econ
Ein Unternehmen der MVV

econ live
Sicherheit und Datenschutz

Sicherheit und Datenschutz in econ live

Maßnahmen zum Schutz Ihrer Daten

econ solutions GmbH I Franz-Josef-Delonge Straße 12 I 81249 München
+49 621 290-5200 I info@econ-solutions.de I www.econ-solutions.de

Inhalt

1. Vorwort

Das Auslagern partieller Dienste in die Cloud bietet enorme Vorteile, löst aber auch Bedenken hinsichtlich Sicherheit und Datenschutz aus. Das Beispiel Onlinebanking veranschaulicht jedoch, dass mit geeigneten Sicherheitsmaßnahmen -und Konzepten ein sicherer Betrieb gewährleistet werden kann. Nachfolgend wird beschrieben, wie die Sicherheit und der Datenschutz in econ live sichergestellt wird.

2. Sicherung der Kommunikationswege

Als Portal-Lösung verbinden sich sowohl die Edge-Geräte (auch Cloud Adapter genannt), also auch die Nutzer über den Web-Browser über einen verschlüsselten Kommunikationskanal mit econ live.

2.1. Verschlüsselung im Detail

Der econ live Server bietet verschlüsselte Verbindungen nach dem TLS 1.2 und dem TLS 1.3 Standard an. Dabei werden die nach Stand der Technik relevanten Funktionen, wie „Forward Security“ und „Downgrade attack prevention“ erfüllt. Die verfügbaren Cipher suites werden regelmäßig dem Stand der Technik angepasst.

2.2. Challenge Response Verfahren

Bei der Kommunikation zwischen Cloud Adapter und econ live Server muss die Authentizität beider Kommunikationspartner sichergestellt werden. Hierzu wird neben der Server-Zertifikatsvalidierung ein sog. Challenge Response-Verfahren durchgeführt. Hierzu wird ein Passwort im Cloud Adapter eingegeben, welches einmalig in econ live bestätigt werden muss (shared secret). Nach jedem Verbindungsaufbau überprüfen beide Kommunikationspartner, ob die Gegenstelle über dasselbe geheime Passwort verfügt, ohne dies selbst zu übertragen. Eine Übertragung von Informationen beginnt erst, wenn die Authentizität beider Kommunikationspartner validiert wurde.

3. Sicherung Ihres Benutzeraccounts

Das Passwort zur Sicherung des econ live Accounts muss angemessenen Passwortrichtlinien genügen. Vor dem Speichern bzw. Überprüfen des Passworts, wird es mit einem kryptografischen Salt ergänzt und anschließend mit einer 512Bit Hashfunktion verschlüsselt. Nach mehrmaliger falscher Eingabe des Passwortes, wird der Zugang umgehend für eine angemessene Zeit gesperrt.
Zur weiteren Sicherung des Benutzeraccounts wird die Aktivierung der 2-Faktor-Authentifizierung empfohlen. Dabei muss bei Anmeldung an einem neuen Gerät oder - bei kritischen Aktivitäten - ein weiterer Identitätsnachweis in Form einer Zahlenkombination erbracht werden.

4. Anomalieerkennung

In econ live überwacht eine ausgeklügelte Anomalie Erkennung sämtliche Nutzeraktivitäten. Wird ein gewisser Schwellenwert erreicht erfolgt die sofortige Sperrung des Kommunikationspartners. So können vollautomatisiert Angriffsszenarien abgewehrt werden.

Gleichzeitig erfolgt eine Anomalie Erkennung durch den Cloud Provider auf Basis von Telemetriedaten.

5. Stetige Überwachung und Aktualisierung

Neben der automatisierten Überwachung erfolgt zudem eine manuelle Analyse von Protokoll- und Telemetriedaten um mögliche Systemfehler, Angriffsszenarien oder technische Mängel sofort erkennen und beheben zu können.

Im Rahmen eines internen Vulnerability-Managements wird die komplette Infrastruktur regelmäßig auf den neuesten Stand der Technik gebracht. Es wird stets nach bekanntwerdenden Schwachstellen von eingesetzten Softwarebasiskomponenten oder Infrastrukturkomponenten geforscht und bei Bekanntwerden umgehend gehandelt.

Nach Bedarf werden zudem Penetrationstests durch externe Dienstleister durchgeführt, damit potenzielle Sicherheitslücken schnell erkannt werden.

6. Vorteile gegenüber On-Premises

In der Cloud betriebene Dienste können in einigen Fällen Sicherheitsrisiken minimieren. Möchte man beispielsweise bei einer lokal betriebenen Lösung den Zugriff über das Internet gewähren, muss eine eingehende Kommunikation zugelassen werden. Das heißt: Die Unternehmensfirewall muss geöffnet werden. Alternativ hierzu, wird oft ein VPN-Zugang ermöglicht. Das Sicherheitsrisiko in beiden Fällen ist enorm: Gelangt der Zugang an Dritte, kann der Angreifer oft auf die komplette Infrastruktur des Unternehmens zugreifen.

Anders ist dies bei Portal Lösungen: Weder das Unternehmen noch entfernte Liegenschaften müssen eingehende Verbindungen in der Firewall freischalten. Die Kommunikation erfolgt verschlüsselt in Richtung Cloud Portal. Sollten die Zugangsdaten an Dritte gelangen, sind die restlichen Daten im Unternehmen weiterhin geschützt.

7. Betriebssicherheit und Redundanz

Die econ live Cloud wird auf einem verteilten Cluster betrieben, wodurch eine hohe Verfügbarkeit gewährleistet ist. Durch den Betrieb in einem verteilten Datenzentrum ist der Reibungslose Betrieb auch bei Stromausfall, Hardwareschäden oder Brand möglich.

8. Mitwirkungspflicht des Kunden

Trotz aller Bemühungen seitens des Cloud Betreibers kann ein sicherer Betrieb nur dann gewährleistet werden, wenn auch die Benutzer mit erweiterten Systemberechtigungen, sowie die Systemintegratoren mitwirken. Folgende Sicherheitsmaßnahmen sollten in jedem Fall erfüllt werden:

- Edge Devices sollten stets durch eine Firewall abgesichert sein, die jegliche eingehenden Verbindungsversuche unterbindet
- Die econ live Zugangsdaten müssen vor Dritten geschützt werden, dürfen nicht weitergereicht oder in Klartext dokumentiert werden
- Econ Accounts mit erweiterten Systemrechten sollten durch 2-Faktor-Authentifizerung gesichert werden.

9. Datenschutz

Die econ solutions GmbH nimmt den Schutz der persönlichen Daten sehr ernst. Wir behandeln Ihre personenbezogenen Daten vertraulich und entsprechend der gesetzlichen Datenschutzvorschriften (insbesondere der europäischen DSGVO) sowie unserer Datenschutzerklärung.

Die Nutzung von Drittanbieter-Diensten wurde auf das absolute Minimum reduziert. Innerhalb des Portals werden beispielsweise keine Inhalte von externen CDNs bezogen, zudem wird auf Analytics-Software verzichtet.

Die Kundendaten werden 6-fach redundant in zwei europäischen Rechenzentren in Amsterdam und Dublin (Stand Juli 2020) gespeichert. Dabei wird die Infrastruktur von Microsoft Azure genutzt. Azure erfüllt als erster bedeutender Cloud Anbieter Datenschutzstandards der ISO/IEC 27701. Zudem wurde Azure als erster Plattform die Einhaltung der EU-Standardvertragsklauseln bescheinigt.

Bei der Speicherung von Projektdaten wird sog. „Transparent data encryption“ angewandt, sodass auch BackUps und Logs verschlüsselt werden.