AUFBAU EINER SICHEREN FERNARBEITSSTRUKTUR

Ein Drittel der IT-Entscheider räumt Datenschutzverletzungen[1] infolge von Fernarbeit ein. Doch wie können Sie gewährleisten, dass Ihre Firmendaten auch dann geschützt sind, wenn es keinen normalen Geschäftsbetrieb gibt?

01.

Schützen Sie Ihre Fernarbeits-Methoden

Die Wahrscheinlichkeit, sich einen Malware-Virus einzufangen, ist ihn privaten Netzwerk zuhause **3.5 mal höher** als im Firmennetzwerk[2]

Cybercriminelle **erkennen**, ob jemand grad privat im Netz agiert oder für die Firma arbeitet

Schützen Sie Ihre Mitarbeiter durch sichere **Fernarbeits-Methoden und verhindern Sie**, dass Sie Daten verlieren oder mit Ihren eigenen Dateien erpresst werden

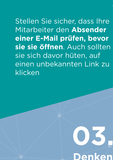
02.

Nehmen Sie sich vor allem vor Phishing-Angriffen in Acht

Bei Phishing-Mails ist das Thema Corona mittlerweile der häufigste **Köder**[3]

In Großbritannien stieg die Zahl der Betrugsfälle allein im Februar und März um über **400 %**[4], die Opfer verloren dabei mehr als 1,6 Millionen Pfund[5]

Stellen Sie sicher, dass Ihre Mitarbeiter den **Absender einer E-Mail prüfen, bevor sie sie öffnen**. Auch sollten sie sich davor hüten, auf einen unbekannten Link zu klicken



03.

Denken Sie an die Sicherheit privater Heimgeräte

Zuhause benutzen Ihre Mitarbeiter Ihren eigenen Drucker oder Scanner

Diese Geräte haben in der **Regel nicht die Standard-Sicherheitsfunktionen** wie die Systeme in Ihrem Firmennetzwerk

Über **25 %** aller Geräte nutzen Internetdienste[6], dadurch sind sie anfälliger für Angriffe

Um Ihre geschäftskritischen Daten zu schützen, sollten Sie bei Ihren Mitarbeitern sicherstellen, dass deren Netzwerk privat und nur über ein **sicheres**, nicht-voreingestelltes Kennwort zugänglich ist

04.

Und vertrauliche Papiere

Stellen Sie sicher, dass Ihre Mitarbeiter mit Unternehmenspapieren so gewissenhaft umgehen, als wären es ihre eigenen Kontoauszüge. **Vertrauliches muss auch außerhalb des Büros** entweder geschreddert oder geschützt aufbewahrt werden

05.

Die beste Methode ist die, nur eine einzige zu haben

Zuhause arbeiten **bedeutet nicht**, dass man in puncto Firmenrichtlinien fünfe gerade sein lässt

Erinnern Sie Ihr Team daran, nur Anwendungen, Netzwerke und Cloud-Lokalitäten zu nutzen, **die vom Unternehmen bereitgestellt werden**

Kostenlose Cloud- und Speichertools, die nicht von Ihnen überprüft wurden, **sind möglicherweise** unsicher

Jeder Angestellte, der mobil arbeitet, muss ein Bewusstsein dafür entwickeln, dass er auf seinem heimischen Sofa die gleichen Sicherheitsstandards einzuhalten hat wie im Firmenbüro.

Nehmen Sie **Kontakt mit Canon** auf, um zu erfahren, wie Sie in diesen turbulenten Zeiten nicht nur überleben, sondern auch florieren und wachsen.

Canon

See the bigger picture

1 https://www.techtarget.com/searchsecurity/news/252484597/Survey-finds-security-issues-with-remote-work
2 https://www.bitdefender.com/blog/hotforsecurity/cybercriminals-can-tell-if-you-are-at-home-or-at-work/
3 https://www.bitdefender.com/blog/hotforsecurity/phishing-remains-the-most-popular-cyber-threat-during-a-pandemic/
4 https://www.cybersecurityintelligence.com/blog/phishing-attacks-increase-during-coronavirus-pandemic-4-1-million-reported-5288.html
5 https://www.theguardian.com/business/2020/jun/29/fraud-victims-lose-record-£16m-during-coronavirus-pandemic
6 https://www.statista.com/statistics/271644/worldwide-free-and-paid-mobile-phone-apps/