Hamburg, April 2022

Cyber extortion: Are ransom payments tax deductible?

A new type of crime is gaining in importance and the number of crimes reported in this context is also rising rapidly. This involves cyber extortion or, in other words, attacks on computer systems or the stored data at public authorities and companies. The professionally organized cyber criminals are not only attacking large companies, but increasingly small companies and the self-employed are also being targeted. The criminals benefit from the fact that the number of home office employees has multiplied since the start of the Corona pandemic. The connection between the devices in the home office and the employer's IT system is often not as well protected against intrusion by unauthorized persons as the normal network at the company location. Communication among employees is also affected by the home office.

Attackers' approach

The typical approach of attackers is to attempt to infiltrate malware (so-called ransomware) into the company's systems. This is often done by means of fictitious e-mails that appear to the recipient to be relevant to the business. The e-mails contain manipulated attachments with malicious code or reload it from the Internet.

The goal of the cyberattacks is to encrypt access to the company's data and, in connection with this, to extort a ransom in exchange for the release of the data. The ransomware starts the encryption with the oldest company data in order to remain undetected for as long as possible and, if possible, also to successively render the daily data backups unusable. In the meantime, the attackers have realized that the threat can be more effective if the data is stolen instead of encrypting it. In many cases, threats are also made to publish the company's data (supplier data with purchase conditions, discounts, payment targets and, on the other hand, customer data of a similar nature as well as personal data). It is therefore not surprising when companies, after considering the possible consequences of publishing or not being connected to the data of their entire business environment, agree to the attackers' terms and pay ransom. These funds are almost always demanded in cryptocurrencies, usually bitcoins. The payments usually end up with unidentifiable individuals / organizations.

Previous legal situation regarding the tax treatment of ransom payments

For the companies concerned, the question immediately arises as to whether or not these ransom payments are business expenses. In the case of ransom payments for the release of kidnapped tradesmen or close relatives, the Federal Fiscal Court (Bundesfinanzhof, BFH) decided this question negatively in its ruling of October 30, 1980 (Case No. IV R 27/77, BStBl. II 1981, 303). The reason given by the court was that the payments were made in order to protect the life of the kidnapped tradesmen and that the payments were therefore not solely prompted by the business, but that private motives were also decisive. In this case, therefore, the expenses were mixed and are excluded from the deduction of business expenses under Section 12 (1) sentence 2 of the German Income Tax Act (EStG).

The legal situation is different, however, if only business data is affected by the extortion. If the payment can be proven to have been made as such, it is generally a business expense because there was a business reason for it. However, not all business expenses are deductible. In the cases discussed here, the company will generally not be in a position to name the recipient of the ransom. Pursuant to Section 160 (1) Sentence 1 AO, the taxpayer must name the final recipient of payments at the request of the tax office. Since cybercriminals are unlikely to act under their real names, this request by a tax office should not be possible. At first glance, the deduction of operating expenses would then have failed according to Section 160 (1) AO. According to the case law to date on this provision, the request of the tax office to name the recipient must be reasonable. Thus, at the time of payment, it must be reasonable for the company to name the person or persons behind the criminal attack, including name and address. This is simply not possible. However, if the request for naming is unreasonable, then the right to the business expense deduction also exists for payments to unknown persons. As early as 1951, the Federal Fiscal Court (Bundesfinanzhof, BFH) established the thesis that the endangerment of the economic existence is a reason to prevent the designation. However, this presupposes that the entrepreneur is not at fault for not being able to name the person (ruling of February 23, 1951 - file no. IV R 81/50 S). It is therefore to be hoped that the tax authorities or, at the latest, the tax courts will interpret the term "economic existence" generously.

Preventing ransom demands

Ideally, business owners should avoid having their economic existence threatened by a cyberattack in the first place. Investing in cybersecurity is usually cheaper than paying a ransom (with an uncertain outcome), while also being an accepted business expense. Modern, AI-based protection measures can reduce the risk of a successful attack by, among other things, isolating clients from the network in the event of unusual behavior. The malware can only cause damage where the user of the corrupted PC has permissions. An authorization concept based on the principle of minimal rights assignment therefore also helps to reduce risks.

Author

Jürgen Dräger
Auditor, tax advisor

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