

Einzeltest Brainloop Secure Dataroom

Nur nicht die Kontrolle verlieren

Allein die Verschlüsselung vertraulicher Dokumente kann nicht sicherstellen, dass Berechtigungen auch außerhalb des Firmennetzwerks eingehalten und Zugriffe nachvollzogen werden können. Dazu müssen das Berechtigungsmanagement und die Protokollierung über die Unternehmensgrenzen hinweg ausgeweitet werden. Mit dem Secure Dataroom von Brainloop soll dies möglich sein. Wir haben uns die Lösung für Sie angesehen.

► Es reicht leider nicht aus, das eigene Unternehmensnetzwerk bestmöglich abzusichern. Denn nicht nur durch die Zusammenarbeit mit externen Partnern verlassen vertrauliche Dokumente das eigene Netzwerk.

Laut einer Umfrage des Hightech-Verbands BITKOM arbeitet bereits jeder zehnte Beschäftigte ganz oder teilweise im Home Office, sodass auch der Datenaustausch mit den eigenen Mitarbeitern nicht an der Netzwerk-Firewall enden kann.

Verschlüsselung reicht nicht aus

Um den Vorgaben zur Datenschutzkontrolle gerecht zu werden, sollten vertrauliche Daten insbesondere bei der Übertragung verschlüsselt werden. Dadurch lässt sich die Gefahr, dass Unbefugte die Daten abfangen und mitlesen, verringern.

Was aber mit den digitalen Dokumenten passiert, nachdem der Empfänger sie entschlüsselt hat, ist nicht ohne Weiteres klar und nachprüfbar.

Berechtigungen und Protokolle auch außerhalb der Firewall nachvollziehen

Geschäftspartnern, die ein geheimes Dokument im Unternehmen nur lesen, aber nicht drucken dürfen, sollte das auch außerhalb des Firmennetzwerks nicht möglich sein. Um das umzusetzen, besteht die Möglichkeit, einem Dokument schon bei seiner Erzeugung je nach Dateiformat Beschränkungen mit auf den Weg zu geben, die ein Drucken durch Unbefugte verhindern.

Was aber, wenn ein Dokument an mehrere Empfänger mit unterschiedlichen Berechtigungen versendet werden soll? Erhält dann jede Berechtigungsgruppe ein unterschiedliches Dokument? Und wie kann man feststellen, was die Empfänger mit den übertragenen Dateien wirklich gemacht haben?

„Sicheres Extranet“: Es ist nicht nur eine sichere Dateiübertragung gefragt!

Um die Zugriffs-, Weitergabe- und Eingabekontrolle sicherzustellen, reicht es deshalb nicht, nur verschlüsselte Dateien via E-Mail oder File Transfer Protocol (FTP) zu übertragen.

Die Dateien müssen das Berechtigungskonzept und die Protokollierung mit sich führen, oder anders ausgedrückt: Es muss ein sicheres und nachvollziehbares Übertragungs- und Speichersystem implementiert werden. Andernfalls verliert man mit der Übertragung der Datei die Kontrolle über die darin enthaltenen personenbezogenen Daten.

Es ist also eine Art sicheres Extranet als Erweiterung des eigenen Netzwerks nötig.

Praxistest des Secure Dataroom 8.0 von Brainloop

Auf dem Markt sind verschiedene Lösungen verfügbar, die einen sogenannten sicheren Datenraum anbieten, also einen abgesicherten Ort im Internet, um dort verschiedenen Benutzern die gemeinsame, unternehmensübergreifende Arbeit an vertraulichen Dokumenten unter Beachtung der unterschiedlichen Berechtigungen zu ermöglichen.

Ein Beispiel dafür ist Brainloop Secure Dataroom 8.0, das wir uns näher angesehen haben.

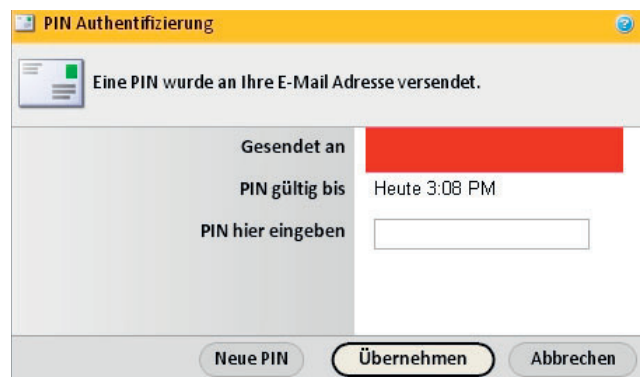
Wie der Anbieter den sicheren Datenraum betreibt

Brainloop sichert folgende Punkte zu:

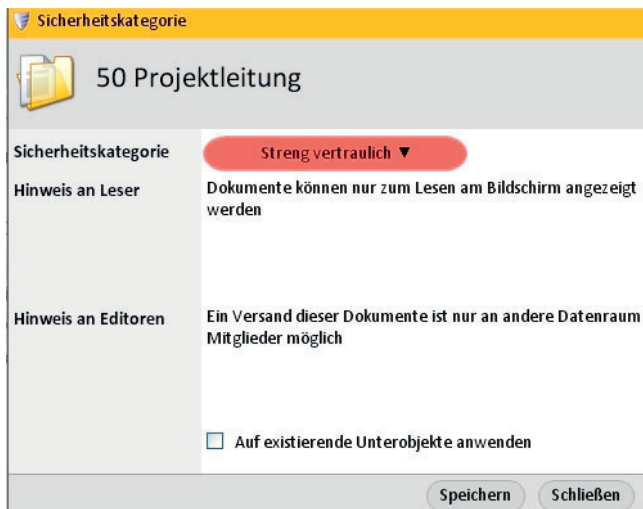
- einen zertifizierten Rechenzentrumsbetrieb in mehreren Ländern
- die Trennung von System- und Anwendungsadministration
- die Erstellung einer wöchentlichen Sicherungskopie für die im Datenraum eingestellten Dokumente
- ein Online-Archiv für die jeweils letzten 21 Tage
- optional eine tägliche Datensicherung
- eine deutsche und eine englische Nutzerhotline rund um die Uhr

Zwei-Faktor-Authentifizierung möglich

Der Datenraum-Administrator des Kunden kann je nach Schutzbedarf vorsehen, dass sich die Nutzer über Benutzername (E-Mail-Adresse) und Passwort sowie ggf. zusätzlich über eine (bei der Eingabe



Je nach Sicherheitseinstellung ist zusätzlich zum Passwort eine Einmal-PIN erforderlich (Bild: O. Schonschek)



Im Datenraum lassen sich Nutzerberechtigungen, Sicherheitszonen und Vertraulichkeitsstufen unterscheiden (Bild: O. Schonschek)

nicht maskierte) PIN identifizieren, die über E-Mail oder SMS zugestellt wird und im Test eine Stunde gültig war.

Möglich sind zudem die Einschränkung der IP-Adressen, von denen aus zugegriffen werden darf, und die zusätzliche Identitätsprüfung über digitale Zertifikate. Die Übertragung zwischen dem sicheren Datenraum und dem Browser des Nutzers erfolgt mit 128-Bit-Verschlüsselung, die Datenspeicherung auf dem Server ist laut Brainloop 256-Bit-verschlüsselt.

Alle Zugriffe auf Dokumente werden genau protokolliert

Die im Datenraum eingestellten Dokumente können dort von den Nutzern je nach Berechtigung angesehen, geändert, verteilt oder auch gelöscht werden. Alle Zugriffe auf die Dokumente werden nutzergenau protokolliert.

Für die Dokumente lassen sich auch Aufbewahrungs- und Löschrufen definieren. Zusätzlich zu den Dokumenten lassen sich Nachrichten und Aufgaben an andere Nutzer innerhalb des Datenraums übertragen.

Datenversand auch an Dritte möglich

Je nach Sicherheitseinstellung des Datenraums können Dokumente Dritten,

die nicht Nutzer des Datenraums sind, zugänglich gemacht werden.

Dabei werden jedoch nicht die Dokumente, sondern nur die Links zu den Dokumenten per E-Mail verschickt. Der Empfänger muss sich dann abhängig vom eingestellten Schutzbedarf mit Passwort und zusätzlicher PIN identifizieren.

Zugriff lässt sich zeitlich begrenzen oder deaktivieren

Die Gültigkeit des Links lässt sich zeitlich begrenzen und nachträglich auch deaktivieren, falls ein Dokument nicht mehr verfügbar sein soll. Ruft der Empfänger das Dokument über den SSL-gesicherten Link auf, wird auch dieser Zugriff protokolliert.

Auf Wunsch kann der Download eines Dokuments durch Dritte anonymisiert werden. In diesem Fall steht nur die E-Mail-Adresse des Absenders im Protokoll. Zudem lässt sich festlegen, dass der Empfänger das Dokument nur ansehen und nicht drucken oder abspeichern darf.

Bei allen Vorteilen auch an Nutzerstatistiken und Profile denken

Brainloop Secure Dataroom 8.0 macht somit eine verschlüsselte Ablage vertraulicher Dokumente im Datenraum ebenso möglich wie den verschlüsselten Versand, die Definition von Berechtigungen und die Protokollierung der Dokumentenhistorie. Der Datenaustausch über die Unternehmensgrenze hinweg wird dadurch genau definierbar und nachvollziehbar.

Aus Sicht des Datenschutzes sollten Sie jedoch bei Einsatz eines solchen Produkts den Nutzern in Ihrem Un-

ternehmen einige Hinweise geben, die der folgende Kasten zusammenfasst.

Oliver Schonschek

Datenschutzhinweise zu Brainloop Secure Dataroom 8.0

1. Der Secure Dataroom protokolliert nicht nur die Veränderung, den Abruf oder den Versand eines Dokuments oder eines Ordners, sondern auch die Nutzeraktivitäten – hier die Zweckbindung der Protokolle und die Information für die Nutzer nicht vergessen!
2. Im Datenraum können freiwillig erweiterte Nutzerprofile mit Mobilnummer, Instant-Messaging-Adresse, Telefonnummer und Postadresse angelegt werden – informieren Sie die Mitarbeiter, dass diese Angaben in der Standardeinstellung für alle anderen Nutzer des Datenraums sichtbar sind.
3. Die Aktivitäten anderer Nutzer im Datenraum lassen sich durch Benachrichtigungsmails oder SMS nachverfolgen (Watchlist).
4. Im Datenraum kann eine Nutzerkommunikation stattfinden, die für alle anderen Nutzer des Datenraums sichtbar ist, wenn nicht das Kennzeichen „Privat“ aktiviert wird.
5. Im Rahmen des erweiterten Zugriffsschutzes werden IP-Adressen erhoben.
6. Wird der Datenraum ohne Abmeldung verlassen, könnte u.U. ein unberechtigter Dritter die Sitzung am gleichen PC wieder aufnehmen (Problem der aktiven Session-ID) – Brainloop gibt einen entsprechenden Nutzerhinweis.
7. Es reicht nicht, wenn der Empfänger einer Mail mit Link zum Datenraum nach PIN-Eingabe und Öffnen des Dokuments das aktive Browserfenster (den Tab) schließt, wenn noch ein anderes Fenster offen ist – ein anderer Nutzer des gleichen PC könnte den Tab wieder öffnen und an die Datei gelangen, solange der Link aktiv ist.