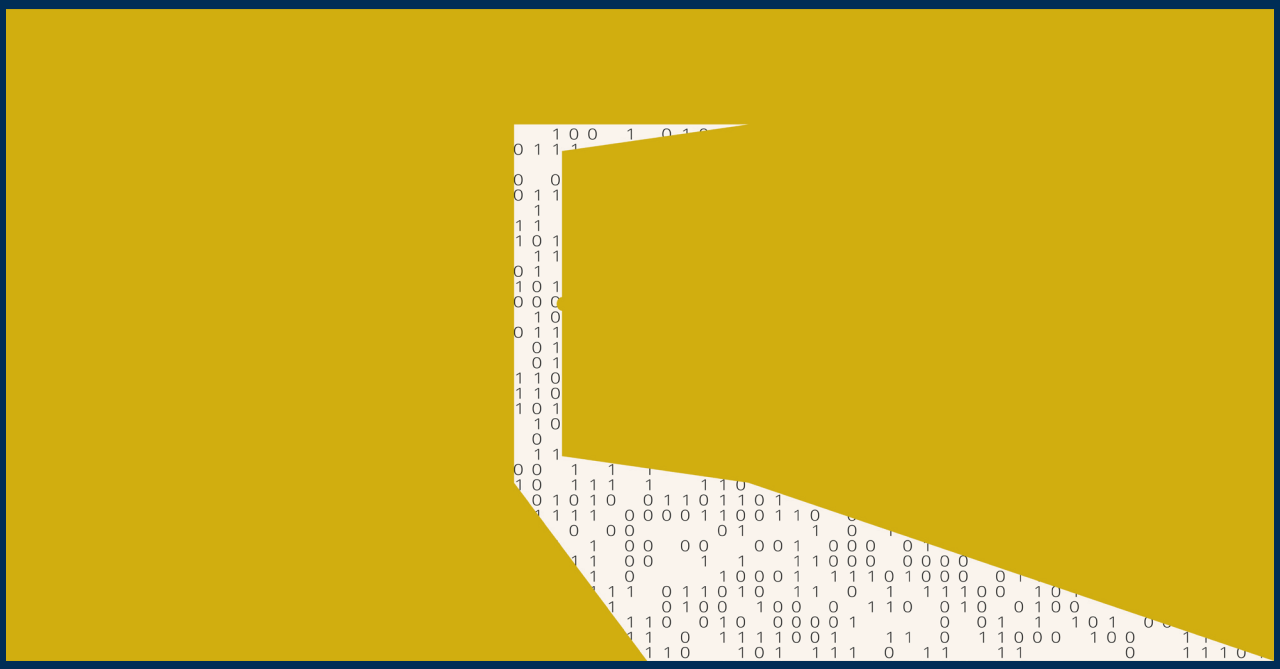
SEP
Hybrid Backup

SEP SECURITY – Sicherheit macht den Unterschied

SEP SECURITY - SEP stellt das Thema Sicherheit an erste Stelle und deckt diverse Sicherheitsaspekte ab, die andere Anbieter nicht bieten können, da SEP in Deutschland/Europa die Software entwickelt sowie Service und Support von Deutschland aus erbringt.

Inhaltsverzeichnis



Risiko Backdoors

Backdoors sind Hintertüren, die in Software eingebaut werden und es ermöglichen unter Umgehung der Sicherheitsmechanismen der Software (und auch Hardware) Zugriff zu erlangen.
Mit diesen Backdoors können Daten eingesehen werden und/oder verändert werden. Gerade US-Produkte sind davon betroffen, denn der US-Geheimdienst NSA gibt den US Herstellern über bestimmte Regularien wie z.B. „Patriot Act" vor in die Produkte Backdoors einzubauen.
China nutzt diese angeblich ebenfalls, was zeigt, dass jede Sicherheitslücke kann von jedem – auch von Hackern - genutzt werden und weitreichende Sicherheitsprobleme mit sich bringen kann. (Quelle: Golem.de, „Wer China sagt, muss auch USA sagen", 4. Dezember 2020, https://www.golem.de/news/juniper-backdoors-wer-china-sagt-muss-auch-usa-sagen-2012-152593.html).

Die NSA lehnte es ab, zu bestätigen, wie ihre Richtlinien bezüglich des speziellen Zugriffs auf kommerzielle Produkte geändert wurden. „Bei der NSA ist es gängige Praxis, Prozesse ständig zu bewerten, um die besten Praktiken zu identifizieren und zu bestimmen", sagte Anne Neuberger, Head of NSA Cybersecurity Directorate.

Zudem haben die Regierungen Großbritanniens, der USA, Australiens, Kanadas, Neuseelands, Indiens und Japans eine Erklärung unterzeichnet, in der sie Technologieunternehmen auffordern, eine Hintertür für verschlüsselte Dienste bereitzustellen. (Quelle: Independent, „US SECURITY AGENCY DOES NOT DENY STILL USING SECRET BACKDOORS IN TECH DEVICES", 29. Oktober 2020).

Keine Backdoors bei SEP!

Als europäischer/deutscher Hersteller garantiert SEP die Freiheit von Backdoors und Datenschutzkonformität. Für Geheimdienste gibt es keine geheimen Hintertüren und somit auch keine Sicherheitslücken, die auch von anderen genutzt werden könnten.

No-Spy Klausel des BMI

– der Beauftragte der Bundesregierung für Informationstechnologie in Abstimmung mit dem IT-Verband Bitkom, d.h. „dass die von ihm zu liefernde Standardsoftware* frei von Funktionen ist, die die Integrität, Vertraulichkeit und Verfügbarkeit der Standardsoftware*, anderer Soft- und/oder Hardware oder von Daten gefährden und den Vertraulichkeits- oder Sicherheitsinteressen des Auftraggebers zuwiderlaufen durch

- Funktionen zum unerwünschten Absetzen/Ausleiten von Daten,
- Funktionen zur unerwünschten Veränderung/Manipulation von Daten oder der Ablauflogik oder
- Funktionen zum unerwünschten Einleiten von Daten oder unerwünschte Funktionserweiterungen.“ (Ziffer 2.3 der EVB-IT Überlassung Typ A-AGB; Ergänzenden Vertragsbedingungen für die Beschaffung von IT-Leistungen (EVB-IT); Besonderen Vertragsbedingungen für die Beschaffung von DV-Anlagen und Geräten (BVB))

SEP erfüllt die No-Spy Klausel!

SEP
Hybrid Backup

BSI-Konformität (Bundesamt für Sicherheit in der Informationstechnik):

„Das Ziel der technischen Richtlinien des BSI (BSI-TR) ist die Verbreitung von angemessenen IT-Sicherheitsstandards. Technische Richtlinien richten sich daher in der Regel an alle, die mit dem Aufbau oder der Absicherung von IT-Systemen zu tun haben. Sie ergänzen die technischen Prüfvorschriften des BSI und liefern Kriterien und Methoden für Konformitätsprüfungen sowohl der Interoperabilität von IT-Sicherheitskomponenten als auch der umgesetzten IT-Sicherheitsanforderungen:“ (Quelle: BSI, Technische Richtlinien).

Verschlüsselung gehört zu den zentralen technischen Elementen. So ist z.B. bei der hocheffizienten und patentierten Si3-Deduplizierung und -Replikation eine Verschlüsselung möglich. Die sichere Datenaufbewahrung wird durch die Verschlüsselung des SEP Si3-DedupStores eingeführt. Nach Zerlegen des Datenstroms in Blöcke und der Komprimierung jedes Blocks, lässt sich nun jeder einzelne Block durch einen Key, der auftragsspezifisch zu definieren ist, verschlüsseln. Zur Wiederherstellung der Daten kann der Key in der Datenbank des Backupservers hinterlegt werden oder der Dateneigentümer muss eine Rücksicherung mit seinem persönlichen Key autorisieren. Diese Verschlüsselung garantiert BSI-Konformität.

DSGVO und Compliance Anforderungen:

die Hybrid Backup Lösung SEP sesam bietet die technische Sicherheit zur Umsetzung der DSGVO mit einer Vielzahl an technischen Mechanismen (siehe „Datenschutzgrundverordnung, NIS-Richtlinie der EU & das IT-Sicherheitsgesetz, Rechtsanwalt und Fachanwalt für IT-Recht Dr. Jens Bücking, S. 13 ff)

Daten und Logfiles bleiben in der EU/Deutschland:

SEP entwickelt die Lösung und leistet den Support von Deutschland aus. Daten und Logfiles gelangen im Unterstützungsfalle nicht außerhalb von Deutschland und auch die Dateneinsicht z.B. bei TeamViewer-Sessions durch den SEP-Support bleibt komplett in Deutschland, so dass auch hier Compliance und DSGVO-Anforderungen gewahrt bleiben. Ebenfalls arbeitet SEP mit deutschen und europäischen MSP-Partnern zusammen, so dass auch hier keine Probleme wegen dem abgekündigten Privacy Shield Abkommen entstehen, d.h. die Daten landen nicht in den USA oder anderen nicht-europäischen Ländern. Denn auch bei der Beauftragung eines MSPs ist der Auftraggeber verantwortlich, dass die Richtlinien zur Datenhaltung (DSGVO, etc.) eingehalten werden und die Verantwortung kann nicht auf den MSP abgegeben werden.

SEP Hybrid Backup

SEP SECURITY-Schlüsselemente:

- Verschlüsselung der Backups auf Sicherungsmedien (Band, DataStore, Si3 DedupStore)
- Verschlüsselung des Datenstromes
- Verschlüsselung der Kommunikation
- Externes Passwort für Rücksicherung nach 4-Augen-Prinzip
- Effizientes Disaster Recovery für Windows und Linux
- Medienbruch: Unterstützung von Offline- und WORM Medien
- Herstellerkonforme Datensicherung und –wiederherstellung
- Sicherung der Daten auf verschiedenen Ebenen möglich (z.B. auf Hypervisor- und Applikationsebene)
- Standortübergreifende Datensicherung
- Automatische Migration bzw. Kopie von Sicherungsdaten auf unterschiedliche Sicherungsmedien
- Volle Unterstützung von Open-Source Betriebssystemen auf Backupclient- und Backupserver-Seite
- Gesetzeskonforme Sicherung aller Unternehmensdaten
- Gewährt die Netzwerksicherheit in Firewall-Umgebungen durch Einschränken der Kommunikation und des Datentransports auf wenige, dedizierte Ports
- Geplanter und automatischer Restore auf Stand-by-Systeme zum Verifizieren der Backups (kann auch für Audits verwendet bzw. dokumentiert werden)
- Disaster Recovery Tests im laufenden Betrieb inklusive Reporting bei physikalischen Umgebungen (Voraussetzung ist ein Test-Target Server) und in virtuellen Umgebungen
- Frei von Spyware

SEP
Hybrid Backup

„Software Made in Germany“ Gütesiegel vom Bundesverband IT-Mittelstand (BITMi e.V.):

„Made in Germany” – drei Worte, die international als Synonym für höchste Qualität und begeisterte Kunden stehen. Die Gründe hierfür? Durchdachtes Design, praxisbewährte Lösungen, ausgereifte Produktionsverfahren, stetige, begeisternde Innovationen, kompetenter Kundenservice, um nur einige zu nennen. SEP sesam Hybrid Backup-/Disaster Recovery-Lösungen bieten dies und schützen plattformübergreifend, heterogene IT-Umgebungen on-premise & in der Cloud, von physischen bis zu virtuellen Umgebungen, Betriebssystemen, Datenbanken & Anwendungen – bis hin zum gesamten SAP Solution Stack.

mehr erfahren

Persönlicher Kontakt 1.

SEP AG
Konrad-Zuse-Straße 5
83607 Holzkirchen
Deutschland
www.sep.de

+49 8024 46331-0

sales@sep.de

Jetzt 30-Tage Vollversion testen! 2.

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

SEP sesam Support Matrix 3.

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