TAC The Assistant Company

Sicherheitsaspekte der Cloud: Was Sie wissen müssen

Dieses Whitepaper gilt für die TAC-Cloud-Produkte und Dienste. Der hierin enthaltene Inhalt entspricht dem Stand vom April 2024 und repräsentiert den aktuellen Stand zum Zeitpunkt der Erstellung. Die TAC-Sicherheitsrichtlinien und -systeme können sich in Zukunft ändern, da wir den Schutz für unsere Kunden kontinuierlich verbessern.

Einleitung

TAC bietet seit mehr als einem Jahrzehnt sichere und zuverlässige Cloud-Dienste an. Unsere Cloud-Service-Angebote sind exklusiv für die TAC-Anwendungssuite und integrierte Partnerdienste. Der Schutz unserer Kunden und ihrer Daten ist eine vorrangige Priorität des Unternehmens und eine gemeinsame Verantwortung aller TAC-Teammitglieder.

Der Ansatz der TAC für die Informationssicherheit basiert auf den drei Grundpfeilern Vertraulichkeit, Integrität und Verfügbarkeit. Dieses Whitepaper konzentriert sich auf die organisatorischen und technischen Kontrollen, die innerhalb der Cloud-Service-Umgebung zum Schutz und zur Sicherung Ihrer Daten eingesetzt werden.

Operative Sicherheit

Schwachstellenmanagement

TAC scannt seine Cloud-Service-Umgebung regelmäßig auf Schwachstellen in Zusammenarbeit mit Arctic Wolf und USD AG. Interne und externe Schwachstellen-Scans werden monatlich durchgeführt. Alle identifizierten Schwächen werden überprüft und je nach Schweregrad und Anwendbarkeit auf die Umgebung priorisiert von TAC oder unserem Hosting-Provider behoben.

Schutz der Endgeräte

Die TAC-Cloud-Services sind von den Client-Netzwerken des Unternehmens isoliert. Jeder Server innerhalb der Cloud-Umgebung verwendet Antiviren- und Malware-Schutz sowie Security Log Monitoring (SIEM).

Netzwerk Firewalls

Die TAC nutzt redundante Netzwerk-Firewalls der Unternehmensklasse mit UTM-Funktionen zum Schutz ihres Cloud-Service-Netzwerks. Die Firewalls werden in einem expliziten Verweigerungsmodus eingesetzt, bei dem nur Datenverkehr mit, von unseren Ingenieuren erstellten Genehmigungen, die definierten Zonen durchqueren darf.

Umgebungs- und Applikations-Monitoring

TAC verfügt über ein robustes, mehrstufiges Überwachungsprogramm, das einen vollständigen Überblick über das Ökosystem der Cloud-Services bietet. Es gibt eine SIEM-Lösung zur Überwachung und zentralen Erfassung von Sicherheitsinformationen und Ereignissen. Zusätzlich gibt es eine automatische Überprüfung und Korrelation von Ereignissen, die eine weitere Überprüfung erfordern. Diese werden an das technische Team weitergeleitet.

Unser Hosting-Provider und unsere Techniker abonnieren Anbieter- und Sicherheits-Mailinglisten und überprüfen diese regelmäßig, um potenzielle Bedrohungen oder anwendbare Sicherheits-Patches zu identifizieren.

Technologie Plattform

Führende Partner für den Rechenzentrumsbetrieb

Das Datacenter der TAC befindet sich in Wien und wird von RKP IT-Solutions betrieben. Die Anlage verfügt über eine Reihe von physischen Sicherheitsvorkehrungen, wie 24/7-Überwachung durch Innen- und Außenkameras, Zaunsystem, Pförtner und vieles mehr. Nur ausgewiesene Mitglieder des RKP IT-Solutions Hosting-Teams haben eine Zugangsberechtigung zum Rechenzentrum.

Um eine 24/7-Betriebszeit zu gewährleisten, verfügt das Datacenter über eine redundante Stromversorgung, die auch ein USV-Batterie-System umfasst, welches das gesamte Rechenzentrum im Falle eines Stromausfalls versorgen kann. Redundante Kühlsysteme sorgen für ein optimales Betriebsklima für die Hardware. Automatisierte Umgebungsüberwachung und Alarmierung reduzieren das Risiko ungeplanter Ausfälle. Jedes Rechenzentrum ist außerdem mit Brandmelde- und Feuerlöschanlagen ausgestattet, um mögliche Schäden im Falle eines Brandes zu verhindern.

Das Rechenzentrum unterhält eine Reihe von Initiativen zur Einhaltung von Industriestandards, um die Sicherheit und den Schutz Ihrer Daten zu gewährleisten (ISO27001, ISAE3402).

Sichere Datenübertragung

Die Sicherung von Daten bei der Übertragung zu unserer gehosteten Umgebung hat für TAC höchste Priorität. Für die Verbindung zu den von der TAC bereitgestellten Anwendungsendpunkten sind nur Transport Layer Security (TLS) 1.2 oder höhere Verschlüsselungsprotokolle zulässig. Dies steht im Einklang mit dem PCI-DSS-Sicherheitsrahmen, der frühere Versionen von TLS (1.1 & 1.0) und dessen Vorgänger SSL (Secure Socket Layer) außer Kraft gesetzt hat. Die Systeme werden regelmäßig gescannt, um einen sicheren Einsatz von Zertifikaten und eine Best-Practice-Implementierung über alle öffentlich zugänglichen Anwendungsendpunkte zu gewährleisten.

Hochverfügbarkeit

Die Redundanz ist in allen Aspekten unserer Umgebungsarchitektur berücksichtigt. Die TAC verwendet redundante physische Server und unterstützende Netzwerk- und Speichersysteme. Unsere redundante Architektur trägt zum Schutz vor Datenverlusten bei und ermöglicht es der TAC, zuverlässige Wiederherstellungszeiten zu bieten.

Die TAC führt monatlich routinemäßige Wartungsarbeiten durch. Die Wartungsfenster sind in der Regel am frühen Morgen für einen Zeitraum von 4 Stunden geplant. Die Vorankündigung erfolgt mindestens 7 Tage im Voraus. Es ist zwar möglich, dass die Anwendung während eines Großteils dieses Zeitfensters ausfallen kann, normalerweise liegt die Ausfallszeit jedoch deutlich darunter.

PCI Compliance

Die TAC überträgt, speichert oder verarbeitet keine Kreditkartendaten. Wir verwenden Tokenisierungslösungen, mit PCI-compliant Gateways, um den PCI- Anwendungsbereich unserer Kunden weiter zu reduzieren. Darüber hinaus wird jedes Quartal ein externer Schwachstellen-Scan durch einen von PCI zugelassenen und gelisteten Scanning-Anbieter durchgeführt.

Datenschutz

Wissenswertes

Die TAC-Kunden sind Eigentümer ihrer Daten. Bitte lesen Sie unsere Datenschutzbestimmungen auf unserer Website (https://www.tac.eu.com/datenschutzerklaerung/).

Datenzugriff und Einschränkungen

Zugriffsrechte für Administratoren

Die Zugriffsrechte auf die Komponenten des TAC-Systems sind auf autorisiertes Personal beschränkt. Darüber hinaus sind Benutzer mit Superuser-Rechten, wie z. B. Systemadministratoren dafür verantwortlich, dass die Zugriffsrechte für alle Benutzer (sowohl Endbenutzer als auch Benutzer mit erweiterten Superuser-Rechten) den eigenen Rollen und Verantwortlichkeiten innerhalb der TAC entsprechen.

Authentifizierung

Die Authentifizierung gegenüber den Komponenten des TAC-Systems erfolgt über einen Benutzernamen und ein Passwort. Es gelten strenge Passwortrichtlinien. Systemadministratoren haben noch strengere Passwortrichtlinien und benötigen einen zusätzlichen Faktor zur Authentifizierung (2FA).

Fernwartung

Der administrative Zugriff auf die Hosting-Umgebung ist nur von einem TAC-Organisationsnetz aus möglich. Nur zugelassene Protokolle dürfen verwendet werden, um sicherzustellen, dass eine vertrauenswürdige Verbindung initiiert, aufgebaut und aufrechterhalten wird. Insbesondere müssen alle Benutzer die zugelassene VPN für den Fernzugriff nutzen, zusammen mit zusätzlichen unterstützenden Maßnahmen, einschließlich der Zwei-Faktor-Authentifizierung. Das Konzept der Zwei-Faktor-Authentifizierung schafft in Kombination mit strengen Passwortrichtlinien eine weitere Sicherheitsebene in Bezug auf die Zugriffsrechte für alle autorisierten Benutzer, denen Fernzugriff auf das Netz gewährt wird.

Darüber hinaus muss auf allen Arbeitsplätzen (sowohl firmeneigene als auch mitarbeitereigene) eine aktuelle Antivirensoftware installiert sein, wobei auch weitere Tools zum Einsatz kommen, um die Datenübertragung zu schützen.

Zugriffsrechte Anwender

Innerhalb der Anwendungsinstanz eines Kunden sind die administrativen Rollen und Zugriffsrechte für die Anwendung zur Cloud-Sicherheit durch rollenbasierte Zugriffskontrolle (RBAC) definiert. Kundenadministratoren haben die Möglichkeit, die Zugriffsrechte von Personen auf die verschiedenen Funktionen und Datenbereiche innerhalb des Systems selbst zu verwalten.

Fazit

Die TAC räumt der Sicherheit als Teil ihrer gesamten organisatorischen Denkweise Priorität ein und arbeitet ständig daran, ihren Schutz vor Bedrohungen im Hinblick auf die sich ständig verändernde Bedrohungslandschaft weiterzuentwickeln. TAC bietet eine Reihe von robusten und mehrschichtigen Schutzmaßnahmen um die Daten ihrer Kunden zu schützen und eine leistungsstarke, hochverfügbare Lösung bereitzustellen. Wenn Sie mehr erfahren möchten, vereinbaren Sie einen persönlichen Beratungstermin.