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

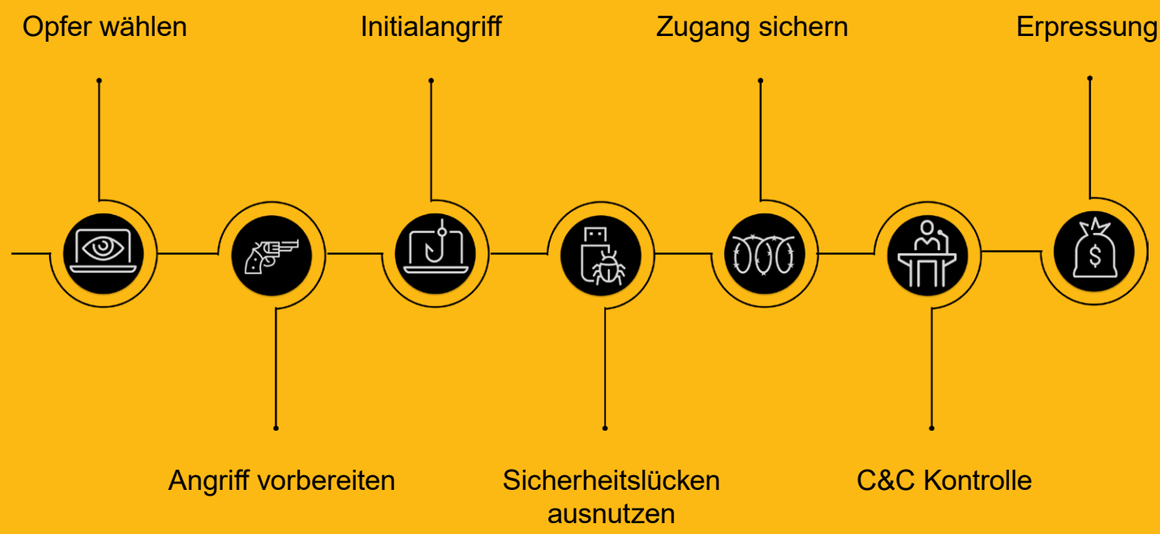
# Cyber Security für KMU

Aufgrund der fortschreitenden Digitalisierung sind Unternehmen gezwungen, sich verstärkt IT-basierten Geschäftsmodellen anzunähern.

Die Abhängigkeit von funktionierenden IT-gestützten Geschäftsprozessen, und dadurch von IT-Systemen, wächst somit ständig. Der Ausfall von IT-Systemen kann innerhalb kurzer Zeit für das Unternehmen zu einer Existenzbedrohung werden.

Diesen Umstand haben Cyberkriminelle in den letzten Jahren immer mehr in den Fokus ihres „Geschäftsmodells“ gerückt. Sie greifen nunmehr bevorzugt kleine und mittlere Unternehmen (KMU) an. Ziel ist es, Lösegelder zu erpressen. Die Absicherung gegen einen möglichen Cyber Angriff wird somit für KMU zum „Pflichtthema“.

Verankert in Stuttgart sind wir als Mitglied des weltweiten Netzwerkes Crowe Global und zugleich als Tochterunternehmen des regionalen Champions RWT der Ansprechpartner für KMU im Bereich Cyber Security.



# Darum wir

Um Ihr Unternehmen bestmöglich auf Angriffe aus dem Cyberraum vorzubereiten, ist unser Leistungsportfolio im Bereich Cyber Security auf einem ganzheitlichen Ansatz begründet:

- Wir führen „Technische Penetrationstests“ in Ihrer IT-Infrastruktur durch, um Ihnen ein realistisches Bild über Ihre IT-Risikosituation zu verschaffen. Unsere Experten unterstützen Sie anschließend auch bei der Ableitung und Umsetzung von Maßnahmen.
- Bei der ausschließlichen Fokussierung auf Gefahren aus dem Cyberraum wird oft der Risikobereich der realen Umwelt vernachlässigt. Unser Portfolio umfasst daher auch Leistungen zum Thema unbefugter und unberechtigter Zutritt zu Unternehmensgebäuden und -örtlichkeiten („Physischer Penetrationstest“).
- Schwachstellenanalysen („Vulnerability Assessments“) für Ihre IT-Systeme und -Landschaften helfen Ihnen, Sicherheitslücken und Fehlkonfigurationen frühzeitig zu erkennen.
- Das Täuschen von Mitarbeitern, und somit das Ausnutzen menschlicher Schwächen, ist für Angreifer oftmals leichter als die Überwindung technischer Schutzmaßnahmen. Die „Awareness Schulung“ Ihrer Mitarbeiter zu Gefahren aus dem Cyberraum stellt daher einen gewichtigen Teil unseres Portfolios dar.

**Wir sichern Ihre Informationen und Daten.**

# Technische Penetrationstests

1

Durch die Digitalisierung entwickeln sich IT-Systeme in immer höherem Tempo weiter. Damit entstehen leider auch kontinuierlich neue Schwachstellen und Sicherheitslücken, die Unternehmen für Cyber Angriffe anfälliger machen.

Regelmäßige qualifizierte technische Prüfungen Ihrer IT-Infrastruktur „auf Herz und Nieren“ werden daher von führenden Sicherheitsexperten als regelmäßiger Bestandteil einer effektiven IT-Sicherheitsstrategie verstanden (sogenannte Cyber Hygiene). Durch die Simulation echter Angriffe auf Ihre IT-Systeme („Technischer Penetrationstest“) kann die Verwundbarkeit der Systeme gegenüber Cyber Bedrohungen realistisch ermittelt werden:

- Ein auf Ihre individuellen Bedürfnisse abgestimmter „Technischer Penetrationstest” (sogenannter Pentest) hilft Ihnen die IST-Situation in Bezug auf Ihre IT-Risiken zu ermitteln. Der Pentest kann auf einzelne Systeme (beispielsweise Webshop) oder auf die gesamte IT-Landschaft angewandt werden.
- Im Rahmen eines Pentests verwenden unsere Spezialisten gängige Sicherheitsprogramme und Angriffswerkzeuge, welche auch von „echten Angreifern“ eingesetzt werden.
- Wir unterstützen Sie auch bei der Ableitung und Umsetzung von Maßnahmen zur Beseitigung der identifizierten Schwachstellen.

# Physische Penetrationstests

2

Durch die ausschließliche Fokussierung auf Bedrohungen aus dem Cyberraum unterschätzen viele Unternehmen die Risiken, welche durch Zutritt von unbefugten Personen zu Unternehmensgebäuden und -örtlichkeiten entstehen. „Physische Penetrationstests“ sind daher ein integraler Bestandteil einer umfassenden Cyber Security Strategie.

Nach Freigabe werden unsere Mitarbeiter versuchen, sich „unberechtigten Zutritt“ zu Ihrem Unternehmen zu verschaffen. Hierdurch können Sie folgende Aspekte Ihrer Schutzmaßnahmen praktisch überprüfen:

- Effektivität und Einhaltung von Zutrittskontrollen zum Unternehmen selbst, sowie innerhalb der Unternehmensgebäude (beispielsweise besonders geschützte Entwicklungsbereiche, Rechenzentrum).
- Effektivität und Einhaltung von Besucherregelungen (beispielsweise zur Begleitung von Besuchern).
- Zugangsmöglichkeiten von unbefugten Personen zu Netzwerken innerhalb des Unternehmens.

# Schwachstellenanalysen

3

Ein hoher Prozentsatz der erfolgreichen Angriffe auf Unternehmen ist auf die Ausnutzung öffentlich bekannter Schwachstellen zurückzuführen. Typische Einfallstore in diesem Bereich sind veraltete Softwarestände und fehlende Sicherheitsupdates.

Unsere Experten validieren Ihre IT-Systeme unter Einsatz gängiger Schwachstellenscanner auf bekannte Sicherheitslücken (sogenannte „Vulnerabilities“). Im Gegensatz zu „Technischen Penetrationstests” werden bei einer Schwachstellenanalyse („Vulnerability Assessment“) keine individuellen Angriffe durchgeführt.

- Unsere Security Analysten untersuchen Ihre IT-Systeme und Netzwerke auf bekannte Schwachstellen.
- Wir bewerten und kategorisieren die identifizierten Schwachstellen zusammen mit den IT-Spezialisten Ihres Unternehmens.
- Wir unterstützen Sie aktiv bei der Ergreifung und Priorisierung notwendiger Gegenmaßnahmen.

# Awareness-Schulungen

4

Als „Social Engineering“ Angriffe werden Angriffsformen bezeichnet, bei denen Personen dazu verleitet werden, sensible Daten zu offenbaren oder schädliche Dateien herunterzuladen. Die bekanntesten Beispiele hierfür sind Phishing E-Mails, betrügerische Telefonanrufe (sogenanntes „Vishing“) oder gefälschte SMS Nachrichten (sogenanntes „Smishing“).

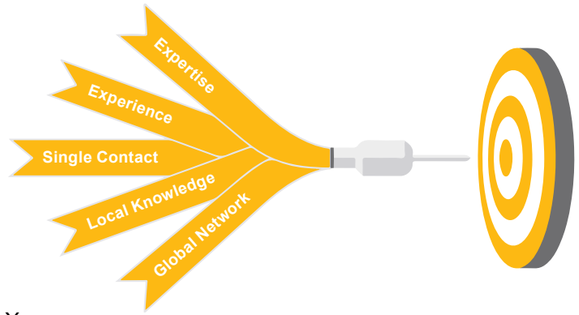
Zur Erlangung eines Zugangs zur IT-Infrastruktur eines Unternehmens sind die Techniken des Social Engineering oft erfolgversprechender als „klassische Hackerangriffe“. Erfahrungsgemäß führt das Ausnutzen menschlicher Schwächen schneller zum Ziel als der Angriff über technische Schwachstellen.

Mit unseren Awareness-Schulungen fördern wir Ihre Mitarbeiter in der intuitiven Erkennung gefährlicher Inhalte. Wir bilden Ihre Mitarbeiter zu einer „Human Firewall“ aus. Unser mehrstufiger Schulungsansatz zielt auf die Entwicklung einer gesunden Grundskepsis Ihrer Mitarbeiter gegenüber potenziell gefährlichen Inhalten.

Ihre Vorteile

- Ihre Mitarbeiter werden regelmäßig mit verschiedenen realen Angriffsszenarien (wie Phishing E-Mails oder SMS) konfrontiert.
- Ihre Mitarbeiter erhalten zielgerichtete Schulungsinformationen dazu, anhand welcher Merkmale sie typische Angriffe besser erkennen können.
- Eine Gesamtauswertung der Resilienz Ihrer Mitarbeiter gegenüber Cyber Bedrohungen ermöglicht Ihnen eine objektive Messung des Fortschritts beim Sicherheitsbewusstsein Ihrer Mitarbeiter und zeigt gegebenenfalls weitere Trainingsbedarfe auf.
- Durch spezifische Vor-Ort-Trainings können die Maßnahmen bei Bedarf intensiviert werden.

# Digitale Herausforderungen sicher meistern.




Cyber Security als Teil eines Informationssicherheitsmanagementsystems.

Einzelne und isolierte Maßnahmen im Bereich von Cyber Security decken nur einen gewissen Teilbereich eines Informationssicherheitsmanagementsystems (ISMS) ab. Die Cyber Security ist daher nur als Teil eines gesamtheitlichen Ansatzes zur Informations- und Datensicherheit zu betrachten.

Allgemeine ISMS wie ISO 27001, CISIS12 oder TISAX verfolgen einen umfassenden Ansatz zum Schutz Ihrer Informationen und Daten. Unsere Experten führen Sie mit Augenmaß durch diese Rahmenwerke, um effizient und zielgerichtet ein passgenaues Maßnahmenbündel für Ihr Unternehmen zu implementieren.

Unsere Experten begleiten Sie durch den Prozess der Implementierung eines ISMS bis zur Zertifizierung.



# Europaweite Zusammenarbeit mit Cyber Security Spezialisten von Crowe Global.

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

## Ansprechpartner

**Rafael Robert Gawenda**
Assoziierter Partner / Geschäftsführer 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**