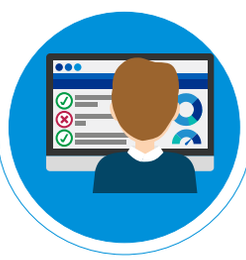
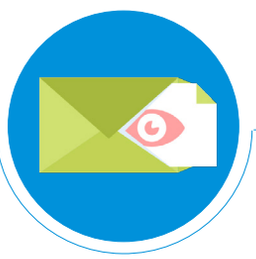
# Cyber-Sicherheit in Zeiten von COVID-19

**COVID-19 verändert unser Leben. Menschen sind beunruhigt, machen sich Sorgen und sehnen sich nach Informationen, Sicherheit und Unterstützung. Organisiertes Verbrechen macht sich diese Ängste zu eigen und nutzt sie aus. Damit sind Sie Ziel der Angreifer.**

Die Auswirkungen des Virus selbst und damit einhergehende Folgemaßnahmen stellen auch Unternehmen vor zahlreiche Herausforderungen. Eine dieser Herausforderungen ist die Sensibilisierung für neue Bedrohungsszenarien und die entschlossene Reaktion auf eine auf das Virus angepasste Bedrohungslage. Spear-Fishing-Kampagnen, gefälschte Webseiten (z. B. mit Weltkarten zur Virusverbreitung) und auch neue Fake President-Angriffe nehmen rasant zu. Neben der Vorbereitung auf diese Angriffsszenarien gehört die Sicherung der IT-Landschaft bei Zugriffen aus dem Homeoffice genauso dazu, wie die adäquate Reaktion, falls ein Angreifer erfolgreich gewesen sein sollte.



- Social-Engineering Angriffe nehmen zu
- Fake Webseiten geben vor, Informationen zum Virus (z. B. eine Weltkarte zur Verbreitung des Virus) bereitzustellen. Ziel ist das Absaugen von vertraulichen Daten und Verbreitung von Schadcode
- Anrufer geben vor zu helfen und verleiten zum Download von Schadsoftware



- COVID-19 bezogene Mails mit Schadsoftware als Anlage
- Ausführbarer Code in Word-Dateien löst den Download von Emotet oder Trickbot aus und verschlüsselt Ihre Systeme
- CEO Fraud/Fake President-Angriffe mit dem Vorwand, Geld im Ausland für die Bekämpfung des Virus zu benötigen

- Angreifer verschlüsseln mittels Ransomware in Not geratene Unternehmen und sogar Krankenhäuser mit dem Ziel, Geld zu erpressen
- Wichtig: Reaktionsmaßnahmen im Ernstfall, Krisenmanagement und IT-Forensik etablieren
- Wichtig: Cybersichere BCM-Prozesse und adäquate IT-Vorfallsreaktion adaptieren

### Sofortmaßnahmen:

- Erhöhen Sie die Sensibilität Ihrer Mitarbeiter bezüglich COVID-19 Phishing-Angriffen, z.B. Newsletter und Schulungen zu COVID-19 bezogenem Phishing
- Mindestanforderungen an einen „cybersicheren" Heimarbeitsplatz schaffen, z. B. VPN und 2-Faktor-Authentisierung („2FA")
- Haben Sie Transparenz über eingesetzte Software und Eigeninstallationen Ihrer Mitarbeiter
- Geben Sie Mitarbeitern, die Remote arbeiten, eine klare Richtlinie, wie eingesetzte Remote-Lösungen verwendet werden sollen/dürfen
- Verschlüsseln Sie Ihre Daten („at rest")
- Stellen Sie sicher, dass Sie flächendeckend sichere Passwörter für Remote-Zugänge einsetzen
- Stellen Sie eine Hotline oder Chats zur Sofortunterstützung bereit oder falls Mitarbeiter Auffälligkeiten (z. B. Phishing) melden möchten
- Deaktivieren von USB-Ports sofern möglich, um ungewollten Datenabfluss zu vermeiden
- Stellen Sie sicher, dass alle Laptops aktuelle Viren- und Firewall-Lösungen besitzen und halten Sie Signaturen auf aktuellem Stand
- Teilen Sie vertrauenswürdige Quellen mit Ihren Mitarbeitern


**Ihre Ansprechpartner**

**Michael Sauermann**
Partner, Head of Forensic Technology
T +49 30 2068-4624
msauermann@kpmg.com

**Christoph Beckmeyer**
Manager, Forensic Technology
T +49 30 2068-4126
cbeckmeyer@kpmg.com


**www.kpmg.de**

**www.kpmg.de/socialmedia**