David Klein
Dipl. Wirtschaftsprüfer
BSc in Betriebsökonomie
Partner TRETOR AG, Basel
Mitglied EXPERTsuisse
david.klein@tretor.ch

Gefährdung durch Cyberkriminelle

Tatort Home-Office

Die Corona-Pandemie hat den Trend zu dezentralem Arbeiten stark beschleunigt. Home-Office hat sich in weiten Bereichen etabliert. Sichere und zuverlässige IT-Umgebungen sind zu einem absoluten Must geworden.

Seit dem ersten Lockdown gilt: Wo immer möglich soll im Home-Office gearbeitet werden. Viele KMU haben quasi über Nacht reagiert und dezentrales Arbeiten ermöglicht. Allerdings waren nicht alle IT-Systeme darauf vorbereitet. So kam es vielerorts notgedrungen zum Kompromiss zwischen Aufrechterhaltung der Mitarbeiterproduktivität und angemessener IT-Sicherheit.

Die Cyberkriminellen reagierten umgehend auf die neue Normalität und folgten den Mitarbeitenden ins Home-Office. Bestehen IT-Sicherheitsmängel in den eigenen vier Wänden, wird diese offene Tür noch so gerne für schädliche Angriffe genutzt. Die steigende Zahl an Cyberangriffen auf KMU bestätigen die Entwicklung. Neben mangelhafter technischer Infrastruktur, stellen häufig die Mitarbeitenden selbst eine Schwachstelle im System dar.

Cyberrisiko: Das Problem sind die Mitarbeitenden

Treten EDV-Probleme in den eigenen vier Wänden auf, versuchen die Mitarbeitenden diese häufig alleine zu lösen. Fast immer handelt es sich dabei um eine Behelfslösung, bei der die IT-Sicherheitsstandards des Büros nicht eingehalten werden. Setzt der Mitarbeitende zu Hause sein privates Gerät ein, bestehen kaum Download-Restriktionen. Jegliche Internetseiten können aufgerufen und Software aller Art auf dem Gerät installiert werden. Eine zentrale Verwaltung und Nachvollzug der Datenflüsse durch das Unternehmen ist nicht mehr möglich.

Dadurch, dass man im Home-Office in der Regel alleine ist, fehlt der schnelle und informelle Austausch mit den Arbeitskollegen. Phishing-Email werden häufiger geöffnet und potentiell schädliche Software kann sich im Unternehmen verbreiten. Cyberkriminelle haben diese Tendenz erkannt und die meisten Angriffe auf IT-Systeme

erfolgen via Email. Und ausserdem befinden sich mobile Geräte nicht in geschützten Büroräumlichkeiten, können vergessen oder gestohlen werden und sie sind nur selten vor neugierige Blicken von Unbefugten gesichert.

Folgen für den Arbeitgeber

Für Unternehmen sind Cyberangriffe besonders schädigend. Häufig wird beim Cyberangriff auf ein IT-System unbemerkt sogenannte Ransomware installiert. Das ist eine Software, welche entweder Dateien oder den gesamten Computer verschlüsselt. Der Cyberkriminelle verschafft sich damit die Kontrolle über die betroffenen Daten und fordert ein Lösegeld. Solange das Lösegeld nicht bezahlt wird, bleiben die Daten verschlüsselt. Wenn sich das betroffene Gerät in einem Netzwerk befindet, beispielsweise in einem Unternehmen, kann sich die Schadsoftware auf das gesamte Netzwerk ausbreiten und alle Geräte darin verschlüsseln. So können Unternehmen oder sogar Krankenhäuser lahmgelegt werden.

Neben der Erpressung bzw. des finanziellen Schaden durch die Lösegeldforderung ergeben sich zahlreiche negativen Folgen für den Arbeitgeber aus einem solchen Angriff. Einerseits führt die Verschlüsselung meist zu einem Betriebsunterbruch, weil alle elektronisch unterstützten Geschäftsprozesse während der Sperrung nicht normal ablaufen können.Zudem können Cyberkriminelle Daten entwenden und möglicherweise trotz Freischaltung nach der Lösegeldzahlung weiterhin missbrauchen.

Zu guter Letzt dürfte der Betriebsunterbruch auch bei den Kunden nicht unbemerkt bleiben. Denn diese sind ebenfalls betroffen, sei es durch Lieferverzögerungen oder fehlenden Support. Je nach Branche kann eine solche Attacke zu massiven Reputationsschäden führen.

Vorbildfunktion der Vorgesetzten

Die Bereitschaft von KMU den Mitarbeitenden Home-Office zu ermöglichen ist erfreulich und zeugt von einem modernen Umgang mit neuen Arbeitsformen. Dies bedingt aber gleichzeitig eine zeitgemässe und den Risiken angepasste IT-Infrastruktur. Neben den Geschäftsprozessen ist also auch das interne Kontrollumfeld auf die digitale Welt auszurichten. Das Bewusstsein der Mitarbeiter in Zusammenhang mit den potentiellen IT-Risiken muss geschärft und vom Vorgesetzten vorgelebt werden.