eschbach

SOFTWARE & DATA SECURITY MIT SHIFTCONNECTOR® CLOUD

www.shiftconnector.com

ISO 9001 QUALITY MANAGEMENT

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

INHALTS-ANGABE

VORWORT

Die Enterprise Plattform Shiftconnector® wurde von eschbach speziell für die Prozessindustrie entwickelt und sorgt seit 2005 für mehr Sicherheit und Effizienz in 24/7-Betrieben. Weltweit vertrauen führende Unternehmen, wie Bayer, DuPont, BASF und Roche, auf Shiftconnector®.

Zunächst als On-Premise-Lösung verfügbar, hat sich eschbach auf die steigende Nachfrage nach Cloud-Lösungen eingestellt und bietet Shiftconnector® seit 2015 als Software-as-a-Service an. Dabei hat bei eschbach Datensicherheit höchste Priorität. eschbach's Information Security Management System ist nach ISO 27001 zertifiziert, das Quality Management System nach ISO 9001. Dadurch wird sichergestellt, dass Verfahren wie eine umfassende Zugangskontrolle und Richtlinien für ein kontrolliertes Change Management vorhanden sind, um unsere Shiftconnector-Cloud zu sichern.

Dieses Whitepaper zeigt, wie eschbach für eine maximale Cloud Security sorgt und gleichzeitig die Vertraulichkeit, Integrität und Verfügbarkeit von Systemen und Daten in der Shiftconnector®-Cloud sichert.

SICHERE ARCHITEKTUR

Infrastruktur

Um ein hohes Maß an Verfügbarkeit und Stabilität zu gewährleisten, wird die Software-as-a-Service-Lösung in einer dedizierten virtuellen Cloud betrieben. Kunden können zwischen einem Cloud-Rechenzentrum mit Standort in Newark (NJ) in den USA oder Standort in Frankfurt am Main (Deutschland) wählen. Für das US-Rechenzentrum liegt ein SOC-2-Report vor. Sowohl das US-amerikanische als auch das deutsche Rechenzentrum sind nach ISO 27001 zertifiziert.

Der Zugang zu Cloud-Systemen und -Applikationen ist durch mehrere Firewall-Schichten gesichert. Die Server sind so konfiguriert, dass sie nur die erforderlichen Ports zulassen. Mit IP-Whitelisting kann der Zugriff auf Kundenressourcen zusätzlich gesichert werden.

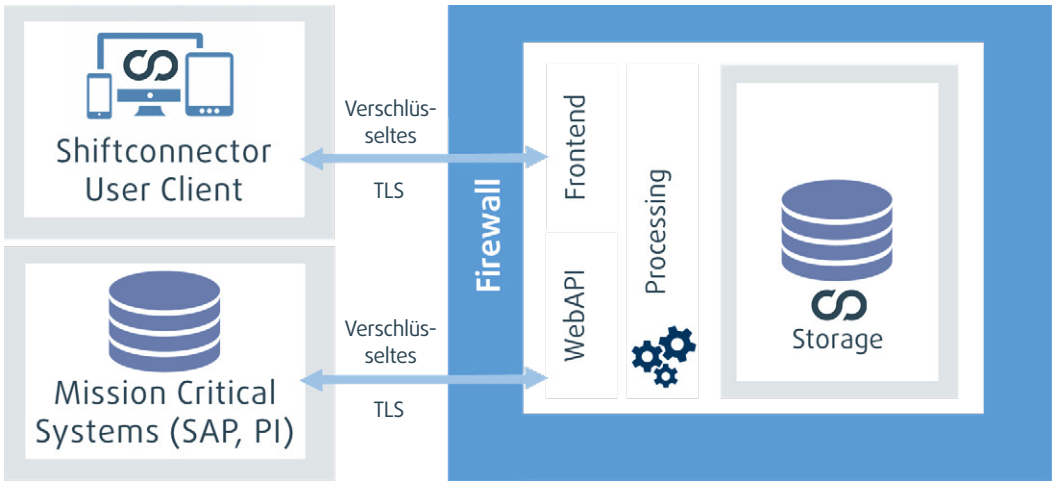
Gleichzeitig wird bei der Software-as-a-Service-Lösung ausschließlich auf *https* gesetzt – auch zur Kommunikation mit Dritten. Dies wird sowohl auf der Server- als auch auf der Anwendungsebene umgesetzt.

Software

Neben der Infrastruktur wird auch die Software maximal gesichert. Für die Entwicklung und den Betrieb von Shiftconnector® befolgt eschbach Richtlinien zur Umsetzung eines sicheren Softwarelebenszyklus.

Security-Maßnahmen sind für eschbach von Anbeginn – von der Aufnahme erster Kundenanforderungen über die Bereitstellung bis hin zum Service nach dem Release – von zentraler Bedeutung. Zu diesen Maßnahmen gehören der Einsatz von Security Champions, Security Code Reviews, automatisierte Sicherheitsanalysen, ein sicherer Build-Prozess und viele mehr. Kritische Werte, wie z.B. die Anwendungseinstellungen oder die Autorisierungs-Tokens für die mobile Shiftconnector® GO-App, werden verschlüsselt gespeichert.

Die Anwendung verfügt über eine Architektur, bei der mehrere Benutzer mit integrierten und erweiterbaren Autorisierungsrollen Zugriff erhalten können. Für die Authentifizierung und Autorisierung unterstützt Shiftconnector® etablierte Identitätsanbieter, wie beispielsweise OpenIDConnect, auf dem Azure AD basiert.



Secure Cloud Infrastructure

SICHERUNG UND BACKUP

Die Zugriffsmöglichkeit auf ein effizientes Backup stellt die Basis zur Sicherung von Betriebsabläufen dar. Dazu gehört nicht nur die Verfügbarkeit der Anwendungen und Systeme, sondern auch der zugrunde liegenden Daten. Insbesondere im Falle eines Datenverlustes, ist die Verfügbarkeit und Integrität eines Backups der Daten von entscheidender Bedeutung.

Um dies erfüllen, setzt eschbach geo-redundante Server und Datenbank-Backups ein. Ausgehend von Zeitintervallen von wenigen Stunden bis hin zu mehreren Monaten werden diese Backups dokumentierten Backup- und Restore-Tests unterzogen, um deren Funktionalität sicherzustellen.

Außerdem gibt es Verfahren für den Umgang mit Störungen und Disaster Recovery, um den weiteren Betrieb zu sichern. Strategien für Disaster Recovery und zur Aufrechterhaltung des Betriebs sind Bestandteil des nach ISO 27001 zertifizierten Information Security Management.

MONITORING

eschbach's Security Monitoring basiert auf Informationen, die aus den internen Netzwerken, Servern, Anwendungsdaten, Konfigurationsdaten und Open-Source-Informationen gewonnen werden. Für das interne Netzwerk und die Cloud-Server überwacht eschbach verschiedene Metriken, um die Verfügbarkeit, den Zustand und die Sicherheit seiner Systeme zu bestimmen. Zusätzliche Endpoint-Protection-Lösungen und Monitoring-Programme überprüfen die Konfiguration der Cloud-Lösung auf Fehlkonfigurationen, die zu einer Schwachstelle führen könnten.

Darüber hinaus werden mit einer Threat Intelligence, wie Honeypots und Open-Source-Quellen, Informationen über Bedrohungen gesammelt. Systeme werden anhand öffentlich zugänglicher Datenbanken mit gemeldeten IPs insbesondere auf Malware oder schädliche Aktivitäten überprüft. Dies bietet eine zusätzliche Sicherheitsebene, die sich nicht nur auf interne, sondern auch auf externe Daten stützt.

eschbach führt Identity Leakage Monitoring durch. Damit können unsichere Zugangsdaten in Verbindung mit der Shiftconnector-Cloud identifziert werden. Wenn zum Beispiel Schadsoftware das Endgerät eines Cloud-Kunden infiziert, könnten theoretisch Anmeldedaten, die zu eschbach's Cloud-Domäne gehören, gestohlen und veröffentlicht werden. eschbach sucht gezielt nach derartigen veröffentlichten Datensätzen. So können Datenlecks gefunden werden, die die Cloud-Sicherheit beeinträchtigen könnten.

eschbach setzt ein internes Experten-Team ein, das sich um die Überwachung und Analyse der Cloud-Lösung kümmert. Im Falle eines Alarms sind verschiedene Nachrichtenkanäle implementiert, um sicherzustellen, dass Kunden schnellstmöglich informiert werden und entsprechend reagieren können.

ANALYSEN UND TESTS

Regelmäßige Tests und Analysen der Infrastruktur und der gehosteten Anwendung sind von entscheidender Bedeutung. Das Security-Team von eschbach arbeitet eng mit externen Partnern, wie der Deutschen Cyber-Sicherheitsorganisation (DCSO)[1], zusammen. Damit können sie mehrere Analysen auf verschiedenen Ebenen der Infrastruktur durchführen.

Infrastruktur

Die eschbach-Cloud-Infrastruktur und ihre (Web-) Server werden jährlich ausgewertet. In den Jahren 2021 und 2022 führte TÜV Rheinland[2] einen externen Penetrationstest durch (Weitere Details). Die Analyse beinhaltet einen Black-Box-Ansatz, der die Analyse von „außen" durchführt. Dabei wird versucht die Infrastruktur aus Sicht eines Angreifers anzugreifen. Einen wichtigen Teil der Analyse stellen bekannte Standards dar. Dabei kommen sowohl automatisierte als auch manuelle Analysen der Cloud-Server und -Dienste zum Einsatz. Die Sicherheit der Cloud wird durch ein mehrstufiges Verfahren von erfahrenen Experten gewährleistet.

Die Cloud-Infrastruktur wird auch von innen durch Compromise Assessments analysiert. Ziel ist es, Spuren von aktuellen und vergangenen Angriffen im System und Netzwerk zu finden. Dies ist insbesondere im Hinblick auf Advanced Persistent Threats relevant. Für die Compromise Assessments arbeitet eschbach eng mit der DCSO zusammen.

Software

Zusätzlich zu eigenen Tests, führte TÜV Rheinland in den Jahren 2021 und 2022 einen Penetrationstest für die Cloud-Instanz der von eschbach gehosteten Software Shiftconnector® durch. Sowohl Black-Box- als auch Grey-Box-Tests wurden durchgeführt, um die Cloud-Anwendung zu verifizieren. Diese Tests orientieren sich an den Richtlinien, die die wichtigsten Sicherheitsrisiken für Webanwendungen darstellen.

---

1 DCSO: Allianz SE, BASF SE, Bayer AG und Volkswagen AG haben 2015 die Deutsche Cybersicherheitsorganisation im Jahr 2015 gegründet, um organisierter Cyberkriminalität und staatlich gelenkter Wirtschaftsspionage zu bekämpfen.

2 TÜV Rheinland steht für Sicherheit und Qualität in nahezu allen Bereichen der Wirtschaft und des Lebens. Vor mehr als 150 Jahren gegründet, ist das Unternehmen heute mit mehr als 20.600 Mitarbeitern einer der weltweit führenden Prüfdienstleister

INCIDENT MANAGEMENT

eschbach's Team unterhält ein umfassendes Programm zur Reaktion auf Vorfälle und zur forensischen Analyse. Für den Fall eines Vorfalls, der die Vertraulichkeit, Integrität oder Verfügbarkeit von Systemen oder Daten beeinträchtigen könnte, verfügt eschbach über umfassende Verfahren zur Früherkennung, Kommunikation, Schadensbegrenzung und forensischen Analyse. Vorfälle, die die Cloud und Kundendaten betreffen, haben höchste Priorität. Darüber hinaus arbeitet eschbach mit der DCSO, um forensische Unterstützung zu leisten und auf Vorfälle zu reagieren.

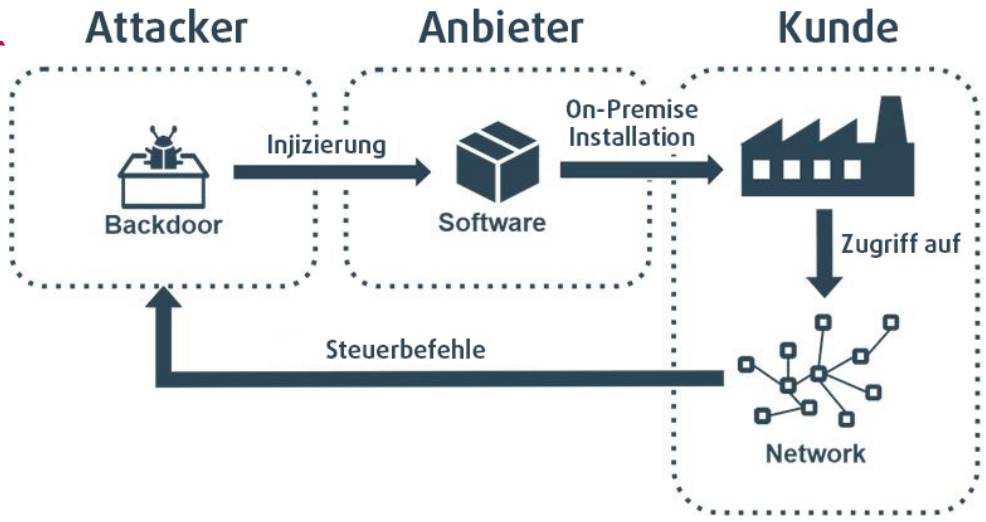
GEFAHREN-LANDSCHAFT

Um die richtigen Maßnahmen und Prioritäten setzen zu können, setzt sich eschbach intensiv mit deren Gefahrenlandschaft auseinander. Insbesondere die Daten der Pharmaindustrie sind ein wertvolles Ziel für Cyber-Kriminelle. Als Softwarelieferant für Branchen mit einem sehr hohen Sicherheitsanspruch, muss eschbach die Bedrohungen seiner Kunden und sich selbst, kennen, verstehen und darauf reagieren können. Aus diesem Grund analysiert eschbach Gefahrenlandschaften und arbeitet dazu eng mit der DCSO zusammen. Auf der Grundlage dieser Erkenntnisse wird eine Sicherheitspriorisierung vorgenommen, die entsprechend der aktuellen Bedrohungslage von eschbach's Kunden und eschbach selbst aufstellt wird. Darüberhinaus ist eschbach ist Mitglied der DCSO-Community, was ihnen einen direkten Austausch mit anderen Experten und den Zugang zu exklusiven Inhalten und Erkenntnissen ermöglicht.

ANGRIFFE AUF LIEFERKETTEN

Vergangene Angriffe auf Software-Lieferketten, wie beispielsweise der SolarWinds-Hack, haben gezeigt, wie gefährlich es ist, Software innerhalb des eigenen Netzwerks und der eigenen Infrastruktur zu betreiben und zu aktualisieren. Im Gegensatz dazu bietet die Verwendung einer SaaS-Lösung zusätzlichen Schutz gegen Angriffe auf Lieferketten. Da die Software nicht direkt im Netzwerk des Kunden platziert wird (im Gegensatz zu On-Premise-Installationen), verfügen die Kunden über eine zusätzliche Sicherheitsebene durch den Browser. Außerdem müssen sich die Kunden nicht um die Systemsicherheit und das Patching kümmern.

Auch bei SaaS-Lösungen sind Schutzmaßnahmen gegen Angriffe auf die Software-Lieferketten erforderlich. Als Gegenmaßnahme hat eschbach einen umfassenden Secure Software Lebenszyklus zum Schutz vor Angriffen auf Softwarelieferketten entwickelt. Dieser Software-Lebenszyklus unterstützt auch die Transformation von DevOps zu DevSecOps. Mehr über zur Sicherung von Softwarelieferketten, den entwickelten sicheren Software-Lebenszyklus und unsere Analysen können Sie in unserem white-paper dazu nachlesen.



eschbach

Um mehr über eschbach oder Shiftconnector® zu erfahren, kontaktieren Sie uns gerne:

www.shiftconnector.com
info@eschbach.com

Europe HQ: +49 (0) 7761 55959-0
Bad Saeckingen, Germany

USA & Canada: +1 (617) 618-5261
Boston, MA

Über eschbach und Shiftconnector®
eschbach mit Hauptsitz in Bad Säckingen, Süddeutschland, und einer Niederlassung in Boston, USA, entwickelt Software für die Prozessindustrie. Shiftconnector® ermöglicht ein neues Niveau der Schichtkommunikation, um die Sicherheit zu erhöhen und die Produktivität der Anlagen zu verbessern. Die mehrfach ausgezeichnete Enterpise Applikation wird weltweit von führenden Unternehmen wie Bayer, DuPont, BASF und Roche eingesetzt. Weitere Informationen unter www.eschbach.com.