5 Tipps:

So schützen Sie sich vor DDoS-Angriffen

Ein DDoS-Angriff kann eine Website oder das gesamte Unternehmen lahmlegen. Mit einigen Schritten können sich kleine und mittlere Unternehmen (KMU) vor den meisten Bedrohungen durch Überlastungsangriffe schützen.

Derzeit werden öffentliche Einrichtungen in Dänemark von DDoS-Angriffen, beispielsweise aus Russland, heimgesucht. Dadurch wird nicht nur der Zugriff der Benutzer auf ihre Websites verhindert, sondern es entsteht auch Unsicherheit und Misstrauen. Alle Unternehmen und Organisationen, unabhängig von ihrer Größe, können betroffen sein.
Ein DDoS-Angriff auf dänische Unternehmen geht meist nicht von professionellen Cyberkriminellen aus. Oft handelt es sich um Streiche von Hobby-Hackern oder verärgerten Kunden, die sich rächen möchten. Leider ist es für jedermann sehr viel einfacher geworden, einen Überlastungsangriff durchzuführen.

Das Kundenvertrauen hat höchste Priorität

Unabhängig davon, woher der Angriff kommt, kann er dem Unternehmen schaden. Während des Angriffs können Kunden die Website nicht mehr besuchen. Gerade KMUs sind stark von ihrer Website oder ihrem Webshop abhängig. Die Angriffe erfolgen meist zu Zeiten, in denen sie am meisten schaden, beispielsweise während des Black Friday. Wenn die Website, das CRM-System oder die Supportkanäle nicht funktionieren, kann dies schnell das Vertrauen schädigen und die Kunden zu Mitbewerbern lenken.
Aus verschiedenen Studien, unter anderem vom Center for Cyber Security, geht hervor, dass die Bedrohung durch Cyberangriffe wächst.
Es ist auch bekannt, dass insbesondere KMUs weiterhin vor Herausforderungen stehen, wenn es um grundlegende IT-Sicherheit geht. Laut des von der dänischen Wirtschaftsbehörde veröffentlichten Reports „Digitale Sicherheit in dänischen KMU“ verfügen knapp die Hälfte der 300.000 KMU des Landes nicht über das empfohlene Sicherheitsniveau im Verhältnis zu ihrem Risikoprofil.

Die Bedrohung wird unterschätzt

Auch im Hinblick auf die Bedrohung durch DDoS-Angriffe sind die meisten dänischen KMUs nicht ausreichend vorbereitet. Dies bestätigt Marie Skouenborg, Leiterin Strategie- und Geschäftsentwicklung im Bereich Digital Solutions beim Glasfaser- und Rechenzentrumsanbieter GlobalConnect. „Die Mittelständler, die über einen angemessenen Schutz vor Cyber-Bedrohungen verfügen, sind häufig diejenigen, die bereits einem Angriff ausgesetzt waren oder bei denen eines der Vorstandsmitglieder dies in einem anderen Unternehmen erlebt hat. Leider ist die Mehrheit der KMU nicht besonders gut vorbereitet, da sie denken, dass sie nicht betroffen sein werden und ein Angriff für sie nicht schwerwiegend sein wird“, sagt Marie Skouenborg von GlobalConnect.

Angriffe schaden dem Geschäft

Obwohl ein Überlastungsangriff nicht so schwerwiegend ist wie ein Ransomware-Angriff, lohnt es sich, sich davor zu schützen. Vor allem, weil man das Risiko mit relativ einfachen Maßnahmen reduzieren kann, sagt Marie Skouenborg: „Ein Angriff kann Geld kosten, Ihrer Marke schaden und im Allgemeinen unnötige Unruhe verursachen - sowohl intern als auch extern. Mit einem sinnvollen Setup können Sie sich sicherer auf das Geschäft statt auf alles andere konzentrieren.“

Sådan garderer SMV'er sig bedst muligt mod et DDoS-angreb

1 **Vurder konsekvenserne.**
Hvor kritisk vil det være for forretningen og kunderelationerne, hvis jeres hjemmeside og andre kanaler er utilgængelige på grund af et DDoS-angreb, og hvor lang nedetid kan I tolerere? Skal nogen kronjuveler beskyttes mere and andre dele af forretningen? Det behøver nemlig ikke handle om at undgå et angreb for enhver pris.

2 **Skyd ikke gråspurve med kanoner.**
Der er ingen grund til at forkøbe sig i unødige sikkerhedsløsninger, selv om nogen måske anbefaler det. Som SMV'er behøver du som udgangspunkt ikke en premium-løsning.

GlobalConnect DDoS beskyttelse findes i tre løsninger afhængig af behov, hvor I kan få installation og vedligeholdelse af udstyr, 24/7-overvågning og adgang til eksperter, som løbende analyserer og står klar til at reagere på angreb.

3 **Når angrebet rammer.**
Afklar sammen med jeres leverandør, hvad reaktionen skal være på et potentielt DDoS-angreb. Skal systemet automatisk mitigere, altså forsøge at stoppe eller begrænse angrebet? Bør systemet i stedet gøre dig opmærksom på det potentielle angreb, så I selv kan vurdere situationen? Eller skal det være op til jer selv at række ud til leverandøren, hvis I oplever noget mistænkeligt? Hensynet er, at der kan være falske positive, fx en usædvanlig stor trafik i forbindelse med en kampagne, som aktiverer forsvarssystemet.

4 **Adskil linjerne.**
Når man har en hjemmeside med en offentlig ip-adresse, er det en rigtig god idé at sikre, at linjen ind er adskilt fra resten af netværket. Tal med jeres leverandør om at adskille båndbredden mellem internettet og den interne trafik i virksomheden, så et DDoS-angreb på hjemmesiden ikke lammer hele virksomheden.

5 **Fordel ansvaret.**
Når et angreb rammer, skal man kunne reagere hurtigst muligt. Derfor skal det være klart, hvem der har ansvaret for dialogen med jeres netværks- og sikkerhedsleverandør. Det kan desuden være en god idé at have en "krise-meddelelse" klar til at lægge på jeres hjemmeside, så brugerne ved, at I er bekendt med problemet og arbejder på at løse det.

Et DDoS-angreb er, når en masse computere eller andre enheder på én gang og i én uendelighed forespørger den samme internetadresse eller sender trafik med et særligt mønster mod for eksempel hjemmesider, mailservere, firewalls og routere. Den massive trafik giver en overbelastning, som lukker ned for adgangen.