

H&K

Ratgeber

Erstellt für die

Warum Sie für Hacker ein leichtes Ziel sind

Ein Leitfaden für den Handwerk-Betrieb 4.0

Wie die richtigen Mechanismen Ihren Betrieb, Ihre Daten und Ihre Kundendaten vor Cyber-Angriffen aus dem Web schützen können und was Sie tun können, wenn es zum Angriff gekommen ist.

HAGEN & KRUSE
VERSICHERUNGSMAKLER SEIT 1901

Mit diesem Hagen & Kruse Ratgeber erfahren Sie, wie Sie Ihren Betrieb im digitalen Zeitalter sicher führen.

Wir zeigen Ihnen in 6 Schritten, wie Sie Ihren Handwerk-Betrieb systematisch vor den Gefahren der Digitalisierung schützen können.

Worum geht es hier?

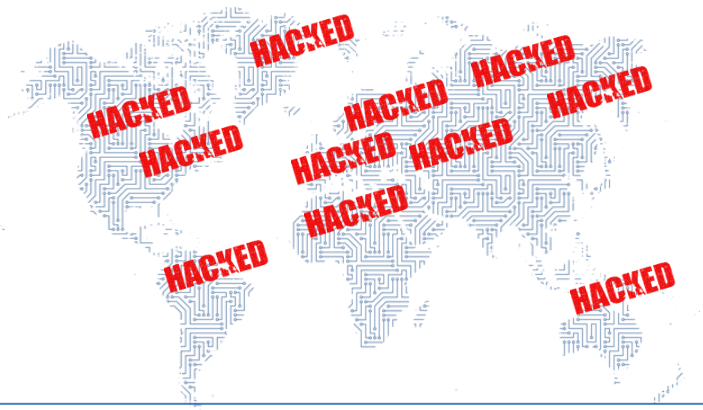
Nicht nur im produzierenden Gewerbe und Großbetrieben hängen heutzutage die meisten Geschäftsprozesse von einer verlässlich und fehlerfrei funktionierenden IT ab. Die Informations- und Kommunikationstechnik ist auch in kleinen und mittelständischen Betrieben Deutschlands wesentlicher Bestandteil des Geschäftes. Studien stützen diese Aussage: 37% der befragten Unternehmen geben an, dass ihnen ihre Computersysteme und Daten am wertvollsten seien (Vgl. KMU Studie 2018 der Gothaer Versicherung). Doch der tatsächlichen Bedrohung und möglicher Schadenshöhen durch Cyber-Angriffe ist sich der deutsche Mittelstand nur selten bewusst. Dies liegt nicht zuletzt daran, dass erfolgreiche Cyber-Angriffe häufig nicht oder nur sehr viel später bemerkt werden.

„Bisher ist ja auch nichts passiert."

Dabei waren allein in den vergangenen 2 Jahren 51% der Unternehmen von einem Cyber-Zwischenfall betroffen (Quelle: Bitkom). Häufig handelt es sich nicht um gezielte Angriffe, sondern breit gestreute Attacken (z.B. „Wanna Cry"). Die Entwicklung zeigt zudem, dass Anzahl, Komplexität und Professionalität der Angriffe zunehmen. Dennoch ist die Einstellung „Bisher ist ja auch nichts passiert" weit verbreitet. Werden bestehende Sicherheitskonzepte nicht kontinuierlich und adäquat an die gestiegene Bedrohungslage aus dem digitalen Umfeld angepasst, kann dies zu ernsthaften Problemen führen. Erschwerend kommt hinzu, dass die Anzahl der Bedrohungen stetig zunimmt, womit auch die Wahrscheinlichkeit, dass ein Betrieb - und sei er noch so klein - von einem Cyber-Angriff betroffen ist, drastisch ansteigt. Derzeit sind 700 Mio Schädlinge bekannt. Doch die findigen Hacker sind den Security-Herstellern immer einen Schritt voraus und finden einen Weg, bisher funktionierende Schutzmechanismen zu umgehen. Je nach Digitalisierungsgrad des eigenen Betriebes kann die Geschäftstätigkeit durch einen Cyber-Angriff komplett zum Erliegen kommen - mit allen Konsequenzen, die damit verbunden sind: Auftragsverlust, Reputationsrückgang, Umsatzeinbußen und Gewinnverlust bis hin zur Existenzbedrohung. Cyber-Sicherheit sollte daher Chefsache sein – egal wie groß oder klein der Betrieb ist.

51% der deutschen Betriebe von Cyber-Attacken betroffen

700 Mio bekannte Schädlinge im Umlauf



Worum geht es hier?

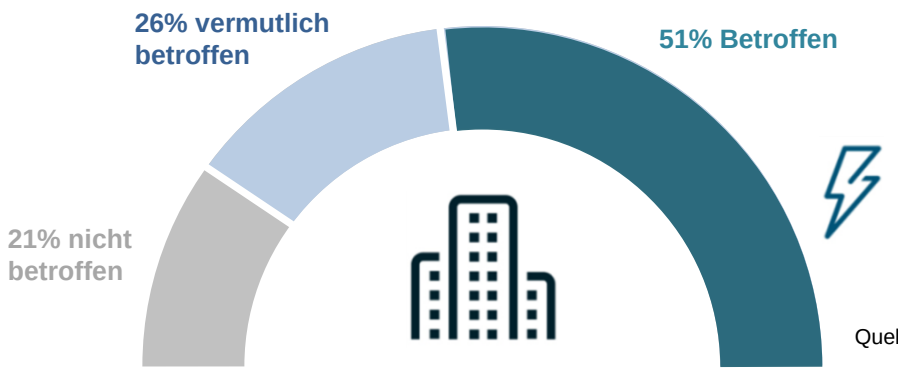
Bedrohungen aus dem Cyber-Raum sind real

Cyber-Schutz ist innerhalb der letzten Jahre zu einem wichtigen Thema in Unternehmen geworden. Dies liegt nicht zuletzt daran, dass die Cyber-Angriffe auf Behörden und Unternehmen immer präsenter in den Medien werden. Zahlreiche Medienberichte verdeutlichen wie real die Bedrohung aus dem Netz tatsächlich ist. Und dies sind nur die Fälle, die bekannt sind und auch publiziert werden. Die Dunkelziffer dürfte noch weitaus höher liegen, da Cyber-Angriffe häufig noch unbemerkt bleiben. Um diesen wirksam zu begegnen, sind funktionierende Schutzsysteme erforderlich. Die rasante Entwicklung der Angriffsszenarien verdeutlicht aber auch, dass es keinen 100%-igen Schutz geben kann.

100%-iger Schutz existiert nicht

Die Anzahl, Komplexität und Professionalität der Angriffe nimmt stetig zu. Die voranschreitende Entwicklung des IoT (Internet of Things) und im mobilen Datenverkehr ermöglichen weitere Angriffspunkte für Cyber-Kriminalität. Aus diesem Grund sollten Unternehmen sich vor Angriffen wappnen.

Wie viele sind betroffen?



Quelle: Bitkom

Im Folgenden wird die aktuelle Lage in Deutschland aufgezeigt. Im Nachgang möchten wir Ihnen Mittel an die Hand geben, um die aktuelle Bedrohungslage einzuschätzen und aufzeigen, welche Maßnahmen ergriffen werden sollten, um den Schutz zu erhöhen und damit eine umfassende Cyber-Strategie zu entwickeln. Des Weiteren zeigen wir Ihnen auf, welche Lösungsansätze am Markt vorhanden sind, um für den Fall der Fälle gewappnet zu sein: eine nicht rechtzeitig erkannte Cyber-Attacke auf den eigenen Betrieb.

Ausgangslage

Deutschland ist weltweit am stärksten bedroht

Gemessen am Schadenumfang des BIP wird Deutschland durch Cybercrime stärker geschädigt als jedes andere Land

Deutschland	1,6 %
Niederlande	1,5 %
USA	0,64 %
Norwegen	0,64 %
China	0,63 %



Quelle: Center for Strategic and International Studies (CSIS)

50 Milliarden EURO
so hoch ist der Schaden für die gesamte deutsche Wirtschaft – pro Jahr



Quelle: Bitkom

51% aller Unternehmen betroffen

In Deutschland wurden in den vergangenen 2 Jahren 51% aller Unternehmen Opfer von Datendiebstahl, Digitaler Wirtschaftsspionage oder Sabotage

Quelle: Bitkom

Schutzschild nur ungenügend



60% der deutschen Unternehmen befinden ihren digitalen Schutz für ausreichend.

100% nutzen immerhin Virenscanner, Firewalls und einen Passwortschutz. 80% schützen ihre Netzwerkverbindung mittels Verschlüsselung. Daten auf Festplatten o.a. Datenträgern werden von 45% verschlüsselt und nur 40% verschlüsseln auch ihren E-Mail-Verkehr.

Quelle: Bitkom

39% besitzen keine Digitalstrategie

Hiervon sind vor allem Unternehmen mit weniger als 100 Mitarbeitern betroffen



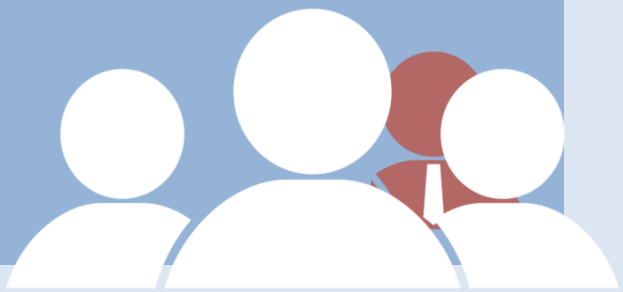
Quelle: Bitkom

Ausgangslage

Wer sind die Täter?

Ein Vorurteil hält sich hartnäckig: die weitläufige Meinung glaubt, die Hacker sitzen in Russland oder China. Dabei sind Hacker oftmals direkt nebenan.

60% ehemalige Mitarbeiter
16% konkurrierende Unternehmen
14% organisierte Kriminalität
13% Kunden
12% Hobby-Hacker
6% ausländische Nachrichtendienste
6% eigene derzeitige Mitarbeiter



Quelle: Bitkom Research

49%
verfügen über ein Notfallmanagement für den Ernstfall

52%
schulen ihre Mitarbeiter oder führen Sicherheitsprüfungen von Bewerbern durch

Quelle: Bitkom

Die Angst ist berechtigt

VIER VON FÜNF UNTERNEHMEN HABEN ANGST vor Cybercrime – dem Missbrauch eines schützenwerten Gutes



Quelle: KPMG, 2016

MOST WANTED

Diebstahl von IT- oder Telekommunikationsgeräten	42 %
Diebstahl von elektronischen Dokumenten	35 %
Sabotage von Betriebsabläufen	33 %
Social Engineering	33 %
Ausspähen von elektronischer Kommunikation	29 %
Abhören von Besprechungen oder Telefonaten	17 %

Quelle: Bitkom Research

Den Hackern auf der Spur

Die besten Schutzsysteme haben den Anspruch, innerhalb von 24 Stunden die Angriffe nicht nur zu entdecken, sondern auch vor ihnen zu schützen. Dabei hilft die heuristische Analyse der Angreifer



Ausgangslage

Cybererpressung

So hoch sind die Forderungen der Erpresser im Durchschnitt:

7.000 Euro

Weltweit beläuft sich die Schadensumme durch Cyberkriminalität pro Jahr auf mehr als:

400.000.000.000 Euro

Quelle: Center für Strategic and International Studies (CSIS)

Je später erkannt, umso höher die Kosten

Die Kosten eines Cyberangriffs **steigen um 44%,** wenn dieser erst nach einer Woche statt innerhalb des ersten Tages entdeckt wird.

Quelle: Kaspersky Lab

Was folgt?

Konsequenzen für die betroffenen Unternehmen

Teure Rechtsstreitigkeiten	34 %
Imageschäden	34 %
Umsatzeinbußen	32 %
Patentrechtsverletzungen	30 %
Ausfall, Diebstahl oder Schädigung von Informationssystemen	27 %
Erpressung mit gestohlenen oder verschlüsselten Daten	30 %



Quelle: Bitkom Research

KEINER IST SICHER

92% der mittelständischen Unternehmen sind betroffen von digitaler Spionage, Sabotage oder Datendiebstahl

92%

Quelle: Bitkom

Denken Sie digital

Fatales Vorurteil: je digitaler ein Unternehmen arbeitet, umso anfälliger ist es für Cyberkriminalität. Diese These wird jedoch widerlegt. Je vertrauter Unternehmen mit der digitalen Welt umgehen, desto selbstverständlicher werden hohe Sicherheitsstandards und effektiver Schutz gegen Cyberangriffe

Quelle: GDV

GRÖßTE GEFAHR Welche Risiken werden am meisten gefürchtet?

44%	40%	39%
Cyberangriffe	Betriebsunterbrechungen	Marktentwicklungen



Quelle: Allianz Global Corporate & Specialty

Typische Angriffsszenarien

Top 5 Attacken

Hacker arbeiten rund um die Uhr daran, Ihre Sicherheitslücken ausfindig zu machen



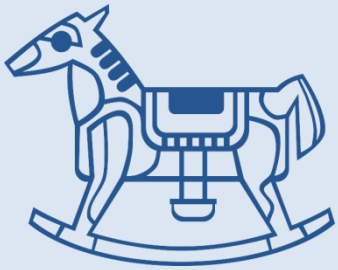
Computerviren
Sie werden häufig durch Datenfreigaben, E-Mail-Anhänge und Web-Downloads in Umlauf gebracht

Computerwürmer
Verbreiten sich in Netzwerkinfrastrukturen ohne menschliches Zutun.



SPAM oder auch Adware
Zur Verbreitung von Werbung genutzt, sind diese mit finanziellen Vorteilen für den Angreifer verbunden. Sie führen dazu, dass der User bei Befall mit Pop-ups und weiteren Werbebannern bombardiert wird.

SPAM



Trojaner
Sie sind speziell dafür entwickelt, um sensible Daten in Netzwerken aufzuspüren und abzugreifen. Meist übernehmen sie die Kontrolle über das IT-System und öffnen dem Angreifer eine Hintertür, durch welche er auch später noch Zugriff auf das System erhalten kann.

Spyware
Mit ihr werden Webbrowser infiziert, was dazu führt, dass diese nicht mehr nutzbar sind. Sie erfasst dann unbemerkt das Nutzungs- und Verhaltensmuster des Users.



Ihre Pflichten

Schutzpflicht

Die EU-Datenschutzgrundverordnung (EU-DSGVO) schreibt vor, dass sämtliche personenbezogenen Daten eines Schutzes bedürfen.



Personenbezogene Daten
(Art. 4 EU-DSGVO)
Alle Informationen, die sich auf eine betroffene Person beziehen.
(…) Darunter fallen z.B.:

- Name
- Adressen
- Telefonnummern
- Fotos
- Geschlecht
- Größe
- Haarfarbe
- Ausweisnummer
- …

- Gesundheit
- Rasse/Ethnie
- Genetische und biometrische Daten
- Sexualleben
- Politische Meinungen
- Gewerkschaftszugehörigkeit
- Religiöse oder philosophische Überzeugungen

Informationspflicht



Aus der Datenschutzgrundverordnung leiten sich zudem Pflichten ab, die Sie zu erfüllen haben, sofern es zu einem Datendiebstahl kommt

Nach Art. 33 und Art. 34 DSGVO müssen Unternehmen, deren sensible Daten gestohlen wurden, unverzüglich und „möglichst binnen 72 Stunden“ **Aufsichtsbehörden und Betroffene** informieren.

72 Std

Nach Art. 82 DSGVO hat jeder Betroffene das Recht auf **Schadenersatz**. Daraus leitet sich auch das Recht auf eine **Rechtsberatung** ab – Unabhängig vom jeweiligen konkreten Verschulden des Unternehmens.

§ §

Und wenn es zum Cyberangriff kommt…

…dann drohen hohe Kosten!

Kosten für IT-Forensik
IT-forensische Untersuchungen dienen der Aufklärung von Cyberangriffen und anderen IT-Vorfällen durch Analyse der in den beteiligten IT-Systemen hinterlassenen Datenspuren.
IT-Forensik-Experten: Tagessatz durchschnittlich 2.500 EUR (abhängig von Leistungen und Vorfall)

Anspruchsbefriedigung & -abwehr
Haftpflichtansprüche aufgrund von Datenrechtsverletzungen (z.B. nach BDSG), Vertragsstrafen wegen Verletzung von Geheimhaltungspflichten und/oder Datenschutzvereinbarungen. Zwingende Fragestellungen nach Datenschutz, der Haftung für Dritte und gegenüber Mitarbeitern, Kunden und auch Informationspflichten müssen geprüft werden.
Sensible Datensätze: 152 EUR je Datensatz ***(Ponemon-Studie 2015)***

Daten- & Systemwiederherstellung
Bei einer Beeinträchtigung eines Systems ist das Ziel die Herstellung eines sicheren Zustands des Systems sowie die Wiederherstellung der betroffenen Daten auf einen Systemstand vor dem Ausfall bzw. Angriff.
IT-Experten interne Kosten: Tagessatz 500 - 1.000 EUR

Betriebsunterbrechung
Bei einer Betriebsbeeinträchtigung sind die kritischen Prozesse und Anwendungen für die Nutzer der IT-Systeme oder für die auf sie angewiesenen Betriebsabläufe nur noch eingeschränkt verfügbar
Bestimmung der Kosten durch Digitalisierungsgrad des Betriebes und historische Daten (Betriebsgewinn + fortlaufende Kosten)

Kosten für Sicherheitsverbesserungen
Ein Cyber-Schadensfall in einer Organisation erfordert meist eine direkt anschließende Verbesserung der vorhandenen Infra- und Prozessstrukturen
Schwachstellenanalyse, Adressierung und Behebung von Schwachstellen, Umsetzung und Lösungsmöglichkeiten

Informations- und PR-Kosten
Die in vielen Jahrzehnten aufgebaute Reputation eines Unternehmens als immaterieller Vermögenswert
Kosten für Information von Dateninhabern (u.a. Anzeigenschaltung, Portokosten, Call-Center-Kosten etc.) PR- und Öffentlichkeitsarbeit

+ Rechtsanwaltskosten
Stundensätze von bis zu **500 EUR**

6 Schritte zum Schutz

Was tun?

Keine lückenhafte Systemschutz-Lösung

Greifen Sie auf führenden Security-Hersteller zurück und führen Sie regelmäßig Sicherheitsupdates durch, sobald diese angeboten werden.

Achten Sie darauf, mehrschichtige Schutzmechanismen zu installieren

EXEMPLARISCH:

Einfallswege	vor der Ausführung	während der Ausführung
Web Control	Live-Schutz	Exploit Prevention
Device Control	Web Security	Host Intrusion Prevention
App Control	Signaturen	Anti-Hacker
Firewall	Deep Learning	Schutz vor Ransomware
	Heuristiken	Speicher-Scan
	Skript-Analyse	Schutz von Passwörtern
	Download Reputation	Botnet-Traffic-Erkennung



Quelle: Sophos

Mitarbeiterschulung

Regelmäßige Schulungen und die Sensibilisierung der Mitarbeiter sind ein wichtiger Teil des eigenen Schutzsystems.

Einen 100%igen Schutz vor Angriffen kann kein Security-Hersteller bieten. Hier sind die Unternehmen gefragt auch selbst aktiv zu werden



Präsenzschulungen | Workshops | Webinare | Inhouse-Schulungen

Fallstudien | E-Learning | Tests | Online-Schulungen | Vorträge

Datenschutz-Trainings | Handouts | Aushänge | Hinweise im Intranet

6 Schritte zum Schutz

Was tun?

Regelmäßige Backups

Backups können im Falle einer Verschlüsselung schwerwiegende Folgen vermeiden.

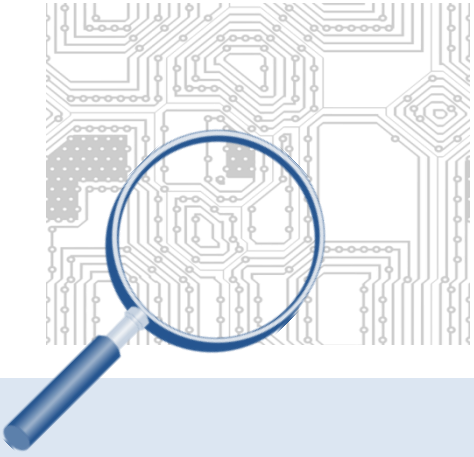
Führen Sie daher regelmäßige und möglichst engmaschige Backups durch, um jederzeit auf Ihre Unternehmensdaten zugreifen zu können.



IT-Infrastruktur auf Schwachstellen kontrollieren

Den Überblick über die eigene IT-Struktur zu behalten, ist oft nicht einfach. Prüfen Sie regelmäßig, ob und welche Risiken bestehen und beheben Sie diese.

Ebenso ist es von Bedeutung, den Umfang der eigenen Daten und deren Wichtigkeit zu kennen. Zugriffsrechte müssen geregelt und überwacht werden.



Machen Sie es zu einem Management-Thema

Die Unternehmensleitung sollte unmittelbar miteinbezogen werden und das Thema „Cyber-Security“ zur Chef-Sache werden.

Eine umfassende Cyber-Sicherheitsstrategie sollte Ziel Ihrer Bemühungen sein. Diese besteht nicht ausschließlich aus reiner Technologie, sondern auch aus Notfallplänen.

6 Schritte zum Schutz

Lösungen am Markt, um im Fall der Fälle gewappnet zu sein

Cyber-Versicherung

Eine Reihe von Versicherern bietet mittlerweile eine sog. Cyber-Police an. Worauf Sie dabei achten sollten und welche Elemente wesentlicher Bestandteil dieser Policen sind, zeigen wir Ihnen auf.



Assistance & Prävention

Assistance

- **24-Stunden-Notfallhotline**
  24/7/365 Erreichbarkeit
- **Krisenberatung**
  Cyber-Krisenplan für den Notfall
- **Hochqualifizierte IT-Dienstleister &-Krisenexperten**
  Unterstützung durch IT-Experten, PR-Berater, Datenschutzanwälte

Eigen-schaden

- **Risiko- und Schwachstellen-Analyse**
  Analyse der Gefährdungslage mit Maßnahmenplan
- **Datenwiederherstellung**
  Wiederherstellung des IT-Systems und der Daten
- **Betriebsunterbrechung**
  Übernahme der fortlaufenden Kosten

Dritt-ansprüche

- **Cyber-Haftpflicht**
  Befriedigung Ansprüche Dritter bei Cyber-Schäden

Fazit

Auf den Punkt gebracht



Unser H&K Ratgeber soll einen Beitrag zum allgemeinen Verständnis zu Cyber-Risiken leisten. Die folgenden Schlagworte sollten Sie für sich mitnehmen:

- Hohe Bedrohungslage im digitalen Umfeld
- Steigende Wahrscheinlichkeit eines Cyber-Angriffs
- Keine 100%-ige Sicherheit vor Cyber-Angriffen
- Datenschutz zwingend erforderlich (EU-DSGVO und BDSG)
- Vielseitige Risiken: Einschränkung des Geschäftsbetriebes, Auftragsverluste, Reputationsschäden, Umsatzeinbußen, Gewinnverluste, Existenzbedrohung
- Hohe Kosten im Schadensfall
- Digitalisierungsstrategie ein Must Have und Chef-Sache
- Umfangreicher Systemschutz durch IT-Lösungen und Mitarbeiterschulungen erforderlich
- Absicherung des Risikos durch eine Cyber-Police

Bei weiteren Fragen zu dem Thema stehen wir bei Hagen & Kruse Ihnen gerne zur Verfügung:

Jörg Enders (Geschäftsführender Gesellschafter)
Tel. 040/30 96 98-17
Jörg Will (Geschäftsführender Gesellschafter)
Tel. 040/30 96 98-23

Hagen & Kruse GmbH & Co. KG
Meßberg 1 • 20095 Hamburg
info@hagenundkruse.de
www.hagenundkruse.de