EN

kapsch
challenging limits

Kapsch BusinessCom

Kapsch security audit services.

Simulating reality to defend against hackers.

Phishing, botnets, trojans: Hacker attacks on IT systems of companies, public authorities, institutions, organizations and private computers are everyday events in a networked world. What approaches do the attackers use? Which methods do they employ to search for and repeatedly identify new security holes? This is where the security audit services of Kapsch come in: You can only achieve lasting security by putting yourself into a hackers mindset. Let's declare war on the hackers! Together with our customers and true to our motto of "Prevent, Protect, Detect, Respond".

Our best weapon for more IT security:

Knowing how the opponent thinks, what he does and what he will do.

You must understand your enemy in order to defeat him. Today's opponents are invisible and act globally. They know everything and use ever more refined methods to overcome even highly complex security systems.

New threats and vulnerabilities in applications and operating systems are discovered nearly every day, while programs that exploit these flaws are usually quickly available. Identifying all vulnerabilities in order to close them in time is practically no longer possible for an administrator alongside his usual daily business.

We become hackers. In order to protect you from them.

Kapsch, Austria's only TÜV Trusted IT Security Auditor, relies on a strong four-"stages" strategy:

We prevent, we protect, we detect and we respond.

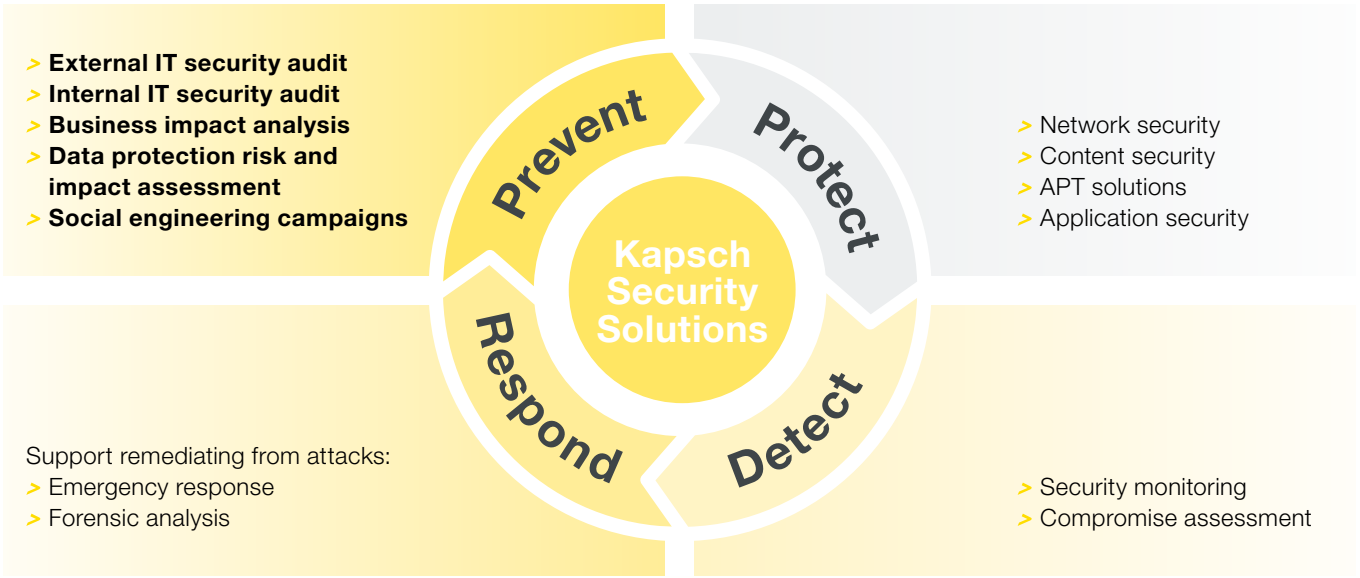
What is required is a security audit that ideally encompasses all system components and applications and utilizes precisely the means and methods that would be used by an attacker to gain unauthorized access to systems. This requires testing methods that are designed from the perspective of the attacker in order achieve the most authentic test scenarios.

Kapsch security audit services will make such real conditions possible. The security audits are performed in accordance with the OSSTMM methods (Open Source Security Testing Methodology Manual), among others. This methodology ensures a uniform result of the security audit to allow for reliable comparisons.

Kapsch carries out security audits according to the quality rules of TÜV Austria. Specialists of Kapsch BusinessCom are certified as TÜV Trusted IT Security Auditors. Thanks to these quality rules, Kapsch customers receive a result that complies with European and international standards.

Kapsch security audit services:

Three core offerings as part of our IT security strategy.



Our audit modules for Prevent.

Increased information security by precautionary measures: Our Prevent offerings encompass everything required to make it as hard as possible for attackers. From internal security audits to awareness workshops. With our additional Detect and Respond audit modules as well as with our Protect security offerings, you have a complete solution that hackers definitely won't like. An overview of our Prevent services is given below.

External IT security audit.

What we do.

> We simulate an attack on the IT system/ network from the outside.

What you get.

> Evaluation of the IT infrastructure accessible via the internet (e.g. mail, FTP and VPN servers, web applications).

Internal IT security audit.

What we do.

> We simulate an attacker who was able to gain access to the internal network.

What you get.

> Evaluation of the internal network (file shares, email- and calendar data, telebanking applications, etc.).

Business impact analysis and risk management.

What we do.

> We determine potential loss, that can be caused by malfunctioning IT systems.
> We identify the quality of the underlying IT systems.

What you get.

> Transformation of technical risks into business risk.
> Development of credible worst case scenarios.
> Assessment of potential loss in monetary values.

Data protection risk and impact assessment.

What we do.

> Regulatory requirements on data protection demand a risk analysis of data-processing systems.
We perform this analysis.

What you get.

> Compliance with reasonable security precautions.
> Data protection risk and impact assessment (DPIA) as required by the EU General Data Protection Regulation (GDPR).

Social engineering campaigns.

What we do.

> We simulate phishing campaigns (cryptolockers).
> We simulate targeted attacks (APT), including spoofed phone calls or onsite visits.

What you get.

> Evaluation of the IT security awareness of the employees.
> Evaluation of the technical security measures against trojans and ransomware.

Our audit modules for Detect and Respond.

In case something is going on: Identify attacks quickly, respond correctly!

Compromise assessment.

What we do.

> We analyze whether your system has already been hacked and whether any active botnet communication can be identified.

What you get

> Network traffic analysis via a monitoring appliance.
> Manual analysis of the top 3 – 7 events based on a time box approach.
> Presentation of critical findings.

Emergency response.

What we do.

> We help to remediate after a system has been hacked.

What you get

> Assessment of attack scope, details and facts.
> Forensic analysis.

Kapsch:

The only TÜV Trusted IT Security Auditor in Austria.

The specialists at Kapsch BusinessCom have been evaluated and certified as TÜV Trusted IT Security Auditors by TÜV TRUST IT TÜV AUSTRIA GMBH. This makes Kapsch the only company in Austria to possess this important certification. In addition, Kapsch BusinessCom employs auditors who have been accredited by Austrian Standards to perform audits according to ÖNORM A 7700. Both organizations therefore confirm that Kapsch BusinessCom security audits are carried out for Kapsch customers according to European and international standards with the highest level of quality.

Our certifications and standards.

- TÜV Trusted IT Security Auditor
- Accreditation to perform audits according to ÖNORM A 7700
- CIS Information Security Auditor according to ISO 27001

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

Play safe for the future – contact Kapsch:

To learn more about our Security solutions please contact us via email
securitysolutions@kapsch.net

Kapsch BusinessCom

Kapsch BusinessCom, a Kapsch Group company, generated revenue of more than EUR 320 million in fiscal year 2015/16 with its 1.200 employees. The comprehensive portfolio of products and solutions of the leading digitalization partner in Austria and the CEE region includes technology solutions for stable, intelligent, and – most importantly – secure ICT infrastructure, in addition to facility solutions for smart building and security technology, multimedia and business services for outsourcing applications, and innovative digitalization solutions that are custom-tailored for specific industries. With its Consult – Deploy – Operate approach, Kapsch is able to cover the entire ICT solution lifecycle for its customers. Kapsch is independent of specific manufacturers and utilizes the best technologies available from the world's leading suppliers, such as Cisco, HP, and Microsoft, and combines them with solutions from its partner network of research institutions and application providers. Kapsch BusinessCom has more than 17,000 customers that include OMV, Allianz, ORF, Erste Bank, Vodafone, and ÖBB, and provides customer service for them both locally and globally in around 40 countries.

>>> www.kapsch.net

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