index.php/Bare_Metal_Recovery_Linux

4.3.2 Disaster Recovery des Backup Servers

Um sich gegen Ausfälle abzusichern, wird ein tägliches Eigenbackup des Backup Servers dringend empfohlen. Auf diesem basiert die Möglichkeit des DR eines kompletten Backup Servers, da hierfür weder BSR Windows noch BSR Linux angewendet werden kann. Er restauriert sich selbst und seine Daten (DB, Lisfiles, etc.) aus den vorhandenen Backups. Dieser Vorgang ist ausführlich im SEP Wiki dokumentiert.

wiki.sep.de/wiki/index.php/SEP_sesam_Server_Disaster_Recovery/de

4.3.3 DR am Zweit-Standort

Hier geht es darum, Backupdaten eines Standorts (insbesondere VMs) an einem zweiten Standort vorzuhalten. Bei einem Ausfall des Standorts kann die Umgebung am zweiten Standort wieder hochgezogen werden und der Produktivbetrieb dort wieder aufgenommen werden. Performanceeinbußen im Betrieb werden temporär akzeptiert.

Je nach den Anforderungen und Vorgaben bzgl. RPO und RTO kann das DR sehr aufwändig werden. Es ist ein Konzept, das auf einer Vielzahl von verschiedensten technischen Umsetzungen basieren kann, die jeweils ihre eigenen Vor- und Nachteile

haben. Die Thematik DR allein würde mehr als ausreichend Inhalt für ein separates White Paper gegeben und kann daher hier nur kurz angerissen werden. Hier eine Auswahl der Möglichkeiten:

- Die Backupdaten können an den andern Standort verbracht werden. Entweder durch Spiegelung der Storage HW oder durch Nutzung der SEP Si3 Deduplizierung oder der Replikationsmöglichkeiten einer DedupAppliance wie z.B. HPE StoreOnce Catalyst Copy.
- Der Zweitstandort kann ein reiner Failover-Standort sein (andere Brandschutzzone) oder selbst ein produktives RZ in einer Außenstelle.
- Es kann dort einen zweiten produktiven Backup Sever haben, an dem die replizierten Backups importiert werden, nur ein Failover Backup Server im Standby Modus oder ein RDS, der im DR-Fall zum Backup Server mutiert.
- Die Metadaten des Backup Servers können mit rsync übertragen werden oder auf einem shared Storage liegen.
- Auch die Cloud als shared Storage für jede Art von Daten ist mittlerweile eine echte Option. Dabei ist je nach Cloud Anbieter sogar die Cloud selbst via IaaS oder Paas als DR Standort nutzbar.
- VMs können entweder bei Bedarf in eine zweite Virtualisierungsumgebung wiederhergestellt, via automatisierten Restore dauerhaft vorgehalten oder über Instant Recovery schnell produktiv gemacht werden.

Da ein ausgereiftes DR-Konzept mit seinen vielen Optionen auf fundierten Erfahrungen beruht, empfehlen wir hier jedem Kunden dringend den Bezug einer kostenpflichtigen Dienstleistung. Es lohnt sich!

https://www.computerweekly.com/de/definition/Disaster-Recovery-DR

4.4 Restores

4.4.1 Automatisierte Restores

In SEP sesam können Restoreaufträge gespeichert und als Termine in einen Zeitplan eingehängt werden. So kann man Restores automatisieren, um z.B. den Restore kritischer VMs sicherzustellen. Ebenso kann man den Restore auf ein Nulldevice machen, um nur die Lesbarkeit eines Backups zu verifizieren. Nach unserer Erfahrung kann ein automatisierter Restore eine Voraussetzung eines internen Methodenhandbuchs oder eine externe Vorgabe (z.B. BSI) sein.

wiki.sep.de/wiki/index.php/4_4_3_Beefalo:Scheduling_Restore/de

4.4.2 Ransomware Isolation

Um die IT-Umgebung gegen infizierte Daten abzusichern, ist in potenziellen Fällen ein Restore in eine isolierte Umgebung empfehlenswert. Insbesondere bei VMware ist der Restore in eine vom Netzwerk getrennte Sandbox sehr leicht mit dem SEP WebUI Restore Assistant oder dem GUI Restore Wizard möglich.

wiki.sep.de/wiki/index.php/5_0_0:VMware_Sandbox_Restore

4.5 Erfahrungen aus dem SEP Support

? **Wie verhalten sich die Kunden nach einem Virusbefall?**

! *Bei bisher allen bekannten Fällen wurde zuerst ein Ermittlungs- und Analyse Team aus externen Spezialisten engagiert, um u.a. den Zeitpunkt, Ausmaß und Verlauf der Infektion festzustellen. In allen Infektionsszenarien wurde aufgrund unzureichender Sicherheitsmaßnahmen auch die Backup-Infrastruktur mit angegriffen. Um diese wiederherzustellen, wurde daher - meist zeitgleich - die professionelle Hilfe der SEP als Dienstleistung beansprucht. Da oftmals die komplette Infrastruktur beim Kunden zusammengebrochen war, kam teilweise nur ein Einsatz vor Ort in Frage.*

? **Was waren die Grundlagen einer erfolgreichen Wiederherstellung?**

! *Um auf die Sicherungen der betroffenen Systeme zugreifen zu können, musste zuerst die Backupinfrastruktur selbst neu aufgebaut werden. Hierbei stellte sich leider oft heraus, dass der „Kopf" der Backup-Infrastruktur – der SEP sesam Server – vom Anwender unzureichend oder nur auf Ransomware ungeschützte Sicherungsmedien gesichert wurde. In jedem Fall lagen aber zumindest ein Teil der Sicherungen von kritischen Systemen auf Band, somit konnten diese auch ohne Sesam Eigensicherung mit etwas Zeitaufwand neu eingelesen werden. War eine Eigensicherung des Sesam Servers vorhanden, konnte sich Einiges an Zeit gespart werden. In keinem der Fälle konnte mehr auf Backups-on-Disk zugegriffen werden. Erweiterte, unver-schlüsselbare Sicherungsziele (Immutable Storage) waren leider in keinem der Fälle im Einsatz.*

? **Wie war der Ablauf eines erfolgreichen Restores?**

! *Sobald die Backupinfrastruktur zum bestmöglichen Stand wiederhergestellt war, wurde in der Regel immer gleich verfahren: Es wurde als erstes Rücksicherungsziel ein dediziertes, abgeschottetes System neu aufgesetzt („Sandbox" - Konzept). Mithilfe des vom Analyseteam identifizierten Infektionszeitpunkts, konnten nun Sicherungssätze, die vor der Infektion geschrieben wurden, auf das „Sandbox"-System zurückgesichert werden. Nach dem ein Sicherungssatz auf die Sandbox erfolgreich zurückgesichert wurde, wurde das System von einem - oder bevorzugterweise mehreren – Antivirenprogrammen gescanned und/oder gezielt auf Spuren des identifizierten Virus überprüft. Erst nach erfolgreicher Überprüfung wurde im letzten Schritt dann auf das eigentliche, produktive Zielsystem zurückgesichert.*

? **Was gibt es für Erkenntnisse nach einem solchen ernsten Vorfall?**

! *Ein durchgestandener Ransomvirusbefall erzeugt bei den Kunden praktisch immer eine dramatisch erhöhte Sensibilität für das Thema Datenschutz. Neue strategisch IT-Projekte werden gestartet - meist unter Beobachtung durch die Geschäftsleitung. Die IT-Sicherheits- und Backupkonzepte werden überarbeitet. Budgets für neue HW (z.B. weitere Backup Storage Möglichkeiten) sind plötzlich kein Thema mehr und werden umgehend freigegeben. Oftmals werden weitere externe IT Security Spezialisten hinzugezogen.*

? **Wie gut kann man sich im Ernstfall auf SEP sesam verlassen?**

! *Klare Aussage: „Noch nie hat ein SEP-Kunde nach einem Ransomware-Angriff keine Daten mehr für einen erfolgreichen Restore zur Verfügung gehabt!“*

5 Regularien

5.1 Deutschland und EU

5.1.1 Gesetzliche Aufbewahrungsvorschriften

Jedes Unternehmen muss sich bzgl. der Aufbewahrung seiner Daten an die allgemein gültigen Gesetze seines Staates richten. Diese klassifizieren die Daten nach verschiedenen Kriterien wie z.B. Art der Daten, Branche des Unternehmens, Datenformat (analog/digital), etc. Aber nicht nur die Aufbewahrung ist geregelt, in vielen Fällen ist auch die Löschung der Daten vorgegeben.

ⓘ www.bundesarchiv.de/DE/Content/Downloads/Anbieten/sgv-aufbewfr-aufbewahrungsvorschriften-und-aufbewahrungsfristen-fuer-schriftgut-in-obersten-bundesbehoerden.pdf?__blob=publicationFile

5.1.2 Datenschutzgrundverordnung (DSGVO/GDPR)

Die Datenschutz-Grundverordnung (DSGVO) von 2016 (Inkrafttreten) bzw. 2018 (Anwendung) vereinheitlicht die Regeln zur Verarbeitung personenbezogener Daten durch Unternehmen, Behörden und Vereine, die innerhalb der Europäischen Union einen Sitz haben. Die englische Entsprechung des Begriffs ist "General Data Protection Regulation (GDPR)", die offizielle Bezeichnung "Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG". Der Umgang mit Kunden- und Mitarbeiterdaten, Daten von Bürgern etc. wird im Zusammenhang mit dem Datenschutz in elf Kapiteln mit insgesamt 99 Artikeln geklärt.

Die Verordnung gilt in allen Mitgliedstaaten und hat Auswirkungen auf weitere Länder und ihre privaten und öffentlichen Einrichtungen. Es sind technische, wirtschaftliche, gesellschaftliche und individuelle Aspekte vorhanden. Es herrschen technikneutrale

Regelungen vor, die soziale Medien und künstliche Intelligenz zu erfassen vermögen. Das Recht auf Vergessenwerden wird formuliert, also auf eine Löschung von (Zugängen zu) persönlichen Informationen, ebenso ein Recht auf Informationsfreiheit (Informationszugangsfreiheit) und Datenübertragbarkeit (Datenportabilität). Verankert sind Prinzipien wie Privacy by Design (der Schutz der Daten wird schon bei der Gestaltung der Systeme berücksichtigt) und Privacy by Default (der Schutz der Daten ist der Normalfall, wobei der Benutzer ihn unter Umständen selbst durch Anpassung der Dienste oder Geräte abschwächen kann).

Für die im Gesetz unter Art. 83 Abs. 5 DSGVO aufgelisteten, besonders gravierenden Verstöße beträgt der Bußgeldrahmen bis zu 20 Millionen Euro oder im Fall eines Unternehmens bis zu 4% des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr, je nachdem, welcher Wert der höhere ist.

dsgvo-gesetz.de/

www.dsgvo-portal.de/dsgvo-bussgeld-datenbank/

5.1.3 No-Spy Regel des BMI

Als No-Spy-Klausel oder auch eine No-Spy-Garantie [5] wird eine Eigenerklärung im Vergabeverfahren und eine Vertragsklausel in öffentlichen Aufträgen bezeichnet, durch die Vertragspartner der öffentlichen Hand versichern, dass sie rechtlich nicht verpflichtet sind, vertrauliche Informationen an ausländische Geheimdienste oder Sicherheitsbehörden weiterzugeben. Eigenerklärung und Vertragsklausel verhindern zwar die Datenweitergabe nicht, erleichtern der öffentlichen Hand jedoch die Beweisführung und die Beendigung des Vertrags im Fall des Verstoßes.

Die Anforderung der Eigenerklärung und die Ergänzung von Vertragsmustern für öffentliche Aufträge um die No-Spy-Klausel hatte das Bundesministerium des Innern mit Erlass vom 30. April 2014 für öffentliche Aufträge des Bundes angewiesen [6]. Die Bundesländer schlossen sich dieser Forderung bei Neuverträgen mit IT-Unternehmen sukzessive an, Anlass dafür waren der NSA-Skandal und die Enthüllungen von Edward Snowden, die den Abfluss von Informationen über IT-Partner der öffentlichen Hand möglich erscheinen ließen.

SEP erfüllt die No-Spy Regel des BMI.

www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2014/no-spy-erlass.pdf

5.1.4 KRITIS

„Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden."

KRITIS-Definition der Bundesressorts

Sektoren und wer kann KRITIS sein:

- Informationstechnik & Telekommunikation
- Gesundheit
- Energie
- Wasser
- Ernährung
- Finanz- und Versicherungswesen
- Transport und Verkehr
- Siedlungsabfall und Entsorgung
- Staat/ Verwaltung
- Medien & Kultur
- Unternehmen im besonderen öffentlichen Interesse
- Digitale Infrastruktur

Bundesamt für Sicherheit in der Informationstechnik

Alle Organisationen aus diesen Sektoren zählen unabhängig von ihrer Größe zu den Kritischen Infrastrukturen (KRITIS). Dies bedingt unter anderem erhöhte Anforderungen an den Datenschutz und somit auch an die Backup Software.

SEP hat eine Vielzahl von Kunden aus dem KRITIS-Bereich und damit große Erfahrung mit den speziellen Herausforderungen und den notwendigen Konzepten dieses Kundenklientels.

www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html

5.1.5 NIS2

EU NIS2 ist der europäische Rahmen für Betreiber einer kritischen Infrastruktur. Diese Richtlinie legt die Cyber Security Mindestanforderungen fest, die ab 2024 diese Unternehmen in einer der 18 Sektoren in die Pflicht nimmt. Das gilt für Unternehmen mit mehr als 50 Mitarbeitern und 10 Mio. Euro Umsatz.

NIS2 löst die bisherige NIS-Direktive ab.

www.bsi.bund.de/DE/Themen/KRITIS-und-regulierte-Unternehmen/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html

5.1.6 Cyber Resilience Act

Die Europäische Kommission hat im September 2022 den Entwurf eines Cyber Resilience Act (CRA) vorgelegt, mit dem sie die Cybersicherheit von Produkten, die miteinander oder

mit dem Internet verbunden werden können, verbessern will. Diese Produkte werden von Unternehmen hergestellt und an Endkunden vertrieben.

digital-strategy.ec.europa.eu/de/library/cyber-resilience-act

5.2 Abkommen mit USA

5.2.1 SCHREMS 2

Praktische Auswirkungen der Rechtsprechung des EuGH auf den internationalen Datentransfer (Rechtssache C-311/18 „Schrems II“):

Der Europäische Gerichtshof hat mit dem Urteil klargestellt, dass personenbezogene Daten von EU-Bürgern nur an Drittländer übermittelt werden dürfen, wenn sie in diesem Drittland einen im Wesentlichen gleichwertigen Schutz genießen wie in der EU. Für die USA hat er ein solches angemessenes Schutzniveau verneint.

www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-Internationales/Auswirkungen-Schrems-II-Urteil.html

5.2.2 Safe Harbour / EU-US Privacy Shield (expired)

Zum Zwecke des Datenschutzes am Ziel – schwerpunktmäßig von privaten Daten – wurde der Datenaustausch zwischen Staaten schon immer durch EU Abkommen geregelt.
Insbesondere mit USA, deren Unternehmen und deren weltweit angebotenen Services und Produkte gab es separate Abkommen. Aber insbesondere die in USA per Gesetz geregelten Zugriffsmöglichkeiten (PATRIOT Act/CLOUD Act) sorgen dafür, dass die Vereinbarungen immer wieder außer Kraft gesetzt wurden und den internationalen IT-Markt verunsicherten.

Nach der Entscheidung im Jahr 2015, das Safe-Harbour Abkommen für ungültig zu erklären und dem gescheiterten EU-U.S.-Privacy Shield im Jahr 2020 haben sich die Präsidentin der Europäischen Kommission Ursula von der Leyen und der Präsident der USA Joe Biden auf einen neuen transatlantischen Datenschutzrahmen (EU-U.S. Data Privacy Framework) geeinigt. Am 13. Dezember 2022 hat die Europäische Kommission den Entwurf einer Angemessenheitsentscheidung für das geplante EU-U.S. Data Privacy Framework bekannt gegeben. Mit diesem Datenschutzrahmen soll wieder eine Nutzung von Tracking-/ Analytic- und Marketing-Tools aus den USA problemlos zulässig sein. Daneben soll auch der Rückgriff auf Standardvertragsklauseln der Vergangenheit angehören. Doch bis dahin übertragen Sie personenbezogene Daten rechtswidrig in die USA, wenn Sie U.S.-Tools nutzen, die eben solche Daten in die USA senden.

ec.europa.eu/commission/presscorner/detail/de/QANDA_22_7632

5.2.3 PATRIOT Act

Der USA PATRIOT Act ist ein US-amerikanisches Bundesgesetz, das am 26. Oktober 2001 vom Kongress im Zuge des Krieges gegen den Terrorismus verabschiedet wurde. Es war eine direkte Reaktion auf die Terroranschläge am 11. September 2001.

USA PATRIOT Act steht als Backronym für
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001,
deutsch etwa: „Gesetz zur Einigung und Stärkung Amerikas durch Bereitstellung geeigneter Instrumente, um Terrorismus aufzuhalten und zu verhindern".

Teile des Gesetzes sind am 1. Juni 2015 abgelaufen und wurden tags darauf am 2. Juni 2015 durch die Bestimmungen des USA Freedom Act ersetzt.

Die Bestimmungen des PATRIOT Act erlauben US-Behörden wie dem FBI, der NSA oder der CIA nicht nur den Zugriff ohne richterliche Anordnung auf die Server von US-Unternehmen. Auch ausländische Tochterfirmen sind nach dem US-Gesetz verpflichtet, Zugriff auf ihre Server zu gewähren; selbst dann, wenn lokale Gesetze dies untersagen.

www.heise.de/newsticker/meldung/Freedom-Act-NSA-und-FBI-duerfen-weiter-Internetdaten-auch-von-US-Buergern-sammeln-4722646.html

5.2.4 CLOUD Act

2018 wurde das Patriot Act vom damaligen US-Präsident Donald Trump um das CLOUD Act (***Clarifying Lawful Overseas Use of Data Act***) erweitert.

Das Gesetz verpflichtet amerikanische Internet-Firmen und IT-Dienstleister, US-Behörden auch dann Zugriff auf gespeicherte Daten zu gewährleisten, wenn die Speicherung nicht in den USA erfolgt.

Umgekehrt können über diesen Weg auch ausländische Firmen Zugriff auf Daten erhalten, die von US-Konzernen im Ausland gespeichert werden. Infolge des Gesetzes sollen bilaterale Abkommen ausgearbeitet werden, die es ausländischen Behörden ermöglichen, ihre Anfragen direkt an die Konzerne zu stellen. Hiermit würde eine gerichtliche Kontrolle bei einer Abfrage außen vor bleiben, was zu Kritik durch Datenschützer geführt hat.

Das Gesetz wurde eingeführt, nachdem US-Behörden in verschiedenen Fällen Probleme hatten, an im US-Ausland gespeicherte Daten zu gelangen. So konnten Unternehmen bis vor Verabschiedung des Gesetzes sich darauf berufen, dass ein Durchsuchungsbeschluss nur in den USA Geltung hat. Internet-Firmen und IT-Dienstleistern kann nach dem Gesetz verboten werden, ihre Benutzer über eine solche heimliche Abfrage von Benutzerdaten zu informieren.

Die US-Datenschutzorganisation *Electronic Frontier Foundation* wertete den CLOUD Act als „gefährliches Gesetz". Das Gesetz sei „nichts Geringeres als ein Eingriff in die Privatsphäre und eine Beschneidung der Grundrechte".

www.heise.de/newsticker/meldung/CLOUD-Act-US-Gesetz-fuer-internationalen-Datenzugriff-und-schutz-verabschiedet-4003330.html

5.3 SEP sesam „Made in Germany“

In Deutschland gelten nicht nur die EU-Gesetze, sondern auch bekanntermaßen die strengsten Datenschutzregeln überhaupt.

SEP sesam als Produkt eines mittelständischen deutschen Software-Unternehmens kann somit gleich mehrere Vorteile vorweisen, die die Einhaltung gesetzlicher Regelungen wie DSGVO oder die No-Spy-Regel erheblich vereinfachen. Hierbei geht es nicht nur darum, dass der Staat keinerlei Zugriff auf die Daten hat (no backdoors), sondern auch im Supportfall bei Fernwartung und Versandt von Logfiles der Verbleib der Daten und Informationen in der EU sichergestellt ist. Dies wird von der SEP mit Unterschrift auf einem Zertifikat bestätigt.

SEP sesam ist optimal geeignet, um die Vorschriften aller Institutionen (wie Staat der EU) voll zu erfüllen!

www.sep.de/de/loesungen/sep-security/

6 Zusammenfassung

Mit dem umfangreichen Schutz in SEP sesam können Daten auch nach unentdeckten Cyberangriffen wiederhergestellt werden.

SEP ist heute eine der robustesten und skalierbarsten Backup-Lösungen auf dem Markt. Ein zentrales Management zur Verwaltung aller Backup-Agenten und Server, ob lokal oder remote, macht es zur perfekten Lösung und lässt sich von kleinen bis zu größeren Unternehmensumgebungen einsetzen.

Viele integrierte Agenten und Funktionalitäten als auch die große Supportmatrix lassen keinen Wunsch offen.

Erleben Sie die Vorteile, die SEP zu bieten hat. Unsere Kontaktdaten und eine 30-Tage-Testlizenz inkl. Demo-Support finden Sie auf unserer Homepage

www.sep.de

Kontakt

+49 8024 463310

sales@sep.de

SEP AG
Konrad-Zuse-Straße 5
83607 Holzkirchen
Deutschland

Jetzt 30-Tage-Vollversion testen!

Die SEP sesam 30-Tage-Vollversion beeinhaltet alle Funktionen zur optimalen Datensicherung & Wiederherstellung, sowie einen persönlichen Demo Support.

SEP sesam Support Matrix

SEP sesam unterstützt ein großes Portfolio an Betriebssystemen, Datenbanken, Virtualisierungsplattformen, Anwendungen und Hardware Snapshots.

Version: 21.04.2023 erstellt von Klaus Riehm