DE

kapsch
challenging limits

Kapsch BusinessCom

Keine Chance für Cybercrime & Co.

Die beste Verteidigung ist eine ganzheitliche Strategie.

Woran sieht man, dass die Angriffe auf IT-Netzwerke immer mehr zunehmen? Richtig: Die Security-Spezialisten von Kapsch haben richtig viel zu tun, und die Aufgaben, die sich dabei stellen, werden immer komplexer. Die Bedrohungen sind ernst, die Angriffe vielfältig, die Methoden ausgeklügelter. Abwehr und Verteidigung gegen Cyberkriminelle: eine echte Herausforderung. Und nur zu bewältigen mit einer ganzheitlichen Sicherheitsstrategie.

Weil die Bedrohungslage sehr konkret ist:
Security Solutions von Kapsch.

Cyberkriminelle Bedrohungen nehmen nicht nur in erschreckendem Maße zu, sie werden auch immer vielfältiger und komplexer. Verschiedenste Angriffsvektoren führen zu unterschiedlichsten Formen der Kompromittierung, gegen die man sich verteidigen muss. Speziell das Thema Ransomware – vor allem in der Form von Cryptolockern – macht den meisten Unternehmen zu schaffen.

Wie sieht ein typischer Angriff aus?

Cyberkriminelle gehen meist sehr strukturiert vor. Ein typischer Angriff zeichnet sich durch mehrere klar definierte Phasen aus:

In einem ersten Schritt werden öffentlich zugängliche Daten des Zielobjektes gesammelt. Dann: Start des Initial Compromise. In dieser Phase wird versucht, durch E-Mails mit Anhängen und Links, direkte Angriffe auf die Infrastruktur, Ausnutzen von Schwachstellen und anderes mehr in das Netzwerk einzudringen. Anschießend beginnt die Ausbreitung innerhalb des Unternehmens. Zu diesem Zweck werden gezielt „Hintertüren“ etabliert. Meist handelt es sich dabei um Remote Access Toolkits oder das Entwenden von VPN-Zugangsdaten.

In weiterer Folge wird nun versucht, die Privilegien innerhalb des Netzwerks zu erhöhen, mit dem Ziel, lokale oder domänenweite Administratorrechte zu erhalten: mit einfachen Methoden wie dem Auslesen einer nicht passwortgeschützten Datei bis zum Ausnutzen von sogenannten „Zero Day“-Schwachstellen. Jetzt können die Angreifer in die entscheidende Phase gehen: Das interne Netz wird ausgekundschaftet, zum Beispiel, um an Informationen heranzukommen, um Schäden anzurichten oder bestimmte Prozesse (Überweisungen, o. Ä.) zu beeinflussen.

Prevent, Protect, Detect, Respond: So begegnet Kapsch den Angriffen.

Dieser cyberkriminelle Zyklus zeigt deutlich, dass solchen Angriffen nur mit einer strukturierten und ganzheitlichen Strategie entgegengesteuert werden kann. Ein Fall für Security Solutions von Kapsch: Unsere Spezialisten agieren und reagieren dynamisch und gesamtheitlich. Kein Aspekt, kein Zugriffsort wird dabei vernachlässigt. Eine Gesamtstrategie zum Nutzen unserer Kunden – basierend auf den vier Security-Segmenten Prevent, Protect, Detect und Respond. Damit wird jeder sicherheitsrelevante Aspekt abgedeckt: Aufdecken von Schwachstellen, Erkennen von strukturellen Problemen, Aufdecken und Analysieren von Angriffsmustern, proaktive und präventive Maßnahmen, Sicherung von Beweismaterial, Abwehr- und Verteidigungslösungen, Aufbau nachhaltiger Schutzmechanismen.

Unser Angebot für Sie:

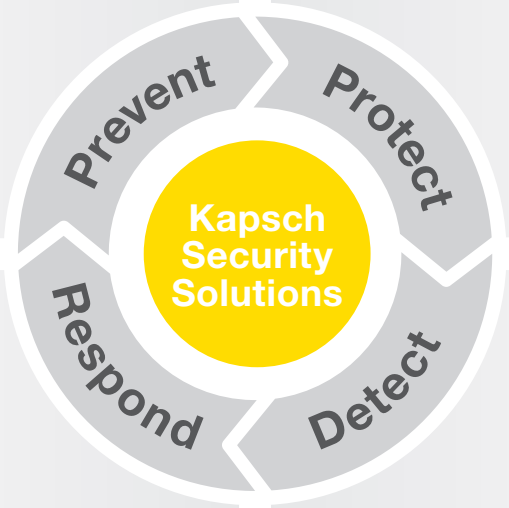
Das ganzheitliche Kapsch-1 x 4 der IT-Security.

Aufdecken von Schwachstellen und Ablauf- und Strukturproblemen.

Die Klassiker unter den Security-Lösungen, von der Firewall bis zur Encryption.

Security Audit
Security Architektur Review
IT Risiko Management
Access Control

Network Security
Content Security
APT Solutions
Application Security



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

Security Monitoring
Compromise Assessment
Vulnerability Assessment

Konkrete Leistungen, die nach einem Angriff wichtig werden.

Erkennen von vorhandenen Systeminfektionen.

Mit Sicherheit möchten Sie jetzt mehr wissen. Ein Fall für das Security Solutions Team von Kapsch: Sprechen Sie am besten gleich mit unseren Spezialisten. Die Cyberkriminellen warten nicht.

securitysolutions@kapsch.net

Prevent:

Schwachstellen erkennen, proaktiv handeln!

Unser Audit-Portfolio.

Organisatorische Sicherheit.
Organisatorische Sicherheit ist der unerlässliche Rahmen für den sicheren Einsatz und Betrieb von IT-Systemen. Dabei stellt Technologie nur eines von vielen Zahnrädern dar, die für komplexe Geschäftsprozesse relevant sind. Hinzu kommen Personen, Organisationsstrukturen, das Gebäudeumfeld, Alltagsabläufe und so weiter. Anforderungen und Vorgaben an den Betrieb und der wirtschaftlich sinnvolle Einsatz von IT ergeben sich also erst aus dem konkreten Business-Kontext. **Eine gesamtheitliche Informationssicherheit erfordert die Betrachtung und Einbeziehung aller dieser Faktoren.** Im Rahmen des Security-Segments „Prevent“ unterstützen Sie unsere Experten bei der Analyse, Erstellung oder Umsetzung organisatorischer Maßnahmen.

Unsere Dienstleistungen:

- ISMS – Information Security Management System (nach ISO 27001)
- Business-Impact-Analysen
- IT-Risikomanagement
- Compliance Audits

Technische Sicherheit.
Technische Sicherheit ist das Fundament für nachhaltige und flächendeckende Sicherheit in der IT Ihres Unternehmens. Wichtig: „Vertrauenswürdige Umgebungen“ gehören der Vergangenheit an. Heute ist alles miteinander vernetzt. Angriffe aus dem Internet oder interne Gefährdungen über Partner- oder Remote-zugänge sind jederzeit möglich und wahrscheinlich. Ein großes Thema in diesem Zusammenhang ist beispielsweise die immer weiter fortschreitende Digitalisierung der Industrie (Smart Factory, Internet der Dinge). **IT-Security muss also ein integraler Bestandteil jeder Anwendung und jedes Netzwerk-elements sein.** Dazu trägt die Abwehr von unbefugten Zugriffen von außen ebenso bei wie die Sicherung kritischer Daten und der Schutz mobiler Endgeräte.

Unsere Dienstleistungen:

- Security Audit der internen und/oder externen Sicherheit
- Compromise Assessment
- Incident Response

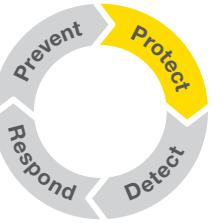
Unser Schulungsportfolio.

In unseren **Awareness-Schulungen** sollen Mitarbeiter darauf vorbereitet werden, mit immer raffinierteren Angriffen umzugehen. Meist ist der Enduser das schwächste Glied in der IT-Sicherheitskette, und genau hier setzen die Security-Experten von Kapsch an.

Im Rahmen der **Kapsch Hacker-Workshops** werden konkrete Anforderungen abgeklärt und Übungen durchgeführt – mit einfachen und praktischen Lösungswegen für den Businessalltag als Ziel. Dabei werden sowohl klassische als auch moderne Angriffstaktiken anhand von interaktiven Demonstrationen gezeigt und deren Auswirkungen illustriert.

Protect:

Netzwerke schützen, Angriffspunkte minimieren!

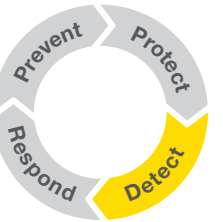


Unser Business Protection Portfolio.
Die Kapsch Security Solutions sind immer „up to date": Unser Produktportfolio folgt höchsten Qualitätsansprüchen, ist klar strukturiert und zu jeder Zeit auf dem neuesten technologischen Stand. Unsere Experten unterziehen die neuesten Angebote am Markt einer kritischen Analyse und überprüfen sie hinsichtlich ihrer konkreten Implementierung bei unseren Kunden. Für alle Anlassfälle stehen damit optimale Leistungen und Produkte zur Verfügung.

- Innovative Lösungen führender Technologiepartner
- Optimale Implementierung und Betreuung durch zertifizierte Experten
- Individuell zugeschnittenes Serviceangebot von Kapsch
- Betreuungszeiträume je nach Anforderungen: in der Normalarbeitszeit bis hin zu „24 x 7 x 365"-Services

Detect:

Infektionen erkennen, Schäden aufdecken!



Unser Serviceportfolio umfasst im Segment „Detect" zwei Lösungskomponenten: **Compromise Assessments und Managed Defense Services.** Hier geht es im Wesentlichen darum, bereits vorhandene Systeminfektionen zu erkennen und zu beseitigen.

Mit **Kapsch Compromise Assessments** werden Netzwerk-Scans durchgeführt. Das Ziel ist die Identifikation vorhandener, aber nicht erkannter Infektionen. Diese können dann entfernt und analysiert werden, um aus den Resultaten neue Maßnahmen zum Schutz der Infrastruktur abzuleiten.

Kapsch Managed Defense wird eingesetzt, um Netzwerktraffic aufzuzeichnen und zu analysieren, um so jede ungewollte Kommunikation zu erkennen. In Reporten, die regelmäßig nach vordefinierten Zeiträumen vorgelegt werden, werden abnormale Vorkommnisse aufgezeigt und die entsprechenden Reaktionsmaßnahmen vorgeschlagen.

Respond:

Angriffsstrategien bewerten, Beweise sichern!

Was ist die richtige Antwort auf einen Angriff? Mit dem Security-Segment „Respond" bieten Ihnen unsere Spezialisten optimale Unterstützung bei sicherheitsrelevanten Ereignissen. Im Rahmen von Incident-Response-Leistungen von Kapsch werden Vorfälle analysiert – mit dem Ziel einer nachhaltigen Bereinigung. Zugleich werden Maßnahmen erarbeitet, um entsprechende Vorfälle für die Zukunft zu verhindern.

Kapsch Incident Response Readiness Workshop
Hier sollen die IT-Verantwortlichen von Unternehmen optimal auf die richtigen Reaktionen im Falle von sicherheitsrelevanten Vorfällen vorbereitet werden. Im Rahmen der Workshops werden gezielt alle Prozesse und Abläufe überprüft, die zuvor gemeinsam definiert wurden. Dadurch kann sehr schnell festgestellt werden, ob im Falle eines Incidents eine korrekte Reaktion stattfinden kann oder ob möglicherweise Prozesse falsch definiert wurden.

Kapsch BusinessCom

Kapsch BusinessCom – ein Unternehmen der Kapsch Group – ist mit mehr als 1.300 Mitarbeitern und einem Umsatz von knapp 310 Millionen Euro einer der führenden ICT-Servicepartner in Österreich, Zentral- und Osteuropa. Eingebettet in die Kapsch Unternehmensgruppe, agiert Kapsch BusinessCom weltweit mit eigenen Niederlassungen in Österreich und mit Gesellschaften in Tschechien, der Slowakei, Ungarn, Rumänien und Polen. Das Gesamtlösungsportfolio des Unternehmens deckt sowohl Informationstechnologie als auch Telekommunikation ab. Kapsch positioniert sich daher als ICT-Servicepartner. Neben der Systemintegration und der kontinuierlichen Optimierung übernimmt Kapsch BusinessCom in immer stärker werdendem Ausmaß auch den vollständigen Betrieb dieser ICT-Lösungen. Kapsch setzt dabei auf Herstellerunabhängigkeit und Partnerschaften mit weltweit technologisch führenden Anbietern wie Apple, Aastra, Avaya, Cisco, EMC, Google, Hitachi, HP oder Microsoft. Gemeinsam mit diesen Partnern agiert Kapsch als Berater, Systemlieferant und Dienstleistungsanbieter bei seinen 17.000 Kunden, vor allem aber als verlässlicher, vertrauenswürdiger und langfristiger Trusted Advisor in einem sich rasant verändernden technologischen Umfeld. Für weitere Informationen:

>>> www.kapsch.net

KBC-Pros_ITSecurity

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