Warth & Klein Grant Thornton

An instinct for growth™

Malware

Investigation

Network

Krisen und Cyberangriffe sicher beherrschen

Incident Response

Cyberangriffe werden nicht nur häufiger, sondern auch komplexer und zielgerichteter. Dabei verfolgen die Angreifer die unterschiedlichsten Ziele und verursachen häufig großen wirtschaftlichen Schaden.

Die Fähigkeit, in komplexen Situationen Cyberangriffe und die möglichen Folgen und Krisen zu beherrschen, ist ein klarer Geschäftsvorteil. Bei Störungen im Betriebsablauf hat eine schnelle und vollständige Wiederherstellung der Daten, Systeme und Prozesse oberste Priorität, wobei digitale Spuren und Beweismittel geschützt werden müssen. Die zeitweilige Nichtverfügbarkeit von IT-Systemen, Datenverlust oder etwa Datendiebstahl hat unmittelbar gravierende Folgen auf die Wirtschaftlichkeit von Unternehmen in allen Branchen.

Warum Warth & Klein Grant Thornton?

Unsere erfahrenen Experten helfen Ihnen, mit Cyber Incident Response optimal auf mögliche Cybervorfälle zu reagieren. Cyber Incident Response bedeutet das Auffinden und Schließen von Sicherheitslücken, Aufklärung des „Einbruchs“ und aller Schäden sowie die Zurückverfolgung des Angreifers. Darüber hinaus werden die Ursachen in Ihrer IT-Umgebung untersucht und das Schadensausmaß ermittelt. Auf Wunsch arbeiten wir hierbei auch eng mit Ihren Rechtsanwälten, Ihrem Cyberversicherer oder den Behörden zusammen.

Unser Bericht enthält Empfehlungen, wie Sie Ihre IT-Umgebung gestalten, Prozesse optimieren und Ihre Organisation perfektionieren können, um Störungen aller Art zu vermeiden. Wir sind bestens vertraut mit aktuellen Cybercrime-Angriffsmustern, wie z. B. Malware, die Ihre Datenträger infiziert, verschlüsselt und im Anschluss Geldbeträge zur Entsperrung verlangt (sog. „Ransomware“), oder Betrügern, die sich als Mitglied der Chefetage ausgeben, um Mitarbeiter dazu zu drängen, Auslandsüberweisungen auszuführen (sog. „Fake President Fraud“ oder „Fake President“).

Wir bewerten gemeinsam mit Ihnen:

- Was kostet Sie der Ausfall pro Tag / Stunde konkret?
- Welche operativen und wirtschaftlichen Folgen ergeben sich für Sie aus dem Datendiebstahl?
- Welche zeitlichen Faktoren müssen eingehalten werden, um weitere wirtschaftliche Schäden zu minimieren?
- Welche Maßnahmen sind im Schadensfall notwendig und sinnvoll für Ihre unternehmerischen Zwecke?
- Wie können Sie vergleichbare Vorfälle künftig vermeiden?

Ihr Mehrwert

Sollte es zu einem Zwischenfall gekommen sein, betreuen Sie unsere IT-forensischen Experten zu sämtlichen IT- Sicherheitsvorfällen wie Hackerangriffen, Datenverlusten etc. Die sofortige Schließung der Sicherheitslücken, Schadensermittlung und Rückverfolgung der Angriffe stehen hierbei neben der Daten- und Systemwiederherstellung im Vordergrund, um entstandene finanzielle und operative Schäden zu minimieren und weitere Negativauswirkungen und Verluste abzuwenden.

Sie profitieren von unserer professionellen Beratung zu Organisation, Abläufen und Technik, um im Falle eines Angriffs oder anderen Vorkommnissen schnell und wirksam reagieren zu können („Incident Readiness“).

Wir haben zahlreiche Cybercrime Investigations durchgeführt und können Ihnen im Bereich Cyber Incident Response mit unserer umfassenden Erfahrung zur Seite stehen.

„Fake President Fraud“: Cybercrime im Finanzsektor

Ein Unternehmen der Versicherungsbranche beauftragte uns mit der Untersuchung eines Cybercrime-Vorfalls:

Der Finanzvorstand hatte eine täuschend echte E-Mail erhalten, die vermeintlich vom Vorstandsvorsitzenden der Gruppe kam. Diese E-Mail enthielt klare Instruktionen, umgehend (und streng vertraulich) Banktransaktionen im Umfang von 3,2 Mio. Euro ins Ausland durchzuführen – und es wurde entsprechend gehandelt. Wir konnten den Vorgang beim Mandanten vollständig aufklären und helfen, 2,1 Mio. Euro zurückzutransferieren.

Maßgeschneiderte Angriffe dieser Art, sog. „Fake President Fraud“, haben seit 2015 deutlich zugenommen. Die beste präventive Gegenmaßnahme ist ein maßgeschneidertes „Cybercrime Awareness Training“ für ausgewählte Mitarbeitergruppen.

Konkrete Verbesserungen nach einem Cyber Incident bei einem Finanzdienstleister

Ein Finanzdienstleister erlitt einen „Einbruch“ in das eigene lokale Netzwerk, bei dem sensible Datensätze nachweisbar entwendet wurden. Wir unterstützten unseren Mandanten bei der Aufklärung (Cyber Incident Response) und konnten einen Innentäter eindeutig identifizieren. Anschließend wurden wir mit der Ausarbeitung von Empfehlungen zur Verbesserung der IT-Security beauftragt:

1. Die IT-Landschaft bedurfte einer gründlichen Inventarisierung sowie der Konsolidierung und konsequenter Außerbetriebnahme von abgelösten Systemen.
2. Regelmäßige interne und externe Penetrationstests liefern kontinuierlich Erkenntnisse für weitere Optimierungen, die anschließend umgehend umsetzt werden.

Cyber Incident in der Rohstoffindustrie – interne Sabotage mit Millionenschaden

Unser Auftraggeber zog uns hinzu, nachdem es zu einigen unerklärlichen Störungen im firmeninternen Netzwerk gekommen war. Noch während der Erstellung des Gesamtlagebildes konnten wir bei einer großen Zahl von Vorfällen sieben Incidents eindeutig als interne Sabotage identifizieren. Der Innentäter konnte mithilfe forensisch gesammelter Beweismittel und eindeutiger digitaler Spuren überführt werden. Es entstand ein umfassender Katalog an Empfehlungen zur Verbesserung der gesamten IT-Landschaft sowie der IT-Security im Speziellen, den der Auftraggeber anschließend umgehend umsetzte.

Auszüge aus unseren Maßnahmen:

1. Empfehlungen für die IT-Organisation: klare Rollenverteilung und Verantwortlichkeiten, Reporting, Schnittstellen zwischen internen Stellen und externen Dienstleistern
2. Beseitigung eklatanter Sicherheitsmängel in der IT-Infrastruktur im Zusammenhang mit den Themen Berechtigungskonzept, Passwort-Management, Patch Management, physische Sicherheit etc.

Die Optimierung der IT-Security half dem Mandanten, nach sechs Monaten „Ausnahmezustand“ wieder zu einem normalen Geschäftsbetrieb zurückzukehren.

Ihre Ansprechpartner

WP/StB Dr. Frank Hülsberg
Senior Partner
T +49 211 9524 8527
E frank.huelsberg@wkgt.com

Helmut Brechtken
Associate Partner
T +49 211 9524 8576
E helmut.brechtken@wkgt.com

Internationale Kompetenz

Auch bei Fragen mit internationalem Bezug müssen Sie nicht auf unsere hohen Qualitätsstandards verzichten. Bei grenzüberschreitenden Aufgabenstellungen arbeiten wir mit dem leistungsstarken Netzwerk Grant Thornton International zusammen. Über 47.000 Mitarbeiter in rund 130 Ländern garantieren Ihnen weltweit hervorragende Services auf einheitlich hohem Niveau – für jede Ihrer Herausforderungen und mit dem richtigen Experten vor Ort.

Warth & Klein Grant Thornton

An instinct for growth™

Warth & Klein Grant Thornton AG ist die deutsche Mitgliedsfirma von Grant Thornton International Ltd (Grant Thornton International). Die Bezeichnung Grant Thornton bezieht sich auf Grant Thornton International oder eine ihrer Mitgliedsfirmen. Grant Thornton International und die Mitgliedsfirmen sind keine weltweite Partnerschaft. Jede Mitgliedsfirma erbringt ihre Dienstleistungen eigenverantwortlich und unabhängig von Grant Thornton International oder anderen Mitgliedsfirmen. Sämtliche Bezeichnungen richten sich an beide Geschlechter. Stand 09/2017