CHECKLISTE

INFORMATIONSSICHERHEIT UND SCHUTZ VOR CYBERANGRIFFEN WÄHREND EINER PANDEMIE

Diese Informationsbroschüre bietet Unternehmen hilfreiche Hinweise zum Schutz vor Cyberangriffen, die während einer Pandemie bei Aufrechterhaltung der Geschäftstätigkeit berücksichtigt werden sollten. Ein fortlaufender Geschäftsbetrieb erfordert in Zeiten, in denen in hohem Maße auf Telearbeit, veränderte Zeitpläne und weitere Methoden zur Fortführung des Kundenkontakts zurückgegriffen wird, besondere Maßnahmen. Diese weichen möglicherweise stark von dem normalen Geschäftsbetrieb ab. Es sind jedoch gerade diese veränderten Regelungen im Zusammenspiel mit weiteren außergewöhnlichen Verhältnissen während einer Pandemie, die Unternehmen mit erheblichen Cyberrisiken konfrontieren. Unternehmen, die sich der Cyberbedrohung bewusst sind und dementsprechend risikogerechte Schutzvorkehrungen treffen, können die von Cyberangriffen ausgehende Gefahr erheblich minimieren.

Cyberkriminelle setzen weiterhin auf Social-Engineering- und Phishing-Methoden, um sich zielgerichteten unbefugten Zugriff auf Unternehmensnetzwerke zu verschaffen. So ist Phishing auch weiterhin die am häufigsten angewendete Taktik derartiger Cyberangriffe, um Ihre Systeme mit Schad- und Ransomware zu infizieren.

Berücksichtigen Sie unsere Empfehlungen in Verbindung mit Ihren bewährten internen Richtlinien, um Cyberangriffen auch während einer Pandemie mit Resilienz zu begegnen:

SOCIAL-ENGINEERING

Vielzählige Unternehmen mussten ihre Geschäftstätigkeiten im Zuge der Pandemie unterbrechen und sehen sich in erhöhtem Maße mit Cyberbedrohungen konfrontiert, die oftmals von Social-Engineering-Methoden ausgehen. Schützen Sie sich und achten Sie besonders auf E-Mails, Telefonanrufe oder Online-Benachrichtigungen mit überzeugenden Inhalten, wie z. B.:

- ☐ Dringende Angelegenheiten, die zum „Abgleich“ Ihre persönlichen Daten erfordern
- ☐ Dringende Hilfegesuche
- ☐ Benachrichtigungen über hohe Gewinne (z. B im Rahmen eines Gewinnspiels oder eines Lotteriegewinns)
- ☐ E-Mails von Managern oder Kollegen, in denen um interne und vertrauliche Informationen gebeten wird

PHISHING

Cyberkriminelle versuchen sich oftmals unbefugten Zugriff auf Unternehmensnetzwerke zu verschaffen, indem sie Benutzer auf eine scheinbar seriöse Webseite locken, die jedoch von den Angreifern selbst gesteuert wird. Weitere Taktiken sind darüber hinaus beispielsweise das Anbieten von Stellen mit vielversprechendem Gehalt oder der Aufruf zum Spenden an vermeintliche von der Pandemie betroffene Unternehmen. Berücksichtigen Sie die folgenden Aspekte, um das von Phishing ausgehende Risiko zu minimieren:

- ☐ Öffnen Sie externe E-Mails oder Anhänge während Ihrer Telearbeitszeit ebenso vorsichtig und bedacht wie in Ihrem Büro.
- ☐ Greifen Sie ausschließlich auf Ihnen bekannte Webseiten zu, da diese nur geringe Angriffsflächen in Bezug auf das Platzieren von Schadsoftware bieten.
- ☐ Prüfen Sie stets den Absender der Ihnen zugehenden E-Mails.
- ☐ Gehen Sie im Zweifelsfall kein unnötiges Risiko ein. Benachrichtigen Sie die Informationssicherheitsverantwortlichen und/oder Ihren IT-Support.

Die aktuelle beispiellose Situation ist mit einem hohen Maße an Angst und Unsicherheit verbunden. Achten Sie dennoch darauf, keine Phishing-Nachrichten mit vermeintlichen Informationen zur Entwicklung der Pandemie zu öffnen.

Diese Broschüre dient nur zu Informationszwecken für FM Global-Kunden im Rahmen des Versicherungsverhältnisses. Aus ihrer Anwendung können keine Haftungsansprüche abgeleitet werden. Die Haftung von FM Global beschränkt sich ausschließlich auf den Inhalt der Versicherungspolicen.

FM Global

CHECKLISTE – SCHADENVERHÜTUNG WÄHREND EINER PANDEMIE

VIDEOKONFERENZEN

Hacker können auf diskrete Art und Weise vertrauliche Daten ausspionieren, die während geschäftlicher Besprechungen über Videokonferenzsoftware ausgetauscht werden. Oftmals werden sensible Daten in diesem Zusammenhang derart gefährdet, dass die Geschäftstätigkeit eines Unternehmens stark beeinträchtigt werden kann. Sofern möglich, sollten Sie die folgenden Schutzvorkehrungen in Erwägung ziehen:

- ☐ Deaktivieren Sie die Standardeinstellung, die es Besprechungsteilnehmern erlaubt, ihren Bildschirm ohne Freigabe durch den Organisator zu teilen.
- ☐ Aktivieren Sie einen Kennwortschutz, damit der Videokonferenz ausschließlich eingeladene Teilnehmer beitreten können.
- ☐ Geben Sie vor, dass der Besprechungsorganisator anwesend sein muss, damit das Meeting beginnen kann.
- ☐ Schließen Sie nicht benötigte Anwendungen und Dokumente, bevor Sie Ihren Bildschirm teilen, um eine unbeabsichtigte Offenlegung sensibler Informationen zu verhindern.
- ☐ Gewähren Sie ausschließlich Benutzern mit einer entsprechenden E-Mail-Domäne die Teilnahme an Ihrer Besprechung.

PATCHES

Sofern bekannte Schwachstellen innerhalb Ihrer Betriebssysteme und Anwendungen bestehen, werden Cyberkriminelle diese möglicherweise gezielt ausnutzen. Mehr und mehr Beschäftigte verwenden ihre Privatgeräte auch für den geschäftlichen Bereich oder im Rahmen von Telearbeit. Dementsprechend sollten diesbezüglich entsprechende Schutzvorkehrungen getroffen werden, um Unternehmensdaten zu schützen, auf die in diesem Zusammenhang zugegriffen wird oder die auf den Geräten gespeichert werden. Schützen Sie Ihre Geräte und Daten, indem Sie die folgenden Aspekte berücksichtigen:

- ☐ Aktualisieren Sie fortlaufend auf die jeweils aktuellste Version Ihres Betriebssystems und spielen Sie neu verfügbare Patches ein.
- ☐ Aktivieren Sie automatische Aktualisierungen und legen Sie diese, sofern möglich, standardmäßig fest.
- ☐ Überprüfen Sie, ob aktuelle Patches für Antivirus- und Antischadsoftware eingespielt sind und ob diese auf die neuste verfügbare Version aktualisiert wurden.
- ☐ Konsolidieren Sie gegebenenfalls die Softwareversionen Ihres privaten und geschäftlichen Geräts.
- ☐ Sichern Sie sämtliche Geräte, über die eine Verbindung zum Firmennetzwerk gestellt wird und die zur Ausführung Ihrer geschäftlichen Tätigkeiten verwendet werden.

HILFREICHE RESSOURCEN (AUF ENGLISCH)

Home-Office: So bereiten Sie Ihr Unternehmen und Ihre Mitarbeiter vor
https://www.ncsc.gov.uk/guidance/home-working

Sicheres Arbeiten über Ihr Heimnetzwerk
https://www.us-cert.gov/ncas/tips/ST15-002

Patches und Software-Aktualisierungen verstehen
https://www.us-cert.gov/ncas/tips/ST04-006

Schützen Ihres Computers am Arbeitsplatz
https://support.microsoft.com/de-de/help/4092059/windows-keep-your-computer-secure-at-work

HAFTUNGSAUSSCHLUSS FÜR EXTERNE LINKS

FM Global ist bemüht, korrekte, aktuelle und verlässliche Inhalte über die Bereitstellung von Links anzubieten; FM Global kann jedoch nicht für durch Dritte bereitgestellte Inhalte haftbar gemacht werden.

Weitere Exemplare dieser Broschüre und zusätzliche FM Global-Informationsmaterialien können Sie jederzeit online unter www.fmglobalcatalog.com bestellen. Selbstverständlich steht Ihnen auch unser Kundenbetreuungsteam gerne zur Verfügung:

- Gebührenfrei: (1)877 364 6726 (Kanada und USA, 08.00 bis 17.00 Uhr ET)
- Tel.: +49-(0)69-15406-140
- E-Mail:EngFrankfurtCustomerServiceDesk@fmglobal.com
- Fax: +49-(0)69-15406-137

P152550_20c_DEU © 2020 FM Global. (03/2020) Alle Rechte vorbehalten. fmglobal.de

FM Insurance Company Limited (Eintragungsnr. 755780, England), mit Sitz in Voyager Place, Maidenhead, Berkshire, SL6 2PJ. FM Insurance Company Limited ist genehmigt durch die Prudential Regulation Authority, geregelt durch die Financial Conduct Authority und die Prudential Regulation Authority.