April 2022

Cybererpressungen: Sind Lösegeldzahlungen steuerlich absetzbar?

Eine neue Kriminalitätsart gewinnt an Bedeutung und auch die Anzahl der in diesem Zusammenhang angezeigten Straftaten steigt rapide. Es geht hierbei um Cybererpressungen oder anders ausgedrückt um Angriffe auf Computersysteme bzw. die gespeicherten Daten bei Behörden und Unternehmen. Die professionell organisierten Cyberkriminellen greifen nicht nur Großunternehmen an, sondern zunehmend sind auch kleine Firmen und Selbständige Ziel der Attacken. Dabei kommt den Kriminellen zugute, dass die Anzahl der Mitarbeiter im Homeoffice sich seit Beginn der Corona-Pandemie vervielfältigt hat. Die Verbindung zwischen den Geräten im Homeoffice und dem IT-System des Arbeitgebers ist häufig nicht so gut gegen das Eindringen durch Unberechtigte geschützt, wie das normale Netz am Unternehmensstandort. Auch die Sicherheit der Kommunikation der Mitarbeiter untereinander wird durch das Homeoffice beeinträchtigt.

Vorgehensweise der Angreifer

Das typische Vorgehen von Angreifern besteht in dem Versuch Schadsoftware (sog. Ransomware) in die Systeme des Unternehmens einzuschleusen. Dies geschieht häufig durch fingierte E-Mails, die dem Empfänger als geschäftsrelevant erscheinen. Die E-Mails enthalten manipulierte Anhänge mit Schadcode oder laden diesen aus dem Internet nach.

Ziel der Cyberangriffe ist die Verschlüsselung des Zugangs zu den Unternehmensdaten und damit verbunden die Erpressung von Lösegeld gegen die Freigabe der Daten. Die Ransomware beginnt die Verschlüsselung bei den ältesten Firmendaten, um möglichst lange unerkannt zu bleiben und nach Möglichkeit auch die täglichen Datensicherungen sukzessive unbrauchbar zu machen. Mittlerweile haben die Angreifer erkannt, dass die Drohkulisse effektiver sein kann, wenn die Daten entwendet werden, anstatt diese zu verschlüsseln. Vielfach wird auch damit gedroht, die Daten des Unternehmens (Lieferantendaten mit Bezugsbedingungen, Rabatten, Zahlungszielen und auf der anderen Seite Kundendaten ähnlicher Art sowie personenbezogenen Daten) zu veröffentlichen. Es ist daher nicht verwunderlich, wenn Unternehmen nach Abwägung der möglichen Folgen aus der Veröffentlichung oder der fehlenden Verbindung mit den Daten ihres gesamten geschäftlichen Umfeldes auf die Bedingungen der Angreifer eingehen und Lösegelder (engl. Ransom) zahlen. Diese Gelder werden fast immer in Kryptowährungen, meist in Bitcoins, verlangt. Die Zahlungen landen i.d.R. bei nicht identifizierbaren Personen / Organisationen.

Bisherige Rechtslage zur steuerlichen Behandlung von Lösegeldzahlungen

Für die betroffenen Unternehmen stellt sich sofort die Frage, ob diese Lösegeldzahlungen Betriebsausgaben sind oder nicht. Bei Lösegeldzahlungen für die Freilassung entführter Gewerbetreibender oder naher Angehöriger hat der Bundesfinanzhof (BFH) diese Frage in

seinem Urteil vom 30. Oktober 1980 (Az. IV R 27/77, BStBl. II 1981, 303) negativ entschieden. Als Grund führte das Gericht hierzu an, dass die Zahlungen erfolgten, um das Leben der entführten Gewerbetreibenden zu schützen und dass die Zahlungen damit nicht allein durch den Betrieb veranlasst wurden, sondern auch private Motive ausschlaggebend waren. Damit lagen hier gemischte Aufwendungen vor, die nach § 12 Abs. 1 S. 2 EStG vom Betriebsausgabenabzug ausgeschlossen sind.

Anders sieht die Rechtslage dagegen aus, wenn nur betriebliche Daten von der Erpressung betroffen sind. Wenn die Zahlung als solche nachweislich erbracht worden ist, liegen grundsätzlich Betriebsausgaben vor, weil eine betriebliche Veranlassung bestand. Allerdings sind nicht alle Betriebsausgaben abzugsfähig. In den hier besprochenen Fällen wird das Unternehmen i.d.R. nicht in der Lage sein, den Empfänger des Lösegeldes zu benennen. Nach § 160 Abs. 1 S. 1 AO muss der Steuerpflichtige auf Verlangen des Finanzamtes aber den endgültigen Empfänger von Zahlungen benennen. Da Cyberkriminelle wohl kaum unter ihrem richtigen Namen auftreten, dürfte dieses Verlangen eines Finanzamtes nicht zu erfüllen sein. Auf dem ersten Blick wäre dann nach § 160 Abs. 1 AO der Betriebsausgabenabzug gescheitert. Nach der bisher zu dieser Vorschrift ergangenen Rechtsprechung muss das Verlangen des Finanzamtes auf Benennung des Empfängers zumutbar sein. Dem Unternehmen muss es damit im Zeitpunkt der Zahlung zuzumuten sein, die Person oder die Personen zu benennen, die hinter dem kriminellen Angriff steckt/stecken und zwar mit Namen und Anschrift. Dies ist schlechterdings nicht möglich. Wenn das Benennungsverlangen aber unzumutbar ist, dann besteht auch für Zahlungen an unbekannte Personen das Recht auf den Betriebsausgabenabzug. Bereits in 1951 hat der BFH die These aufgestellt, dass die Gefährdung der wirtschaftlichen Existenz ein Grund ist, die Benennung zu verhindern. Das setzt allerdings voraus, dass den Unternehmer kein Verschulden daran trifft, dass er den Namen nicht nennen kann (Urteil vom 23. Februar 1951 – Az. IV R 81/50 S). Es bleibt daher zu hoffen, dass die Finanzverwaltung oder spätestens die Finanzgerichte den Begriff der „wirtschaftlichen Existenz" großzügig auslegen.

Lösegeldforderungen verhindern

Idealerweise sollten es Unternehmer gar nicht erst soweit kommen lassen, dass die wirtschaftliche Existenz durch einen Cyberangriff bedroht wird. Eine Investition in Cybersicherheit ist meist günstiger als die Zahlung von Lösegeld (mit ungewissem Ausgang) und zugleich eine akzeptierte Betriebsausgabe. Moderne, KI-basierte Schutzmaßnahmen können das Risiko eines erfolgreichen Angriffs verringern, in dem sie u.a. Clients bei ungewöhnlichem Verhalten vom Netzwerk isolieren. Die Schadsoftware kann nur dort Schaden anrichten, wo der Benutzer des korrumpierten PCs Berechtigungen hat. Auch ein Berechtigungskonzept nach dem Prinzip der minimalen Rechtevergabe hilft daher Risiken zu reduzieren.

Jürgen Dräger
Wirtschaftsprüfer, Steuerberater

Ingo Köhne
CEO IT-Consulting, CISA, CISM, PMP