DE

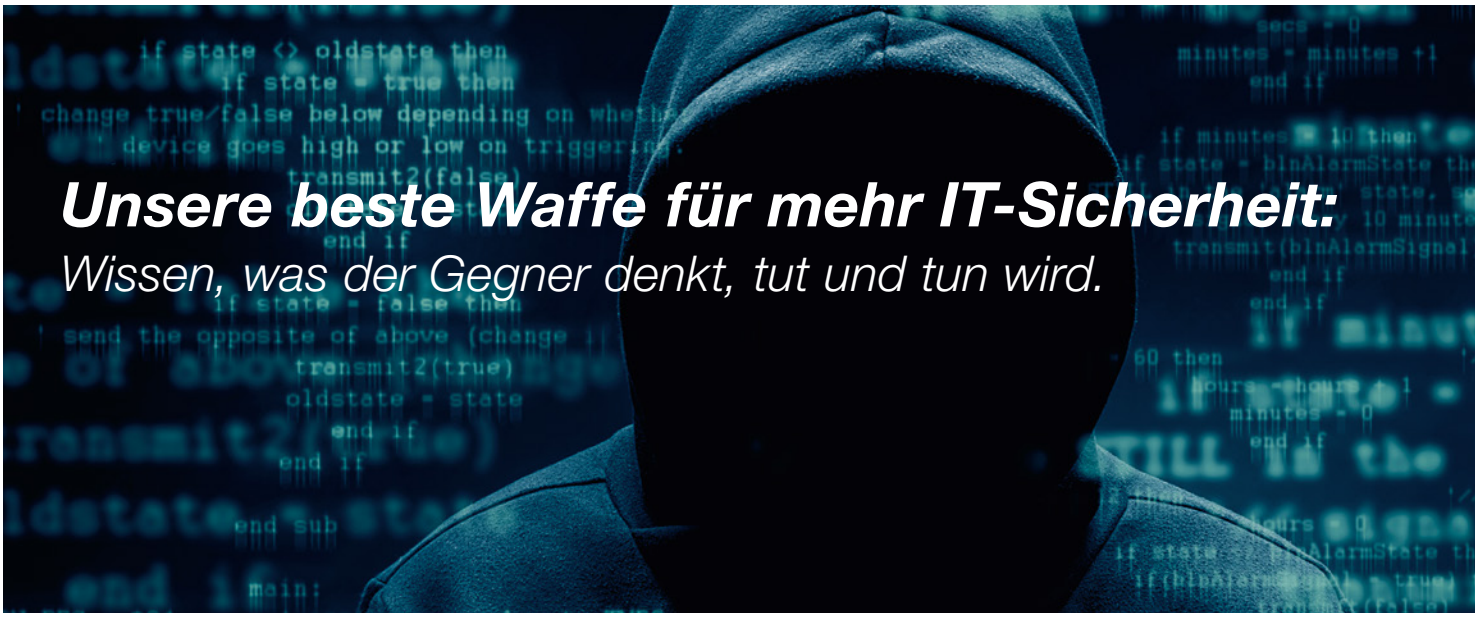
kapsch
challenging limits

Kapsch BusinessCom

Kapsch Security Audit Services.

Realität simulieren, Hacker abwehren.

Phishing, Botnets, Trojaner: Hackerangriffe auf IT-Systeme von Unternehmen, Behörden, Institutionen, Organisationen und auf private Rechner gehören zum Alltag einer vernetzten Welt. Wie gehen die Angreifer vor? Mit welchen Methoden suchen und finden sie immer neue Sicherheitslücken? Hier setzen die Security Audit Services von Kapsch an: Nur wer weiß, wie Hacker ticken, wie sie denken und arbeiten, wird langfristig an Sicherheit gewinnen. Sagen wir Hackern den Kampf an! Gemeinsam mit unseren Kunden und getreu unserer Maxime „Prevent, Protect, Detect, Respond“.



Unsere beste Waffe für mehr IT-Sicherheit:

Wissen, was der Gegner denkt, tut und tun wird.

Nur wer seinen Feind kennt, kann ihn schlagen. Die Gegner von heute sind unsichtbar und agieren global. Sie wissen alles und nutzen immer raffiniertere Methoden, um selbst hochkomplexe Abwehrsysteme zu überwinden.

Praktisch jeden Tag werden neue Gefahren und Sicherheitslücken in Applikationen und Betriebssystemen entdeckt – und meistens sind Programme, die diese Lücken ausnützen, rasch verfügbar. Alle Lücken zu identifizieren, um sie rechtzeitig schließen zu können, ist für einen Administrator neben seinem Daily Business praktisch nicht mehr möglich.

Wir werden zu Hackern. Damit Sie vor ihnen geschützt sind.

Kapsch, Österreichs einziger TÜV Trusted IT-Security Auditor, setzt auf eine starke Vier-Säulen-Strategie:

Wir beugen vor, wir schützen, wir identifizieren und wir reagieren.

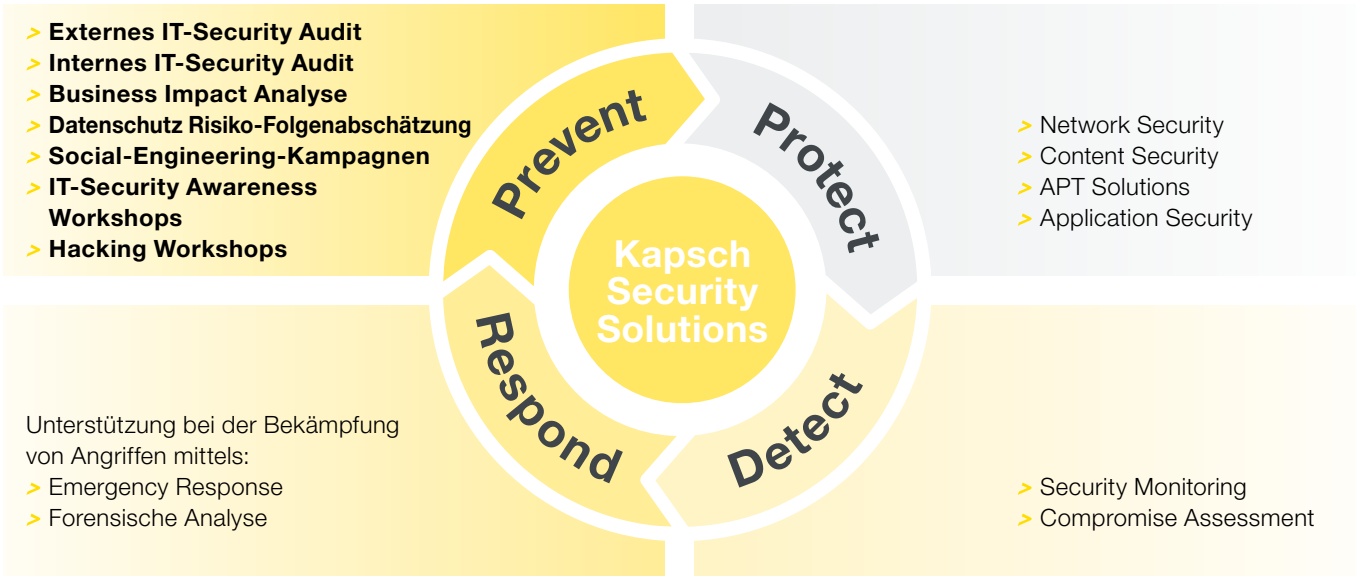
Eine Sicherheitsüberprüfung möglichst aller Systembestandteile und Anwendungen mit genau jenen Mitteln und Methoden, die ein Angreifer anwenden würde, um unautorisiert in das System einzudringen, ist notwendig. Dies erfordert Testmethoden, die sich des Blickwinkels der Angreifer bedienen, um möglichst reale Testsituationen zu schaffen.

Solche Realbedingungen werden im Rahmen der Security-Audit-Dienstleistungen von Kapsch möglich gemacht. Die Security Audits werden unter anderem nach der OSSTMM (Open Source Security Testing Methodology Manual)-Methode durchgeführt. Mit dieser Methode wird das Ergebnis des Security Audits einheitlich und daher vergleichbar gemacht.

Kapsch führt Security Audits nach den Qualitätsrichtlinien von TÜV Austria durch. Spezialisten der Kapsch BusinessCom sind als TÜV Trusted IT-Security Auditor zertifiziert. Kapsch-Kunden erhalten durch diese Qualitätsrichtlinien ein Ergebnis nach europäischen und internationalen Standards.

Kapsch Security Audit Services:

Drei Kernangebote im Rahmen unserer IT-Security-Strategie.



Unsere Audit Module zu Prevent.

Mehr Informationssicherheit dank effizienter Vorsorge: Unsere Prevent-Angebote umfassen alles, was nötig ist, um es Angreifern so schwer wie möglich zu machen. Vom internen Security Audit bis zum Awareness-Workshop. Mit unseren weiteren Audit-Lösungsbausteinen zu Detect und Respond sowie mit unseren Protect-Securitylösungen steht Ihnen eine Komplettlösung zur Verfügung, die Hacker gar nicht lieben werden. Im Folgenden unsere Prevent-Leistungen auf einen Blick.

Externes IT-Security Audit.

Das machen wir.

> Wir simulieren einen Angriff auf das IT-System/Netzwerk von außen.

Das haben Sie davon.

> Überprüfung der über das Internet erreichbaren IT-Infrastruktur (z. B. Mail-, FTP- und VPN-Server, Web-Applikationen).

Internes IT-Security Audit.

Das machen wir.

> Wir simulieren einen Angreifer, der Zugang zum internen Netzwerk erhalten konnte.

Das haben Sie davon.

> Überprüfung des internen Netzwerks (Dateifreigaben, E-Mail- und Kalenderdaten, Telebanking-Anwendungen …).

Business Impact Analyse und Risiko Management.

Das machen wir.

> Wir erheben drohende Schadenssummen, die wegen nicht ordnungsgemäß funktionierender IT-Systeme entstehen.
> Wir erfassen die Qualität der zugrunde liegenden IT-Systeme

Das haben Sie davon.

> Transformation von technischen Risiken in Geschäftsrisiken.
> Erarbeitung von Credible-Worst-Case-Szenarien.
> Bewertung drohender Folgeschäden in monetären Größen.

Datenschutz Risiko-Folgenabschätzung.

Das machen wir.

- Datenschutzrechtliche Vorgaben verlangen eine Risikoanalyse datenverarbeitender Systeme. Wir führen diese Analyse durch.

Das haben Sie davon.

- Einhaltung angemessener Sicherheitsvorkehrungen.
- Datenschutz-Risiko-Folgenabschätzung, wie von der EU-Datenschutz-Grundverordnung (DSGVO) verlangt.

Social-Engineering-Kampagnen.

Das machen wir.

- Wir simulieren breit gefächerte Phishing-Kampagnen (Cryptolocker).
- Wir simulieren gezielte Angriffe (APT), auch per Telefon oder vor Ort.

Das haben Sie davon.

- Überprüfung der IT-Security-Awareness der Mitarbeiter.
- Überprüfung der technischen Sicherheitsmaßnahmen gegen Trojaner und Ransomware.

IT-Security Awareness Workshops.

Das machen wir.

- Wir erarbeiten mit Ihnen, wie moderne Cyber-Attacken funktionieren und wie man sie von legitimer Kommunikation unterscheiden kann.

Das haben Sie davon.

- Ihre Endanwender wissen Bescheid über aktuelle Sicherheitsbedrohungen.
- Ihre Endanwender wissen, wie Cyber-Angriffe als solche erkannt und schon im Vorfeld verhindert werden können.

Hacking Workshops.

Das machen wir.

- Wir verwandeln uns in professionelle Hacker – und spielen alltägliche Angriffsszenarien durch.

Das haben Sie davon.

- Wir verschaffen Ihnen tiefe Einblicke in die „dunkle Welt“ der Cyberkriminellen und vermitteln wertvolles und anwendbares Sicherheits-Know-how.

Unsere Audit Module zu Detect und Respond.

Falls doch etwas passiert: Angriffe schnell erkennen, richtig reagieren!

Compromise Assessment.

Das machen wir.

- Wir analysieren, ob Ihr System bereits gehackt wurde und ob eventuell aktive Botnet-Kommunikation zu identifizieren ist.

Das haben Sie davon.

- Netzwerkverkehrsanalyse mittels Monitoring Appliance.
- Manuelle Analyse der Top 3–7 Top-Events nach dem Timebox-Ansatz.
- Abschlusspräsentation.

Emergency Response.

Das machen wir.

- Wir helfen, wenn schon „etwas passiert ist“ und das System angegriffen wurde.

Das haben Sie davon.

- Sachverhaltsfeststellung.
- Forensische Analysen.

Kapsch:

Der einzige TÜV Trusted IT-Security Auditor in ganz Österreich.

Die Spezialisten von Kapsch BusinessCom sind als TÜV Trusted IT-Security Auditor von der TÜV TRUST IT TÜV AUSTRIA GMBH überprüft und zertifiziert. Damit ist Kapsch das einzige Unternehmen in Österreich, das über diese wichtige Zertifizierung verfügt. Darüber hinaus beschäftigt Kapsch BusinessCom Auditoren, die von Austrian Standards zur Durchführung von Audits nach der ÖNORM A 7700 akkreditiert wurden. Beide Organisationen bestätigen damit, dass Kapsch BusinessCom Security Audits gemäß europäischen und internationalen Standards mit bestmöglicher Qualität für seine Kunden durchführt.

Unsere Zertifizierungen, Normen und Standards.

- TÜV Trusted IT-Security Auditor
- Akkreditierung zur Auditdurchführung nach ÖNORM A 7700
- CIS Information Security Auditor nach ISO 27001
- CIS Information Security Manager
- CISSP (Certified Information Systems Security Professional)
- GPEN (SANS GIAC Penetration Tester)
- GCFA (SANS GIAC Certified Forensic Analyst)
- OSCP (Offensive Security Certified Professional)
- CCE (Certified Computer Examiner)
- CHFI (Computer Hacking Forensic Investigator)
- CompTIA Security+

Normen und Standards:
http://www.isecom.org/osstmm
http://www.owasp.org
http://www.iso.org
http://www.a7700.org
http://www.it-tuv.com

TÜV AUSTRIA TRUSTED IT-SECURITY AUDITOR TÜV TRUST IT TÜV AUSTRIA GMBH

ÖNORM A 7700

Gehen Sie mit Kapsch auf Nummer sicher.

Informieren Sie sich in einem persönlichen Gespräch über unsere IT-Security-Services. Kontaktieren Sie uns per Mail an **securitysolutions@kapsch.net**

Kapsch BusinessCom

Kapsch BusinessCom ist ein Unternehmen der Kapsch Gruppe und die 1.200 Mitarbeiterinnen und Mitarbeiter erzielten im Geschäftsjahr 2015 einen Umsatz von über 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_SecAudit

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