

CYBER SECURITY OPERATION CENTER

Das neue Cyber Security Operation Center von Reply ist eine Einrichtung, die sich auf die Bereitstellung von Sicherheitsservices auf Premiumniveau spezialisiert hat, die auf die Anforderungen und Prozesse des Kunden sowie auf die speziellen Bedrohungen des Sektors, in dem der Kunde tätig ist, zugeschnitten sind.

Das Cyber Security Operation Center von Communication Valley Reply wurde ursprünglich geschaffen, um die Sicherheitsanforderungen von Banken und Finanzinstitutionen zu erfüllen. Es stellt seine Ressourcen und seine Expertise aber auch Unternehmen zur Verfügung, die in ebenso komplexen Umfeldern wie Einzelhandel, Fertigung und Versorgung tätig sind.



SCHÜTZEN SIE IHR GESCHÄFT

**24 STUNDEN AM TAG,
365 TAGE IM JAHR**

CYBER SECURITY OPERATION CENTER

Das Cyber Security Operation Center ist ähnlich wie ein Kontrollturm täglich rund um die Uhr mit Sicherheitsanalysten, Systemingenieuren, Sicherheitstestern und Malware-Experten besetzt.

Die vom Cyber Security Operation Center (CSOC) angebotenen Services beruhen auf einem neuen Modell zur Sicherheitsüberwachung, in dem auf einer ersten Stufe hochspezialisierte Analysten zum Einsatz kommen. So reduziert das Modell von der allerersten Servicestufe an die Reaktionszeiten und beschleunigt die Umsetzung notwendiger Gegenmaßnahmen.

Eine präventive Erkennung und Echtzeitverwaltung von Sicherheitsvorfällen sind entscheidende Faktoren für die Gewährleistung eines angemessenen Schutzes von Netzwerk, Daten und Diensten in Unternehmen. Im Cyber Security Operation Center führt ein Team aus Experten mithilfe führender Technologien eine Echtzeitüberwachung, Sicherheitsbewertungen sowie die Verwaltung von Sicherheitseinrichtungen durch.

THE SERVICES



CYBER SECURITY MANAGEMENT

Services für Cybersicherheitsmanagement (**Cyber Security Management**) stellen die grundlegenden Sicherheitsmanagementaktivitäten des Kunden sicher. Insbesondere bildet die Sicherheitsüberwachung (Security Monitoring) das primäre Werkzeug zur Erkennung und Handhabung von Sicherheitsvorfällen.

Dieser Service basiert auf der Sammlung und Korrelierung von Ereignissen im Zusammenhang mit der Infrastruktur, den Anwendungen und Systemen des Kunden.

Alle Informationen werden durch die Advanced Security Analytics-Plattform gesammelt, welche die Analyse

der von heterogenen Quellen und von verschiedenen Kunden gesammelten Ereignisse erleichtert.

Ausgehend von diesem Ansatz optimiert das CSOC die Fähigkeit, auch ausgefeilteste Angriffsformen zu erkennen und gleichzeitig durch die logische Trennung der Daten und Informationen zu verschiedenen Clients ein Höchstmaß an Datenschutz sicherzustellen.

Dieselbe Plattform wird auch von Systemingenieuren und Malware-Experten zur Bereitstellung vertikaler Dienste verwendet, wie beispielsweise: Informationen über Cyberbedrohungen (Cyber Threat Intelligence), Erkennen von Sicherheitsverletzungen und Domänenüberwachung.

CYBER SECURITY MANAGEMENT 1	SECURITY TESTING ASSESSMENT SERVICES SYSTEM SECURITY POLICY 1,1	SECURITY DEVICE MANAGEMENT STRONG AUTHENTICATION 1,2	CYBER THREAT INTELLIGENCE CREDENTIAL / CREDIT CARD MONITORING BREACH DETECTION & EARLY WARNING DARK WEB THREAT MONITORING ANTI DEFAACEMENT & DOMAIN MONITORING 1,3	LOG MANAGEMENT SECURITY MONITORING SIEM MANAGEMENT & CONFIGURATION 1,4
--	--	---	--	--

FRAUD MANAGEMENT

Mit der verbreiteten Nutzung von Online- und Multichannel-Diensten war eine Zunahme betrügerischer Aktivitäten verbunden, sowohl in Hinblick auf deren Anzahl als auch auf deren Komplexität. Diese Aktivitäten zielen im Allgemeinen auf den Diebstahl von Identitäten und Anmeldedaten sowie auf das Erlangen anderer, für Betrugsversuche nützlicher Informationen ab.

Im Mittelpunkt der von CSOC gebotenen Services für Betrugsmanagement (**Fraud Management**) stehen die Identifizierung und Analyse von Malware

für verschiedene Arten von Geräten ebenso wie die Erkennung und Schließung geklonter Websites für Phishing-Kampagnen, die Analyse betrügerischer Finanztransaktionen sowie bei komplexen Betrugsszenarien die Untersuchung von Sicherheitsvorfällen einschließlich forensischer Analyse.

Das CSOC bietet Technologien und Anwendungen, die eine Betrugserkennung dank der Analyse und Identifizierung ungewöhnlichen Verhaltens in Browsersitzungen ermöglichen.

FRAUD MANAGEMENT 2	ACTIVE FRAUD PREVENTION AND MALWARE INTELLIGENCE 2,1	MOBILE ROGUE APPLICATION HUNTER 2,2	ANTIPHISHING SERVICES 2,3	BRAND ABUSE MONITORING SOCIAL MEDIA THREAT MONITORING 2,4
---	--	---	---	--



MANAGED NETWORK SECURITY

Services für verwaltete Netzwerksicherheit (**Managed Network Security**) sollen die vereinheitlichte Verwaltung von Netzwerkinfrastrukturen unterstützen, mit harmonisierten Zugangs- und Verwaltungssystemen für die bei den verschiedenen Kunden des CSOC betriebenen Servicegeräte.

Über eine einzige Verwaltungskonsole können Systemingenieure nun in organisierter und strukturierter Weise Maßnahmen ergreifen, sowohl zur Handhabung von Vorfällen als auch in Bezug auf gewöhnliche und außergewöhnliche Wartung sowie Patches, Tuning und Änderungen.

Zentrale Merkmale der Infrastruktur des Centers sind:

- Flexibilität bei der Verwaltung der verschiedenen von unseren Kunden eingesetzten Technologien.
- Standardisierung und Austausch von Methoden für Systemzugang und -verwaltung.
- Sicherheits- und Bereichsstrukturierung, sowohl im Hinblick auf die Kundenumgebungen als auch auf die Infrastruktur des CSOC.
- Sorgfältiges Konfigurationsmanagement, mit angemessener Speicherung, Backup-Sicherung und Versionierung. Hohes Maß an Verfügbarkeit und Redundanz.

MANAGED NETWORK SECURITY	SECURE NETWORK DESIGN AND IMPLEMENTATION	NETWORKING REMOTE & ON-SITE SUPPORT SERVICES	DEVICE & SOFTWARE SUPPLY AND SUPPORT	NETWORK ENGINEER SUPPORT NOC & COMPLEX NETWORK CONSULTING
3	3,1	3,2	3,3	3,4

ENTERPRISE MOBILITY SERVICES

Die zunehmende Nutzung von Mobilgeräten und dazugehörigen Inhalten hat einen erhöhten Bedarf für unternehmensspezifische Werkzeuge und Dienste zur Folge, um die Regulierung der Mobilanwendungen sowie der diesbezüglichen Sicherheit handhaben zu können. Heute werden immer mehr persönliche Geräte im Unternehmenskontext genutzt (Bring Your Own Device), was für Unternehmen Chance und Risiko zugleich darstellt. Das CSOC kann den Kunden bei der Entwicklung einer Strategie unterstützen, um die Vorteile des BYOD-Modells zu maximieren, ohne dabei die notwendige Einhaltung von Sicherheitsrichtlinien zu vernachlässigen. Services für individuelle Datenverarbeitung (End User Computing) überwachen und verwalten Workstations und Mobilanwendungen

sowie deren Sicherheit und stellen ausgehend von einem 8x5- oder 24x7-Dienstmodell ein spezialisiertes Angebot für die Kunden sicher, je nach den individuellen Anforderungen. Die Mobilitätsservices für Unternehmen (Enterprise Mobility Services) des CSOC unterstützen Kunden bei der Verwaltung von Geräten und mobilen Anwendungen, um so die vollständige Kompatibilität mit Plattformen zur Mobilgeräteverwaltung (Mobile Device Management) sowie die Einhaltung grundlegender Sicherheitsprinzipien zu gewährleisten. Das CSOC unterstützt den Kunden sowohl bei der Entwicklung sicherer Geschäftsanwendungen als auch bei der Absicherung von Drittanwendungen. development of secure business applications, as well as in "securing" third party applications.

ENTERPRISE MOBILITY SERVICES	END USER COMPUTING	DEVICE MANAGEMENT	MOBILE APPLICATION SECURITY	IDENTITY & SECURITY MANAGEMENT
4	4,1	4,2	4,3	4,4



COMMUNICATION VALLEY REPLY ist das Unternehmen der Reply-Gruppe, das sich auf die Bereitstellung verwalteter Sicherheitsdienste spezialisiert hat. Über sein Cyber Security Operation Center – ein nach ISO27001 zertifiziertes europäisches Kompetenzzentrum im Bereich verwalteter Sicherheitsdienste, das an 365 Tagen im Jahr rund um die Uhr tätig ist – stellt Communication Valley Reply für Unternehmen Geschäftskontinuität sowie Betrugserkennung und -management, Sicherheitsüberwachung und -erprobung sowie verwaltete Netzwerksicherheit bereit. Communication Valley Reply bietet spezialisierte Services für den Finanzsektor an: Identifizierung und Analyse von Malware, Erkennung von zur Durchführung spezieller Phishing-Kampagnen erstellten Websites und Analyse betrügerischer, häufig hochkomplexer Transaktionen, oft einschließlich forensischer Analysen.

Communication Valley Reply arbeitet mit führenden Forschungsinstituten, mit internationalen Universitäten sowie mit führenden Technologiepartnern zusammen, um zum bevorzugten Anbieter verwalteter Sicherheitsdienste in Europa zu werden.

CYBER SECURITY OPERATION CENTER

Via Robert Koch 1/4, Turm B
20152 Mailand, Italien

COMMUNICATION VALLEY REPLY

ITALIEN

Via Robert Koch 1/4, Turm B
20152 Mailand, Italien

DEUTSCHLAND

Arnulfstraße 27,
80335 München, Deutschland

VEREINIGTES KÖNIGREICH

38 Grosvenor Gardens, London
SW1W 0EB, Vereinigtes Königreich

www.communicationvalley.com
csoc@reply.com