DE

kapsch
challenging limits

Kapsch BusinessCom

Kapsch Cyber Defense Center.

Monitor. Detect. Respond.

Im Kampf gegen Cyberkriminelle und Hacker wird nur der Erfolg haben, der intelligenter, reaktionsschneller und effizienter handelt als die Angreifer selbst. Mit seinem neuen Cyber Defense Center bietet Kapsch Unternehmen und Behörden jetzt ein hochwirksames Instrumentarium, Cyberangriffe aller Art zu entdecken. Für Analyse, Gefahrenabwehr und Gegenreaktion.

Kapsch Cyber Defense Center:

Das 2-in-1-Konzept für schnelle Reaktion und effiziente Abwehr.

Die durch Cyberkriminalität verursachten Schäden sind beträchtlich: Spionage und Diebstahl geistigen Eigentums, Angriffe auf Vertraulichkeit, Integrität und Verfügbarkeit, Entwendung von Vermögenswerten. Als Konsequenz hat Kapsch das Cyber Defense Center (CDC) ins Leben gerufen. Es reagiert schnell auf Angriffe und hilft effizient Gegenmaßnahmen einzuleiten.

Kapsch Cyber Defense Center (CDC).

Die Module.

Kapsch Managed Defense Service (MDS).

- Network Security Monitoring
- Endpoint Detection and Response
- Log Analysis
- Vulnerability Scanning
- Proactive Data Acquisition

Kapsch Emergency Response (ER).

- Live Data Acquisition
- Reaktion auf Sicherheitsvorfälle
- Aufklärung und Bereinigung
- Garantierte SLA-Zeiten

Modulares Konzept mit hoher Wirksamkeit.

Das Kapsch Cyber Defense Center ist in zwei Bereiche strukturiert, die synergetisch zusammenarbeiten: **Kapsch Managed Defense Services (MDS)** und **Kapsch Emergency Response Services (ER).** Kapsch MDS ist ein sowohl proaktiver als auch reaktiver Service: An unterschiedlichen Punkten – Netzwerk, Endpoint, Logfiles – werden sicherheitsrelevante Informationen gesammelt und laufend analysiert, um Angriffe und Anomalien zu erkennen. Im Falle von Security Incidents bieten diese Daten die Basis für tiefgreifende Analysen. Kapsch ER ist ein rein reaktives Service: Bei der Erkennung oder dem Verdacht eines Sicherheitsvorfalls durch das eigene Unternehmen oder durch Externe hilft und unterstützt Emergency Response bei der Analyse und der Aufklärung. Das Ziel: Eindämmung des sicherheitsrelevanten Vorfalls und Rückkehr zum Normalbetrieb des Unternehmens.

Jahrzehntelange Erfahrung, umfassendes Spezialwissen.

Im Kapsch Cyber Defense Center arbeitet ein Team aus hochqualifizierten und spezialisierten Security-Analysten. Sie sind seit vielen Jahren im Bereich Incident Response, Intrusion Detection, digitaler Forensik und Penetration Testing tätig und verfügen über eine Vielzahl von Zertifizierungen. Dank ihrer Erfahrung und ihres Know-hows in der Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen kann das Sicherheitsniveau drastisch angehoben und die Zeit bis zur Erkennung eines Problems enorm reduziert werden. Bei den Auswertungen erkennt das CDC-Team Angriffe jenseits von Schadsoftware und kann auch Zusammenhänge zwischen Alarmen und kritischen Events herstellen.

Aufgrund dieser Fähigkeiten und mit dem Wissen über die TTPs – Tools, Tactics und Procedures – der Angreifer kann erst das gesamte Ausmaß eines Angriffs eruiert und dargestellt werden. Entsprechend den Anforderungen und Gegebenheiten können ein, mehrere oder alle der nachfolgenden Module in das Service aufgenommen werden. Je mehr das Kapsch CDC „sieht“, umso vollständiger wird das Bild und umso schneller können Angriffe erkannt, verifiziert und nachvollzogen werden.

Kapsch Managed Defense Service.

Proaktiv. Reaktiv. Modular.

Kapsch Managed Defense Service (MDS) erhöht die Visibility im Netzwerk und erfasst dabei alle Netzwerkelemente: Geräte, Applikationen, Daten und natürlich auch die User. MDS erkennt Angreifer, identifiziert kompromittierte Systeme und hilft, mit den richtigen Mitteln auf diese Angriffe zu reagieren.

MDS setzt auf die Verbindung von Mensch und Maschine: Eine effiziente Kombination aus analytischem Denken, aus der Erfahrung und dem Know-how der Kapsch Cyber Defense Center-Mitarbeiter und aus der technischen Unterstützung unterschiedlicher Tools.

Network Security Monitoring.

Überwachung des Netzwerkverkehrs und Analyse des Geschehens auf Verdächtiges und auf Aktivitäten, die Schäden verursachen könnten. Durch den Einsatz von Network Monitoring Appliances erhält das Kapsch Cyber Defense Center umfassende Einblicke und „sieht“, was im Netzwerk passiert. Um Anomalien zu identifizieren, werden unterschiedliche Methoden wie proprietäre Intrusion Indication Signaturen, Reputationen, diverse Intelligence Feeds und manuelle Analysen eingesetzt. Für die Nachvollziehbarkeit wird der gesamte Datenverkehr für mehrere Tage aufgezeichnet („Full Packet Capture“) und komplett indiziert. Analysen von Verbindungsdaten („Net Flows“) liefern zusätzlich wichtige Hinweise und Indikatoren.

Endpoint Detection and Response.

Kontinuierlicher und umfassender Fokus auf die Aktivitäten der Endpoints. Unabhängig davon, ob der Endpoint mit dem Netzwerk verbunden ist oder nicht, werden Änderungen von dem System laufend mitgeschrieben, nachvollziehbar gemacht und Anomalien durch unterschiedliche mathematische und statistische Modellierungen erkannt. Es können aktuelle oder in der Vergangenheit aufgetretene Endpoint-Aktivitäten untersucht werden, ob diese nun vor ein paar Sekunden, vor Tagen oder vor Monaten aufgetreten sind. Alle relevanten Daten werden für spätere Analysen gesichert, kompromittierte Systeme unter Quarantäne gestellt.

Log Analysis.

Cyberkriminelle können an jedem Punkt zuschlagen. Durch das CDC-Tool Log Analyse bekommt man eine unternehmensweite Sicht auf die Dinge. Dabei werden Logdaten von den unterschiedlichsten Systemen, die global über die Welt verteilt sein können, gesammelt, aggregiert und analysiert. Die Daten werden mit unterschiedlichen analytischen Verfahren ausgewertet, untersucht und korreliert.

Vulnerability Scanning.

Durch regelmäßige Vulnerability Scans können bestehende Sicherheitslücken schnell erkannt und reported werden. Dadurch ist es möglich, existierende Risiken zu beheben, beziehungsweise das Wissen über Schwachstellen in die Untersuchungen der CDC-Analysten einzubeziehen. Die Scans laufen in regelmäßigen Abständen über die kritischen Systeme der Infrastruktur.

Proaktive Datensicherung.

Im Kapsch Cyber Defense Center werden relevante Daten rund um einen Angriff aufgezeichnet und für spätere Untersuchungen vorgehalten. Die Daten werden ausschließlich innerhalb des Kundennetzwerks gespeichert und verlassen das Unternehmen nicht.

Kapsch Emergency Response.

ER weiß, was zu tun ist.

Emergency Response Service (ER) hilft durch Investigation und Remediation bei der Einschätzung, Analyse und Aufklärung von Sicherheitsvorfällen, die vom Unternehmen selbst oder durch Dritte erkannt werden. Zunächst werden Umfang und Ausmaß des Incident auf Basis der vorhandenen Informationen bestimmt. Dann werden die entsprechenden Daten und sonstigen Anhaltspunkte gesichert. In einer gemeinsamen Strategie von Unternehmen und Kapsch Cyber Defense Center wird entschieden, wie man optimal auf den Incident reagiert, wie der Vorfall eingedämmt werden und das Netzwerk wieder in den Normalbetrieb übergehen kann.

Live Datensicherung.

Im Bedarfsfall sichert das Kapsch CDC Daten von verdächtigen Systemen, damit diese auf Indikatoren eines Angriffs untersucht werden können.

Garantierte SLA-Zeiten.

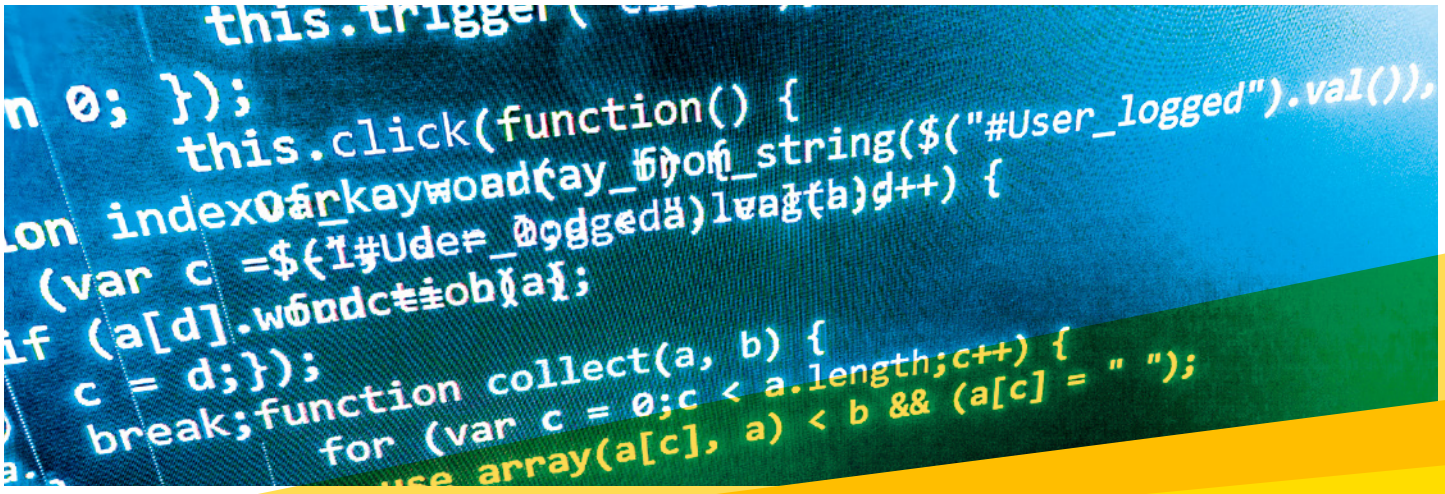
Die Unterstützung erfolgt zu den im Service Level Agreement garantierten Zeiten, remote oder direkt vor Ort.

Kapsch Managed Defense Service: Die Vorteile

- Validierung von verdächtigem Verhalten
- Alert Triage
- Threat Hunting
- Strukturierte und standardisierte Analysen

Kapsch Emergency Response: Die Vorteile

- Schnelle Beseitigung und Eliminierung der Bedrohung aus dem Netzwerk
- Schäden minimieren
- Rasche Wiederherstellung des Normalbetriebes



Kapsch Cyber Defense Center: Features und Leistungen.

- **Menschliche Intelligenz**
  Identifizierung von Angriffen jenseits von Schadsoftware
  Erkennen von Zusammenhängen zwischen Alarmen und einzelnen Events
- **Hochqualifizierte Analysten**
  Zusammen mehr als 30 Jahre Incident Response und digitales Forensik-Know-how
  International anerkannte Zertifizierungen (CISSP, GCFA, GCFE, CCE, …)
- **Persönlicher Kontakt**
  Analysten kontaktieren den Kunden bei echten verifizierten Alarmen
  Unterstützung bei den Untersuchungen und den Clean-Up-Prozessen

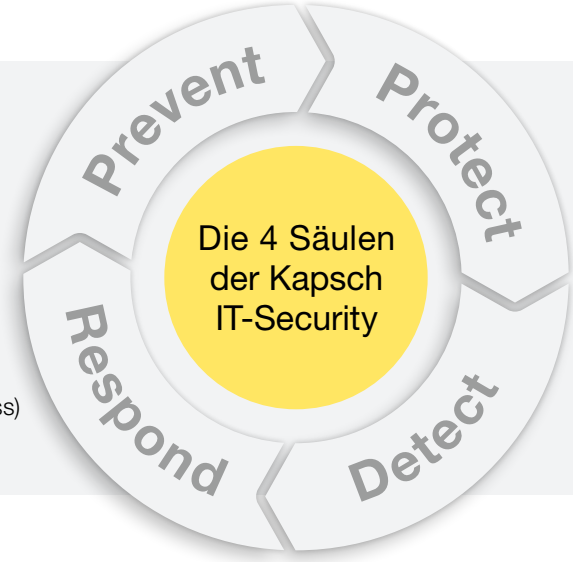
Sicherheit im Netz:

So schließt sich der Kreis.

Der Kapsch Security Circle zeigt im Kern die Strategie und Vorgehensweise des Cyber Defense Centers. Das IT-Security-Konzept von Kapsch, Österreichs einzigem TÜV-Trusted-IT-Security Auditor, verfolgt eine konsequente Vier-Säulen-Strategie: Wir beugen vor, wir schützen, wir identifizieren, wir reagieren.

Prevent
- Security Audit
- Access Control
- Security Architecture Review
- IT-Risiko-Management

Respond
- Unterstützung bei der Bekämpfung von Angriffen
- Incident Response (Readiness)
- Forensische Analyse



Protect
- Network Security
- Content Security
- APT-Solutions
- Application Security

Detect
- Security Monitoring
- Compromise Assessment
- Vulnerability Assessment

Kapsch Cyber Defense Center: Die Mehrwerte.

- Reduziert die Zeit, um Angriffe zu erkennen (lt. Security Hersteller Reports ~200 Tage)
- Regelmäßige proaktive Suche nach Anomalien
- Schnelle Alarmierung bei Erkennung sicherheitsrelevanter Incidents
- Umfassende Bewertung der Events durch Kapsch Security Analysten
- Regelmäßige Berichte über Events, Analysen und Aufzeigen von notwendigen Maßnahmen

Kapsch BusinessCom

Kapsch BusinessCom ist ein Unternehmen der Kapsch Gruppe. Die 1.200 Mitarbeiterinnen und Mitarbeiter erzielten im Geschäftsjahr 2016/17 einen Umsatz von rund 320 Millionen Euro. Das umfangreiche Lösungsportfolio des führenden Digitalisierungspartners in Österreich und CEE umfasst Technology Solutions (für stabile, intelligente und vor allem sichere ICT-Infrastruktur), Facility Solutions (für smarte Gebäude- und Sicherheitstechnik und Multimedia) und Business Services (für Outsourcing und innovative Digitalisierungslösungen mit Branchenfokus). Mit dem Ansatz „Consult, Deploy, Operate“ ist Kapsch in der Lage, den gesamten Lebenszyklus von ICT-Lösungen bei seinen Kunden abzudecken. Kapsch arbeitet herstellerunabhängig und setzt die jeweils besten Technologien weltweit führender Anbieter wie beispielsweise Cisco, HP oder Microsoft ein und kombiniert diese mit Lösungen aus seinem Partnernetzwerk an Forschungseinrichtungen und Applikationsanbietern. Kapsch BusinessCom hat über 17.000 Kunden (u. a. OMV, Allianz, ORF, Erste Bank, Vodafone, ÖBB) und betreut diese lokal wie auch global in rund 40 Ländern.

>>> www.kapsch.net

Pros-CyberDefenseCenter

Kapsch BusinessCom AG | Wienerbergstraße 53 | 1120 Wien | Österreich | T +43 50 811-0 | kbc.office@kapsch.net | www.kapsch.net