FORENSIC READINESS CONSULTING
SEIEN SIE VORBEREITET

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

RISIKEN ERKENNEN – DATEN SCHÜTZEN – VORBEREITET SEIN

Innerhalb von IT-Systemen und Anwendungen werden immer komplexere Geschäftsprozesse abgebildet und sensible Daten verarbeitet. Damit erhöht sich zunehmend das Risiko für Unternehmen, in den Fokus krimineller Aktivitäten zu gelangen. Die Cyberangriffe können einerseits von extern aus dem Internet kommen, interne Angreifer dürfen allerdings auch nicht vernachlässigt werden. Die Statistik des Bundeskriminalamts zeigt, dass die Fälle von Datenveränderung und Computersabotage in den letzten Jahren stark gestiegen ist.

CYBERANGRIFFE SIND REALITÄT

Einen 100-prozentigen Schutz vor Angriffen gibt es nicht. Doch gilt es die IT-Systeme und sensiblen Daten bestmöglich zu sichern sowie die Weichen für eine erfolgreiche forensische Untersuchung, nach einem erfolgreichen Angriff, zu stellen. Im Rahmen einer Analyse der IT-Landschaft und -Prozesse können unsere Security Experten die notwendigen Maßnahmen für eine Forensic Readiness erkennen und bei deren Umsetzung unterstützen.

Die Prä-forensische Analyse betrachtet dabei verschiedenste technische und organisatorische Faktoren:

- Sicherheitsorganisation
- Rechtliche Rahmenbedingungen
- Sicherheitsmechanismen
- Nachvollziehbarkeit
- Logfileintegrität
- Datenintegrität
- Angrifferkennung

IHRE VORTEILE AUF EINEN BLICK

- **Interne und externe Angriffe oder Angriffsversuche zeitnah erkennen**
- **Angemessen reagieren**
- **Gesetzliche Vorschriften kennen**
- **Forensische Nachuntersuchung unterstützen**
- **Urheber von Angriffen identifizieren**
- **Aus Vorfällen lernen**
- **Prozesse optimieren**
- **Eigene Risiken kennen**
- **Langfristig Kosten senken**

T · · Systems ·

IHR FAHRPLAN FÜR EINE FORENSIC READINESS

Im Rahmen einer IST-Analyse ihrer IT-Landschaft und -Prozesse können unsere Security Experten die notwendigen Maßnahmen für eine Forensic Readiness erkennen und bei deren Umsetzung unterstützen. Diese prä-forensische Analyse betrachtet dabei verschiedenste technische sowie organisatorische Faktoren ihrer Systeme und Ihres Unternehmens. Im Ergebnis werden zum einen Maßnahmen zur Protokollierung und Absicherung Ihrer IT-Landschaft definiert. Weiterhin werden Möglichkeiten zur erfolgreichen und zeitnahen Erkennung von Sicherheitsvorfällen aufgezeigt sowie die Strukturen zur professionellen und schnellen Reaktion auf diese geprüft. Dabei steht immer im Fokus, relevante Systeminformationen, die als mögliche Beweismittel innerhalb einer forensischen Untersuchung genutzt werden können, zu protokollieren und zu sichern.

1 REAGIEREN

- Verbesserung der Sicherheitsorganisation
- Bewertung von Datenschutzrichtlinien
- Definition von Speicherfristen sowie Meldepflichten
- Maßnahmen zur Angriffsreaktion

2 ERKENNEN

- Nachvollziehbarkeit von Systemzugriffen
- Prüfung der Datenintegrität
- Logmechanismen optimieren
- Maßnahmen zur Angriffserkennung

3 OPTIMIEREN

- Analyse der IT-Infrastruktur
- Bewertung der aktuellen Sicherheitsmaßnahmen
- Prüfung der Analysefähigkeit von Daten
- Maßnahmen zur Erkennung und Beseitigung von Sicherheitslücken

HERAUSGEBER

T-Systems Multimedia Solutions GmbH
Riesaer Straße 5
D-01129 Dresden
Tel.: +49 (0) 351 - 2820 - 0
www.t-systems-mms.com

IHR ANSPRECHPARTNER

Thomas Haase
Tel: +49 (0) 351 - 2820 - 2206
Mobil: +49 (0) 175 - 5884 475
E-Mail: t.haase@t-systems.com

T · · Systems ·