Deloitte.

ADV - Ransomware

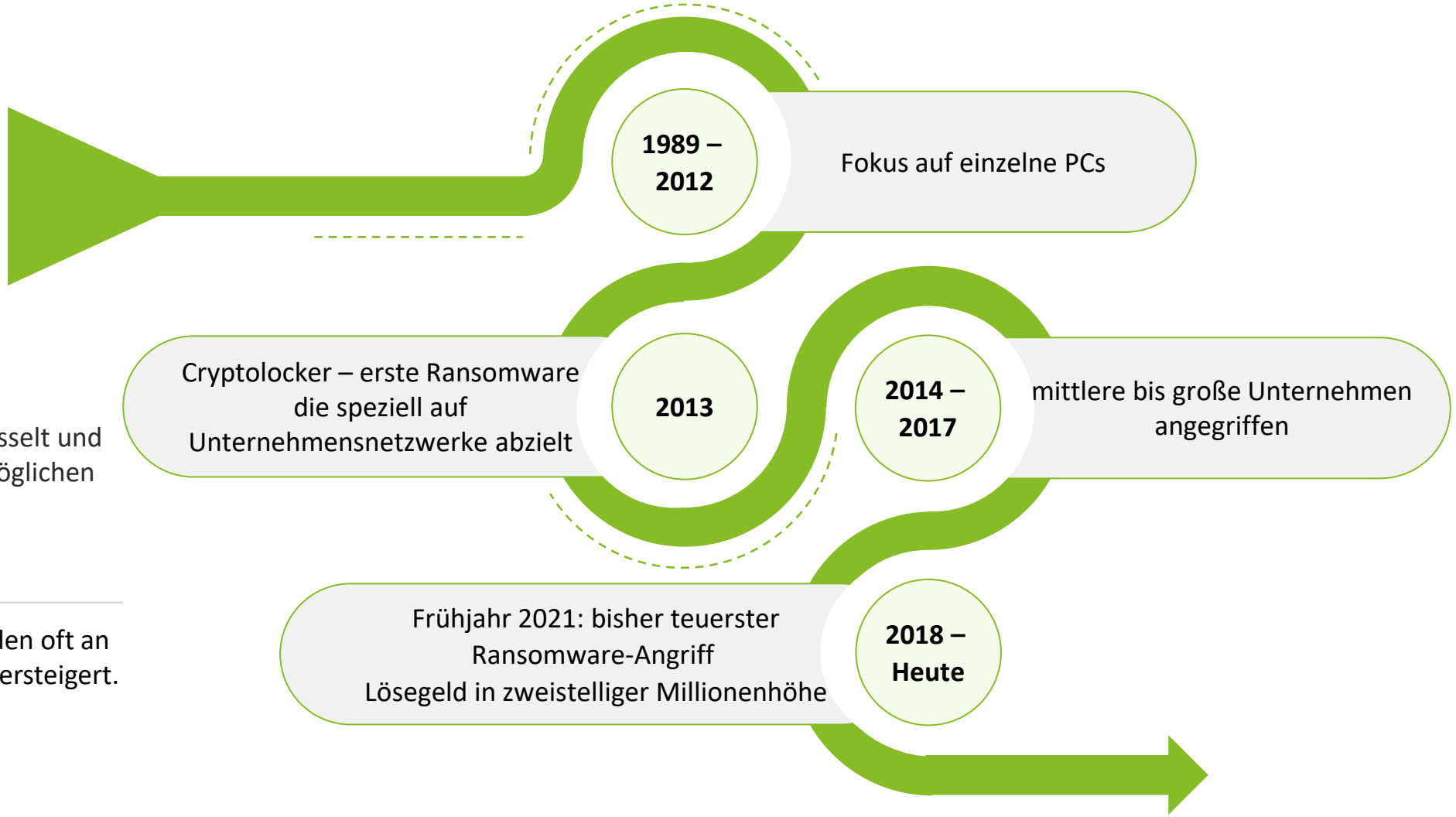
Wien | 05.09.2023

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



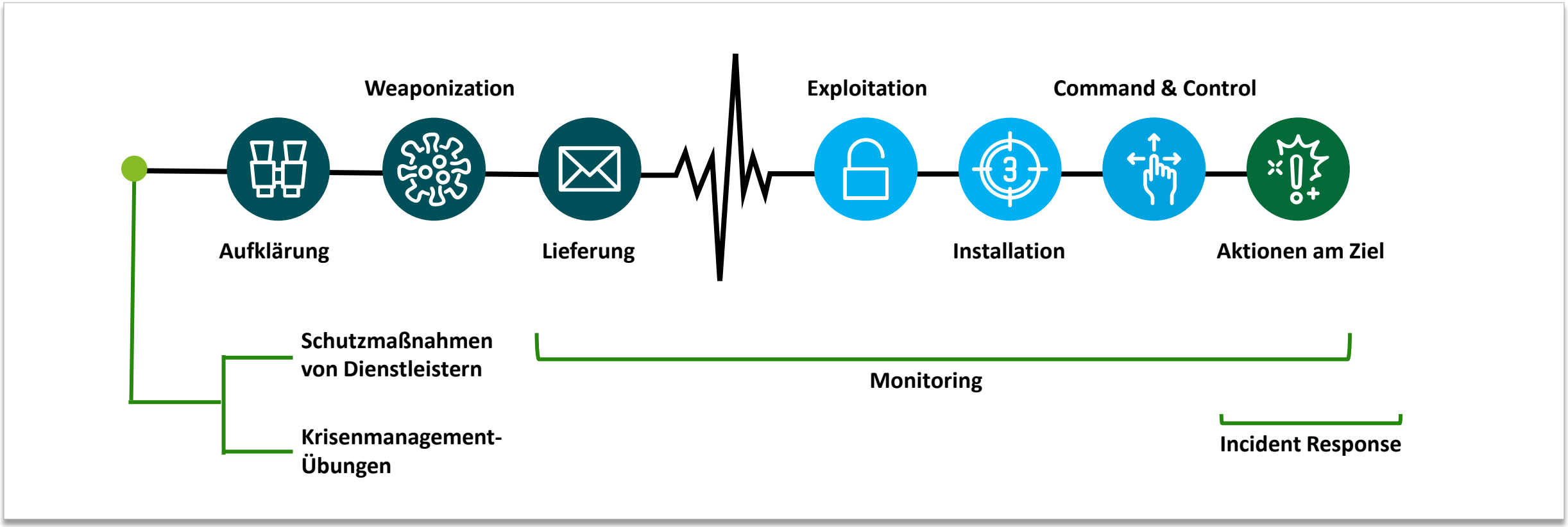
Doppelte Erpressung:

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

2 Deloitte Toolbox

3 Notfallplan für BCM

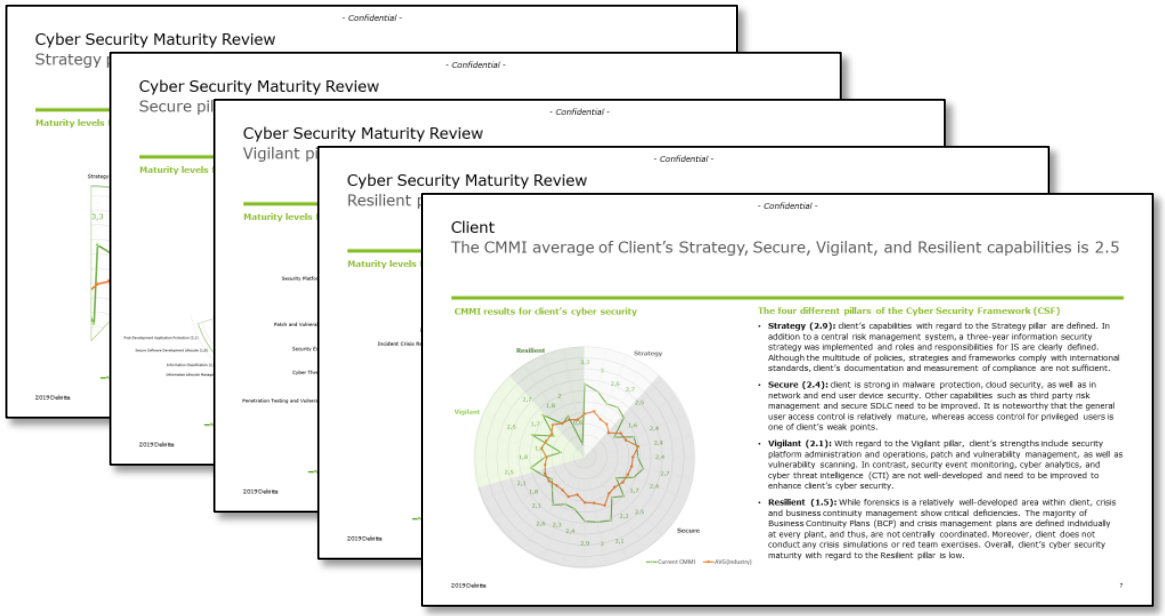
4 Notfallsimulation

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**



Abschlussbericht

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

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*

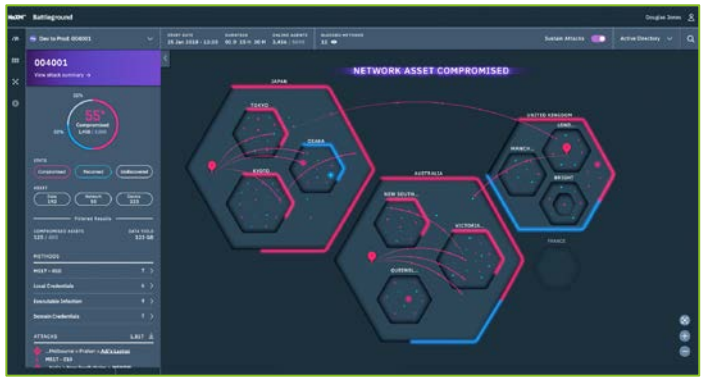
- **Bericht mit Schwachstellen** und **Empfehlungen** zur Behebung
- Detaillierte visuelle Darstellung des **Pfades bei Angriffsszenarien** zu kritischen Assets

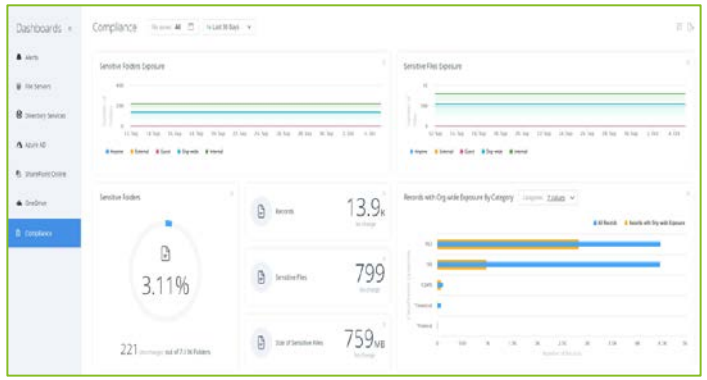
Data Security: Mit Varonis*

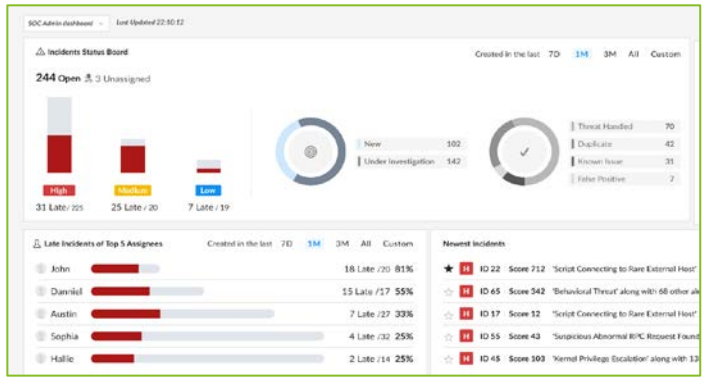
- **Klassifizierung** von unorganisierten Daten aus unterschiedlichsten Datenquellen
- Identifikation und **Simulation** von **unerwünschten Zugriffen** auf Daten

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

Auswertung **bestehender Notfallmanagementprozesse** und ITSCM Rahmenbedingungen

Berücksichtigung der Ergebnisse aus den vorherigen Modulen

Umfassendes **Deloitte Wissen in den Bereichen BCM und ITSCM**

Workshop / Interviews

Erstellung der **Notfallpläne** in **Abstimmung** mit Kundenbedürfnissen.

Notfallplan für die Integration in ihr IT Service Continuity Management

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

Krisenmanagement

Strategien und Entscheidungskriterien

Rollen und Verantwortlichkeiten

Business Impact Analyse

Textbausteine für die Krisenkommunikation

Auswirkungsanalyse

Diskussion und Fragen

Deloitte.

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