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 im als auch außerhalb Ihres Unternehmens. Mit einem sinnvollen Setup können Sie sich sicherer auf das Geschäft statt auf alles andere konzentrieren.“

> **Ein Angriff kann Geld kosten, Ihrer Marke schaden und im Allgemeinen unnötige Unruhe verursachen - sowohl im als auch außerhalb Ihres Unternehmens. Mit einem sinnvollen Setup können Sie sich sicherer auf das Geschäft statt auf alles andere konzentrieren.”**

Marie Skouenborg
GlobalConnect

So schützen sich KMU am besten vor einem DDoS-Angriff

1 **Die Konsequenzen einschätzen**
Wie kritisch wird es für das Geschäft und die Kundenbeziehungen sein, wenn Ihre Website und andere Kanäle aufgrund eines DDoS-Angriffs nicht verfügbar sind? Wie viel Ausfallzeit können Sie tolerieren? Sollten bestimmte Bereiche stärker geschützt werden als andere Teile des Unternehmens? Es muss nicht darum gehen, einen Angriff um jeden Preis zu vermeiden.

2 **Angemessen vorbeugen**
Es gibt keinen Grund, jede Sicherheitslösung zu implementieren, die verfügbar ist. Als KMU benötigen Sie in der Regel keine Premium-Lösung.

Der GlobalConnect DDoS-Rundumschutz aus diesem Grund in drei Stufen erhältlich. Sie erhalten Installation und Wartung von Geräten, Überwachung rund um die Uhr und Zugriff auf Experten, die Angriffe kontinuierlich analysieren und bereit sind, darauf zu reagieren.

3 **Erstellen eines Notfallplans**
Klären Sie mit Ihrem Dienstleister, wie auf einen möglichen DDoS-Angriff reagiert werden soll. Sollte das System den Angriff automatisch abschwächen, d. h. versuchen, ihn zu stoppen oder einzuschränken? Soll das System Sie stattdessen vor dem möglichen Angriff warnen, damit Sie die Situation selbst einschätzen können? Oder wenden Sie sich selbst an den Lieferanten, wenn Ihnen etwas Verdächtiges auffällt?
Es sollte hierbei beachtet werden, dass es auch zu einem Fehlalarm kommen kann. So könnte außergewöhnlich großer Traffic im Zusammenhang mit einer Kampagne das Abwehrsystem auslösen, obwohl kein Angriff vorliegt. So können Sie entscheiden, ob ein echter Verdacht vorliegt.

4 **Trennen Sie die IP-Adresse vom Netzwerk**
Wenn Sie eine Website mit einer öffentlichen IP-Adresse haben, ist es von Vorteil, sicherzustellen, dass der Zugang vom Rest des Netzwerks getrennt ist. Sprechen Sie mit Ihrem Lieferanten über die Trennung der Bandbreite zwischen Internet und internem Datenverkehr im Unternehmen, damit ein DDoS-Angriff auf die Website nicht das gesamte Unternehmen lahmlegt.

5 **Verantwortliche benennen**
Bei einem Angriff müssen Sie schnellstmöglich reagieren können. Daher muss klar sein, wer für den Dialog mit Ihrem Netzwerk- und Sicherheitsanbieter verantwortlich ist. Es kann auch sinnvoll sein, eine „Krisenmeldung“ auf Ihrer Website bereitzuhalten, damit die Benutzer wissen, dass Sie sich des Problems bewusst sind – und aktuell an einer Lösung arbeiten.

Von einem DDoS-Angriff spricht man, wenn eine große Anzahl von Computern oder anderen Geräten gleichzeitig und ununterbrochen dieselbe Internetadresse anfordert oder Datenverkehr nach einem bestimmten Muster beispielsweise an Websites, Mailserver, Firewalls und Router sendet. Der massive Datenverkehr verursacht eine Überlastung, die den Zugang zum Internet unterbricht.