//ACTAPORT

Der Actaport Datensafe

WHITEPAPER

DATENSCHUTZ UND DATENSICHERHEIT

Cloud Computing wird seit vielen Jahren erfolgreich eingesetzt, gerade auch in sensiblen Bereichen. Dennoch gibt es mancherorts noch Vorbehalte bezüglich der Sicherheit und des Schutzes von Daten in der Cloud. Viele Anwender und IT-Verantwortliche kleinerer Unternehmen sind der Meinung, ihre Daten seien in einer Inhouse-Infrastruktur besser vor Missbrauch, Diebstahl und Katastrophen geschützt. Einer sachlichen Überprüfung hält diese Meinung aber nicht stand, denn große Cloud-Plattformen wie z.B. Microsoft Azure, auf dem Actaport aufbaut, bieten ein Sicherheitsniveau, das mit einer selbstbetriebenen „On Premise“-Infrastruktur kaum erreicht werden kann.

Anders ausgedrückt: **Professionelles Cloud Computing ist deutlich sicherer als lokal in der Kanzlei betriebene Server.** In diesem Whitepaper werden die wesentlichen Aspekte rund um das Thema „Datenschutz und Datensicherheit bei Actaport“ erläutert, um diese für manche Anwender vielleicht provokant klingende Aussage zu belegen. Das im Folgenden vorgestellte Sicherheitskonzept stellt den **Actaport Datensafe in der Cloud** dar.

SCHUTZ GEGEN PHYSIKALISCHEN DATENVERLUST

Actaport speichert alle Daten in den deutschen Rechenzentren (RZ) der Microsoft Azure-Plattform. Dabei kommen die jeweils höchsten verfügbaren Level der angebotenen Dienste zum Einsatz. Im Ergebnis bedeutet dies:

• **Lokale Redundanz.** Dokumente werden nach einem Dreifachverfahren redundant gespeichert, d.h. jeder Schreibvorgang eines Dokumentes wird innerhalb des RZs auf drei unterschiedlichen Speichersystemen abgelegt. Erst wenn die Speicherung auf dem dritten Medium erfolgreich war, gilt der Gesamtvorgang als erfolgreich. Microsoft garantiert für dieses LRS (lokal redundanter Speicher) eine Sicherheit von 99,9999999999%.

• **Geo-Redundanz.** Zusätzlich zur lokalen Redundanz nutzt Actaport die Geo-Redundanz-Funktionen der Microsoft Cloud. Dies bedeutet, dass alle Speicheroperationen zusätzlich in einem zweiten RZ durchgeführt werden. Wenn das primäre RZ in Frankfurt liegt, werden

alle Daten zusätzlich in einem sekundären RZ (z.B. in Berlin) gespeichert. Bei Ausfall des primären RZ kann ohne Unterbrechung auf dem Datenbestand des sekundären RZ weitergearbeitet werden.

• **Backups.** Alle Datenbanken werden über einen Point-In-Time (PIT)-Mechanismus gesichert. Eine Sicherung erfolgt alle 5 Minuten und die Datensicherung wird 35 Tage aufgehoben. Da wir auch im Backup-Bereich das Feature „Geo-Redundanz“ einsetzen, werden diese Sicherungen synchron auf zwei unterschiedliche regionale Standorte übertragen.

In der Summe dieser Eigenschaften bietet die Actaport Lösung einen maximalen Schutz gegen Datenverluste durch Hardwareausfälle, (Natur-)Katastrophen sowie software- oder anwendungsbedingte Datenkorruption, die durch eine lokal betriebene Infrastruktur nicht erreicht werden kann.

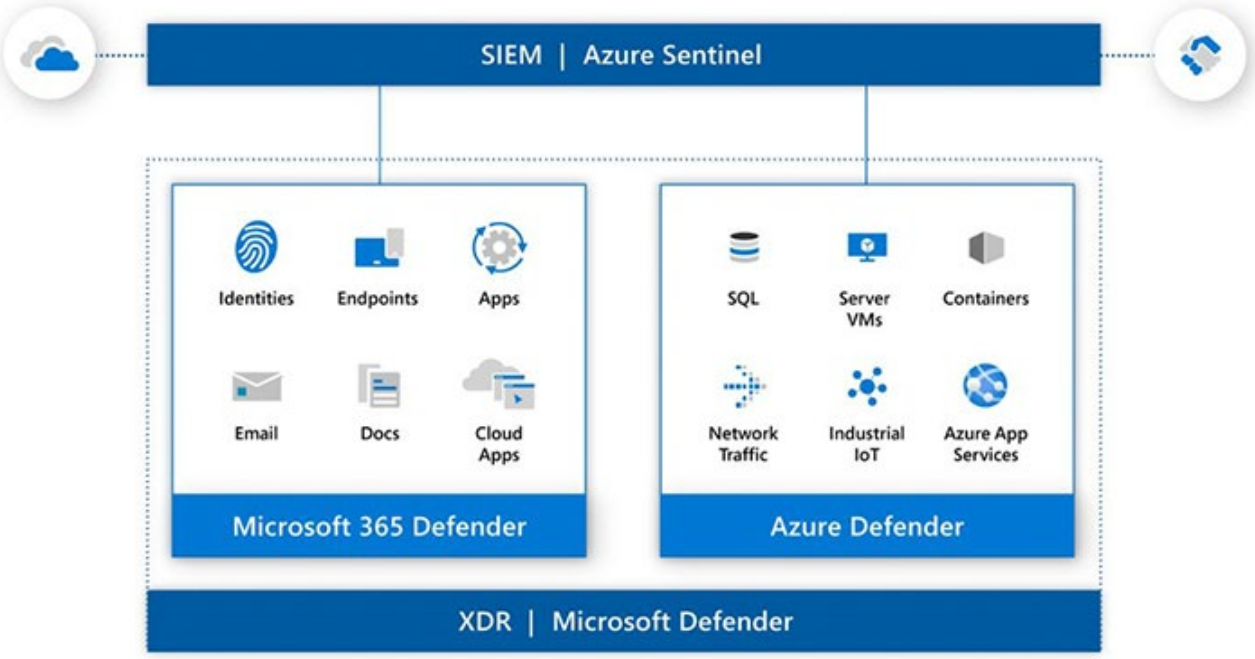
Dieses sehr hohe Schutzniveau gilt natürlich auch in Bezug auf Gefahren durch Einbruch und physikalischen Datendiebstahl. Die Rechenzentren der Microsoft Cloud werden professionell bewacht und verfügen über ein ausgeklügeltes System an Zugangskontrollen, die entsprechende Vorfälle faktisch ausschließen.

SCHUTZ GEGEN CYBER-KRIMINALITÄT

Eine Schattenseite der Digitalisierung ist die Cyber-Kriminalität, die zunehmend systematisch und organisiert (teilweise auf staatlicher Ebene) erfolgt. Die damit verbundenen Risiken sind nicht auf den Verlust eigener Daten beschränkt, sondern dehnen sich im Fall der Kaperung von Servern durch Schadsoftware auch auf Dritte aus: Das Opfer wird zum Mittäter in der Kette kriminellen Verhaltens. Selbst wenn durch die Einhaltung der einschlägigen Richtlinien die Delegation von Verantwortung und Haftung verbessert werden kann: Wer möchte z. B. seinem Mandanten erklären, dass es vielleicht nicht nur zu Datenverlusten in der eigenen Kanzlei gekommen ist, sondern im schlimmsten Fall der Kanzlei-Server die Ursache für die Kompromittierung der Mandanten-IT war?

Verschiedene Eigenschaften der Microsoft-Infrastruktur stellen auch auf diesem Gebiet ein Maximum an Sicherheit her:

• **KI-gestützte Gefahrenanalyse und -abwehr.** Mit SIEM (Security Information & Event Management) und XDR (Extended Detection & Response) sichert Microsoft in einem integrierten Konzept sowohl die Azure-, als auch die 365-Cloud gegen Cyber-Bedrohungen ab.



Quelle und weitere Informationen: https://www.microsoft.com/de-de/security/business/threat-protection

• **Ständig aktuelle Systemumgebung.** Ein wesentlicher Aspekt einer sicheren Infrastruktur ist die Aktualität aller Komponenten von Betriebssystem-Patches bis zu Datenbank- und Komponenten-Versionen. Hier spielt die Cloud, bei der letztlich nur ein einziges System gepflegt werden muss, ihre Stärken voll aus. Sicherheits-Updates werden mit der Fertigstellung durch die Entwicklung sofort aktiv, während sie auf lokal betriebenen Systemen erst installiert werden müssen. Ein großer Teil aktueller und medienwirksamer Fälle von teilweise schwerwiegenden Einbrüchen in lokale Serverstrukturen (in Unternehmen und staatlichen Organisationen) sind auf diesen zeitlichen Faktor zurückzuführen.

• **Kurze Update-Zyklen der Anwendung.** Actaport führt mindestens wöchentlich eine Aktualisierung seines Produktivsystems durch und steht damit sofort allen Anwendern zur Verfügung. Dies dient nicht nur der Auslieferung neuer und verbesserter Funktionalität und der Behebung von Fehlern, sondern ist auch hochgradig sicherheitsrelevant. Moderne Software-Lösungen bestehen aus hunderten von Modulen und Bibliotheken, von denen jede einen potentiellen Angriffsvektor darstellt. Wird eine lokal installierte Software einmal im Quartal (oder noch seltener) aktualisiert, können auch Sicherheits-Updates dieser vielen Komponenten nur in diesem Rhythmus auf den neuesten Stand gebracht werden.

DATENSICHERHEIT DURCH VERSCHLÜSSELUNG

Eine besondere Rolle kommt im Bereich des Cloud-Computings dem Thema der Verschlüsselung von Daten zu. Actaport bedient sich der State of the Art-Technologien und ergänzt

die im Rahmen der Microsoft-Infrastruktur bereits vorhandenen Verschlüsselungsmethoden durch weitere Maßnahmen, um den besonderen Anforderungen der Rechtspflege im Allgemeinen und des Berufsrechts im Besonderen möglichst optimal zu entsprechen.

TRANSPORTVERSCHLÜSSELUNG

Um die Sicherheit der Daten auf den Transportwegen zu gewährleisten, kommt das TLS Verfahren zum Einsatz. Die Sicherheit der Zertifikate und der eingesetzten Technologien wird regelmäßigen Tests unterzogen.

SCHLÜSSELTRESORE

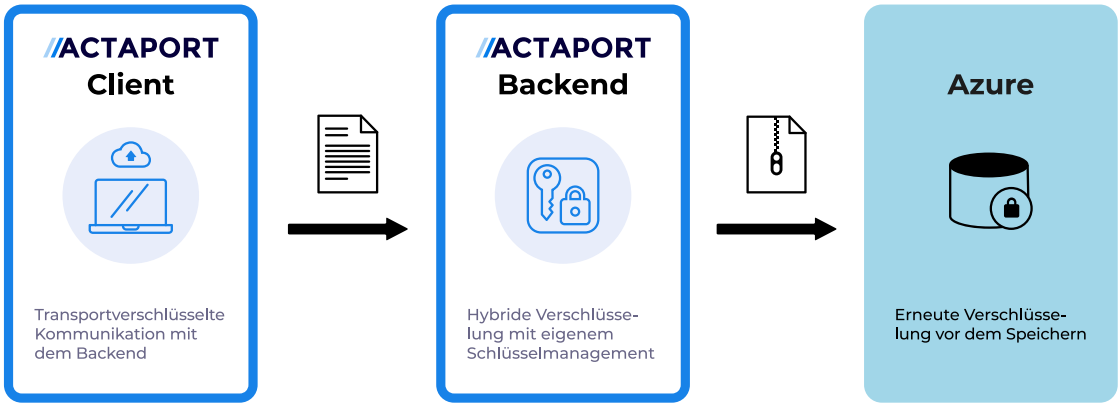
Für sämtliche Verschlüsselungen werden sogenannte Schlüssel bzw. Schlüsselpaare benötigt. Für dieses Schlüsselmanagement wird ein Schlüsseltresor verwendet, der individuelle Schlüsselpaare für jeden Actaport Benutzer enthält, die getrennt in separaten Bereichen gespeichert werden. Um diesen Bereich des Tresors zu öffnen, bedarf es eines signierten Benutzer-Tokens, das nur ausgestellt wird, wenn sich der Benutzer erfolgreich am Identity-Management-Service authentifiziert hat. Die Gültigkeit des Tokens wird dabei bei jedem Zugriff – also jedem Funktions- oder Bereichsaufruf in Actaport – implizit validiert. Ihr sogenannter privater Schlüssel verlässt dabei nie den Tresor, die Verschlüsselung der Daten erfolgt immer innerhalb des Tresors. Damit wird ein weiterer möglicher Angriffspunkt – der lokale Computer – ausgeschlossen.

DOKUMENTVERSCHLÜSSELUNG

Da es sich bei Dokumenten um große Datenmengen handelt, muss die Verschlüsselungslösung performant und dabei sicher sein. Beides wird durch eine sogenannte Hybrid-Verschlüsselung gewährleistet. Dabei wird für jedes Dokument ein individueller Schlüssel (Inhaltsschlüssel) erzeugt, mit dem das Dokument mit Hilfe des symmetrischen AES-Verfahrens verschlüsselt wird. Das AES-Verfahren allein ist zwar schnell, genügt aber den von uns auferlegten Sicherheitsanforderungen noch nicht ganz. Um dies zu gewährleisten, wird der Inhaltsschlüssel anschließend mit einem zusätzlichen asymmetrischen Verfahren verschlüsselt. Hier kommt wieder der Schlüsseltresor zum Einsatz, der diesen Vorgang über-

nimmt. Der verschlüsselte Schlüssel wird nun zusammen mit dem verschlüsselten Dokument gespeichert.

Mit diesem Verfahren ist sichergestellt, dass ausschließlich registrierte Benutzer ihr Dokument entschlüsseln können und die Betreiber der Applikation und der Infrastruktur sowie andere Dritte keine Möglichkeit der Einsicht haben. Selbst ein erfolgreicher „Datendieb“ fände immer nur verschlüsselte, für ihn nicht lesbare Dokumente vor.



DATENVERSCHLÜSSELUNG

Ebenso wie Dokumente können auch die Metadaten, also etwa Akten, Fristen und Kontakte, sensible Daten enthalten. Damit diese im ruhenden Zustand von Dritten nicht eingesehen werden können, kommt eine sogenannte Transparent Data Encryption (TDE) zum Einsatz. TDE wird verwendet, um Datendateien aus der Azure SQL-Datenbank in Echtzeit mit einem Datenbankverschlüsselungsschlüssel zu verschlüsseln. TDE schützt dabei die Daten- und Protokolldateien über die Verschlüsselungsalgorithmen AES und Triple Data Encryption Standard (3DES). Die Verschlüsselung der Datenbankdatei erfolgt auf Datenbank-Seitenebene. Diese Seiten in einer verschlüsselten Datenbank werden verschlüsselt, bevor sie auf den Datenträger geschrieben werden und entschlüsselt, bevor sie in den Arbeitsspeicher eingelesen werden.

Besonders sensible Daten, beispielsweise Kontodaten für externe Services wie IMAP Benutzerdaten, werden nochmals separat über den Schlüsseltresor verschlüsselt, bevor diese Daten in der Datenbank gespeichert werden.