
Crowe
Cyber Security
RWT Crowe IT Consulting
Audit / Tax / Advisory
Smart decisions. Lasting value.

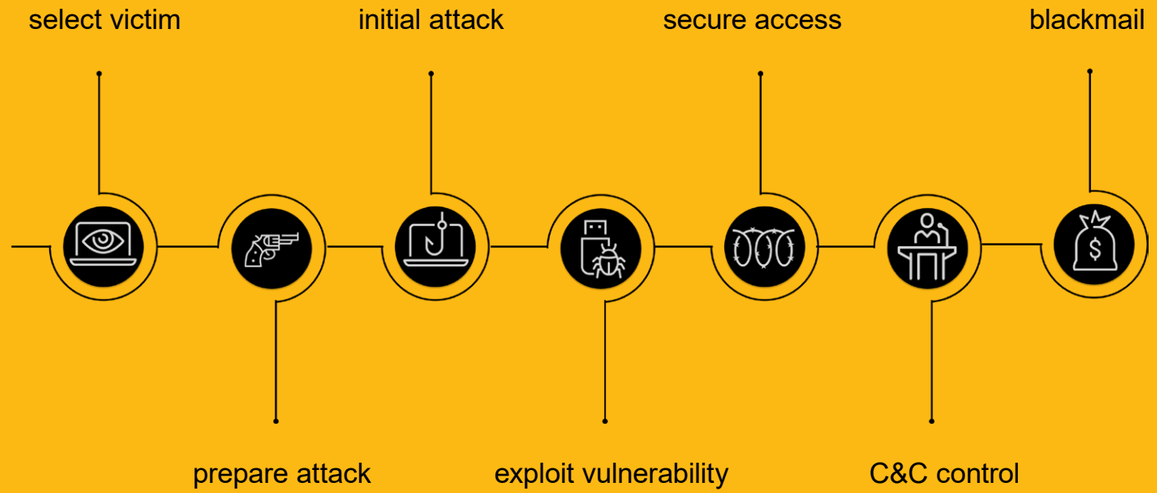
Cyber Security for SMEs

Due to the progressing digitalization, enterprises are forced to turn towards more IT-based business models.

For the companies, the dependency on the functioning IT-based business processes, and thereby the IT-systems themselves, is increasing more and more. IT-outages therefore have the potential to quickly become an existential threat to the survival of the company.

Cyber criminals have also realized this, and thus have been aligning their “business model” to this fact during the last few years. Today, they have also set their sights on small and medium enterprises (SMEs). Their ultimate goal is to successfully extract ransom from their victims. Protecting themselves from cyber attacks has therefore become a “must” also for SMEs.

We are located in Stuttgart, but we are also a proud member of the Crowe Global worldwide network. We are a subsidiary of the Regional Champion RWT Group and at the same time the prime consultants for SMEs in the field of Cyber Security.



Choosing us

Our service portfolio is based on a holistic approach to best help you in protecting your business from cyber attacks:

- We conduct Technical Penetration Testing in your IT-environment to help you get a clear picture about your cyber risks. Our experts will, of course, also assist you in deriving and implementing the appropriate countermeasures.
- When dealing with cyber risks, one tends to neglect the risks of the real world. In order to protect your company from these threats, our portfolio also contains services regarding unauthorized access to your company’s locations and buildings.
- Our Vulnerability Assessments of your IT-systems and your IT-infrastructure will aid you in identifying security loopholes and misconfigurations.
- For an attacker, it is often easier to trick your employees into divulging sensitive data than to circumvent technical protection measures. Our Awareness Trainings regarding threats from Cyberspace therefore make up a big portion of our service portfolio.

Most importantly, we secure your information and data.

Technical Penetration Testing

1

Digitalization forces IT-systems to evolve more and more rapidly. Unfortunately, this also leads to a situation where vulnerabilities and security loopholes are increasing constantly, making businesses more prone to cyber attacks.

For leading IT security experts, the regular execution of technical assessments of your IT-infrastructure is an essential part of “cyber hygiene”. Technical Penetration Testing (“Pen Testing”) simulates an attack on your IT-systems to realistically evaluate your security posture:

- Our Pen Tests are tailor-made to your requirements and will help you to get a clear picture of your As-Is situation regarding IT-risks. The Pen Testing can be performed against specific systems (e.g. a webshop) or against your IT-infrastructure as a whole.
- Our experts will use common security applications and attack tools, also utilized by real attackers, during the execution of the Pen Test.
- We will also assist you in deriving and implementing the appropriate countermeasures.

Physical Penetration Testing

2

With the constant newsflash about companies falling victim to attacks from Cyberspace, one tends to solely focus on threats from this realm. The truth is: the real world also has its own unique set of threats up its sleeve. Regarding IT-security, unauthorized access to a company's location or to its buildings is the most prolific of all physical threats. RWT's Physical Penetration Testing is the best answer to it.

After your approval, our experts will try to gain "unauthorized access" to your company. This will help in testing the following aspects of your physical security measures:

- Effectiveness of your access control systems in regard to gaining access to your company's location and to enter specific areas within your locations (e.g. R&D areas, data center, etc.).
- Effectiveness of your visitors policies and procedures.
- Can an unauthorized person in my company also gain access to the network?

Vulnerability Assessments

3

A high percentage of successful cyber attacks on companies are caused by the exploitation of publicly known vulnerabilities. Typical attack vectors are outdated software and missing security patches.

Our experts will employ well-established vulnerability scanning software in your environment in order to scan your IT-systems for vulnerabilities. Contrary to Pen Testing, no attacks will be performed during a Vulnerability Assessment.

- Our Security Analysts will scan your IT-systems and networks for known vulnerabilities.
- We assess and categorize the identified vulnerabilities together with your IT-experts.
- We actively assist you in deriving and prioritizing the appropriate countermeasures.

Awareness-Trainings

4

The „Human Firewall“

“Social Engineering” is a term coined for all attacks that are aimed at getting your employees to divulge sensitive information or to download harmful files. The most common examples of this form of attack are Phishing E-Mails, fraudulent telephone calls (so-called “Vishing”) or faked text messages (“Smishing”).

Employing the techniques of Social Engineering, in order to gain access to a company’s IT-infrastructure, is often more promising than a “typical hack” for an attacker. Experience has shown that exploiting human weakness is often more effective than attacking technical vulnerabilities.

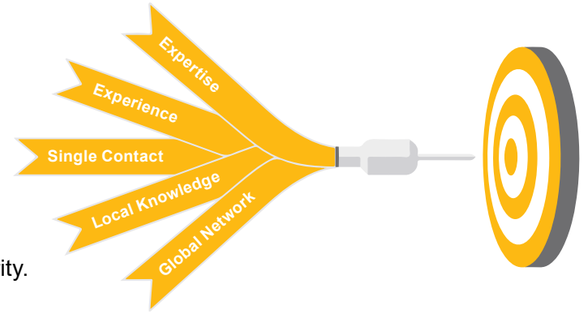
Our Awareness Trainings will help your employees to intuitively identify possible threats. We will turn your employees into a “Human Firewall”. Our multi-level training concept aims at the development of a commonsensical skepticism against Social Engineering Attacks in your employees.

Our service offering

- Your employees will be faced with different real attack scenarios (e.g. Phishing E-Mails or fake text messages) on a regular basis
- We will provide purposeful training content that explains the characteristics of typical Social Engineering Attacks to your employees.
- A measurement of the resilience of your workforce against cyber threats enables you to objectively track your progress in shaping and building the security awareness across your company.
- Tailor-made onsite trainings can be used to intensify your efforts.

Mastering the challenges of the digital world.

Cyber Security as part of an Information Security Management System.



The different measures that are usually employed as part of a Cyber Security Strategy only cover specific parts of an overall Information Security Management System (ISMS). Cyber Security must therefore be perceived as a subset of a holistic approach to Information and Data Security.

In general, ISMS like ISO 27.001, CISIS12 or TISAX (automotive industry) follow a comprehensive approach to protect information and data. Our specialists will guide you through these frameworks in order to implement efficient and fruitful measures in your company.

Our experts accompany you through the whole process of implementing an ISMS all the way to your certification.

International collaboration with Cyber Security Specialist of Crowe Global in Europe.

RWT Crowe IT Consulting GmbH
Olgastrasse 86
70180 Stuttgart
+49 711 319 400-00

Your Contacts

Rafael Robert Gawenda
Associated Partner / Director IT Consulting
+49 711 319 400-138
rafael.gawenda@crowe-rwt.de

Benjamin Schlotz
Managing Consultant
+49 711 319 400-137
benjamin.schlotz@crowe-rwt.de

rwt-it-consulting@crowe-rwt.de
www.crowe-rwt.de