HEUKING KÜHN LÜER WOJTEK

Schutz vor Cyber-Attacken

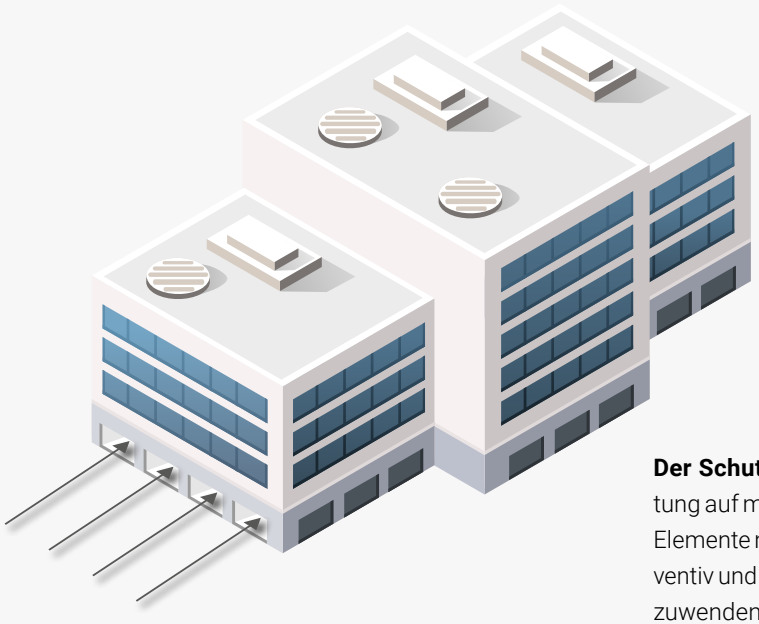
PRÄVENTION UND INCIDENT RESPONSE

Integrierte Unterstützung zur
Vorbeugung und Begegnung von Cyberangriffen

RECHTSANWÄLTE UND STEUERBERATER

HERAUSFORDERUNG

Cyberangriffe stellen ein relevantes Problem für Unternehmen dar. Einerseits steigt mit zunehmender Digitalisierung und Vernetzung die Relevanz der IT für Geschäftsprozesse und das Funktionieren des Unternehmens, andererseits nimmt die Zahl zu und die Methodik der Angriffe auf IT-Systeme wird komplexer. Die Arten von Cyberangriffen sind vielfältig.



Der Schutz vor Cyberangriffen und die Vorbereitung auf mögliche IT-Krisenfälle sind daher zentrale Elemente moderner Unternehmensführung, um präventiv und regressiv Schaden vom Unternehmen abzuwenden. Doch wie kann man Cyberangriffe bestmöglich verhindern und welche Maßnahmen sind effektiv, wenn es dennoch zu einem erfolgreichen Cyberangriff gekommen ist?

So geschehen die häufigsten Cyberangriffe

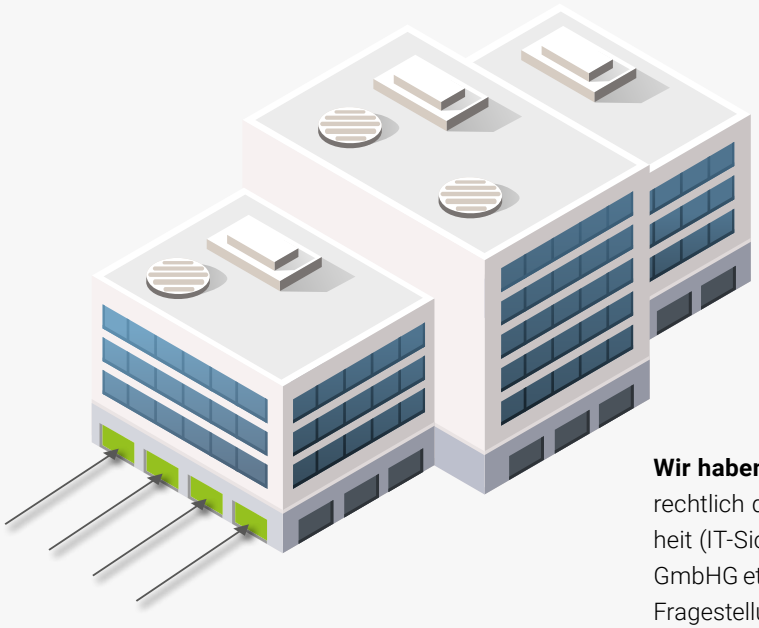
- Gezieltes Hacking von Webservern
- Drive-by-Exploits
  (Ausnutzen von Schwachstellen in Browsern)
- Phishing
  (gezielte Schadsoftware-Infiltration per fingierter E-Mail)
- Distributed-Denial-of -Service-Angriffe
  (Einsatz von Botnetzen zur Störung der Erreichbarkeit von Webservern)

Erfolgreiche Cyberangriffe haben einschneidende Folgen für die betroffenen Unternehmen, wie z.B.

- Ausfall oder Beeinträchtigung der unternehmensinternen IT
- Beeinträchtigung bis zum kompletten Ausfall der Geschäftsabläufe in Produktion und Rechnungsprozess
- Gefährdung und Beeinträchtigung der Reputation des Unternehmens, seiner Produkte und seiner Repräsentanten
- Gefährdung von Geschäftsgeheimnissen
- Manipulation der Geschäftsprozesse
- Datenverlust

LÖSUNG

1. Präventive Unterstützung beim Aufsetzen eines IT-Sicherheitskonzepts



Wir haben ein Konzept entwickelt, das nicht nur rechtlich die gesetzlichen Vorgaben zur IT-Sicherheit (IT-Sicherheitsgesetz, EU-DSGVO, TMG, AktG, GmbHG etc.) abdeckt, sondern auch die operativen Fragestellungen durch die Einbeziehung von Dienstleistern mit Spezialisierung in den Bereichen IT-Sicherheitstechnik und Kommunikation einbindet. In abgestimmter Vorgehensweise können wir Sie damit nicht nur bei der bestmöglichen Prävention von Cyberangriffen unterstützen, sondern auch einen möglicherweise erfolgreichen Angriff präventiv vorbereiten, um im Krisenfall kurzfristig und angemessen reagieren zu können.

Unser Konzept beinhaltet insbesondere folgende Leistungen:

Recht

- Risikoanalyse im Hinblick auf IT- und datenschutzrechtliche Schwachstellen
- Prüfung und ggf. Anpassung von bestehenden, sicherheitsrelevanten Verträgen unter Berücksichtigung aktueller Vorgaben zum Stand der Technik
- Absicherung von Geschäftsgeheimnissen unter Berücksichtigung der nationalen Umsetzung zur EU-Richtlinie 2016/943 zum Know-How-Schutz
- Unterstützung bei der Einführung oder Optimierung eines IT-Compliance-Management-Systems Prüfung und ggf. Anpassung bestehender Verträge im Hinblick auf sicherheitsrelevante Aspekte
- Erstellung von Informationsmaterial für Mitarbeiter zur Vorsorge vor und zum richtigen Umgang mit Cyberangriffen
- Durchführung von Inhouse-Schulungen zu rechtlichen IT-Sicherheitsvorgaben
- Auf Wunsch weitere individualisierte Beratungsleistungen

IT-Sicherheitstechnik
in Kooperation mit spezialisierten IT-Sicherheitsunternehmen

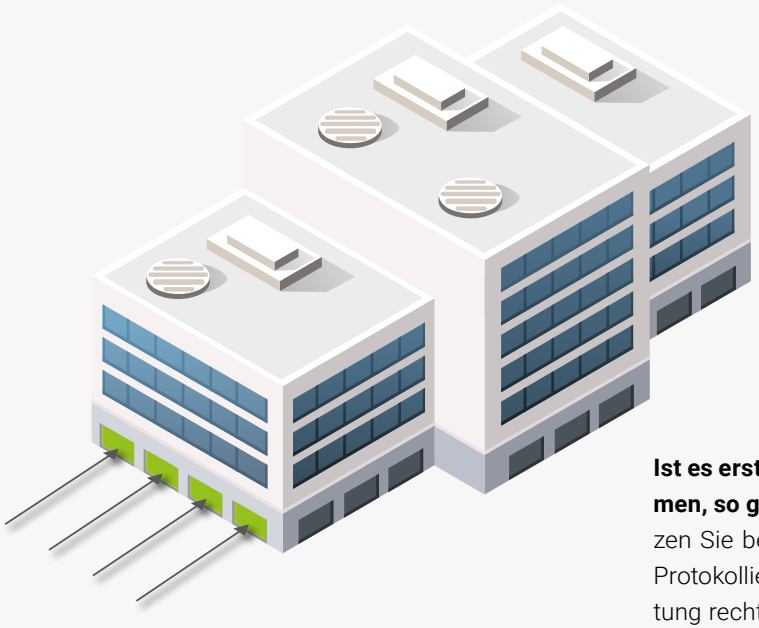
- Risikoanalyse im Hinblick auf technische Schwachstellen
- Erstellung eines technischen Vorfallreaktionsplans (Incident Response)
- Unabhängige Beratung zum Einsatz effektiver IT-Sicherheitslösungen

Kommunikation
in Kooperation mit spezialisierten Kommunikationsagenturen

- Erstellung eines kommunikativen Vorfallreaktionsplans (Incident Response)
- Unabhängige Beratung zur Vorbereitung effektiver Kommunikationslösungen

LÖSUNG

2. Regressive Unterstützung beim Umgang mit Cyberangriffen



Ist es erst einmal zu einem Cyberangriff gekommen, so gilt es schnell zu handeln. Wir unterstützen Sie bei der Feststellung des Ausmaßes, der Protokollierung und Beweissicherung, der Einleitung rechtlicher Maßnahmen wie Meldung an die Aufsichtsbehörden/Betroffenen oder Erstattung von Strafanzeigen sowie bei der rechtskonformen Kommunikation nach außen.

So unterstützen wir Sie, wenn es zu einem Cyberangriff gekommen sein sollte:

IT-Sicherheitstechnik
in Kooperation mit spezialisierten IT-Sicherheitsunternehmen

- Wiederherstellung von Prozesssicherheit
- Wiederherstellung von ggf. kompromittierten Daten
- Beweissicherung
- Verhinderung zukünftiger Angriffsrisiken

Kommunikation
in Kooperation mit spezialisierten Kommunikationsagenturen

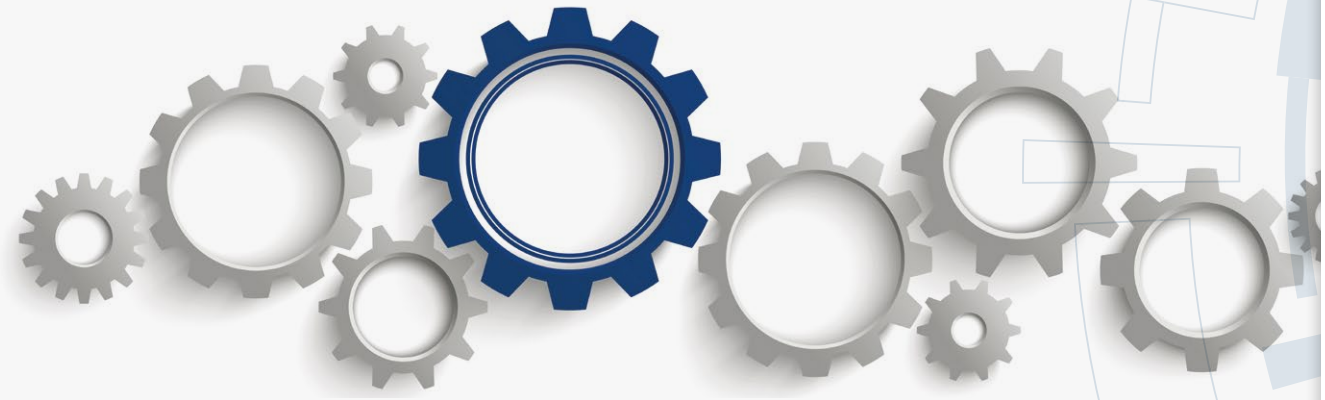
- Unterstützung bei Kommunikationsmaßnahmen nach außen
- Herstellung von One-Voice-Policy im Unternehmen

Recht

- Kommunikation mit den Aufsichtsbehörden (Art. 33 DSGVO)
- Rechtssichere Vorbereitung von Kommunikationsmaßnahmen
- Abwehr von Haftungsszenarien und etwaige Regressmaßnahmen gegen Dritte
- Geltendmachung von Ansprüchen gegenüber Dienstleistern
- Arbeitsrechtliche Begleitung im Falle von Fehlverhalten von Mitarbeitern
- Begleitung von Ermittlungsbehörden im Interesse des Unternehmens

REFERENZEN

Wir unterstützen Sie im Bereich Cybersicherheit



Heuking Kühn Lüer Wojtek verfügt über eine langjährige Expertise im Bereich Cyber Security. Zwölf Rechtsanwälte aus unterschiedlichen Praxisgruppen haben sich auf den Bereich spezialisiert. Unsere Experten arbeiten seit Jahren eng mit spezialisierten IT-Forensikern, gerichtlich vereidigten IT-Sachverständigen und IT-Security-Beratern zusammen.

Darüber hinaus verfügen unsere Anwälte über enge Kontakte zu Unternehmen aus der Versicherungswirtschaft, die neuartige Produkte wie „Cyber-Policen" entwickeln, um die technisch nur schwer abzusichernden Restrisiken durch einen adäquaten Versicherungsschutz abzufedern.

Die Task Force Cyber Security ist Teil der Praxisgruppe IP, Media & Technology, in der 60 Anwälte in den Bereichen Gewerblicher Rechtsschutz, Medien und Technologie beraten.

www.heuking.de

Unsere Erfahrungen im Bereich IT-Sicherheitsrecht (Auszug):

- Erstellung eines umfangreichen Gutachtens zu relevanten Akteuren der IT-Sicherheitsarchitektur Deutschlands für das Bundesamt für Sicherheit in der Informationstechnologie (BSI)
- Beratung im Rahmen des Streits von Versicherungsgeber und Versicherungsnehmer über die Möglichkeit der Inanspruchnahme einer „Cyber-Police" nach einem Hacking
- Erstellung von IT-Sicherheit-Policies
- Erstellung von Vertragsbedingungen für Penetration-Tests
- Erstellung eines Gutachtens über die Möglichkeit der Untersuchung der Cybersicherheit der Produkte von Wettbewerbern
- Umfangreiche Beratung zur IT-Sicherheit im Zusammenhang mit Art 32 DSGVO
- Beratung von KRITIS-Betreiber zu verschiedenen Rechtsfragen

CHECKLISTE

Ist mein Unternehmen angemessen vor Cyberangriffen geschützt?

Die Prüfung folgender Checkliste gibt Ihnen eine erste Indikation, ob in Ihrem Unternehmen ein angemessener Schutz vor Cyberangriffen besteht:

- ✓ Sicherstellung der Einspielung von Patches von Hardware und Software unverzüglich nach deren Erscheinen
- ✓ Risikoklassifizierung von Systemen, Software und Betriebssystemen und Tracking von Incidents
- ✓ Standardmäßige Ausmusterung von Systemen, die mit Software und Betriebssystemen arbeiten, die nicht mehr mit aktuellen Sicherheitsupdates versorgt werden
- ✓ Implementierung einer gemanagten Antivirenlösung für sämtliche Clients und Server
- ✓ Einsatz eines dynamisch tagesaktuell befüllten reputationsbasierten IP-Filtern auf der Firewall
- ✓ Einsatz von rechtlich zulässiger Überwachungssoftware zum Aufspüren von auffälligem Verhalten
- ✓ Vorhandensein einer Passwortrichtlinie, deren Einhaltung automatisiert gewährleistet wird, mit besonderen Anforderungen für und an Administratoren
- ✓ Aktivierung sämtlicher Log-Quellen und detaillierte Protokollierung von Systemaktivitäten
- ✓ Einsatz von Verschlüsselungstechnik für Speichermedien und Endgeräte (Clients, mobile Geräte)
- ✓ Vorhandensein von Vorgaben für das Verhalten bei Cyberattacken
- ✓ Schulung von Mitarbeitern auf das Thema IT-Sicherheit – Detektieren von Gefährdungen und der Umgang mit diesen sowie das Verhalten bei Cyberangriffen