Private Data Room der sichere Datenraum

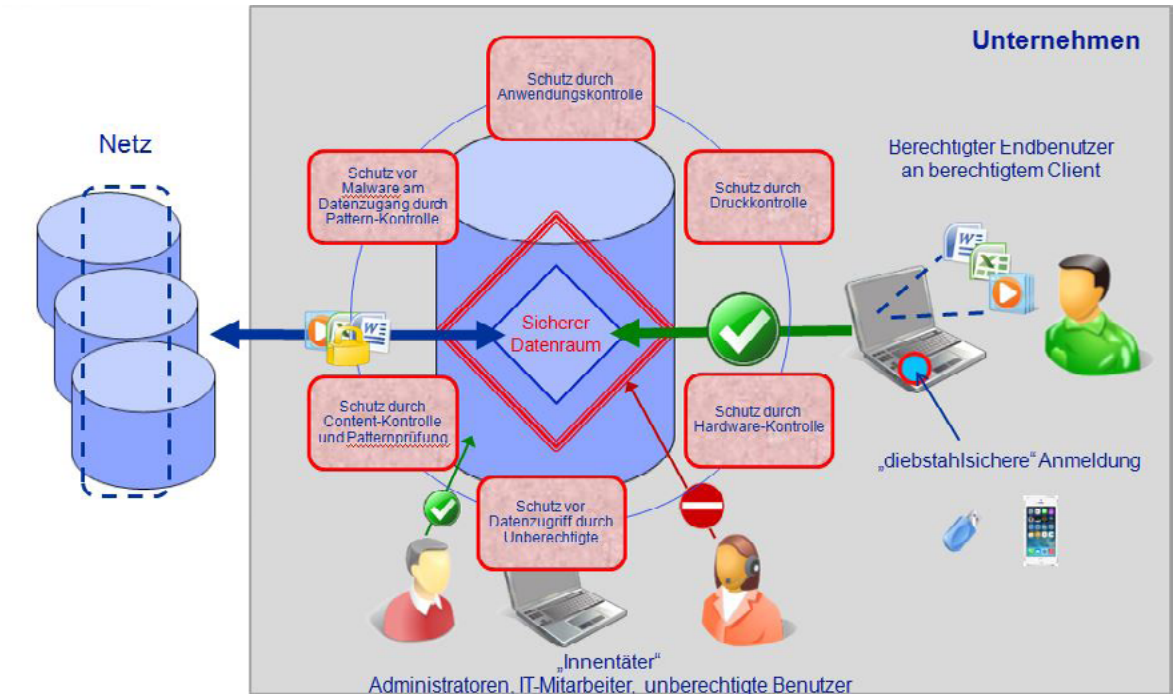
- **Wann ist ein Datenraum sicher?**
- **Wie wird der sichere Datenraum geschützt?**

Das Problem

Nach der Identifikation der eigenen Kronjuwelen – also der wichtigsten Daten des Unternehmens – stehen viele Unternehmen vor der Frage wie gehe ich jetzt mit dem Schutz der Daten um. Meist geht es um ein hohes Maß an Vertraulichkeit (gegenüber Dritten aber auch Teilen des eigenen Unternehmens oder externen Mitarbeitern im Unternehmen), aber oft auch um einen Teil Integrität insbesondere Schutz vor unberechtigter Veränderung und Verfügbarkeit insbesondere dem Schutz vor Verlust. Dabei geht es am Ende vom Tag darum einen sicheren Datenraum zu schaffen, der den eigenen Anforderungen entspricht. Neben der **sicheren Datenschleuse**, die den Zufluss an Daten geeignet vorbereitet, gilt es die vielen dabei möglichen Fehler nicht in der eigenen IT 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 Information 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 Angriffe von IT-Administratoren, nicht berechtigen Benutzern und so gut wie möglich auch gegen die nicht legale Datenmitnahme und Nachlässigkeiten von berechtigten Anwendern schützt. Das heißt IT-Administratoren und IT-Mitarbeiter dürfen nie Zugriff auf den Klartext der Daten im sicheren Datenraum haben – auch nicht durch Netzwerkanalyse - müssen aber trotzdem ihren Standard-System-Management-Aufgaben nachgehen können: z.B. Backup-Recovery, Verfügbarkeit der IT prüfen, Troubleshooting etc.



Gleichzeitig muss der **Private Data Room** natürlich vor Infiltrationen von außen geschützt werden, so dass kein Schadcode in den sicheren Datenraum kommt. Insofern sind bei einem hohen Schutzbedarf die eingehenden Daten immer durch Schleusen und Datenwaschstationen einzubringen.

Der Datenaustausch zwischen verschiedenen IT-Elementen im Private Data Room wird so reguliert, dass die Datenübergabe ebenfalls nur in berechtigten Kanälen stattfinden kann, also keine Datenkopien durch Screenshots oder Kopieren und Übergabe mittels einer Zwischenablage möglich sind. Applikationen, die besondere Berechtigungen haben, können technisch dazu berechtigt werden. Alle 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 erfolgen muss, führen besondere, sicherheitsbewusste Dialoge den Anwender durch das Management.

Kundenseitig wird der Schutzbedarf definiert und bestimmt, ob alle Schutzelemente implementiert werden oder auf einzelne aus Kosten- oder Komfortgründen verzichtet wird.

Private Data Room der sichere Datenraum

Wie wird der sichere Datenraum geschützt?

Schutz vor Malware am Datenzugang

- Prüfung aller eingehenden Dateien auf:
  - Verschleierung durch Verschlüsselung, Archive, Einbettung.
  - Herstellen des Klartextes unter Berücksichtigung von Benutzerdialogen für die Entschlüsselung.
  - Erkennen von eingebettetem, ausführbaren Code (Exe, DLL, Java, Makro, …).
  - Reinigung von Daten mit (eingebettetem) ausführbaren Code durch Abbildung auf geeignete Formate mit geeigneten Prozessen (je nach Schutzbedarf durch Hardwaretrennung).
- Kontrolle von allen zu startenden Prozessen und Zuordnung zu einer Anwendung verhindert Schadcode.
- Nahtlose Einbettung von beliebigen Drittprodukten z.B. Anti-Virenprogramme.

Content-Kontrolle und Pattern-Prüfung

- Content-Kontrolle von jeder Datei beim Lesen und Schreiben auf vorgetäuschten Dateinamen, auf eingebetteten, ausführbaren Code, …
- Zugriffsrechte auf Dateitypen können je Rechner, je User, Usergruppe, je Datenlokation (inkl. Cloud, Hardware, Festplatte , Directoryname, logischer oder physikalischer Pfad, Netzwerkshares), je Dateiname, je Anwendung, je Handlungskontext individuell gesetzt werden – multiple Wildcards werden unterstützt wo sinnvoll.
- Content Filter regeln Monitoring von Dateitypen filigran
- Jeder Dateityp wird inhaltlich geprüft:
  - Ist der Dateiinhalt authentisch?
  - Sind in der Datei unerwünschte Elemente eingebettet?
- Blockieren nicht erwünschter Dateiinhalte, Identifikation erwünschter Dateiinhalte.

Schutz durch Kontrolle der Hardware

- Identifikation und Inventarisierung der Initialhardware.
- Erweiterte Funktionen für die Personalisierung von Hardware zur Unterscheidung baugleicher Elemente.
- Verbot unberechtigter Hardware.
- Schutz vor dem unberechtigten Einbringen oder Auswechseln von Hardware wie z.B. Festplatten, Netzwerkkarten etc.
- Schutz vor verstecktem Schadcode auf erlaubter Hardware (z.B. BadUSB).
- Schutz vor verdeckten Kanälen bei der Kommunikation der Geräte mit den Betriebssystemen und den Anwendungen.

Schutz vor Datenverlust

- Alle Kanäle zum „Abtransport der Daten werden überprüft und entlang der definierten Richtlinien:
  - Geblockt
  - Mit Haftungsübernahme und Protokollierung genehmigt
  - Protokolliert
  - Zwangsverschlüsselt
  - Bei Bedarf modifiziert (z.B. gekürzt oder im Datenformat verändert – z.B. Ausdruck verboten)
- Revisionssichere Protokollierung aller Vorgänge und Inhalte.
- Algorithmen zum sicheren Löschen von Daten werden je Datenträger automatisch richtig angewendet.

Schutz durch Anwendungskontrolle

- Jede Anwendung wird in das System „eingecheckt".
- Jede Anwendung wird vor Start identifiziert und authentisiert.
- Benutzerberechtigungen auf Anwendungen sorgen dafür, dass nicht jeder Anwender besonders sensible Anwendungen starten kann.
- Content Filter regeln den Rechteraum der Anwendung – auf sicherheitskritische Informationen wie z.B. Root Zertifikate können nur besondere Anwendungen zugreifen.
- Jeder Prozessstart wird eindeutig einer Anwendung und einem User zugeordnet.
- Feingranulare Steuerung des Datenaustausches zwischen den Anwendungen (Zwischenablage, Print Screen, Dateizugriffe unterschieden nach Laufwerk, Directory, lesend, schreibend …).
- Durch die Content-spezifischen Rechte der Anwendungen, die auch gegenüber den Benutzerrechten höherwertig sein können, besteht die Möglichkeit zusammen mit der Automatisierung sichere Prozesse abzubilden, in welche der Anwender nicht eingreifen kann. Diese Prozesse sind z.B. beim Datenneuzugang notwendig um die Daten beim ersten Speichern bereits geeignet zu verschlüsseln.

Schutz durch Druckkontrolle

- Verbot unberechtigter Ausdrucke.
- Berechtigte Ausdrucke werden mit einem Wasserzeichen individualisiert, so dass jede Seite jedes Ausdruckes optisch unterschiedlich ist – das Wasserzeichen kann auf Wunsch maschinen-lesbar und / oder menschlich-lesbar sein.
- Ausdrucke werden im wirklich gedruckten Format beweissicher archiviert – der Zugang zu dem Archiv kann individuell durch Rollen und auch vier und mehr-Augen Authentisierungen geschützt werden.

itWatch GmbH
Aschauer Str. 30
81549 München
Tel: +49 (89) / 6203 010 0
Fax: +49 (89) / 6203 010 69
www.itWatch.de
info@itWatch.de