Wie kommen Cyber-Kriminelle ans Ziel?

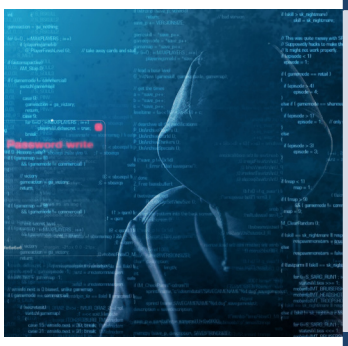
Home-Office

Durch den schnellen Umstieg vieler Unternehmen auf Home-Office-Konzepte steigt die Komplexität der Unternehmensnetzwerke. Sicherheitsmaßnahmen wachsen nicht im gleichen Tempo mit. Cyberangriffe werden dadurch überhaupt nicht oder erst sehr spät erkannt und das Schadenpotenzial erhöht sich.
Hinweis: Vielfach wird von den Mitarbeitern sogar private Hardware eingesetzt, auf die der Betrieb keinen Einfluss nehmen kann.

Veraltete Software

Aus Kostengründen nutzen viele kleine und mittelständische Betriebe oftmals ältere Programme oder Betriebssysteme. Für diese Software gibt es jedoch regelmäßig keine Sicherheitsupdates mehr. Damit wird ein erfolgreicher Cyberangriff umso wahrscheinlicher.

Darknet



Eine Untersuchung von 1.000 mittelständischen Betrieben hat ergeben, dass bei über der Hälfte dieser Firmen die E-Mail-Adressen von Mitarbeitern und deren Passwörter im Darknet zu finden waren. Diese Adressen reichen Cyber-Kriminellen bereits aus, um mittels Erpressungstrojanern – sogenannte Ransomware – einen Angriff auf das jeweilige Unternehmen zu starten. Die Attacken lassen sich leicht realisieren, da im Darknet die hierfür erforderliche Ransomware gleich mit erhältlich ist.

Ransomware

Insbesondere Ransomware-Zahlungen (Verschlüsselungen) und Datenerpressungen waren 2020 die häufigsten Methoden. Viele Kriminelle organisieren sich in Netzwerken, um Zugriff auf neue Technologien zu erhalten und diese für eigene Angriffszwecke zu nutzen. Das größte Risiko bei diesen Angriffen ist die automatische Verbreitung durch glaubwürdige E-Mails von infizierten Geräten bzw. dessen Kontoinhabern.

Die Continentale