Mandanteninfo: Betrugsversuche durch Cyberkriminalität

Sehr geehrte Damen und Herren,

in den letzten Wochen hören wir vermehrt Nachrichten über akute Fälle von Cyberkriminalität aus unserer Mandantschaft. Wir möchten Sie deshalb über dieses Thema informieren.

Jeder Unternehmer sollte seine Mitarbeiter und Kunden für dieses Thema sensibilisieren und Maßnahmen zur Abwehr solcher Angriffe ergreifen.

Bei diesen Fällen handelt es sich nicht um hochkomplexe Schadsoftware oder Firewall Angriffe, sondern häufig um vermeintlich „banalen“ Trickbetrug.

Hier zwei konkrete Beispiele aus unserer Mandantschaft:

Beispiel 1:

Die verantwortliche Mitarbeiterin im Rechnungswesen erhält E-Mails von der Absenderadresse des Geschäftsführers. Es wird eine Konversation aufgebaut, bei der die Art und Weise der Ansprache (duzen, Erwähnung von Kollegen) nicht auf einen fremden Dritten hinweisen. Nach einigen Fragen (Stand der Bankkonten, etc.) wird auf die dringende Überweisung über einen Betrag von 50.000 Euro für eine Rechnung an eine fremde Firma gedrängt. Die Mitarbeiterin führt die Überweisung aus.

Die an die Bank weitergegebene Überweisung kommt dem zuständigen Kundenbetreuer „auffällig“ vor. Durch seine Rückfrage bei dem Kunden kann die tatsächliche Überweisung verhindert werden. Ohne das „Eingreifen“ der Bank wäre der Betrag unwiderruflich den Betrügern gezahlt worden.

Beispiel 2:

Eine Sachbearbeiterin erhält einen Anruf von einem vermeintlichen Mitarbeiter der Microsoft Service Hotline. Der vermeintliche Microsoft Mitarbeiter berichtet von einer konkreten Sicherheitslücke in einem MS Office Programm. Er müsse sich kurz per „Teamviewer“ auf den Rechner der Mitarbeiterin aufschalten. Bereitwillig lässt die Mitarbeiterin dies zu. Der Kriminelle kann in aller Ruhe Daten abrufen und an den Einstellungen in der Software Veränderungen vornehmen. Auf diese Art und Weise hätte auch eine Schadsoftware installiert werden können, die den Betrieb zunächst handlungsunfähig macht.

Die o.g. Beispiele machen deutlich, dass Kriminelle versuchen, durch die geänderten Arbeitsweisen (Homeoffice, digitale Prozesse) mittelständische Unternehmen durch Trickbetrügerein zu bestehlen. Hierbei wird auch das Vertrauen in IT-Fachleute gezielt ausgenutzt.

Erste Maßnahmen zur Abwehr:

Grundsätzlich sollten alle Mitarbeiter kurzfristig für dieses Thema sensibilisiert werden.

Weiterhin hat in Unternehmen bei Zahlungen und Rechnungsfreigaben immer ein „Vier-Augen-Prinzip“ zu erfolgen. Dabei sollten im Rahmen der Freigabe keine externen Kommunikationswege wie z.B. E-Mail-Programme etc., auf die auch Dritte ohne größere Probleme zugreifen können, eingesetzt werden.

Mittelfristige Maßnahmen:

Die Prozesse der Rechnungsfreigabe und der Zahlungsfreigabe sollten grundsätzlich in regelmäßigen Abständen auf den Prüfstand gestellt werden. Hierbei sollte auch die Fluktuation von Mitarbeitern berücksichtigt werden (Bankvollmachten für bereits ausgeschiedene Mitarbeiter etc.). Darüber hinaus sollten die eigenen Mitarbeiter in regelmäßigen Abständen über die Risiken von Cyberangriffen informiert werden. Die Erfahrung zeigt, dass eine regelmäßige Sensibilisierung die Wachsamkeit erhöht.

Wir hoffen Ihnen mit dieser Information geholfen zu haben.

Bei Rückfragen stehen wir Ihnen gerne zur Verfügung.

Viele Grüße

Ihr Team von W&N