

ADV - Ransomware

Wien | 05.09.2023

Gerald Kattnig
Director | Cyber Risk

Ransomware | Definition und Historie

Ransomware: Software, die gezielt dazu verwendet wird, den Zugriff auf Daten, bis zum Eingang einer Lösegeldzahlung, zu blockieren

Die Geschichte der Ransomware

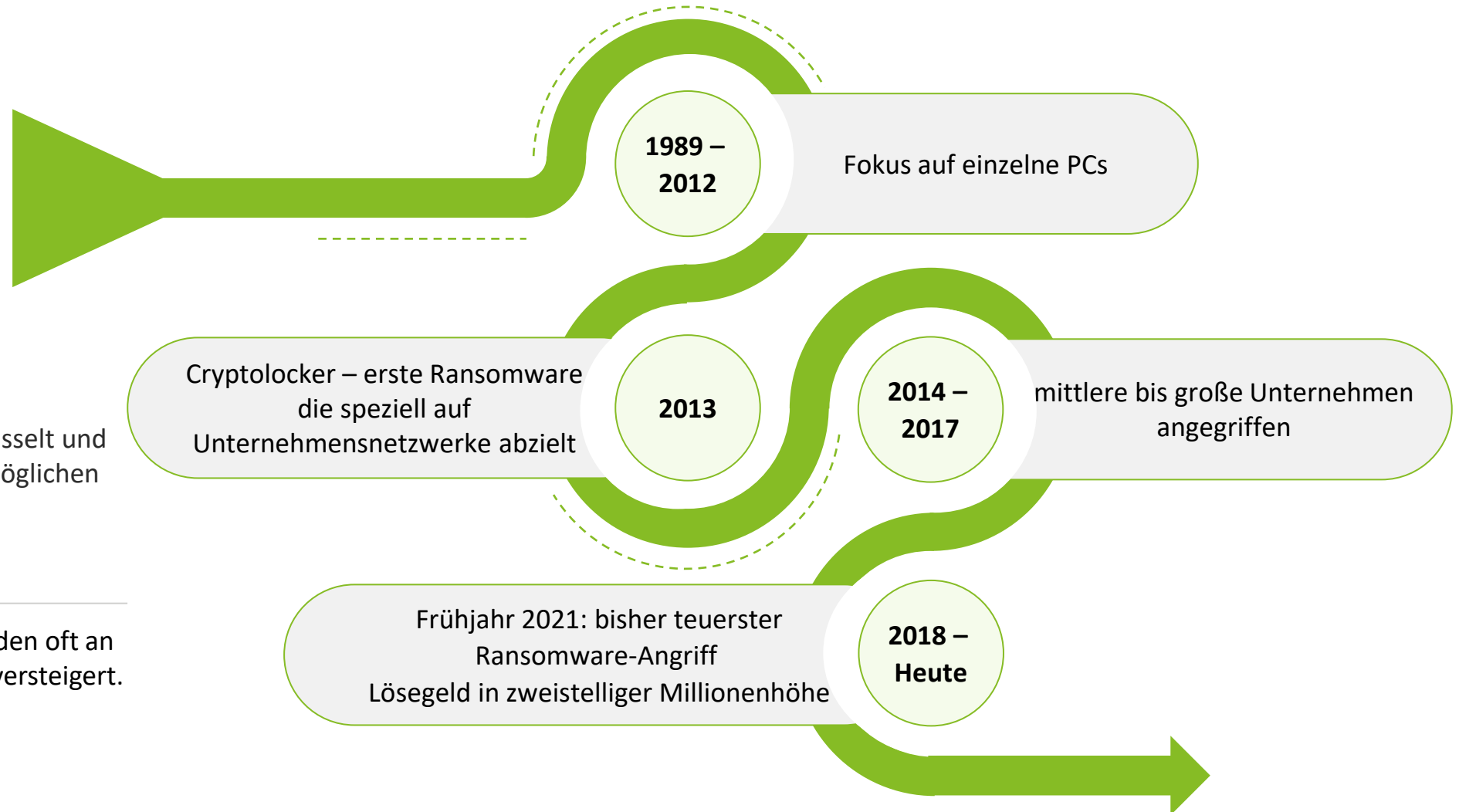


Doppelte Erpressung:

Daten werden verschlüsselt und exfiltriert, um höchstmöglichen Druck aufzubauen

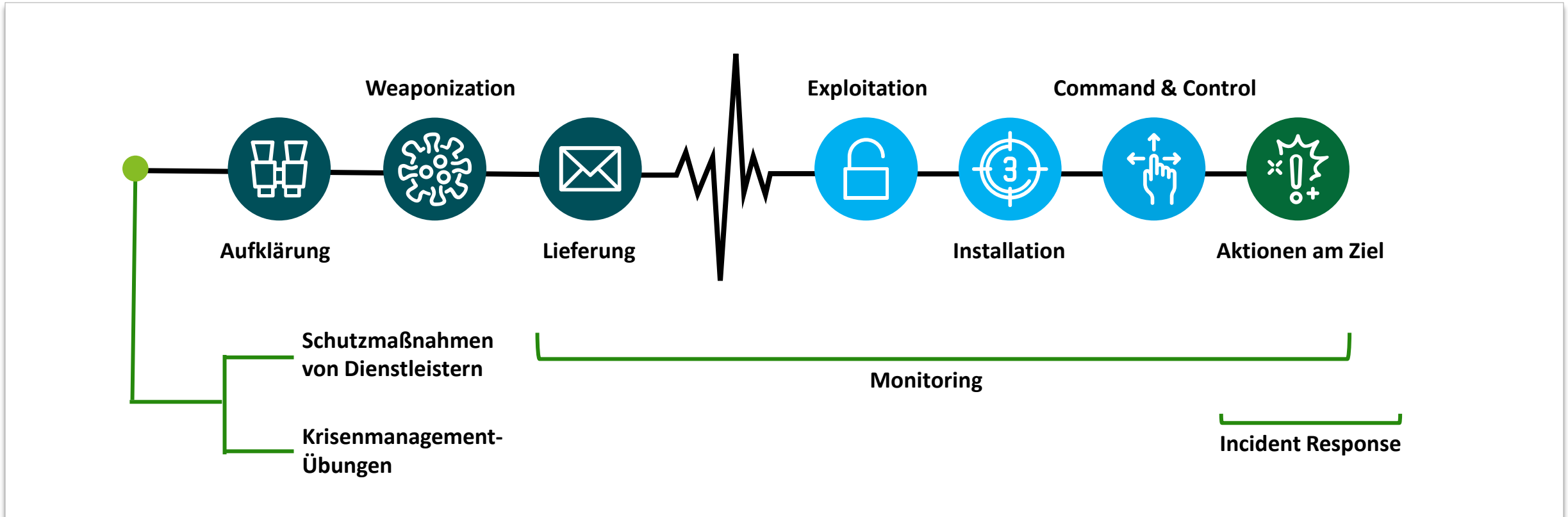


Gestohlene Daten werden oft an den Höchstbietenden versteigert.



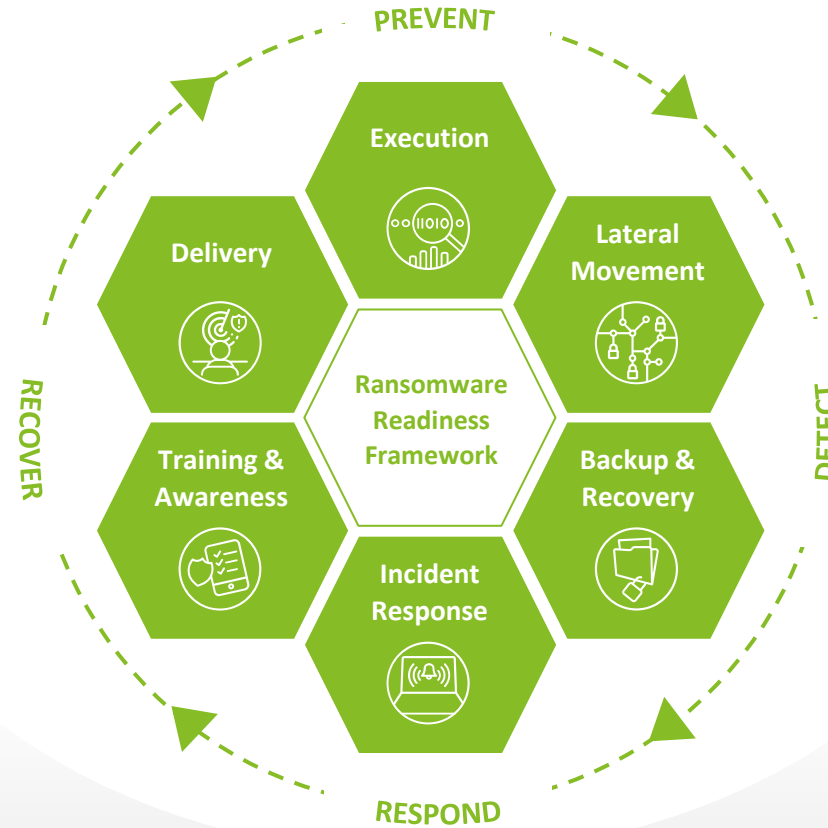
Ransomware Kill-Chain

Proaktive Maßnahmen zur Vorbereitung und Aufbau der Infrastruktur sind essentiell, um Cyber-Angriffe abzuwehren



Deloitte Ransomware Readiness Framework

Schritte zur Ganzheitlichen Cybersicherheit



Key Benefits



Sichtbarkeit von Schwachstellen
im Netzwerk



Verständnis über die aktuellen
Reaktionsmöglichkeiten



Identifizierung von
Optimierungspotenzialen

Unser Ransomware-Assessment Approach

Unser Ransomware-Assessment lässt sich in vier Module aufteilen.

Projektmanagement

1 Initiale Reifegradbestimmung



3 Notfallplan für BCM



2 Deloitte Toolbox



4 Notfallsimulation



Modul 1: initiale Reifegradbestimmung

Durch unser Quick Assessment können Verbesserungspotentiale aufgedeckt und konkrete Maßnahmen zur Minimierung von Cyber-Risiken abgeleitet werden.

Unser Ansatz

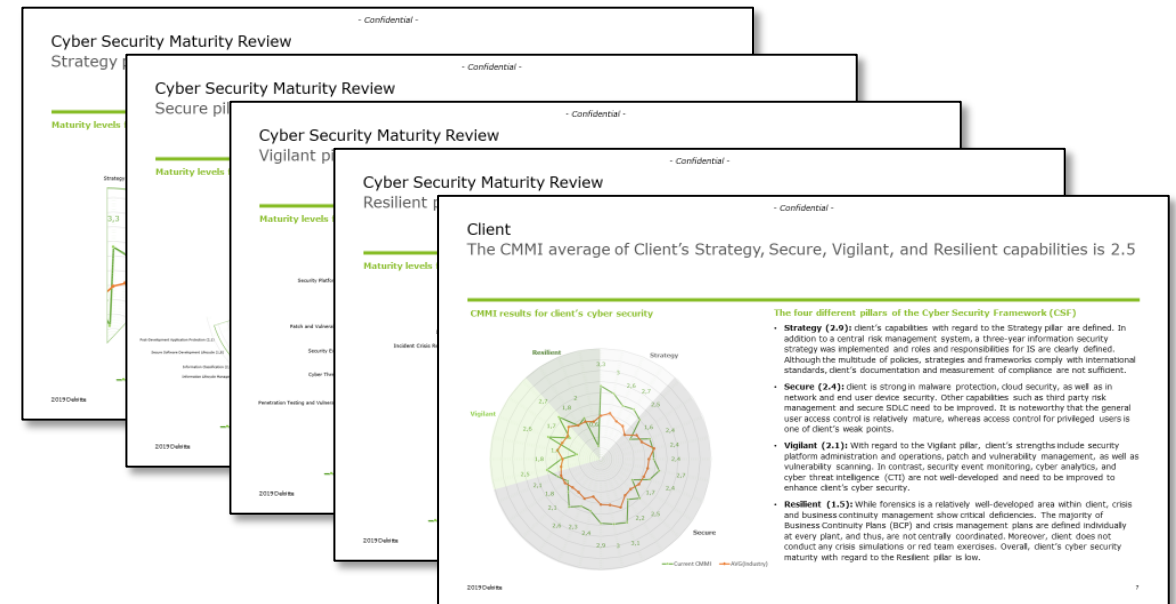


1 Cyber Security Maturity Assessment – Interviews

2 Workshop zur Identifikation von Verbesserungspotentialen

3 Übergabe spezifischer Handlungsempfehlungen

- ✓ Identifikation von Cyber-Risiken basierend auf festgestellten Lücken
- ✓ Erarbeitung priorisierter Handlungsempfehlungen
- ✓ Konkreter Umsetzungsplan



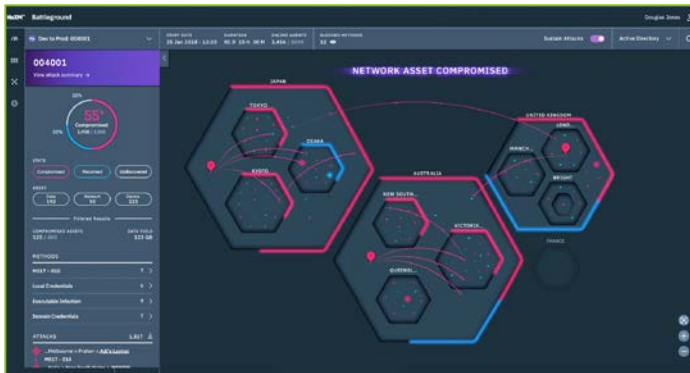
Abschlussbericht

Modul 2: Technisches Assessment mit der Deloitte Toolbox

Unsere Toolbox wird immer auf dem neusten Stand gehalten. Für die technische Analyse verwendete Applikationen werden immer auf die Bedürfnisse des Kunden abgestimmt.

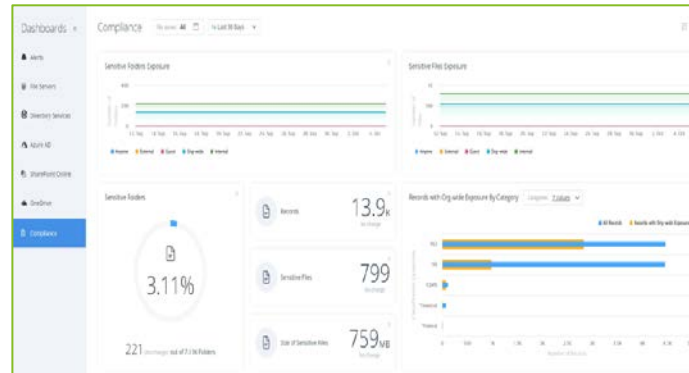
Endpoints: Mit XM Cyber*

- **Bericht mit Schwachstellen und Empfehlungen** zur Behebung
- Detaillierte visuelle Darstellung des **Pfades** bei Angriffsszenarien zu kritischen Assets



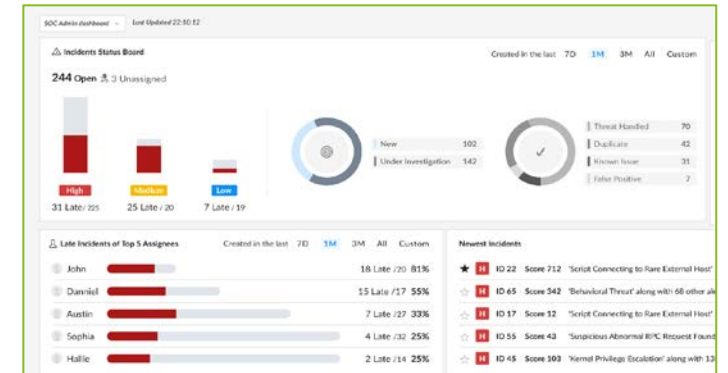
Data Security: Mit Varonis*

- **Klassifizierung** von unorganisierten Daten aus unterschiedlichsten Datenquellen
- Identifikation und **Simulation** von **unerwünschten Zugriffen** auf Daten



Netflow: Mit Palo Alto*

- Systemseitige Erfassung und Auswertung von **Netflow Daten**
- Reports über **Schwachstellen** und **Malware-Infektionen** im **Branchenvergleich**



* Exemplarische Applikationen aus dem Deloitte Ransomware Applikations-Portfolio

Modul 3: Schreiben von Notfallplänen

Um angemessen auf einen Ransomware Vorfall reagieren zu können, ist eine gute Vorbereitung essentiell



Modul 4: Notfallsimulation

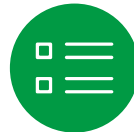
Awareness bis in die Vorstands-Ebene

Übergeordnete Zielstellung von Krisensimulationen

Steigerung der Awareness
aller Beteiligten



Verifizierung von Strukturen
und Prozessen & Erhebung
des Ist-Zustands



Erhöhung der
Handlungssicherheit und
Reaktionsfähigkeit



Identifikation von
Handlungsfeldern und
Verbesserungspotenzialen



Auseinandersetzung mit
Worst-Cases in sicherem
Rahmen



✓ Auseinandersetzung mit **realitätsnahen Worst-Case-Szenarien**

✓ **Krisensicherheit**

✓ erhöht die **Reaktionsfähigkeit**

✓ Steigert die **Awareness**



Typische Erkenntnisse

Beispielhafte Ergebnisse und Empfehlungen eines Ransomware Assessments



Diskussion und Fragen





Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited („DTTL“), dessen globales Netzwerk von Mitgliedsunternehmen und deren verbundene Unternehmen innerhalb der „Deloitte Organisation“. DTTL („Deloitte Global“), jedes ihrer Mitgliedsunternehmen und die mit ihnen verbundenen Unternehmen sind rechtlich selbstständige, unabhängige Unternehmen, die sich gegenüber Dritten nicht gegenseitig verpflichten oder binden können. DTTL, jedes DTTL Mitgliedsunternehmen und die mit ihnen verbundenen Unternehmen haften nur für ihre eigenen Handlungen und Unterlassungen. DTTL erbringt keine Dienstleistungen für Kundinnen und Kunden. Weitere Informationen finden Sie unter www.deloitte.com/about.

Deloitte Legal bezieht sich auf die ständige Kooperation mit Jank Weiler Operenyi, der österreichischen Rechtsanwaltskanzlei im internationalen Deloitte Legal-Netzwerk.

Deloitte ist ein global führender Anbieter von Dienstleistungen aus den Bereichen Wirtschaftsprüfung, Steuerberatung, Consulting, Financial Advisory sowie Risk Advisory. Mit einem weltweiten Netzwerk von Mitgliedsunternehmen und den mit ihnen verbundenen Unternehmen innerhalb der „Deloitte Organisation“ in mehr als 150 Ländern und Regionen betreuen wir vier von fünf Fortune Global 500® Unternehmen. "Making an impact that matters" – ca. 415.000 Mitarbeiterinnen und Mitarbeiter von Deloitte teilen dieses gemeinsame Verständnis für den Beitrag, den wir als Unternehmen stetig für unsere Klientinnen und Klienten, Mitarbeiterinnen und Mitarbeiter sowie die Gesellschaft erbringen. Mehr Information finden Sie unter www.deloitte.com.

Diese Kommunikation enthält lediglich allgemeine Informationen, die eine Beratung im Einzelfall nicht ersetzen können. Deloitte Touche Tohmatsu Limited („DTTL“), dessen globales Netzwerk an Mitgliedsunternehmen oder mit ihnen verbundene Unternehmen innerhalb der „Deloitte Organisation“ bieten im Rahmen dieser Kommunikation keine professionelle Beratung oder Services an. Bevor Sie die vorliegenden Informationen als Basis für eine Entscheidung oder Aktion nutzen, die Auswirkungen auf Ihre Finanzen oder Geschäftstätigkeit haben könnte, sollten Sie qualifizierte, professionelle Beratung in Anspruch nehmen.

DTTL, seine Mitgliedsunternehmen, mit ihnen verbundene Unternehmen, ihre Mitarbeiterinnen und Mitarbeiter sowie ihre Vertreterinnen und Vertreter übernehmen keinerlei Haftung, Gewährleistung oder Verpflichtungen (weder ausdrücklich noch stillschweigend) für die Richtigkeit oder Vollständigkeit der in dieser Kommunikation enthaltenen Informationen. Sie sind weder haftbar noch verantwortlich für Verluste oder Schäden, die direkt oder indirekt in Verbindung mit Personen stehen, die sich auf diese Kommunikation verlassen haben. DTTL, jedes seiner Mitgliedsunternehmen und mit ihnen verbundene Unternehmen sind rechtlich selbstständige, unabhängige Unternehmen. .

Für weitere Informationen kontaktieren Sie
Deloitte Services Wirtschaftsprüfungs GmbH.
Gesellschaftssitz Wien | Handelsgericht Wien | FN 44840 t

© 2023 Deloitte Services Wirtschaftsprüfungs GmbH