CORONA

Homeoffice in Zeiten von CORONA

Wie Sie sich am besten vor Cyberrisiken schützen können!

IN AUSNAHMESITUATIONEN SIND BEDROHUNGEN AM HÄUFIGSTEN!!!
Sobald Geräte außerhalb der Netzwerkinfrastruktur eines Unternehmens installiert und mit neuen Netzwerken/ WLAN verbunden werden, erweitert sich die potenzielle Angriffsfläche, die rasch zum Türöffner für Cyberkriminelle wird.
Beziehen Sie Informationen rund um das Thema CORONAVIRUS ausschließlich aus vertrauenswürdigen und offiziellen Quellen.
Hacker benutzen CORONAVIRUS als Türöffner (Malware, Ransomware, Trojaner, ...)!

Das CORONAVIRUS wird bereits seit Ausbruch als Köder genutzt und tarnt sich hinter Datei-Namen zu Video-Informationen in Bezug auf aktuelle Entwicklungen oder Schutzmaßnahmen.

Damit sensible Daten geschützt bleiben beachten Sie folgendes:

1. Installation der neuesten Updates
2. Nutzung eines VPN-Zugangs für eine sichere Verbindung zum Unternehmensnetzwerk
3. Alle Unternehmensgeräte mit geeigneter Sicherheitssoftware schützen (bestenfalls mit der Funktion Löschung von Arbeitsdaten, sofern ein Gerät als verloren oder gestohlen gilt)
4. Verschlüsselung, starke Passwörter sowie 2 Faktor-Authentifizierung einrichten
5. Beschränken von Zugriffsrechten
6. Mitarbeitern Awareness kommunizieren
7. Keine Anhänge oder verdächtigen Links öffnen, die exklusive Neuigkeiten versprechen
8. Einrichten einer Sicherheitshotline für Ihre Mitarbeiter
9. Aufklärung der Mitarbeiter, die bis dato noch keine Homeoffice Erfahrung haben: Wie komme ich in ein Online-Meeting? Wo finde ich meine Dateien? Wie komme ich zu meiner Remote Sitzung?

Datenschutz & Homeoffice:
Auch rund um das Thema Datensicherheit müssen diverse Fragen geklärt werden:

Wird mit einem privaten oder dienstlichen Gerät gearbeitet? Erfüllen private Geräte dieselben technischen Sicherheitsstandards wie die Betrieblichen? Ist der Datentransfer gesichert und verschlüsselt? Wie erfolgt die Datenlöschung von Privatgeräten? Wer haftet, wenn man sich im privaten Netzwerk Schadsoftware einfängt?

Welche Unterlagen dürfen das Unternehmen überhaupt verlassen? Wie ist gesichert, dass die Dokumente nicht verloren gehen oder von Dritten eingesehen werden? Und was ist zu tun, wenn das doch passiert?

ARES
preventing
leaks

Cyber Security
Consulting | Operations | Education

Sowohl zu Cyberfragen als auch zu DSGVO-Fragen können Sie jederzeit gerne unsere Hotline kontaktieren!

ARES Hotline: 0800 0800 22
E-MAIL: emergency@ares-ci.com

Wir helfen Ihnen!
Bleiben Sie gesund und alles Gute für die nächsten Wochen!

ARES Cyber Intelligence GmbH
+43-676-3109332
Bauernstr. 9 | 4600 Wels | Austria

www.ares-ci.com