Service Level Agreement

(Leistungsbeschreibung)

CDC Emergency Response Service

Code: MS-ERS
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 Emergency Response Service

Der Auftragnehmer unterstützt mit dieser Dienstleistung bei der Analyse und Aufklärung von Cyber-Sicherheitsvorfällen.

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

Wiederkehrende Leistungen	AN	AG
Analysieren von Endpoint- und Serversystemen und Logfiles „verdächtiger“ Systeme		
Analyse von Windows Systemen (EDR) Das Cyber Defense Center (CDC) überwacht Server und Clients mit der eingesetzten End Point Detection and Response Lösung (EDR). Auf den Systemen wird ein Agent installiert, der Änderungen und Artefakte am System aufzeichnet und Metainformationen an ein zentrales Management sendet. Die Installation obliegt dem Auftraggeber – wird jedoch vom CDC unterstützt und bereitgestellt. Anomalien, Angriffe und Malware können, in Kombination des EDR Agent sowie des CDC Know-hows, erkannt werden. Dieser Agent wird im Detektionsmodus, für den forensischen Zugriff auf das betroffene System (Betriebssystem Windows), betrieben. Zusätzlich bietet dieser jedoch auch die Möglichkeit auf IOCs, Signaturen sowie verhaltensbasierenden Anomalien zu alarmieren. Durch diesen Agenten ist es möglich direkt nachzuvollziehen, was genau auf den Endgeräten passiert ist, welche Daten von einem Angreifer oder einer Schadsoftware verändert oder erstellt werden bzw. welche Systeme in einem Data Breach involviert waren. Es ist möglich auch die sogenannte Ost-West Kommunikation (Lateral Movement) von Angreifern zu erkennen. Dies ist die Kommunikation eines Angreifers innerhalb des kompromittierten Netzwerks.	R/A	C/I

Wird ein System als kompromittiert identifiziert, besteht die Möglichkeit dieses System unter Quarantäne zu setzen und nur noch zu speziellen Systemen kommunizieren zu lassen. Unabhängig davon, ob sich das kompromittierte System gerade im Firmennetzwerk befindet. Incident Response mit Hilfe anderweitiger Tools – Linux Analyse Incidents welche aus diversen Gründen nicht mit einem EDR Agent analysiert werden können, sind mittels weiterer CDC Tools oder Fernzugriffen zu analysieren. Speziell für Linux/Unix Systeme wird hierbei aus Effizienzgründen primär auf eine System-Live-Zugriff Analyse gesetzt. Es werden die forensischen Artefakte sowie Log-Dateien der/des Linux System/s vom Analysten ausgewertet. Hierfür muss dem CDC Zugriff auf diese Systeme durch den Auftraggeber gegeben werden. Eine Agent-basierende Analyse ist zudem alternativ möglich, wenn auch ineffizienter. Analyse der bereitgestellten sicherheitsrelevanten Log-Dateien Analyse von diversen Log-Dateien (Cloud, Webserver etc.) gegenüber etwaigen erfolgreichen Angriffen wird durch das CDC durchgeführt. Dies basiert anhand der vom Auftraggeber bereitgestellten Log-Dateien. . Die Vorgehensweise ist hierbei vor allem von der Art des Incident bzw. der Log-Dateien abhängig. Eine anschließend tiefere Analyse, kann nach Auswertung der Ergebnisse dieser Dateien mit Hilfe des EDR Agents oder Live-Zugriffen, gegenüber dem kompromittierten System geschehen.		
Erstellen eines Berichtes über Cyber-Sicherheitsvorfälle		
Der Auftraggeber erhält einen Report, der in einer Management Summary einen Überblick über die Analysen und die daraus gewonnenen Erkenntnisse enthält. Zusätzlich liefert der Bericht in einem separaten Abschnitt detaillierte Informationen, wie die Ereignisse analysiert und klassifiziert wurden.	R/A	C/I
Definieren von Maßnahmen und Unterstützung bei der Eindämmung der Bedrohung		
Spezialisten des Auftragnehmers empfehlen dem Auftraggeber Maßnahmen zur Eindämmung der Bedrohung und nehmen eine koordinierende Rolle bzgl. der Bereinigung bzw. Remedierung des Sicherheitsvorfalles ein. Der Auftragnehmer kann den Auftraggeber dabei gerne unterstützen, die Verrechnung erfolgt nach tatsächlichem Aufwand zum gültigen Stundensatz.	R/A	C/I

Rahmenbedingungen für die Leistungserbringung

Der Auftragnehmer hat direkten oder indirekten Zugriff auf die Systeme mit administrativen Rechten, um Daten zu sichern und auf alle Dateien inkl. Hauptspeicher zugreifen zu können. Die Bereitstellung von Dokumentation wie Netzwerkplan, IP-Adressen – Servernamen – Services, etc. und aller technischen Rahmenbedingungen durch den Auftraggeber ist Voraussetzung.
Bei Bedarf wird temporär ein Analysewerkzeug auf den Endgeräten installiert. Der Auftragnehmer benötigt während des gesamten Analysezeitraums Zugriff auf die Werkzeuge (Appliance).

Nicht enthaltene Leistungen
Analyse von Mobile- sowie Smartphones
Analyse von Apple (iOS/MAC OSX) Systemen
Analyse von ICS/OT Systemen, welche nicht auf Linux oder Windows Betriebssystemen basieren
Installation, Deinstallation sowie Ausführung der CDC Tools (z.B. EDR) beim Auftraggeber
Durchführen von On-Demand Antivirenscans
Analyse von Systemen die nicht unter der Hoheit des AG stehen
Technische Remedierung bzw. Bereinigung des Unternehmensnetzwerk
Umsetzung der im Incident Report empfohlenen Maßnahmen
Aktives in Kontakt treten oder Verhandeln mit Angreifern (z.B. bei etwaigen Ransom- oder Lösegeldforderungen)
Durchführen von DSGVO Meldungen im Auftrag des AG
Direkte Kommunikation bzw. Koordination von behördlich hinzugeschalteten Institutionen
Bereitstellen von Vorort Incident-Ressourcen (Incident Handler bzw. Koordinator oder Incident Responder) unterbindenden Zeiten
Forensische Analyse die unter Anwendung der gerichtlich verwertbaren Prozesse basieren. D.h. die Vorgehensweisen werden so gewählt, dass der Sicherheitsvorfall schnellstmöglich bereinigt werden kann (Incident Response) nicht jedoch die gerichtliche Verwertbarkeit gegenüber rechtlichen Instituten sicherstellt
Koordinierung der Remediation/Bereinigung des Incidents (optional)