Service Level Agreement

(Leistungsbeschreibung)

CDC Network Security Service

Code: FS-CDC-NSM
Version: 3.0
Gültig ab 01.01.2025

CANCOM Austria AG // Wienerbergstraße 53 // 1120 Wien // Österreich // T +43 50 822 0 // info@cancom.com
HG Wien FN 178368g // Firmensitz Wien // UID ATU46276408 // InterzeroNr. 155219
Raiffeisenlandesbank Oberösterreich // BIC: RZOOAT2L // IBAN: AT35 3400 0000 0009 7899 // Creditor-ID: AT17ZZZ00000029797
www.cancom.at

Leistungen des Auftragnehmers

Dieses Dokument beschreibt die Serviceleistungen des Servicemoduls, welche im Rahmen des zwischen dem Auftraggeber (AG) und Auftragnehmer (AN) abgeschlossenen Vertrages erbracht wird. Die Verantwortlichkeiten der beschriebenen Leistungen sind auf Basis eines RACI-Modells abgebildet. Begriffserklärungen sowie Kontakt Informationen des Customer Service Center sind unter folgendem *Link* zu finden.

Sofern nichts Gegenteiliges vereinbart ist, gelten standardmäßig folgende Serviceziele: Servicezeit „SNAZ“ (NWH) mit einer Reaktionszeit von 4 Stunden.

CDC Network Security Service

Network Security Monitoring bezieht sich auf die Überwachung von Netzwerken und Systemen, um deren Leistung, Verfügbarkeit und Sicherheit sicherzustellen.

Initiale Leistungen	AN	AG
Bestandsaufnahme der bestehenden IT-Infrastruktur und Abstimmung der erforderlichen technischen Services mit dem Auftraggeber	R/A	C/I
Implementieren der beim Auftraggeber installierten NSM Appliance	R/A	C/I
Hinterlegen der Kontaktdaten der vom Auftraggeber definierten Ansprechpersonen im Service Management System des Auftragnehmer	R/A	C/I
Definieren, Einrichten und Testen des Zuganges	R/A	C/I

Wiederkehrende Leistungen	AN	AG
Prüfung des Netzwerkverkehrs auf Anomalien mittels Signaturen und Reputationsdaten		
Im Modul für Network Security Monitoring (NSM) wird der Datenverkehr am Egress Point erfasst, also dem Punkt, an dem Daten in das Unternehmen hinein- oder herausgehen. Diese Daten werden an die NSM-Appliance des Auftragnehmers gesendet, wo sie vollständig und verschlüsselt über mehrere Tage gespeichert werden. Der gespeicherte Traffic wird automatisiert und teilautomatisiert auf Anomalien und Angriffe hin überprüft, wobei auch manuelle Analysen bei Auffälligkeiten durchgeführt werden. Zur Erkennung von Anomalien werden verschiedene Technologien eingesetzt, darunter Intrusion Detection Systeme, Threat Intelligence und Reputationslisten, statistische und mathematische Auswertungen sowie Algorithmen. Auch die Überprüfung von übertragenen Dateien, wie beispielsweise ausführbaren Dateien, ist Teil des Prozesses. Network Security Monitoring am Egress Point ermöglicht nicht nur die Entdeckung von Angreifern, die ins Netzwerk eindringen möchten, sondern auch die Identifizierung kompromittierter Systeme, die mit ihren Command-and-Control-Servern im Internet kommunizieren wollen. Diese Kommunikationsrichtung wird üblicherweise als Nord-Süd-Kommunikation bezeichnet. Die Erkennung von Ost-West-Kommunikation, also dem Datenverkehr zwischen einzelnen Systemen innerhalb des Netzwerks, ist dabei jedoch nicht abgedeckt.	R/A	C/I

Analyse der Daten, Deklaration von erkannten, sicherheitsrelevanten Bedrohungen		
Nach der Analyse und Feststellung, dass eine Bedrohung für die Sicherheit oder eine Sicherheitslücke im Netzwerk besteht, erfolgt unverzüglich eine Benachrichtigung des Auftraggebers über diese Ergebnisse.	R/A	C/I
Erkennung von Anomalien mittels Threat Intelligence		
Um seine Analysen mit mehr Inhalten und Anhaltspunkten zu bereichern, integriert der Auftraggeber Threat Intelligence. Diese Art der Intelligence wird aus verschiedenen Quellen bezogen, die laufend auf ihre Qualität und Nutzen überprüft und evaluiert werden. Falls eine Quelle nicht den Anforderungen des Cyber Defense Center entspricht, wird sie durch eine andere ersetzt. Es werden verschiedene Arten von Threat Intelligence eingesetzt, darunter: Open Source Intelligence (OSINT): Informationen, die aus öffentlich zugänglichen Quellen stammen. Kommerzielle Intelligence verschiedener Hersteller: Informationen von kommerziellen Anbietern von Threat Intelligence. Intelligence von internationalen CERT-Verbünden: Informationen von internationalen Computer Emergency Response Teams (CERT), die in einem Verbund zusammenarbeiten.	R/A	C/I
Security Reports über Bedrohungen und Risiken inklusive Darstellung der erforderlichen Maßnahmen		
Gemäß der getroffenen Vereinbarung erhält der Auftraggeber in regelmäßigen Abständen einen Security Report vom Auftragnehmer. Dieser Bericht bietet in einer Management Summary einen Überblick über die Bedrohungen im Netz, darunter Top Threats mit Risikobewertung und detaillierte Informationen zu den jeweiligen Bedrohungen. Zusätzlich werden technische Details zu Analyse- und Klassifizierungsergebnissen bereitgestellt. Im Rahmen des Berichts werden sowohl kurz- als auch langfristige Maßnahmen entwickelt, die darauf abzielen, zukünftige Bedrohungen zu verhindern oder zumindest zu erschweren. Diese Maßnahmen werden dem Auftraggeber im Bericht als Empfehlungen präsentiert. Wenn mehrere Module aus dem Angebot des Auftragnehmers eingesetzt werden, werden die Ergebnisse dieser Module in einem umfassenden Bericht zusammengefasst. Die Präsentation und Diskussion des Berichts finden zuvor festgelegten Zeitabständen statt.	R/A	C/I

Mitwirkungspflichten des Auftraggebers	AN	AG
Bereitstellung von Dokumentationen		
Der Auftraggeber stellt im Rahmen des Onboarding-Prozesses sämtliche erforderliche Dokumentation bereit, darunter den Netzwerkplan sowie Informationen zu IP-Adressen, Servernamen und genutzten Services. Zusätzlich müssen alle technischen Voraussetzungen seitens des Auftraggebers erfüllt werden.	C/I	R/A
Bereitstellung von notwendiger Hardware		
Der Auftragnehmer stellt dem Auftraggeber ein Webportal zur Verfügung, auf dem alle relevanten Security Incidents eingesehen werden können. Um dieses Portal nutzen zu können, muss der	C/I	R/A

Auftraggeber dem Auftragnehmer eine virtuelle Maschine bereitstellen, da das Portal lokal beim Auftragnehmer gehostet wird.		

Rahmenbedingungen für die Leistungserbringung

Der Auftragnehmer benötigt während der gesamten Vertragslaufzeit kontinuierlichen Zugriff auf die Cyber Defense Center (CDC) Appliance. Der Auftraggeber selbst hat keinen direkten Zugriff auf die Appliance oder die darauf gespeicherten Daten. Nach Abschluss der Vertragslaufzeit wird der Auftragnehmer die Daten auf der CDC Appliance löschen.
Während des Onboarding-Prozesses ist der Auftraggeber dafür verantwortlich, notwendige Dokumente auszufüllen und verfügbare IT- und Personalressourcen bereitzustellen. Dies beinhaltet die Einrichtung einer virtuellen Appliance gemäß den Vorgaben des Auftragnehmers, die Bereitstellung von Microsoft-Lizenzen während der Implementierungsphasen und des Betriebs der Services sowie die aktive Unterstützung bei der Einrichtung des Fernzugriffs.
Zur effizienten Kommunikation und Koordination werden auftraggeberseitig bis zu fünf Ansprechpartner festgelegt, die als Schnittstelle für den laufenden Betrieb dienen.

Nicht enthaltene Leistungen

Analysen von Endpoint- oder Serversystemen und Logfiles jeglicher Systeme des Auftraggebers
Umsetzung der im Security Report empfohlenen Maßnahmen
Umsetzung von Maßnahmen um einen Security Incident einzudämmen
Neuinstallation oder Patchen von Systemen
Technische Voraussetzung um Netzwerktraffic abzugreifen