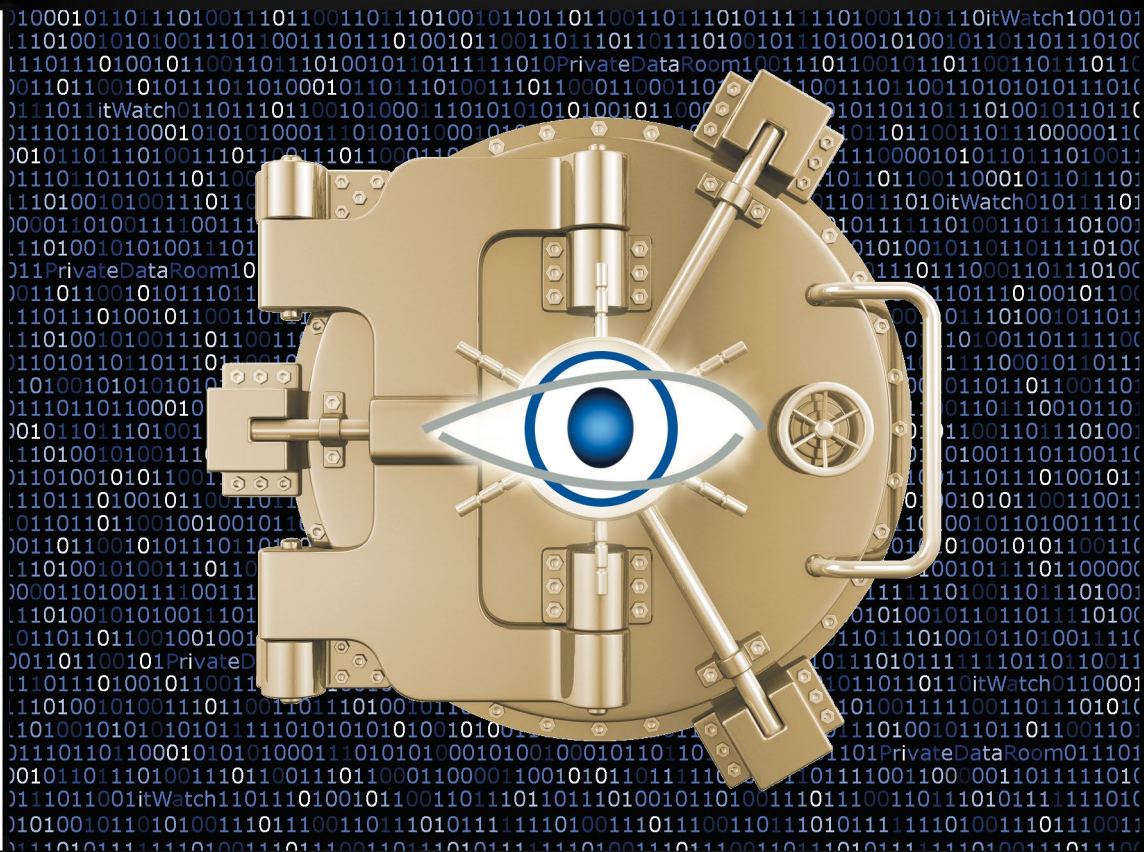


# Private Data Room



So schützen Sie Ihre Datenjuwelen!



**itWatch GmbH**

Aschauer Str. 30  
D-81549 München

Tel.: +49 (0) 89 62 03 01 00  
Fax: +49 (0) 89 62 03 01 069

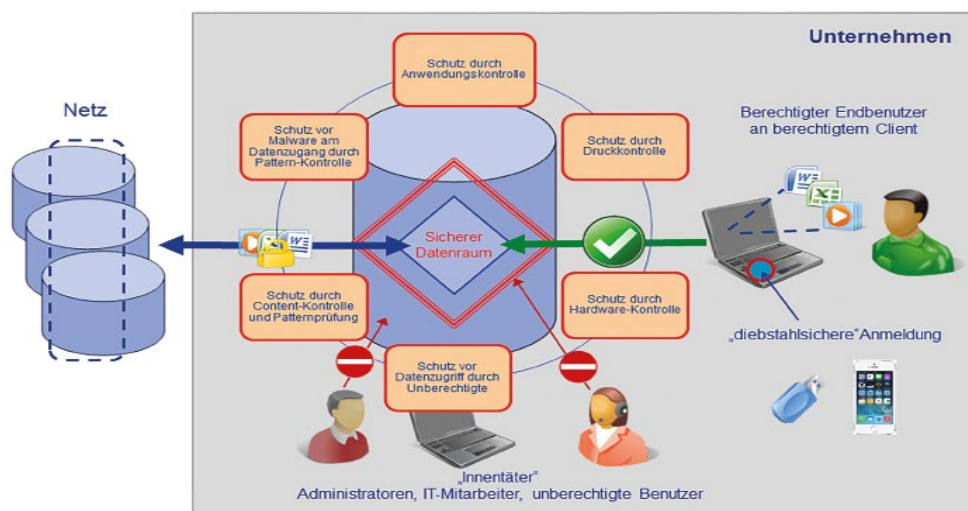
[www.itWatch.de](http://www.itWatch.de)  
[www.info@itWatch.de](mailto:www.info@itWatch.de)

## Das Problem

Die Kronjuwelen – also die wichtigsten Daten des Unternehmens – sind leicht identifiziert. Nur wenige Personen dürfen darauf zugreifen – häufig dürfen die IT-Mitarbeiter nicht im Klartext auf die sensiblen Daten zugreifen. Wie kann das adäquate Maß an Vertraulichkeit gegenüber Dritten aber auch Teilen des eigenen Unternehmens oder externen Mitarbeitern im Unternehmen, mit einem zusätzlichen Integritätsbeweis und dem Schutz vor unberechtigter Veränderung und dem Schutz vor Verlust gewährleistet werden? Es geht darum, einen sicheren Datenraum zu schaffen, der den eigenen Anforderungen entspricht. Neben der sicheren Datenschleuse, die den Zufluss der Daten geeignet säubert, gilt es die vielen dabei möglichen Fehler und Angriffsszenarien nicht in der eigenen IT – auf den eigenen Daten zu erleben.

## Wann ist ein Datenraum sicher?

Die Informationen aus dem **Private Data Room** verlassen den sicheren Datenraum nur über genehmigte vordefinierte Kanäle – das Ausspähen solcher Informationen ist weder organisatorisch noch technisch möglich. Dazu zählen alle Daten des **Private Data Room** insbesondere natürlich Authentisierungsdaten wie Passworte, PINs für Chipkarten etc. Der Schutz vor Ausspähen ist so organisiert, dass er gegen aktive Angriffe von IT-Administratoren, nicht berechtigten Benutzern und auch gegen die nicht legale Datenmitnahme und Nachlässigkeiten von berechtigten Anwendern schützt. Das heißt IT-Administratoren und nicht berechtigte IT-Mitarbeiter haben nie Zugriff auf den Klartext der Daten im sicheren Datenraum – auch nicht durch Netzwerkanalyse oder „low-level-Angriffe“ – können aber trotzdem ihren Standard-System-Management-Aufgaben nachgehen: z.B. Backup-Recovery, Verfügbarkeit der IT prüfen, Troubleshooting etc.



Gleichzeitig schützt der **Private Data Room** vor Infiltrationen von außen, so dass kein Schadcode in den sicheren Datenraum kommt. Insofern werden bei einem solchen Schutzbedarf die eingehenden Daten immer durch Schleusen und Datenwaschstationen **itWash**<sup>1</sup> eingebracht. Im **Private Data Room** ist die Datenübergabe nur über berechtigte Kanäle möglich, also keine Datenkopien durch Screenshots oder Kopieren oder Übergabe mittels einer Zwischenablage. Applikationen, die besondere Berechtigungen haben, werden technisch dazu berechtigt, ohne dass ein Anwender die Rechte selbst erhält. Alle Hardwareelemente und Applikationen im sicheren Datenraum werden registriert und authentisiert. Jede sicherheitsrelevante Aktion wird protokolliert. Aktionen, welche die Sicherheit des Gesamtsystems verändern würden, erfordern eine starke Mehr-Faktor-Re-Authentisierung und bei Bedarf eine vier oder mehr Augen-Aktivität. Nachdem im sicheren Datenraum das IT-Management ohne weitere IT-Kenntnisse erfolgt, führen besondere, sicherheitsbewusste Dialoge den berechtigten Anwender durch das Management. Kundenseitig wird der Schutzbedarf definiert und bestimmt, welche Schutzelemente implementiert werden und ob auf einzelne Schutzkomponenten aus Kosten- oder Komfortgründen verzichtet wird.



IT Administratoren und IT-Mitarbeiter dürfen nie Zugriff im Klartext auf die Daten im sicheren Datenraum haben. Dadurch entstehen im Krisenfall keine ungerechtfertigten Verdächtigungen.



IT-Administratoren und IT Mitarbeiter müssen Standard-System-Management-Aufgaben nachgehen können:

- ⦿ Backup - Recovery
- ⦿ Verfügbarkeit der IT prüfen
- ⦿ Troubleshooting

## Wer braucht einen sicheren Datenraum?

1. **Vorstände** bereiten ein sensibles M&A Meeting vor
2. **Aufsichtsräte** werden über die Strategie des Unternehmens informiert
3. in der **Personalabteilung** werden die Daten besonders sensibler Stellen geführt
4. die Innovationen werden für ein **Patent** vorbereitet
5. **Ausschreibungen** dürfen nur von wenigen Personen während eines definierten Zeitfensters bearbeitet werden
6. **Integritätsschutz** mit Änderungsprotokoll für freigegebene Unternehmensinformationen

## Abwehrfähigkeiten des Private Data Room

- ⦿ Starke Multifaktorausauthentisierung der berechtigten Anwender
- ⦿ Schutz vor Malware am Datenzugang
- ⦿ Authentisierung und Kontrolle der Hardware
- ⦿ Content-Kontrolle und Pattern-Prüfung für Anwender UND Applikationen
- ⦿ Schutz vor Datendiebstahl
- ⦿ Anwendungskontrolle und privilegierte Anwendungen
- ⦿ Starke Verschlüsselung der Daten bei der Lagerung und bei der Netzwerkübertragung
- ⦿ Härtung der Betriebssysteme - Umgebungen auf welchen die Daten im Klartext verarbeitet werden
- ⦿ Kontrolle aller Outputwege inkl. Druckkontrolle mit Wasserzeichen etc.

<sup>1</sup> nähere Informationen zu itWash finden Sie auf dem itWatch Factsheet itWash oder unter <http://www.itwatch.de/Produkte/itWash>

© 2017, itWatch GmbH München, Alle Rechte vorbehalten. ReCAppS, DeviceWatch, PDWatch, XRayWatch, dataEx, DevCon, CDWatch, AwareWatch, ReplicationWatch, PDWatch2Go, PrintWatch, RiskWatch, LogOnWatch, MalWareTrap, itWash, Private Data Room, itWESS2Go, itWatch Enterprise Security Suite und ApplicationWatch sind Produkte der itWatch GmbH. Die genannten Fremdanwendungen sind durch deren Hersteller geschützt.