



Digital Forensics and Incident Response

KPMG. Make the Difference.



Ganzheitliche Unterstützung: Prävention und professionelle Reaktion im Ernstfall

In einer digital vernetzten Welt sind Unternehmen zunehmend Ziel von Cyberangriffen. Die jüngste KPMG Studie „Cybersecurity in Österreich 2025“ bestätigt eine alarmierende Zunahme der Bedrohungen: Cyberattacken auf heimische Unternehmen finden mittlerweile täglich statt und die Anzahl der Angriffe hat sich in den letzten Jahren mehr als verdoppelt. Diese Vorfälle können nicht nur den Geschäftsbetrieb lahmlegen, sondern auch zu Reputationsverlusten und hohen finanziellen Schäden führen.

**DFIR-Notfallhotline:
+43 1 31332-2407**

Wir begleiten Sie umfassend beim Schutz Ihrer Organisation – und das beginnt schon weit vor dem Ernstfall. Im Rahmen unserer **präventiven Unterstützung** analysieren und optimieren wir gemeinsam mit Ihnen Ihre bestehenden Prozesse zur **Erkennung und Bewältigung von Sicherheitsvorfällen**. Wir helfen Ihnen, Schwachstellen frühzeitig zu identifizieren, Abläufe zu verbessern und technische wie organisatorische Maßnahmen so zu gestalten, dass potenzielle Angriffe möglichst früh erkannt und professionell abgewehrt werden können. So schaffen wir gemeinsam die Grundlage dafür, dass es idealerweise gar nicht erst zu einem Notfall kommt.

Um diese Prozesse optimal anwenden zu können, ist **Training** unerlässlich. Wir simulieren mit Ihnen verschiedene **Incident-Response- und Notfallszenarien**, damit Ihr Team im Ernstfall routiniert, sicher und effizient reagieren kann. Durch regelmäßige Trainings und praxisnahe Übungen stärken

wir die **Handlungssicherheit** Ihrer Mitarbeiter:innen und sorgen dafür, dass alle Prozesse im Ernstfall reibungslos ineinandergreifen.

Sollte es dennoch zu einem Sicherheitsvorfall kommen, stehen wir Ihnen mit unserer **gesamten Expertise** zur Seite: Unsere Spezialist:innen unterstützen Sie bei der schnellen **Eindämmung** des Angriffs, der **Wiederherstellung** Ihrer Systeme und der **forensischen Aufklärung** der Ursachen. In unserem hochmodernen forensischen Labor analysieren wir Daten sicher und effizient, um Angriffswege, Täter und Schadensausmaß präzise zu identifizieren und rechtssichere Beweise zu sichern.

Unser Ziel ist es, Ihre Systeme **schnell** und **sicher** wieder in Betrieb zu nehmen, um die **Betriebsunterbrechung so kurz wie möglich** und die dadurch entstehenden **Kosten so gering wie möglich** zu halten.



Sie wollen sich Kriminellen stark und vorbereitet entgegenstellen?

Dabei setzen wir auf umfassende lokale Expertise und ein **internationales Netzwerk an Fachspezialist:innen**. Ob es um die Analyse von Malware, die Aufklärung komplexer Datenexfiltrationen oder eDiscovery geht – wir haben die richtigen Expert:innen zur Hand. Dank unserer **24/7-Bereitschaft** können Sie sich darauf verlassen, dass Sie im Notfall jederzeit auf unsere Unterstützung zählen können.

Um Sie optimal auf potenzielle Angriffe vorzubereiten, bieten wir ein umfassendes Leistungsportfolio. Wir unterstützen Sie beim Aufbau, der Weiterentwicklung und dem Training Ihrer IT-Security-Teams sowie im Notfall- und Krisenmanagement.

Sollten Sie Ziel eines Angriffs werden, begleiten wir Sie und Ihre Expert:innen im Incident-Management und bieten technische Unterstützung in den Bereichen Forensik und Wiederherstellung Ihrer Dienste.



Aufbau und Weiterentwicklung eines Incident-Response-Teams: Wir unterstützen Sie dabei, ein schlagkräftiges Team für die Reaktion auf Sicherheitsvorfälle zu etablieren und gezielt weiterzuentwickeln. Dabei gehen wir individuell auf Ihre Organisation ein, um Ihr Team stark und reaktionsfähig zu positionieren.



Incident-Response-Prozesse erarbeiten und optimieren: Wir analysieren und gestalten gemeinsam mit Ihnen alle Abläufe rund um die Erkennung, Bewertung und Bewältigung von Vorfällen – individuell und praxisnah. So sind Sie in der Lage, Angriffe zeitnahe zu identifizieren sowie schnell und präzise zu reagieren.



Notfallmanagement entwickeln und üben: Wir erstellen mit Ihnen maßgeschneiderte Notfallmanagement-Prozesse und trainieren diese regelmäßig in realistischen Szenarien, um die Handlungssicherheit Ihres Teams zu stärken.



Forensische Analysen: In unserem forensischen Labor führen wir detaillierte Analysen durch – egal, ob es sich um einen Security Incident oder einen Betrugsfall handelt. Wir identifizieren Angriffswege, Täter und Schadensausmaß und sichern rechtssichere Beweise.



Unser Incident Response Retainer bietet Ihnen unseren Support zu jeder Tages- und Nachtzeit. Aber wir wollen nicht nur im Notfall von Ihnen hören. Wir streben eine ganzheitliche Partnerschaft an, um gemeinsam mit Ihnen eine zukunftsichere Abwehr von Bedrohungen sicherzustellen.



Cloud-Forensik und Response: Auch in modernen Cloud-Umgebungen stehen wir Ihnen zur Seite: Wir unterstützen Sie bei der forensischen Analyse und Reaktion auf Sicherheitsvorfälle in Cloud-Infrastrukturen – damit Sie auch in der Cloud jederzeit handlungsfähig bleiben.

KPMG.
Make the
Difference.

Kontakt

Für weitere Informationen wenden Sie sich bitte an einen unserer Experten oder besuchen Sie uns unter [kpmg.at](https://www.kpmg.at)



Stefan Prinz
Advisory

M +43 664 883 69091
stefanprinz@kpmg.at



Simon Andraschek
Advisory

M +43 664 883 08793
sandraschek@kpmg.at

[kpmg.at](https://www.kpmg.at)



© 2025 KPMG Austria GmbH Wirtschaftsprüfungs- und Steuerberatungsgesellschaft, eine österreichische Gesellschaft mit beschränkter Haftung und ein Mitglied der globalen KPMG Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer private English company limited by guarantee, angeschlossen sind. Alle Rechte vorbehalten.