3 FRAGEN AN… JENS-PHILIPP JUNG, GESCHÄFTSFÜHRER LINK11

1. Herr Jung, DDos-Attacken zählen zu den ältesten Formen von Cybercrime. Wie gefährlich und aktuell ist diese Angriffsform?

Mit Distributed Denial of Service (DDoS)-Attacken legen Angreifer schon seit über 15 Jahren Ziele lahm. Doch was sich früher vor allem gegen Gaming-Server oder E-Commerce-Websites richtete, hat inzwischen alle Branchen und Unternehmen jeder Größenordnung erreicht. Die Zahl der Angriffe wächst dabei besorgniserregend. Das Link11 Security Operation Center (LSOC) verzeichnet jeden Tag über 100 solcher Attacken auf Ziele in Deutschland, Österreich und der Schweiz. Immer häufiger misst das LSOC bei den Attacken Spitzenbandbreiten, die weit über 50 bis 60 Gbps hinausgehen und die 100-Gbps-Marke überschreiten.

Die Angreifer sind außerdem sehr einfallsreich darin, neue Infrastrukturen für die Umsetzung von DDoS-Attacken zu schaffen. Sie haben Zugriff auf eine ITK-Infrastruktur mit wachsender Bandbreite und einer steigenden Anzahl internetfähiger Geräte wie Home Router, Smartphones aber auch Cloud-Server, die mit falschen Kreditkarteninformationen angemietet werden. Nach unserer Einschätzung werden DDoS-Attacken immer noch gefährlicher.

2. Welche Schäden können erfolgreiche DDos-Attacken verursachen?

Jeden Tag haben Unternehmen, Websites und staatliche Institutionen nach DDoS-Attacken Probleme mit der Verfügbarkeit und Performance ihrer Infrastrukturen. Die Ausfallzeiten der gar nicht oder nur unzureichend geschützten Ziele können bis zu mehreren Tagen betragen. Das iPad-Kassensystem orderbird, die Hosting-Anbieter Strato und Uberspace sowie Teamviewer, die die Fernwartungen am PC ermöglichen, aber auch die Websites der großen Kinoketten in Deutschland sind in den vergangenen Monaten in Deutschland erfolgreich attackiert worden.

Der Fall des Schweizer Unternehmens Digitec hat eindrücklich gezeigt, dass die Folgen von DDoS-Attacken weit über die Website hinausreichen können. Die wiederholten und lang anhaltenden Angriffe Mitte März 2016 gegen einen Online-Händler von Unterhaltungselektronik ließen neben dem Online-Shop auch das ERP-System ausfallen. Die Folge: Die Verkaufsfilialen und das Callcenter, das den Kundenservice abwickelt, fielen ebenfalls aus. Angesichts solcher Vorfälle treffen immer noch zu wenige Unternehmen proaktive Schutzvorkehrungen.

3. Wie können Unternehmen sich vor diesen Angriffen schützen?

DDoS-Attacken gibt es in vielen Varianten. Simple Angriffstechniken lassen sich leicht und zu 100 Prozent abwehren. Dem gegenüber stehen neue Angriffsformen auf die Netzinfrastruktur von Unternehmen. Das sind nach unseren Analysen zunehmend komplexe Attacken, die mit spezifischer Malware Sicherheitslücken ausnutzen. Andere Angreifer versuchen, über eine sehr große Bandbreite mit über 100 Gbps zum Ziel zu

kommen. Die Praxis zeigt, dass die meisten Unternehmen mit ihrer IT-Security nicht in der Lage sind, der zunehmenden DDoS-Bedrohung eine angemessene Abwehr entgegenzusetzen. Es erfordert einen hohen finanziellen und personellen Einsatz sowie tägliches Training, um auf Augenhöhe mit den Angreifern zu bleiben.

Die zuverlässigste Lösung, um Unternehmen gegen DDoS-Attacken zu schützen, ist daher die Umleitung des Datenverkehrs über einen externen Schutzanbieter. So ein professioneller DDoS-Schutz verfügt über ein hochentwickeltes Filterzentrum mit Spezialisten in 24/7-Bereitschaft und die entsprechenden Ressourcen, um den unerwünschten Datenverkehr herauszufiltern.