17.07.2023

What is a “Denial of Service” attack?

Over the past few weeks, we kept reading about attacks on companies or public institutions left unable to continue their normal operations. Quite often, a so-called DDoS attack is behind this.

Time and again, Internet criminals manage to paralyse whole corporations or administration departments. Increasingly, this is achieved using ransomware, i.e. a ransom or encryption Trojan. Another method frequently used of late is the Distributed Denial of Service attack.

A DDoS attack is a distributed attack on a company’s website or server. Many devices (mostly those which are part of a bot net) bombard their target with innumerable requests during such an attack. The result: Due to overload, the attacked website or server relents to the pressure and is no longer available, or only to a limited degree. Blackmail attempts are frequently the reason behind DDoS attacks. If no payment is made, criminals will threaten to repeat the attacks.

Unfortunately, there is no 100% sure-fire way of protecting yourself against Denial of Service attacks. Companies can use auditing services to detect DDoS attacks at an early stage and block them. Due to the distributed nature of such attacks, this is only ever possible to a certain degree. Reducing the target area usually helps to reduce any effects of such an attack – you can find more information on this in our article “Denial-of-Service attack (https://www.ebas.ch/en/denial-of-service-attack/) “ and in our “Tips for SME (https://www.ebas.ch/sme) “ category.