DDoS und Ransomware

Warum DDoS-Attacken eine wachsende Bedrohung sind

18. Oktober 2022, 11:05 Uhr | Autor: Birger Kaudasch / Redaktion: Lukas Steiglechner

Distributed-Denial-of-Service-Attacken stellen eine wachsende Bedrohung für die IT-Sicherheit dar. Auch weil die Kriminellen sie nutzen, um Ransomware in die Unternehmensnetzwerke einzuschleusen. Vor allem Unternehmen der kritischen Infrastruktur sind hier gefährdet.

DDoS-Angriffe (Distributed Denial of Service) werden nicht nur immer häufiger, sondern auch immer komplexer. Daher ist es wichtig, sich entsprechend zu schützen. Laut dem Global Threat Analysis Report stieg die Anzahl der DDoSAttacken zuletzt weltweit um 37 Prozent – und das sind nur die registrierten Fälle. Eine Gefahr, die auch von der Bundesregierung erkannt wurde. Deshalb hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) bereits festgelegt, dass Unternehmen, die der kritischen Infrastruktur angehören, eine hohe Geldstrafe droht, sollten sie nicht über einen entsprechenden Schutz verfügen. Aber auch nicht-kritische Unternehmen sind nicht sicher.

Zunächst ist hier ein Blick auf die weltpolitische Lage wichtig: Von einem politischen Hintergrund – abgesehen davon, möglichst hohen gesellschaftlichen Schaden anzurichten – ist die wahrscheinlichste Motivation für einen Cyberangriff Geld. DDoS und andere Cyberangriffe zielen in der Regel darauf ab, Geld vom betroffenen Unternehmen zu erpressen. Entweder wird das Unternehmen dafür komplett lahmgelegt oder die DDoS-Attacke dient der Ablenkung, um in dem geschwächten System Ransomware zu platzieren, die zum Beispiel sensible Daten abgreift oder verschlüsselt, um weiteres Lösegeld zu erpressen.

Mögliche Auswirkungen einer DDoS-Attacke

Die Auswirkungen eines solchen Angriffes können verheerend sein, auch wenn es sich nicht um ein KRITIS-Unternehmen handelt – also ein Unternehmen, das Dienstleistungen zur Daseinsvorsorge der Bevölkerung anbietet wie etwa Energie, Finanzwesen, Verkehrsinfrastruktur oder Krankenhäuser. Nutzer können im Online-Shop nichts mehr bestellen, EC-Zahlung ist nicht mehr möglich oder die Standorte eines einzelnen Unternehmens können nicht mehr miteinander kommunizieren. Selbst Firmen, deren Dienstleistungen nicht direkt über das Internet vertrieben werden, sind in ihrer Arbeitsfähigkeit massiv eingeschränkt, da zum Beispiel Mitarbeiter aus dem Homeoffice oder remote nicht mehr auf das Firmennetzwerk zugreifen können. Auch VoIP-Telefonie – mittlerweile der Standard in Deutschland – ist dann nicht mehr möglich. Dazu kommt, dass verstärkt RDDoS-Angriffe registriert werden. Das sind die oben genannten Kombinationen aus DDoS und Ransomware, bei denen unter anderem die firmeneigenen Daten verschlüsselt und nur gegen Lösegeld wieder entschlüsselt werden. Möglich ist hierbei auch das Abgreifen sensibler oder geheimer Daten zum Beispiel zur Wirtschaftsspionage. Die öffentlich bekanntgewordenen Angriffe auf kommunale Einrichtungen vom Anfang dieses Jahres haben gezeigt, dass es Wochen und Monate dauern kann, bis ein angegriffenes System wieder vollständig hergestellt ist. Letztendlich geht mit einem erfolgreichen Angriff auch immer ein gewisser Reputationsverlust des Unternehmens einher, der zu weiteren Umsatzeinbußen und einem dauerhaften Imageschaden führen kann.

Schutzmaßnahmen, die ergriffen werden können

Was DDoS-Attacken so effektiv macht ist, dass eine Firewall das Problem meist noch verschärft, da sie das eigentliche Ziel des Angriffs ist. Entweder bricht die Firewall unter der Last der Anfragen zusammen oder sie erkennt die Attacke und schaltet das komplette System ab, sodass der Angriff unterm Strich doch erfolgreich war. Es hilft nur eine Kombination aus Firewall und professioneller DDoS-Mitigation. Das BSI hat dafür bislang 14 Firmen qualifiziert, bei denen ein entsprechender Schutz eingekauft werden kann. Grundsätzlich gibt es zwei gängige technische Methoden: Eine cloudbasierte Lösung, bei der alle externen Anfragen ans Unternehmen erst durch eine Art digitale Filteranlage müssen, die dann die „schlechten" aussortiert. Oder aber eine Lösung vom jeweiligen Internetanbieter, bei der der Verkehr zwischen dem Internet und dem Unternehmen permanent überwacht und auffällige Anfragen herausgefiltert und über spezielle Systeme im Netz des Internetproviders bereinigt werden.

Zunehmende Komplexität durch 5G und IoT

Mit Blick auf die Zukunft gibt es drei Faktoren, die DDoS-Angriffe in den nächsten Jahren noch gefährlicher machen. Erstens die wachsende Komplexität der Attacken. Das bedeutet unter anderem, dass die Angreifer nicht nur einen, sondern mehrere Vektoren gleichzeitig benutzen, um ins System zu gelangen, denn auch unter den Cyberkriminellen sehen wir eine gewisse Professionalisierung und Weiterentwicklung. Hinzu kommt der weltweite Ausbau von 5G und anderer hoher Bandbreiten, wodurch ebenfalls mehr und intensivere Angriffe ermöglicht werden, da noch mehr Anfragen mit größeren Datenpaketen gleichzeitig an das anvisierte Ziel gesendet werden können. Dritter Faktor ist die zunehmende Anzahl an Endgeräten sowohl im Internet der Dinge (IoT) als auch in mobilen Netzen: Glühlampen, Kühlschränke, Heizungsanlagen – immer mehr Alltagsgegenstände werden internetfähig und sind nur in den seltensten Fällen mit Blick auf die Informationssicherheit konzipiert worden. Sie können leicht von Kriminellen für Angriffe gekapert und so Teil von sogenannten Botnetzen werden.

Birger Kaudasch, IT-Security- und Datacenter-Architekt, EWE Tel

EWE