1 Aktuelle Informationen – Cyber-Security

Themen dieser Ausgabe:

- Schäden durch Angriffe
- Angriffsziele und Auswirkungen
- Schutz und Sicherheit
- Cyber-Security-Check
- Scope, Gegenstand und Beurteilung
- Vorgehensweise, Methoden, Ziele

Ausgabe Nr. 1/2021 (Januar)

Sehr geehrte Mandantin,
sehr geehrter Mandant,

nachfolgend haben wir in dieser Ausgabe aktuelle Informationen zur Cybersicherheit zusammengestellt.

Cybersicherheit 2021

Schäden in Millionenhöhe

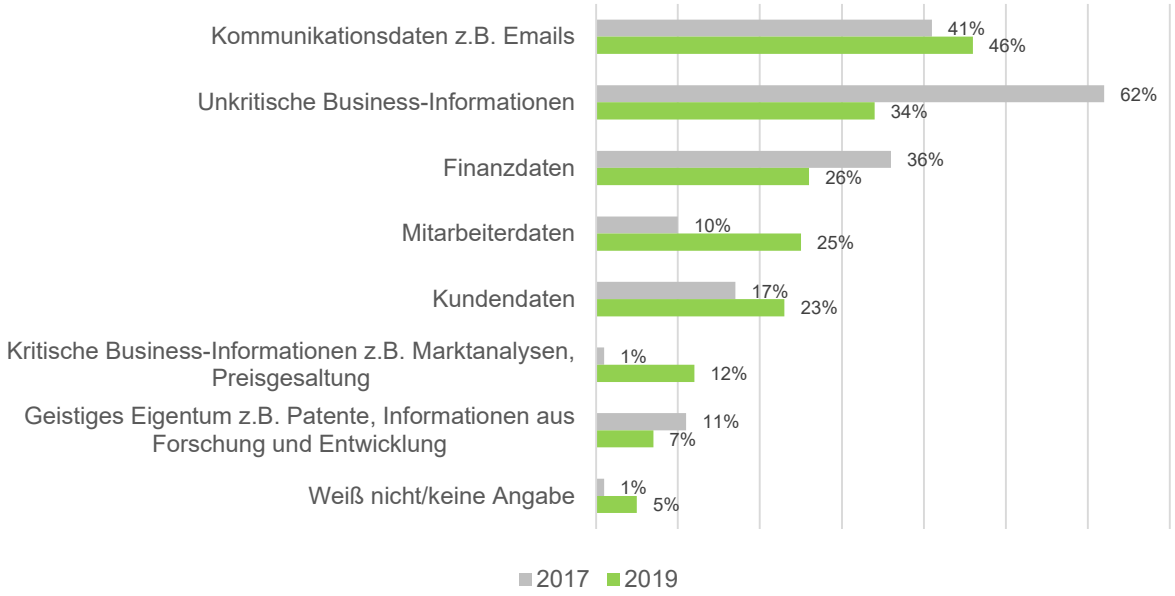
Cybersicherheit, Cyber-Angriffe oder Cyber-Kriminalität sind im Jahr 2021 längst keine unbekannten Schlagwörter mehr. Nahezu täglich berichtet die Presse über Datendiebstahl, Verschlüsselungstrojaner oder DDoS-Attacken bei großen, renommierten Unternehmen. Die Zahl der Angriffe und das Ausmaß des Schadens steigen stetig, sodass sich die Frage stellt, wer bzw. welche Institution sich hinter diesen Angriffen verbirgt. Häufig werden die Angriffe von gut organisierten Netzwerken durchgeführt, die mit ihren Werkzeugen in der Lage sind, auch in große, gut geschützte Firmennetzwerke einzudringen. Der Schaden kann je nach Ausgangslage und Angriff in die Millionen gehen. Die Chance die Angreifer zu finden, ist dagegen verschwindend gering. Dieser Trend hat sich durch die Corona-Krise noch verstärkt.

Angriffsziele und Auswirkungen

Doch was sind die eigentlichen Ziele der Angriffe? Laut des DsiN Praxisreports Mittelstand 2020 meldeten fast 46 Prozent der befragten Unternehmen in den vergangenen Monaten Cyberangriffe auf

ihr Unternehmen. Bei großen Konzernen liegt der Wert bei fast 70 Prozent[1].

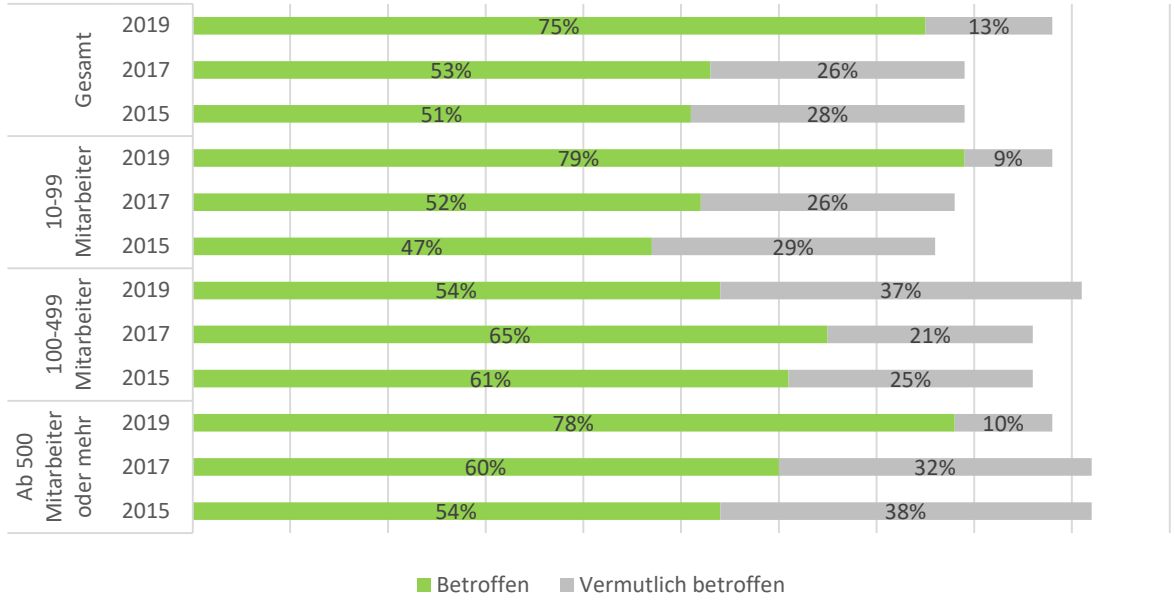
nachträglich kaum festzustellen ist, welcher Schaden tatsächlich entstanden ist.



Für diese Daten interessieren sich die Datendiebe (eigene Darstellung nach Bitkom)

Die Auswirkungen der Angriffe können von einzelnen ausgefallenen Rechnern bis hin zu kompletten Produktionsausfällen durch verschlüsselte Unternehmensnetzwerke reichen. Einen Schaden zu beziffern, fällt in diesen Fällen oft schwer, da teilweise

Neben finanziellen Einbußen kann der Verlust von Kundendaten oder Unternehmens-Know-How die Folge sein. In Zeiten der Corona-Pandemie haben solche Angriffe für einige Unternehmen oftmals existenzielle Folgen.



Betroffene Unternehmen nach Betriebsgrößenklasse (eigene Darstellung nach Bitkom)

[1] DsIN Praxisreport Mittelstand 2020 – Studie von Deutschland sicher im Netz e.V.

Betroffen sein kann faktisch jedes Unternehmen. Schlussfolgernd lässt sich feststellen, dass sowohl die Unternehmensgröße als auch die Branche wenig Einfluss darauf haben, ob das Unternehmen Ziel eines Cyberangriffs wird oder nicht. Die Einstellung „Bis heute ist uns ja auch nichts passiert“ sollte daher zwingend hinterfragt werden.

Schutz und Sicherheit

Die enormen Schäden und der drastische Anstieg der Angriffe vermitteln oftmals das Bild, dass Unternehmen diesen Gefahren schutzlos ausgesetzt sind. Das Risiko Opfer eines potenziellen Angriffs zu werden, besteht definitiv und kann in keinem Fall vollständig ausgeschlossen werden. Das Schadensausmaß und die Eintrittswahrscheinlichkeit hingegen kann durch das Unternehmen selbst maßgeblich beeinflusst werden.

Um die Sicherheit zu erhöhen, sind gerade in kleinen mittelständischen Unternehmen oftmals grundlegende Basismaßnahmen ausreichend, um ein bestehendes signifikantes Risiko zu reduzieren.

Voraussetzung ist ein angemessenes Bewusstsein für die IT und den damit verbundenen Risiken für die Organisation. Nur wer sich dem Risiko bewusst ist, kann auch gezielt geeignete und angemessene Maßnahmen ergreifen.

Aufgrund der zunehmenden Komplexität von IT-gestützten Geschäftsprozessen sollte bei einer Bewertung ein IT-Spezialist hinzugezogen werden. Hierfür hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den sog. Cyber-Security-Check etabliert.

Cyber-Security-Check

Ein Cyber-Security-Check ist ein hilfreicher Baustein für Unternehmen, um objektiv festzustellen, welche Stärken und Schwächen innerhalb der IT vorhanden sind. Der Cyber-Security-Check wurde von Experten der Allianz für Cyber-Sicherheit, welche sich aus Experten des BSI und der BITKOM e.V. zusammensetzt, ins Leben gerufen.

Ziel ist es, jedem Unternehmen die Möglichkeit zu geben seine IT-Sicherheit signifikant zu erhöhen. Dies erfolgt durch Hinzunahme von Experten mit einer Personenzertifizierung, die mit einer objektiven Bewertung und hilfreichen Handlungsempfehlungen zur Seite stehen.

Geeignete Berater sind meist als Certified Information Systems Auditor oder als Cyber Security Practitioner tätig.

Scope, Gegenstand der Beurteilung

Der Scope, also der Beurteilungsgegenstand eines Cyber-Security-Checks ist abhängig von der jeweiligen Organisation. Hierbei können verschiedene regulatorische Regelungen als auch Basismaßnahmen des BSI zugrunde gelegt werden.

Um mit Ihnen ein individuelles Prüfprogramm zusammenstellen zu können, führen wir vor jedem Cyber-Security-Check ein Vorgespräch, um ein gemeinsames Verständnis für den Prüfungsgegenstand zu erzielen. Auf dieser Basis kann anschließend eine Beauftragung erfolgen. Entscheidend für uns ist, gemeinsam mit Ihnen die relevanten Prüffelder zu bestimmen.

Durchführung des Cyber-Security-Checks

Die Durchführung erfolgt in sechs Schritten:

1. *Beauftragung*

Voraussetzung für die Durchführung eines Cyber-Security-Checks ist eine schriftliche Beauftragung durch die Organisation.

2. *Risikoeinschätzung*

Noch vor der Vor-Ort-Beurteilung führen wir mit Ihnen eine Risikoeinschätzung durch. Hierbei wird mittels Schadenshöhe und Eintrittswahrscheinlichkeit eine Risikokennzahl ermittelt. Darauf basierend können wir die Beurteilungstiefe sowie die Wahl der Stichproben bei der Durchführung risikoorientiert bestimmen.

3. *Dokumentensichtung*

Die Dokumentensichtung beinhaltet eine grobe Sichtung der zur Verfügung gestellten Unterlagen. Hierbei werden beispielsweise IT-Rahmenkonzepte, eine Aufstellung kritischer IT-gestützter Geschäftsprozesse sowie das Sicherheitskonzept der Gesellschaft herangezogen. Sollten diese Dokumente nicht bereitstellt werden können, kann dieser Schritt auch durch Interviews mit den Verantwortlichen erfolgen.

4. *Zeitliche und inhaltliche Planung*

Auf Basis der in Schritt 1-3 gewonnenen Erkenntnisse stimmen wir die zeitliche und inhaltliche Planung mit Ihnen ab. Hierbei planen wir selbstverständlich ausreichende Pufferzeiten ein, um einen reibungslosen Ablauf gewährleisten zu können.

5. *Vor-Ort-Beurteilung*

Unsere Vor-Ort-Beurteilung beginnen wir mit einem kurzen Kickoff-Gespräch, um den genauen zeitlichen Ablauf mit den jeweiligen Ansprechpartnern festzulegen. Im Rahmen unserer Vor-Ort-Beurteilung führen wir Interviews mit den Verantwortlichen. Auf Basis von ausgewählten Stichproben überzeugen wir uns von den implementierten Kontrollen. Sollten wir im Rahmen der Durchführung schwerwiegende Sicherheitsmängel feststellen, werden wir Sie umgehend darüber informieren. Während der noch anhaltenden Corona-Pandemie führen wir die Vor-Ort-Beurteilung in Form von Online-Meetings durch. Dabei können wir uns auch virtuell von den Gegebenheiten überzeugen.

6. *Berichterstellung*

Unsere Ergebnisse werden wir im Anschluss an die Vor-Ort-Beurteilung schriftlich festhalten und Ihnen in Form eines Berichts zur Verfügung stellen. Neben den Ergebnissen enthält jeder Bericht eine Ausführung des jeweiligen Handlungsbedarfs. Dabei geben wir Ihnen als unabhängige Berater umfassende Praxistipps für die Umsetzung.

Weiterführende Informationen erläutern wir Ihnen gerne in einem gemeinsamen Online-Meeting! Wir freuen uns auf Ihre Rückmeldungen!

Kontakt

RFS IT GmbH
Depotstraße 5 1/2
86199 Augsburg

Telefon: 0821 40879393
E-Mail: info@rfs-it.de

Widersprechen

Wir möchten Sie ausdrücklich darauf hinweisen, dass Sie der Verwendung Ihrer E-Mail-Adresse jederzeit widersprechen können. Weiterführende Hinweise zum Datenschutz finden Sie auf unserer Homepage www.rfs-it.de

RFS IT GmbH
Depotstraße 5 1/2
86199 Augsburg

Telefon: +49 821 40879393
E-Mail: info@rfs-it.de
Internet: www.rfs-it.de

Sitz: 45133 Essen, Am Alfredusbad 8
Registergericht Essen, Reg-Nr. HRB 28543
USt-IdNr. DE 314393389

Geschäftsführung:
Andreas Schneider