Grant Thornton

Digital Advisory

Security

Cyber- und IT-Security.

Der Ausfall von IT-Systemen, dadurch ausgelöste Betriebsunterbrechungen und der Verlust von Daten gehören zu den größten Geschäftsrisiken für Unternehmen.

Umfassende IT-Sicherheit für Ihr Unternehmen.

Trotz des Wissens um Cyber- und IT-Risiken besitzen viele Unternehmen noch keine formalen Richtlinien zur Informations- und IT-Sicherheit.

Warum ist Cyber Security so wichtig?

Die stetig wachsende Menge an Daten und Informationen zählt heute oft zu den wichtigsten Unternehmenswerten, die vor Diebstahl und Manipulation geschützt werden müssen. Wer die Sicherheit seiner IT-Systeme und Daten gewährleisten will, sollte sich daher mehrere Fragen stellen:

- Ist das Sicherheitsniveau unserer IT-Landschaft angemessen?
- Haben wir alle wesentlichen Cyber-Risiken adressiert?
- Sind unsere Daten ausreichend gegen Cyberangriffe und Diebstahl durch unbefugte Dritte und Innentäter abgesichert?
- Haben unsere Prozesse und Systeme Schwachstellen?
- Entsprechen unsere Maßnahmen für Cyber/IT-Sicherheit den tatsächlichen Bedrohungen?
- Sind unsere Mitarbeiter ausreichend auf die Gefahren vorbereitet?
- Können das Unternehmen und die Mitarbeiter unmittelbar und richtig auf Angriffe reagieren?

Unsere Lösung für Ihre Sicherheit

Wir helfen Ihnen, Ihr Unternehmen umfassend gegen die Gefahren im Bereich der Cyber/IT-Sicherheit zu wappnen:

Präventiv. Proaktiv. Reaktiv.

Präventiv

im Rahmen einer IT-/Cyber-Sicherheitsanalyse.

- Cyber Security Audit
- Awareness-Schulungen
- Cyber Risk Assessment
- Malware-Analyse
- Code Review
- ISMS
- Mobile Apps
- IT Security

Proaktiv

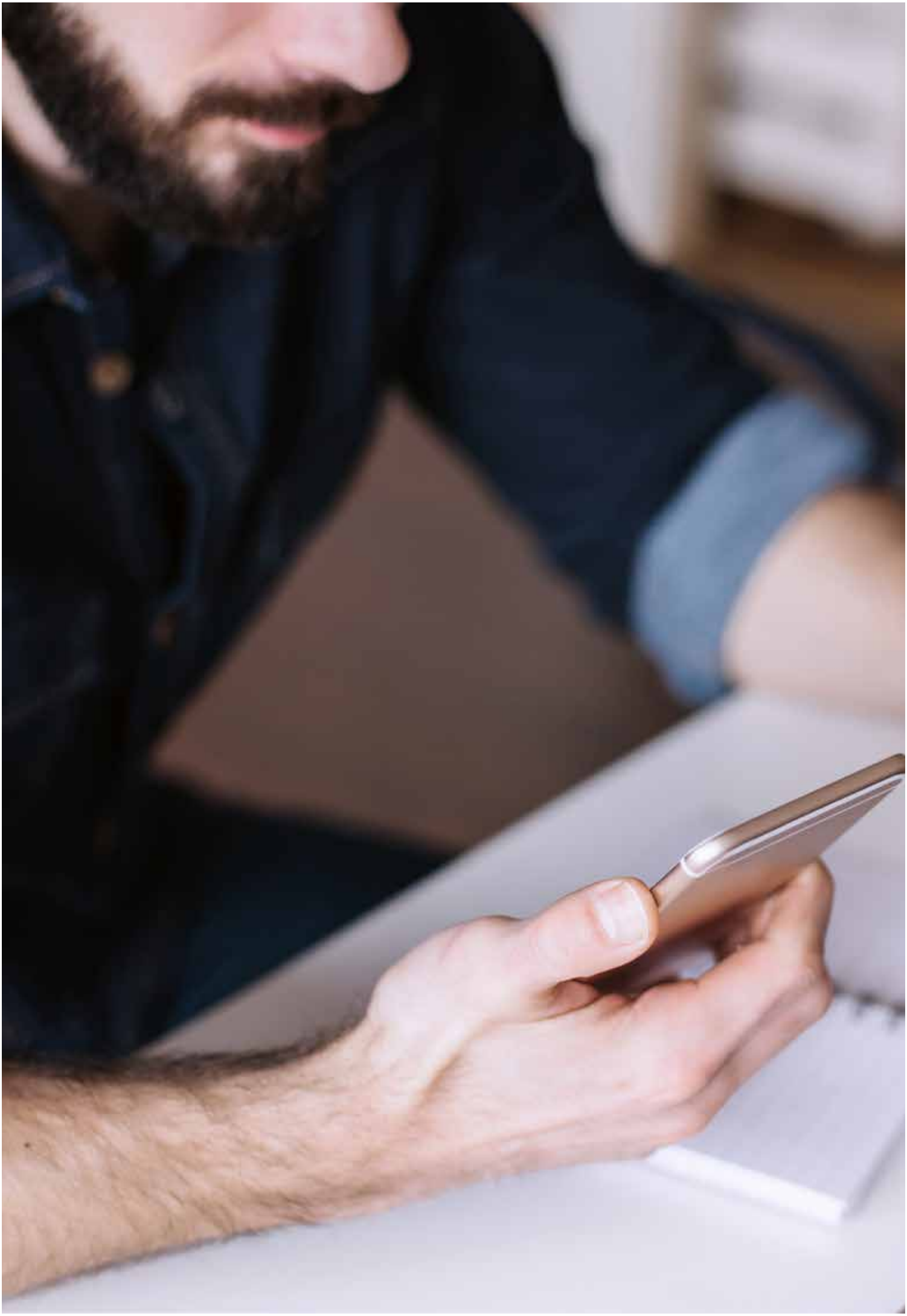
in der Entwicklung einer auf Sicherheit orientierten IT-Strategie und einem Vulnerability Assessment.

- Penetration Testing
- eDiscovery
- Business Continuity
- Vulnerability Assessment

Reaktiv

Sollte tatsächlich ein Ernstfall eintreten, unterstützen wir Sie mit unseren lokalen und internationalen Expertinnen und Experten aus dem Bereich Incident Management, um eingetretene Vorfälle so rasch wie möglich in den Griff zu bekommen. Bei Bedarf führen wir auch vor Gericht verwertbare forensische Dokumentationen zur Unterstützung weiterer Ermittlungen durch.

- Incident Response
- Fraud Investigation
- Forensische Analyse



Cyber-Security-Services.

Um Ihr Unternehmen optimal vor Cyber/IT-Risiken und -Gefahren zu schützen, bieten wir Ihnen eine Reihe von Beratungsleistungen. Dabei können Sie unter anderem aus folgenden Bausteinen wählen:

Cyber- / IT-Security Audit

Unser ganzheitliches Cyber/IT-Security-Audit hilft Ihnen, einen besseren Überblick über mögliche Schwachstellen Ihrer IT-Organisation, -Prozesse und -Systeme zu gewinnen. Gemeinsam mit Ihrer IT-Abteilung erstellen wir eine Bestandsaufnahme von Organisation, Prozessen, Systemen und bereits vorhandenen technischen und operativen Sicherheitsmechanismen. Dabei evaluieren wir auch alle sicherheitsrelevanten Prozesse, wie beispielsweise das Patch-Management, die Datensicherung oder das Mobile-Device-Management und helfen bei der richtigen Konfiguration von Systemen und Sicherheitsmechanismen, wie beispielsweise Firewalls. Auf Wunsch beraten wir Sie auch in der Planung Ihres Netzwerks unter Sicherheitsaspekten, zum Beispiel, um besonders sensible Systeme wie Produktionssteuerungen (Industrie 4.0, IOT) in eigenen Subnetzen zu segregieren.

Penetrationtest / Web-Penetrationstest

Um Ihre IT-Systeme optimal abzusichern, empfehlen wir einen Penetrationtest. Dabei nehmen unsere Experten die Rolle eines Angreifers ein und testen, welche Schwachstellen die IT-Systeme in Ihrem Unternehmen aufweisen und auf welche kritischen Systeme und Daten sich dadurch zugreifen lässt.

So decken wir auch Schwachstellen auf, die ein automatischer Scan allein nicht finden würde und sichern Ihr Unternehmen gegenüber gezielten Attacken bestmöglich ab.

Schwachstellenanalyse

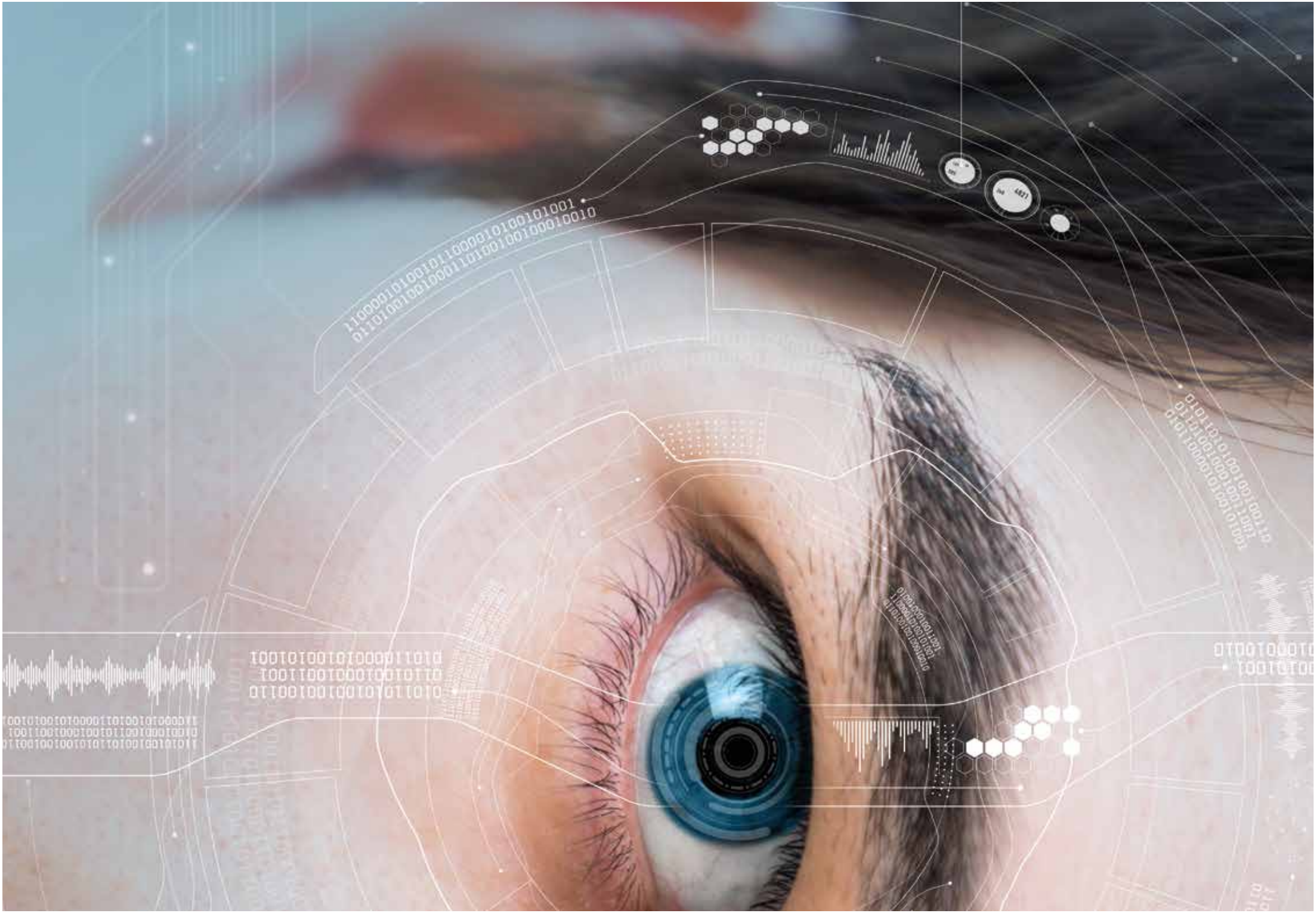
Bei einer Schwachstellenanalyse überprüfen wir Ihre IT-Systeme mit Hilfe marktführender Tools auf bekannte Schwachstellen, Fehlkonfigurationen und operative Sicherheitsrisiken, wie beispielsweise schwache Passwörter oder veraltete Software. Dabei prüfen wir sowohl aus der Perspektive eines externen Angreifers als auch aus der Innenansicht, um die Perspektive eines Mitarbeiters oder Gastes abzubilden. Auch ihre WLAN-Netzwerke unterziehen wir einer ausführlichen Prüfung und decken so zum Beispiel eventuelle Schwachstellen bei der Zugangskontrolle auf.

Awareness-Schulungen

Eines der größten IT-Sicherheitsrisiken für Unternehmen ist aktuell der sorglose Umgang von Mitarbeitern mit Angriffsversuchen per E-Mail oder Social-Engineering. So ließen sich zum Beispiel viele Infizierungen mit Erpressungstrojanern (Ransomware) oder Angriffe durch sog. „President Fraud“ verhindern, wenn Mitarbeiter E-Mails mit infizierten Anhängen besser erkennen würden. Bei unseren Awareness-Trainings schulen wir Ihre Mitarbeiter, Angriffsversuche zu erkennen und richtig damit umzugehen. So werden viele Angriffe bereits im ersten Stadium gestoppt.

Ihr Mehrwert

Eine IT-Sicherheitsanalyse durch unsere Experten macht Ihre IT-Systeme widerstandsfähiger gegen die vielfältigen Cyber-Bedrohungen, denen Unternehmen jeden Tag gegenüberstehen. Damit helfen wir Ihnen, eine höhere Ausfallsicherheit der IT-gestützten Prozesse in Ihrem Unternehmen zu erreichen und kritische Daten besser zu schützen. Hacker, Wirtschaftsspione und Innentäter haben es erheblich schwerer, Ihrem Unternehmen zu schaden.



Ihr Ansprechpartner.

Dr. Cornelius Granig
Senior Advisor
Compliance Technology
& Cyber Security

T +43 1 505 4313
M +43 664 3369013
E cornelius.granig@at.gt.com

Dr. Cornelius Granig ist bei Grant Thornton Austria für die Bereiche Cyber Security, Krisenmanagement und Compliance-Technologie verantwortlich, in denen er über mehr als 20 Jahre Praxiserfahrung verfügt.

Vor seinem Wechsel in die Beratungsbranche war Dr. Granig als Vorstand im Banken- und Versicherungsbereich und als Geschäftsführer internationaler Technologieunternehmen tätig. Er ist Autor des Fachbuches „Darknet", akkreditierter Cyber-Security-Experte bei Europol und Mitglied der Whistleblower-Taskforce bei Transparency International. Sein Wissen gibt er regelmäßig einem breiten Publikum in diversen Publikationen, durch Fachvorträge sowie im Rahmen von Radio- sowie Fernsehauftritten weiter.

Dr. Granig studierte Politikwissenschaft an der Universität Wien und absolvierte an der Donau Universität Krems ein Master-Studium im Bereich E-Government und New Public Management.

Schwerpunkte

- Analyse und Minimierung von Cyber-Risiken
- Gegenmaßnahmen bei Cyber-Angriffen
- Entwicklung, Auswahl und Betrieb sicherer IT-Anwendungen
- Betriebliches Kontinuitätsmanagement
- Unternehmensweites Krisenmanagement
- Auswahl und Einsatz von Hinweisgebersystemen für Whistleblower

Forensic Services.
Incident Response.

Wenn es um den Ernstfall geht, sind unsere Expertinnen und Experten zur Stelle – notfalls rund um die Uhr. Wir unterstützen Sie nicht nur bei Cyber-Vorfällen, Wirtschaftskriminalität oder Streitigkeiten, sondern entwickeln geeignete Strategien im Bereich der Prävention, um zukünftige Vorfälle möglichst zu verhindern.

Sei es ein Cyber-Angriff, ein Datenleck oder der Verdacht auf klassische Wirtschaftskriminalität: Tritt der Ernstfall ein, unterstützen Sie unsere Expertinnen und Experten in den notwendigen Belangen: Wir verfügen über umfassende Erfahrungen aus Sachverständigentätigkeiten für die Justizbehörden und begleiten Sie diskret in der Aufarbeitung der Situation. Zuvorderst sichern wir Ihre Systeme und eliminieren die Gefahr der fortgesetzten Tatbegehung. Parallel sorgen wir für die korrekte Beweissicherung, vor allem im Bereich digitaler Daten. Im Anschluss führen wir unabhängige unternehmensinterne Untersuchungen mit zuverlässigen Methoden und umfangreichem Know-how über klassische Tatmuster durch. Auf diese Weise gewinnen Sie rasch einen Überblick, können Verantwortlichkeiten leichter erheben und Schäden genauer abschätzen.

Gemeinsam mit Ihnen und Ihrer Rechtsvertretung entwickeln wir individuelle strategische Lösungen und Handlungsoptionen – von der Täteridentifikation bis hin zur Behördenkommunikation, der kommunikativen Krisenbegleitung und der Durchführung von internationalen Maßnahmen zum Asset Recovery. Falls es zu gerichtlichen oder außergerichtlichen Auseinandersetzungen kommen sollte, haben Sie basierend auf unseren Untersuchungsergebnissen eine beweiskräftige, durch einen Sachverständigen gefertigte Dokumentation zur Hand.

Basierend auf den Erkenntnissen der forensischen Untersuchung besteht als Nachbereitungsmaßnahme die Möglichkeit, die Prozesse und Compliance-Strukturen Ihrer Organisation zu optimieren. So definieren wir z. B. Frühwarnindikatoren, die Ihrem Team zukünftig das rasche Erkennen von typischen Unregelmäßigkeiten ermöglichen.

Ihr Ansprechpartner

für forensische Projekte, Business Risk Services und Compliance

Mag. Georg H. Jeitler, BA MBA
Partner | Gerichtssachverständiger
Forensic & Advisory

T +43 1 505 4313 2068
M +43 664 1616388
E georg.jeitler@at.gt.com

Grant Thornton

grantthornton.at