



Digital Forensics & Incident Response

IT-Sicherheitsvorfälle meistern & Beweise sichern

Schnelle Hilfe im IT-Notfall

Im Falle eines IT-Sicherheitsvorfalls ist Zeit Ihr stärkster Gegner. Denn kommt es zu einem Schadensereignis muss schnell und effizient vorgegangen werden, um den Cyber-vorfall abzuwehren und den laufenden Betrieb wiederher-zustellen.

Ihre Vorteile

- Schnelle Eindämmung des Cybervorfalls: Im IT-Notfall definieren wir die erforderlichen organisatorischen & technischen Maßnahmen zur Abwehr des Vorfalls
- Professionelle Analyse & Beweissicherung: Wir be-geben uns für Sie auf digitale Spurensuche, analy-sieren Vorfälle & sichern Daten und Beweise
- Rasche Wiederaufnahme des Geschäftsbetriebes: Wir unterstützen Sie dabei, den laufenden Betrieb schnellstmöglich wiederherzustellen.
- Fundierte Handlungsempfehlungen für die Zukunft: Mit dem Abschlussreport erhalten Sie Handlungs-empfehlungen zur Abwehr zukünftiger Angriffe

Unsere Leistungen: Ganzheitlicher Ansatz im Krisenfall

Incident Response: Erfolgreiche Abwehr von Angriffen

Im Ernstfall ist schnelles Handeln gefragt: Je effektiver Sie auf einen IT-Sicherheitsvorfall reagieren, desto höher ist die Chance, Datendiebstähle oder Verschlüsselungen von Systemen zu verhindern bzw. einzudämmen.

Unser Incident Response Team unterstützt Sie bei der Eindämmung von Schäden, der Wiederaufnahme des Geschäftsbetriebes und der Aufklärung des Vorfalls – remote sowie vor Ort.

Aber auch vor oder nach einem Cyber-Sicherheitsvorfall sind unsere Expert:innen für Sie da, beispielsweise durch die Erstellung eines Incident Response Management Plans oder forensische Analysen.

Digital Forensics: Den Tätern auf der Spur

Sie sind Ziel eines Cyberangriffs geworden und möchten aufklären, wie es zu dem Vorfall kam bzw. wer dahinter steckt?

Unsere IT-Forensiker:innen machen entsprechende Datenspuren auf Ihren IT-Systemen ausfindig, werten diese aus, ermitteln den Schaden und sichern Beweise.

Lessons learned: Indem wir den Angriff rekonstruieren, decken wir zudem auf, über welchen Weg dieser erfolgte, und geben Ihnen geeignete Handlungsempfehlungen zur Behebung an die Hand.

Unsere Vorgehensweise im IT-Notfall



Fallaufnahme



Ersthilfe



Beweissicherung



Forensische
Analyse



Wiederherstellung/
Bericht

Ad Ons

- Fachkundige Remote- & Vor-Ort-Unterstützung: Unsere IR-Expert:innen sind sowohl remote als auch vor Ort für Sie da.
- Onboarding Service: Kommunikationsplan, abgestimmte Prozesse etc.
- Vorgehen nach internationalen Standards: Unsere Expert:innen orientieren sich an Industrie-standards wie BSI IT-Forensik, ISO/IEC 27042/27043 & NIST 800-61.
- Definierte Service-Level
- Compromise Assessment: Angriffserkennung, forensische Daten (-grundlage), Handlungsempfehlungen
- DFIR Rahmenvertrag/-as-a-Service: garantierte Servicelevel, vereinfachte Incidentprozesse
- BCM: Disaster & Recovery Pläne für schnelle Wiederanlaufzeiten
- Krisenmanagement



Notfallkontakt

E-Mail: it-notfall@tuvit.de

Telefon: +49 30 200 770033

Über uns: DIGITALISIERUNG. SICHER. GESTALTEN. Wir beraten Kunden in ihrem Bestreben, das Vertrauen in robuste, hoch verfügbare IT-Infrastrukturen und -Organisationen zu stärken und begleiten Auftraggeber auf ihrem Weg der sicheren digitalen Transformation. Die TÜV NORD IT Secure Communications GmbH & Co. KG gehört zum Geschäftsbereich IT der TÜV NORD GROUP und tritt gemeinsam mit ihrem Schwesterunternehmen, der TÜV Informationstechnik GmbH, unter der Dachmarke TÜVIT auf.

Kontakt: Carsten Keil | Tel.: +49 160 888 54 06 | c.keil@tuvit.de

TÜV NORD IT Secure Communications GmbH & Co. KG | Hohenzollerndamm 184 | 10713 Berlin
tuvit-consulting.de

