Service Level Agreement

(Leistungsbeschreibung)

CDC Vulnerability Management

Code: FS-CDC-VUL
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 Vulnerability Management

Vulnerability Management in der Cyberabwehr bezeichnet den Prozess der Identifizierung, Bewertung und Behandlung von Sicherheitslücken in Computersystemen, Netzwerken und Anwendungen, um das Risiko von Sicherheitsverletzungen zu minimieren.

Initiale Leistungen	AN	AG
Bestandsaufnahme der Assets mit dem Kunden	R/A	C/I
Implementieren des Asset Monitorings	R/A	C/I
Hinterlegen der Kontaktdaten der vom Kunden definierten Ansprechpersonen im Service Management System des Auftragnehmers	R/A	C/I

Wiederkehrende Leistungen	AN	AG
Prüfung der in der Netzwerkumgebung betriebenen Assets auf Software-Schwachstellen		
Das Vulnerability Management (VUL) Modul führt automatisierte Prüfungen der Netzwerkumgebung durch, um unbekannte IT-Assets zu identifizieren. Zudem werden alle IT-Assets, sowohl bekannte als auch unbekannte, auf bereits bekannte Software-Schwachstellen getestet (Schwachstellen-Scan). Auf Wunsch des Auftraggebers kann ein authentifizierter Scan durchgeführt werden, der tiefere Einblicke in das Zielsystem ermöglicht. Hierfür müssen die notwendigen Zugangsdaten (Credentials) vom Auftraggeber bereitgestellt werden. Die Überprüfung der Systeme erfolgt kontinuierlich mithilfe von Tools führender Anbieter aus der Cyber Security-Branche. Die Ergebnisse, die sämtliche gefundenen Schwachstellen umfassen, dienen als Grundlage für die weitere Verfolgung, bis diese behoben, gepatcht oder abgemildert sind. Auf Wunsch kann der Auftraggeber über die Erkennung unbekannter Geräte im Netzwerk informiert werden, um zusätzliche Transparenz zu gewährleisten.	R/A	C/I
Analyse der Daten & Deklaration von erkannten, sicherheitsrelevanten Bedrohungen		
Wird nach der Schwachstellenanalyse festgestellt, dass eine Bedrohung der Sicherheit (z.B. eine Sicherheitslücke im Netzwerk) besteht, wird der Auftraggeber über diese in Form des übermittelten Scan Ergebnisses informiert.	R/A	C/I

Security Reports über Bedrohungen und Risiken inklusive Darstellung der erforderlichen Maßnahmen		
Der regelmäßige Security Report für den Auftraggeber bietet gemäß Vereinbarung eine Management Summary mit einem Überblick über Netzbedrohungen, einschließlich Top Threats mit Risikobewertung und detaillierten Informationen zu jeder Bedrohung. Der Bericht enthält darüber hinaus ausführliche technische Details, die die Analyse und Klassifizierung der Ereignisse betreffen. Die Scan-Ergebnisse werden umfassend beschrieben und enthalten Maßnahmenempfehlungen, die darauf abzielen, zukünftige Bedrohungen zu verhindern oder zumindest zu erschweren. Diese Empfehlungen werden dem Auftraggeber zusammen mit dem Bericht als Handlungsempfehlung präsentiert.	R/A	C/I

Mitwirkungspflichten des Auftraggebers	AN	AG
Bereitstellung von Dokumentationen		
Bereitstellung von Dokumentation (Netzwerkplan, IP-Adressen – Servernamen – Services) und aller technischen Voraussetzungen durch den Auftraggeber.	C/I	R/A
Bereitstellung von notwendiger Hardware und Lizenzen		
Der Auftragnehmer stellt dem Auftraggeber ein Webportal zur Verfügung, über das alle relevanten Security Incidents eingesehen werden können. Hierfür muss der Auftraggeber dem Auftragnehmer eine virtuelle Maschine zur Verfügung stellen, da dieses Portal lokal beim Auftraggeber betrieben wird. Dazu gehört beispielsweise die Einrichtung der 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.	C/I	R/A

Rahmenbedingungen für die Leistungserbringung

Der Auftragnehmer benötigt während der gesamten Vertragslaufzeit kontinuierlichen Zugriff auf die Managed Defense Appliance. Der Auftraggeber hat keinen Zugriff auf die Appliance und die darauf befindlichen Daten. Am Ende der Vertragslaufzeit erfolgt die Löschung der Daten auf der Endpoint Appliance durch den Auftragnehmer.

Während des Onboarding Prozesses liegt es in der Verantwortung des Auftraggebers, notwendige Dokumente auszufüllen und verfügbare sowie projektbezogene IT- und Personalressourcen bereitzustellen.

Der Auftraggeber ist dafür zuständig, maximal fünf Ansprechpartner als Schnittstelle für den laufenden Betrieb festzulegen.

Nicht enthaltene Leistungen

Analysen, Darstellung und Nachverfolgung der erforderlichen Maßnahmen zur Eindämmung und Behebung

Analysen von Endpoint- oder Serversystemen sowie Logfiles jeglicher Systeme des Auftraggebers
Umsetzung der im Security Report empfohlenen Maßnahmen
Neuinstallation oder Patchen von Systemen
Firewall-, Routing- oder sonstige Netzwerkkonfigurationen
Herstellung technischer Voraussetzungen auf allen notwendigen System des Auftraggebers um Netzwerkscans durchzuführen (z.B. Firewall Freischaltungen, Einrichten von Benutzerberechtigungen für authentifizierten Scans, …)
Implementierung authentifizierter Scans für sonstige Asset Klassen außer für Windows und Linux Systeme (z.B. für DBs, NW Devices, …)