Dr. Geisler, Dr. Franke & Kollegen
Dr. Geisler, Dr. Franke Rechtsanwälte Partnerschaft mbB

AKTUELLE INFORMATIONEN

Für Sie zusammengefasst...

www.rae-geisler-franke.de

Cyberkriminalität

Welche Gefahren drohen durch Cyberangriffe, wie schützen Sie Ihr Unternehmen und welche Vorteile bietet eine Cyberversicherung?

Inhaltsverzeichnis

Dr. Geisler, Dr. Franke · Rechtsanwälte Partnerschaft mbB · Am Zwinger 2-4 · 33602 Bielefeld · Tel.: 0521 / 55 75 19 0 · Fax: 0521 / 55 75 19 16

A. Einleitung

Cyberangriffe gehören aktuell zu den größten Geschäftsrisiken von Unternehmen und haben allein im Jahr 2020/2021 einen Schaden in dreistelliger Milliardenhöhe verursacht.

Trotz dieser immensen Schäden befassen sich viele Unternehmen nicht oder nicht ausreichend mit dieser Gefahr, vermutlich auch deshalb, weil es sich für die meisten um ein unbekanntes Terrain handelt. Aus diesem Grund wurde dieses Skript entwickelt. Es soll dem Unternehmer einen gut verständlichen (Kurz-) Überblick über dieses komplexe Thema geben und insbesondere aufzeigen, welche Gefahren konkret durch Cyberangriffe drohen, wie sich Unternehmen davor schützen können und welche Vorteile eine Cyberversicherung bietet. Dieses Skript wurde aus einem interdisziplinären Team bestehend aus Rechtsanwälten der Kanzlei Dr. Geisler, Dr. Franke Part. mbB, Versicherungsexperten der TOPLINE INSURANCE Broker, IT-Spezialisten der Perseus Technologies GmbH und Datenschutzexperten der SecData GmbH entwickelt. Dadurch wird die Erfahrung und das Wissen von Fachleuten aus den einschlägigen Kompetenzgebieten gebündelt, um so einen optimalen Nutzen für Sie zu gewährleisten.

B. Warum ist die Gefährdungslage zur Cyberkriminalität aktuell so hoch?

Herr Vakalis (*Head of Sales, Perseus*): Der Krieg zwischen Russland und der Ukraine hat die Lage noch einmal verschärft! In den vergangenen Wochen wurden vermehrt Versuche von Phishing-Angriffen gemeldet, die sich auf den aktuellen Konflikt beziehen. Beispielsweise werden täuschend echt wirkende E-Mails im Namen von Banken versendet. Die Verfasser geben vor, verifizieren zu wollen, ob alle Kundinnen und Kunden der Bank sich an die Sanktionen der EU gegenüber Russland halten. Sie werden aufgefordert, bis zu einem vorgegebenen Datum die persönlichen Daten zu bestätigen. Andernfalls wird mit der Schließung des Kontos gedroht. Die E-Mail enthält einen Link, der angeblich zur Website der Bank führt. Dahinter verbirgt sich allerdings eine gefälschte Website zum Abgreifen von Kundendaten. Das Ergebnis können ein leer geräumtes Bankkonto, die Installation von

Ransomware auf den Firmenrechnern oder die Veröffentlichung sensibler Daten im Darknet sein.

Tipp:

Klicken Sie keinesfalls auf die Links in solchen E-Mails. Gehen Sie mit einer gesunden Skepsis und Vorsicht heran und kontaktieren Sie Ihre Bank. Dort kann man Ihnen sagen, ob eine solche E-Mail tatsächlich versendet wurde - Banken versenden diese Art von Informationen oftmals in Papierform - und sind im Zweifelsfall dankbar über diese Art von Hinweisen.

Ebenfalls sind aktuell gefälschte Websites im Umlauf, die zu Spendenaktionen für die Unterstützung der ukrainischen Bevölkerung oder Geflüchteter aufrufen. Dabei werden laut Bundesamt für Sicherheit in der Informationstechnik (BSI) die potentiellen Opfer darum gebeten, Geld zu überweisen, das angeblich Menschen bei der Flucht aus umkämpften Städten und Gebieten in der Ukraine helfen soll. Allerdings kommt das Geld nicht dort an, wo es benötigt wird.

Tipp:

Auch hier gilt: Vermeiden Sie es, auf den Link in der E-Mail zu klicken. Wenn Sie dennoch mit einer Spende helfen möchten, tun Sie dies direkt über die Website einer als seriös bekannten Hilfsorganisation.

Doch auch abgesehen von der aktuellen Situation ist die Gefahrenlage aufgrund ihrer Dynamik äußerst kritisch. Ein gutes Beispiel aus der jüngsten Vergangenheit ist das Aufdecken der Sicherheitslücke Log4Shell in der weltweit genutzten Java-Bibliothek Log4j. Die Ausnutzung dieser Schwachstelle ermöglichte es Angreifern, ferngesteuert und ohne Authentifizierung in die Systeme potentieller Opfer zu gelangen und beispielsweise Schadsoftware zu installieren, die Kontrolle des Systems zu übernehmen oder sensible Daten zu stehlen.

Innerhalb kürzester Zeit wurden Patches für die Schwachstelle veröffentlicht, gleichzeitig tauchten aber immer wieder neue Angriffsmuster von Cyberkriminellen auf. Kriminelle Hacker und Cybersicherheits-Profis lieferten sich sozusagen ein Kopf-an-Kopf-Rennen.

C. Sind Fitnessstudios auch von dieser Gefährdungslage betroffen?

Herr Vakalis (*Head of Sales, Perseus*): Ja! Jedes Unternehmen, unabhängig von seiner Größe oder der Branche kann in das Visier von Cyberkriminellen geraten. Mittlerweile stellt sich nicht mehr die Frage, ob ein Unternehmen Cyberkriminellen zum Opfer fällt, sondern wann.

Dabei sind Fitnessstudios besonders attraktive Ziele, da sie aufgrund eines breiten Kundenstamms viele personenbezogene Daten verarbeiten, beispielsweise Namen, Geburtsdaten, Anschriften und Bankverbindungsdaten ihrer Kundinnen und Kunden.

D. Kann ein Studio trotz Auslagerung von Daten an eine Cloud betroffen sein?

Herr Vakalis (*Head of Sales, Perseus*): Mit der Nutzung einer Cloud zur Datenspeicherung sinkt die Wahrscheinlichkeit, dass Cyberkriminelle an die Daten gelangen. Einen Cyberangriff, bei dem es zum Betriebsausfall und zu Lösegeldforderungen kommt, ist dadurch allerdings nicht in Gänze ausgeschlossen. Daher ist es für jedes Unternehmen von essentieller Bedeutung, eine eigene Cybersicherheitsstrategie zu verfolgen und diese auch langfristig umzusetzen.

E. Was sollten Studiobetreiber aktuell unternehmen, um ihre IT-Sicherheit zu verbessern?

Herr Vakalis (*Head of Sales, Perseus*): Cybersicherheit ist ein Thema, mit dem Unternehmen sich dauerhaft und umfassend beschäftigen sollten. Grundsätzlich sollte das Bewusstsein für die Angreifbarkeit vorhanden sein: Es kann jede und jeden von uns treffen.

Zur Verbesserung der IT-Sicherheit zählen einerseits technische Maßnahmen wie Firewalls und Antiviren-Programme. Genauso wichtig ist es auf der anderen Seite, den Faktor Mensch zu berücksichtigen. 70 % aller erfolgreichen Cyberangriffe werden durch einen unbedachten Klick auf einen böswilligen Link oder den versehentlichen Download von Schadprogrammen verursacht. Dies kann verhindert werden, indem alle Mitarbeitenden eines Fitnessstudios die entsprechende Sensibilisierung gegenüber dem Thema Cybersicherheit erfahren. Dieses beinhaltet beispielsweise Schulungen zu Cyberrisiken und Datenschutz. Darüber hinaus sollten alle Mitarbeitenden wissen, wie sie sich im Falle eines Cyberangriffs zu verhalten haben, nämlich ähnlich wie im Brandfall. Für einen nachhaltigen Erfolg der Cybersicherheitsstrategie müssen solche Themen von der Studioleitung forciert, dauerhaft in die Kommunikation eingebunden und vorgelebt werden.

F. Nehmen die Schadensfälle innerhalb der Cyberversicherung aktuell zu?

Herr Schumann (*Managing Director, Topline Insurance Broker*): Über die letzten Jahren haben die Schadensfälle in der Versicherungsbranche zur Cyberversicherung extrem zugenommen. Auch die aktuelle Kriegssituation treibt diese Entwicklung leider weiter an. Dabei kommt es weniger zu gezielten Cyberattacken auf deutsche mittelständige Unternehmen, sondern vielmehr handelt es sich hierbei um Kollateralschäden. Cyber-Risiken haben sich mittlerweile zum bedrohlichsten Unternehmensrisiko etabliert und der Abschluss einer Versicherung hiergegen ist zum absoluten Standard geworden.

G. Mit welchen Schäden muss ein Fitnessstudio dabei rechnen?

Herr Schumann (*Managing Director, Topline Insurance Broker*): Der Schadendurchschnitt innerhalb der Cyberversicherung in der Versicherungsbranche variiert je nach Befragung sehr stark, liegt aber einheitlich deutlich über 25.000,00 EUR. Festzuhalten bleibt jedoch, dass ein einzelner Schadensfall häufig im 6-stelligen Bereich liegt.

Betroffenen steht ggf. ein Schadensersatzanspruch nach § 82 Abs. 1 DSGVO gegenüber dem Studio zu. Deshalb besteht die Gefahr eines besonders großen Schadens, da im Regelfall eine große Menge an personenbezogenen Daten vom Studio gespeichert und verarbeitet

werden. Wegen dieses riesigen Datenumfangs können allein die Drittschäden betroffener Kunden des Studios schnell in die Höhe schießen.

H. Welche Kosten übernimmt eine Cyberversicherung konkret im Schadensfall?

Herr Simons (*Managing Director, Topline Insurance Broker*): Die wesentlichen versicherten Kosten lassen sich in 4 Punkte unterscheiden:

- Eigenschäden

  - Wiederherstellung eigener Daten und Programme
  - Schäden aus Erpressung/Bedrohung

- Betriebsunterbrechung

  - Ausfall vom Rohertrag

- Fremdschäden

  - Forderungen der Payment-Card-Industry (Kreditkartenschäden)
  - Wiederherstellung fremder Daten und Programme
  - Ansprüche aus Persönlichkeitsrechtsverletzung

- Service-/Kosten

  - Schadenfeststellung und –behebung
  - PR-Beratung/Reputation nach Schadenfall
  - Rechtsanwaltskosten

I. Gibt es eine spezielle Cyberversicherung für die Fitnessbranche?

Herr Simons (*Managing Director, Topline Insurance Broker*): Ja. Wie auch bei anderen Spezialprodukten, die von TOPLINE INSURANCE Broker exklusiv für die Fitnessbranche entwickelt wurden, wird der Markt kontinuierlich geprüft, umso auf die aktuellen Absicherungsbedürfnisse der Studiobetreiber einzugehen. Gemeinsam mit dem Produktpartner, der SIGNAL IDUNA, wurde kürzlich die Cyberversicherung für die Fitnessbranche überarbeitet.

Konkret wurden die Beiträge für die Fitnessstudios deutlich gesenkt und die Risikofragen im Antrag reduziert. Der Beitrag richtet sich nach dem Umsatz des Fitnessstudios und beginnt bereits bei einer Jahresprämie von 540,00 EUR. Im Schadensfall steht ein interdisziplinäres Netzwerk den Kunden zur Verfügung.

Auf die aktuelle Sicherheitslücke Log4 wurde bereits eingegangen. Für Bestandskunden der TOPLINE INSURANCE Broker wurde bereits ein Service eingerichtet, um zu überprüfen, ob das Unternehmen von der Sicherheitslücke bedroht ist. Dieser Service wird nun erweitert für alle Empfänger dieses Newsletters. Die Überprüfung kann unter dem Link :

https://www.cysmo.de/business-suite/log4shell/signaliduna.html

durchgeführt werden. Die anfallenden Kosten für diesen Sicherheitscheck übernimmt die SIGNAL IDUNA vollständig.

J. Fazit:

Rüsten Sie sich für die kommenden Herausforderungen in einer immer digitaler werdenden Welt, indem Sie sich und Ihr Unternehmen bestmöglich gegen die Gefahren schützen, die von stetig wachsender Cyberkriminalität ausgehen. Dies vor allem durch die dargestellten technischen Schutzmechanismen, die Aufklärung der Mitarbeiter und eine Absicherung durch eine Versicherung. Ohne das Bestehen einer Cyberversicherung kann ein Cyberangriff schnell einen wirtschaftlichen Schaden verursachen, der nicht allein vom Studio abgefangen werden kann.

Im Schadensfall braucht es zudem auch rechtliche Unterstützung. Falls personenbezogene Daten betroffen sind, ist eine korrekte und zügige Vorgehensweise gegenüber den zuständigen Datenschutzbehörden angezeigt. Zudem stellen sich zahlreiche weitere rechtlichen Herausforderungen, für die Iie im Schadensfall „keinen Kopf haben“.

Unser interdisziplinäres Team hilft, kontaktieren Sie uns.

Dr. Geisler, Dr. Franke & Kollegen
Dr. Geisler, Dr. Franke Rechtsanwälte Partnerschaft mbB

Rechtsanwälte

Dr. Geisler, Dr. Franke Rechtsanwälte Partnerschaft mbB

Am Zwinger 2-4 33602 Bielefeld

Tel. 0521 / 557519-0

Fax: 0 521 / 55 75 19 16

E-Mail: info@kgfk.de

Homepage: www.kgfk.de

TOPLINE INSURANCE BROKER

Schumann & Simons GmbH & Co. OHG

Wiesenau 2

60323 Frankfurt a.M.

Telefon: 069-82364903

E-Mail: info@topline-insurance.de

Homepage: https://topline-insurance.de/

SecData

SecData GmbH

Am Zwinger 2-4

33602 Bielefeld

Telefon: 0521/557519-333

Fax: 0521/557519-16

E-Mail: info@secdata.gmbh

Homepage: https://www.secdata.gmbh/datenschutz-vom-profi.html

Perseus Technologies GmbH

Hardenbergstraße 32

10623 Berlin

Telefon: +49 (30) 959998080

E-Mail: info@perseus.de

Homepage: www.perseus.de