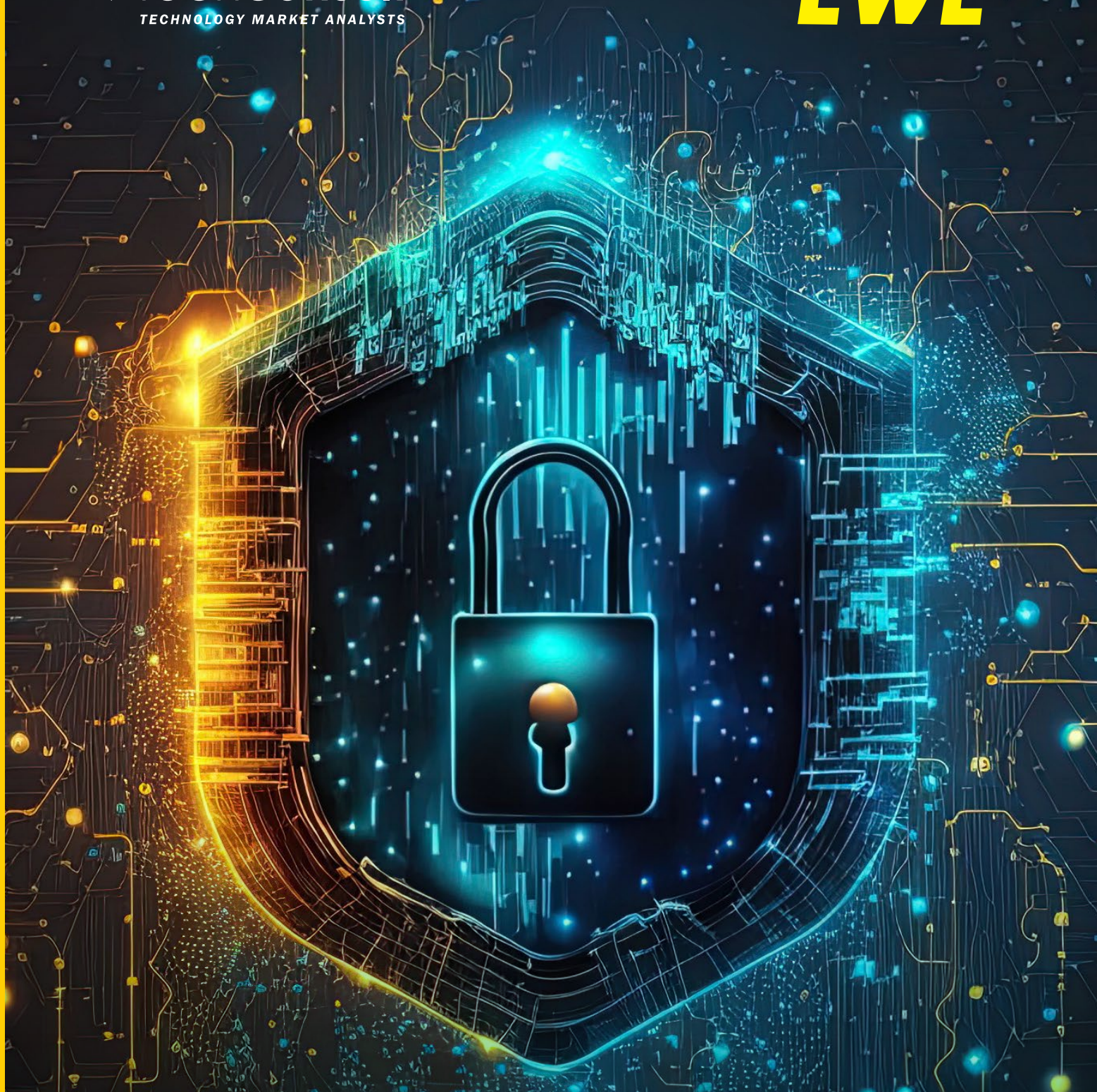
techconsult
TECHNOLOGY MARKET ANALYSTS

Unterstützt durch

EWE



DDoS-Angriffe

Eine Gefahr für jedes Unternehmen

Inhalt

Sonstiges
Aufgrund von Rundungsanpassungen summieren sich einige Summen möglicherweise nicht zu 100%.
Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in dieser Studie die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Vorwort

Ob Online-Händler, Kritische Infrastrukturen oder Behörden, jedes Unternehmen und jede Institution, die mit dem Internet verbunden ist, kann Opfer von Cyberangriffen werden. Eine Form dieser Cyberangriffe stellen DDoS-Attacken dar. Bei DDoS-Angriffen versuchen Cyberkriminelle die Internetdienste von Unternehmen oder staatlichen Institutionen mit einer großen Anzahl an Anfragen zu überlasten. Dabei ist die Einstiegshürde für Cyberkriminelle niedrig. Sie können sich beispielsweise bei kriminellen Organisationen einen Service für DDoS-Angriffe mieten oder kaufen und so ohne Vorkenntnisse DDoS-Angriffe starten.

Ziel von DDoS-Angriffen ist es, Unternehmen oder Institutionen einen möglichst großen Schaden zuzufügen. Die Motive dafür sind vielschichtig und reichen von Erpressung, über politisch motivierten Protest bis hin zur Schwächung von Wirtschaft und Infrastrukturen als Waffe im Cyberkrieg durch staatliche Akteure.

Doch wie genau sieht die Bedrohungslage durch DDoS-Attacken in deutschen Unternehmen aus? Mit welchen Maßnahmen versuchen sich Unternehmen vor DDoS-Attacken zu schützen? Und wie schätzen diese ihr eigenes Schutzniveau ein?

Um diese Fragen zu beantworten, wurden im November 2022 im Rahmen dieser Studie 201 Entscheidende oder stark am Entscheidungsprozess beteiligte Personen zu ihrem Einsatz von DDoS-Schutz, der Häufigkeit von DDoS-Attacken oder auch den Folgen erfolgreicher DDoS-Angriffe befragt.

Häufigkeit von DDoS-Angriffen steigt

Der 22. Juli 1999 ist ein besonderes Datum der Informatikgeschichte. An jenem Tag wurde die US-amerikanischen University of Minnesota von einem Netzwerk aus 114 Computern, die mit dem schädlichen Skript Trin00 infiziert waren, angegriffen. Die infizierten Computer sendeten eine große Anzahl von Datenpaketen an die Server der Universität und legten auf diese Weise die Website der Universität für mehrere Tage lahm. Dieses Ereignis gilt seitdem als erster erfasster Distributed-Denial-of-Service-Angriff. Im Februar 2000 folgte die wohl berüchtigtste DDoS-Attacke. Ein 15-jähriger Schüler namens Michael „Mafiaboy" Calce startete einen massiven DDoS-Angriff gegen große Unternehmen wie Yahoo, Amazon, Dell oder auch eBay. Die Folgen waren verheerend und führten unter anderem zu Chaos an der Börse. Dieser Vorfall trug dazu bei, das Bewusstsein für die Notwendigkeit von DDoS-Schutz zu schärfen und führte zur Entwicklung neuer Methoden zur Abwehr von DDoS-Angriffen. Gleichzeitig war dieser Angriff auch der Beginn einer neuen Ära der Cyberkriminalität, da er die Leistungsfähigkeit von DDoS-Angriffen demonstrierte. Auf diesen DDoS-Angriff folgten viele weitere, die an Häufigkeit und Schwere zugenommen haben und bis heute andauern.

Bei Distributed-Denial-of-Service-Attacken (DDoS) werden gezielte, parallel ausgeführte Überlastungsangriffe auf Internetdienste ausgeführt.

Es gibt viele verschiedene Arten von DDoS-Attacken, beispielsweise volumetrische DDoS-Angriffe oder Angriffe auf Anwendungs- oder Protokollebene. Damit wollen Cyberkriminelle die Verfügbarkeit von Webseiten, Diensten oder auch ganzen Netzwerken zusammenbrechen lassen.

Angreifer nutzen diese Art von Angriff, um gezielt Schaden anzurichten, manchmal jedoch auch, um andere Angriffe zu verschleiern oder gar erst zu ermöglichen. Die Motivation der Angreifer ist dabei vielfältig und reicht von Erpressung über gezielte Schädigung der Konkurrenz oder politische Motive bis hin zur Schwächung von Wirtschaft und Infrastruktur ganzer Nationen als Waffe in einem Wirtschaftskrieg.

DDoS-Angriffe sind für Personen mit böswilliger Absicht relativ einfach, ohne Kenntnisse oder Erfahrung, durchführbar. Dafür können sie beispielsweise DDoS-Services mieten oder kaufen, um über die Botnetze von Cyberkriminellen DDoS-Angriffe ohne großen Aufwand zu starten. Durch diesen einfachen Zugang zu derartigen Angriffen, stellen DDoS-Attacken eine große Gefahr für sämtliche Unternehmen und Institutionen dar. Denn jedes Unternehmen, das über eine Online-Infrastruktur verfügt, ist ein potenzielles Ziel von DDoS-Attacken.

Mehrheit der Unternehmen von DDoS-Attacken betroffen

DDoS-Angriffe sind mittlerweile eher die Regel als die Ausnahme. Lediglich 13 Prozent der im Rahmen dieser Studie befragten Unternehmen gaben an, noch nie Opfer solcher Attacken geworden zu sein. Tendenziell nimmt die Gefahr mit der Unternehmensgröße zu. Das Niveau bereits angegriffener Unternehmen in kleineren und mittleren Unternehmen ist jedoch schon immens hoch. So waren beispielsweise fast 80 Prozent der Unternehmen mit weniger als 49 Mitarbeitenden, sowie rund 75 Prozent der Unternehmen zwischen 50 und 99 Mitarbeitenden bereits Opfer von DDoS-Attacken.

Darüber hinaus ist auch die Häufigkeit von DDoS-Angriffen in den vergangen zwei Jahren angestiegen. Knapp 20 Prozent der Unternehmen konnte sogar einen starken Anstieg von DDoS-Angriffen in den vergangenen zwei Jahren erkennen. Ein weiteres Drittel spürte einen leichten Anstieg.

Ein gutes weiteres Viertel gab zudem an, dass die DDoS-Angriffe zwar nicht zugenommen haben, aber auf einem konstanten Niveau geblieben sind. Und nur sieben Prozent konnten einen Rückgang der DDoS-Angriffe erkennen.

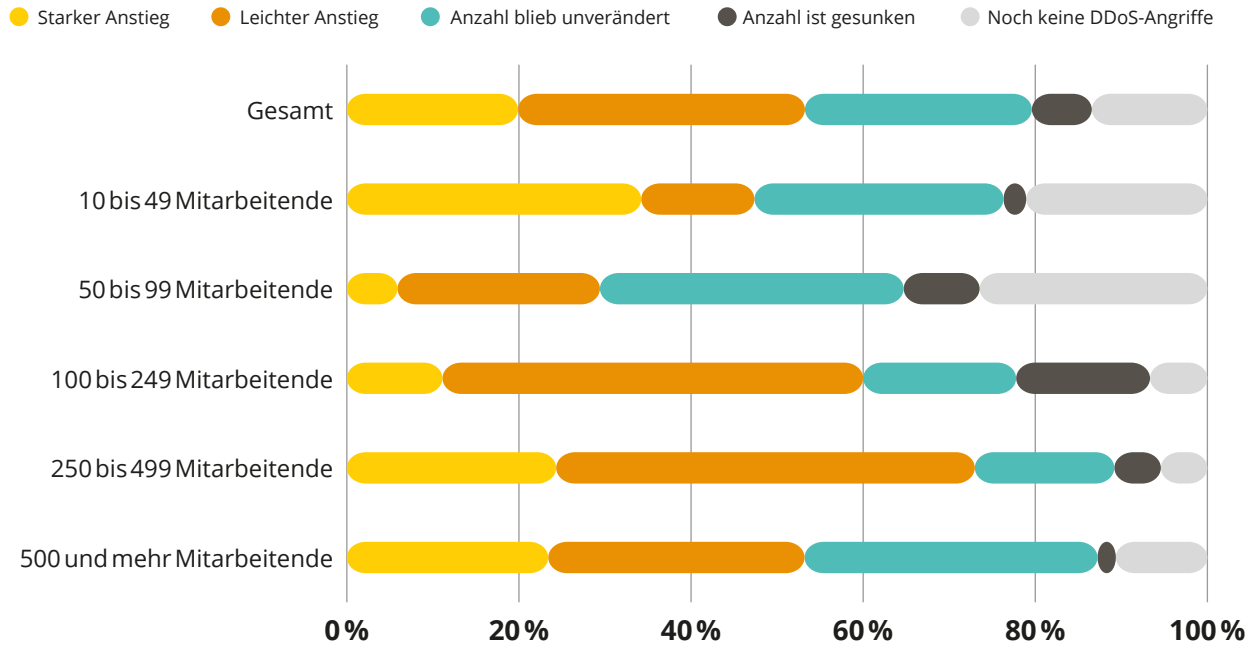
Tendenziell besonders im Fokus von DDoS-Attacken waren mittelgroße Unternehmen. So konnte beispielsweise fast ein Viertel der Unternehmen mit 250 bis 499 Mitarbeitenden einen starken Anstieg und fast die Hälfte einen leichten Anstieg feststellen.

Auch die steigende Quantität der Angriffe, wenn sie erfolgen, spart die kleineren Unternehmen nicht aus. Knapp mehr als ein Drittel der Unternehmen mit weniger als 50 Mitarbeitenden verzeichneten einen starken Anstieg. Weitere 13 Prozent konnten einen leichten Anstieg erfassen.

Ein aktuelles Beispiel zeigt auch, wie DDoS-Angriffe nicht nur Unternehmen gefährden, sondern auch als Angriff auf demokratische Strukturen genutzt werden. Im November 2022 wurde die Webseite des Europaparlaments direkt nach Verabschiedung einer Resolution, die Russland als Unterstützer des Terrorismus deklariert hatte, von einer kremlnahen Hackergruppe durch einen DDoS-Angriff lahmgelegt. Dieses Beispiel verdeutlicht, dass DDoS-Angriffe nicht nur zur persönlichen Bereicherung von Cyberkriminellen verwendet werden, sondern auch anlassbezogen stattfinden können. Äußert sich beispielsweise ein Unternehmen oder eine Behörde kritisch gegenüber anderen Akteuren, kann die Wahrscheinlichkeit Opfer von DDoS-Attacken zu werden, ansteigen.

Häufigkeit von DDoS-Angriffen

Basis: 201 Unternehmen



Viele Unternehmen setzen fälschlicherweise auf die Firewall

Aufgrund des hohen Gefahrenpotenzials von DDoS-Attacken haben viele Unternehmen die Notwendigkeit erkannt, sich mit entsprechenden Lösungen vor DDoS-Angriffen zu schützen. Um diesen Schutz aufzubauen, können Unternehmen beispielsweise auf eine dedizierte Inhouse-Lösung oder auch auf einen DDoS-Protection Cloud Service setzen.

Hybride Lösungsansätze, bei denen eine Kombination aus Inhouse-Lösungen sowie Cloud-Diensten zum Einsatz kommt, werden von rund 41 Prozent der Unternehmen verwendet. Praktisch gleichauf ist auch der Einsatz von externen Dienstleistern mit gut 40 Prozent. Inhouse-Lösungen werden von rund einem Drittel der Unternehmen verwendet.

Betrachtet man die Einsatzgrade in den verschiedenen Größenklassen, kann man teils deutliche Unterschiede erkennen. So arbeiten beispielsweise kleinere und mittlere Unternehmen, auch bedingt durch den oftmals vorherrschenden Mangel an internem Know-how, öfter mit Managed Service Providern zusammen als größere Unternehmen. Nur knapp 30 Prozent der Unternehmen mit 500 bis 999 Mitarbeitenden und 33 Prozent der Unternehmen mit mehr als 1.000 Mitarbeitenden setzen auf die Expertise eines externen Dienstleisters. Unternehmen mit weniger als 50 Mitarbeitenden (47 Prozent), 100 bis 249 Mitarbeitenden (42 Prozent) und 250 bis 499 Mitarbeitenden (49 Prozent) setzen hingegen vermehrt auf Managed Service Provider zum Schutz vor DDoS-Attacken.

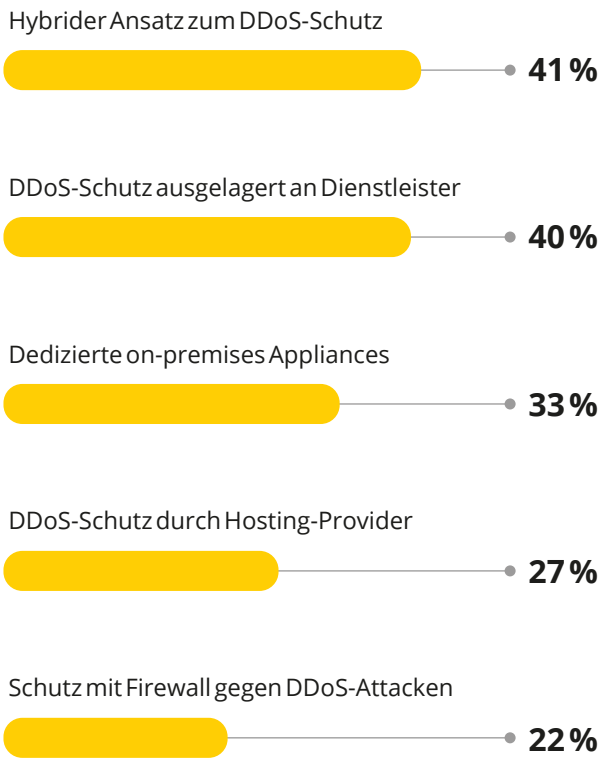
Leider verwendet ein nicht geringer Anteil an Unternehmen keinen dedizierten DDoS-Schutz. Mehr als ein Fünftel der befragten Unternehmen verfügt lediglich über eine Firewall. Insbesondere kleinere Unternehmen verwenden fälschlicherweise eine Firewall als DDoS-Schutz. Fast 30 Prozent der Unternehmen mit weniger als 49 Mitarbeitenden, sowie rund ein Viertel der Unternehmen mit 50 bis 99 Mitarbeitenden und 100 bis 249 Mitarbeitenden verwendet ausschließlich eine Firewall.

Die Firewall hilft zwar dabei, Schadsoftware aus dem Unternehmen fernzuhalten, ist jedoch für die Abwehr von DDoS-Attacken gänzlich unzureichend. Firewalls sind zu keiner Zeit darauf ausgelegt, gezielte DDoS-Attacken abzuwehren.

Im Gegenteil: Firewalls oder andere Intrusion Prevention Systeme selbst können das Ziel von DDoS-Angriffen sein und sind selbst Teil des DDoS-Problems. Firewalls sind aufgrund ihrer Funktionsweise oftmals sogar das erste Opfer von DDoS-Angriffen. Dabei werden Firewalls so stark überlastet, dass das Unternehmensnetzwerk in die Knie gezwungen wird. Firewalls müssen selbst vor DDoS-Angriffen geschützt werden.

Einsatzgrade von DDoS-Schutz

Basis: 201 Unternehmen | Mehrfachnennungen



Erfolgreiche DDoS-Angriffe mit verheerenden Auswirkungen

Sind Cyberkriminelle mit DDoS-Angriffen erfolgreich, so hat das für Unternehmen eine Reihe von schwerwiegenden Konsequenzen. Und in vielen Fällen wird es erstmal eins: teuer! Für 46 Prozent der Unternehmen, die Opfer von DDoS-Angriffen waren, erhöhten sich die internen Kosten. Die betroffenen Dienste für Mitarbeiter oder Kunden wiederherzustellen, kann zu einem langwierigen und kostspieligen Unterfangen werden, denn oft haben die Angriffe länger anhaltende Auswirkungen auf die IT-Infrastruktur. Beispielsweise kann die Netzwerkleistung durch die Überlastung verlangsamt werden oder die Verfügbarkeit der eigenen Websites eingeschränkt werden.

Cyberkriminelle verwenden DDoS-Angriffe auch gerne als Ablenkungsmanöver für gefährlichere Angriffe. Cyberkriminelle können beispielsweise die Server eines Unternehmens mit Täuschungsverkehr eines DDoS-Angriffs überfluten und währenddessen Daten stehlen oder verschlüsseln, um von den Opfern Lösegelder für die Herausgabe der Daten einzufordern.

Und genau solche Datenverluste und Ransomware-Angriffe im Rahmen von DDoS-Attacken traten bei fast 40 Prozent der Unternehmen tatsächlich ein.

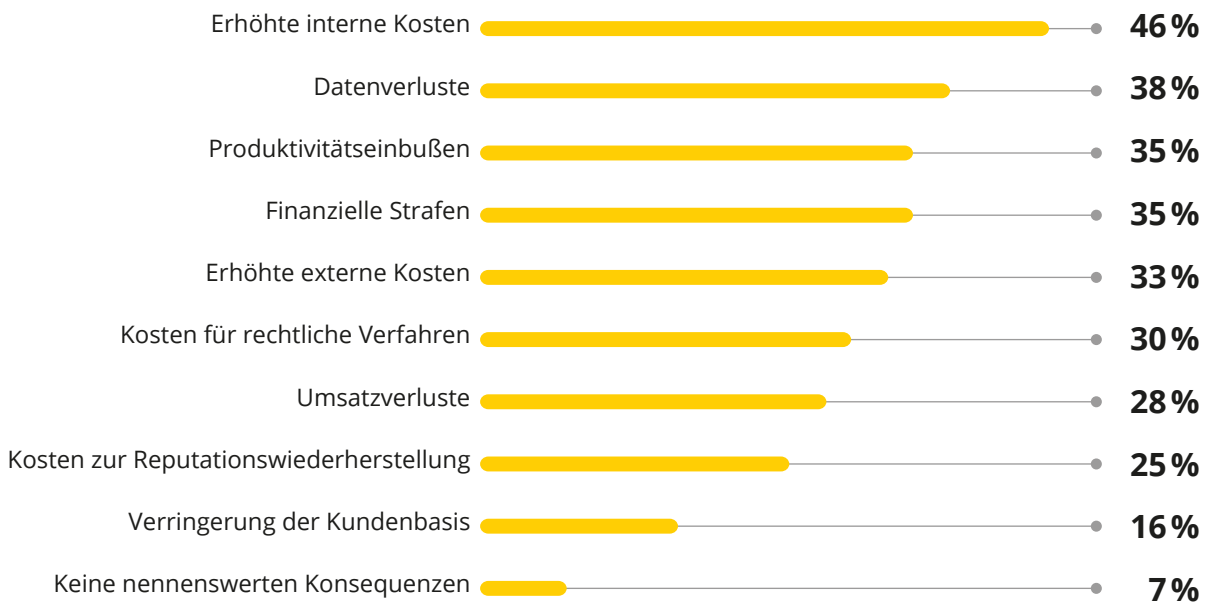
Auch jene Unternehmen, die bisher kein Opfer von DDoS-Angriffen waren, fürchten vor allem die Gefahr von Datenverlusten und Ransomware.

37 Prozent
der Unternehmen, die bisher keine Opfer von DDoS-Angriffen waren, befürchten vor allem Datenverluste.

Solche Datenverluste können darüber hinaus auch noch empfindlichen Strafen im Rahmen der DSGVO nach sich ziehen. Besonders gravierende Verstöße werden mit bis zu 20 Millionen oder bis zu 4 Prozent des weltweit erzielten Jahresumsatzes, je nachdem welcher Wert höher ist, geahndet. Aber auch weniger gewichtige Verstöße führen zu hohen Bußgeldern von bis zu zehn Millionen Euro beziehungsweise zwei Prozent des Umsatzes.

Folgen von DDoS-Angriffen

Basis: 174 Unternehmen | Mehrfachnennungen



Nur 4 von 10 Unternehmen können große DDoS-Angriffe abwehren

Im Hinblick auf die steigende Gefahr durch DDoS-Angriffe, wurden die Teilnehmer dieser Studie um eine eigene Einschätzung der Robustheit ihrer IT-Infrastruktur gegenüber DDoS-Attacken gebeten. Knapp 40 Prozent gaben an, dass sie zwar grundsätzlich gegen kleinere DDoS-Angriffe geschützt sind, jedoch größere Angriffe nicht mehr bewältigen können.

Gut gegen alle Arten von DDoS-Angriffen sehen sich knapp 39 Prozent der befragten Unternehmen aufgestellt. Das trifft insbesondere auf die allergrößten Unternehmen mit mehr als 1.000 Mitarbeitenden zu, von denen 70 Prozent ihre IT-Infrastruktur robust genug ansehen. Mit Ausnahme von Unternehmen bis 49 Mitarbeitenden (24 Prozent), sehen sich in den anderen Größenklassen jeweils etwas mehr als ein Drittel der Unternehmen gut gegen große DDoS-Angriffe aufgestellt.

Darüber hinaus sind sich weitere 13 Prozent der Unternehmen im Klaren darüber, dass ihre IT-Infrastruktur nicht einmal kleinen DDoS-Angriffen standhalten kann, wobei der Anteil bei Unternehmen mit weniger als 50 Mitarbeitenden sowie zwischen 100 und 249 Mitarbeitenden deutlich höher liegt. Hier sehen sich fast ein Viertel nicht gut gegen DDoS-Angriffe geschützt.

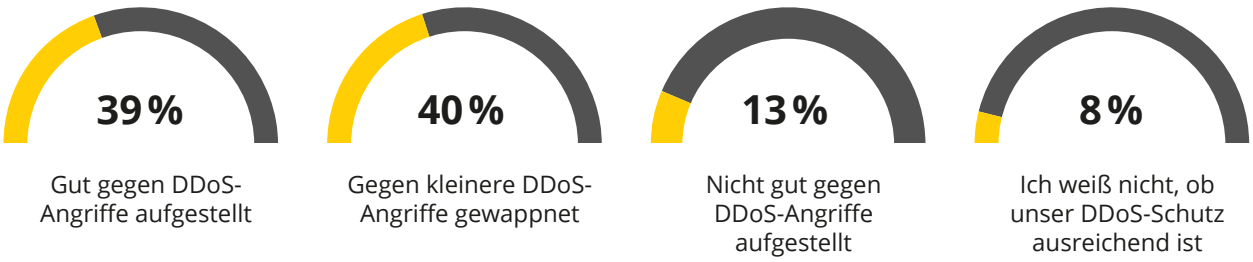
Weitere 8 Prozent sind sich zudem unsicher, ob sie über ausreichenden DDoS-Schutz verfügen. Dies trifft besonders auf jene Unternehmen zu, die sich fälschlicherweise nur mit einer Firewall gegen DDoS-Angriffe zu schützen versuchen. Fast die Hälfte jener Unternehmen, die sich nur mittels einer Firewall gegen DDoS-Angriffe schützen, ist sich unsicher, ob die Firewall überhaupt als Schutz ausreicht.

Interessant ist auch, dass sich Unternehmen mit dediziertem DDoS-Schutz, deutlich besser gegen DDoS-Angriffe aufgestellt sehen, als jene die nur eine Firewall verwenden.

Unternehmen, die über einen nicht ausreichenden oder nicht mehr zeitgemäßen DDoS-Schutz verfügen oder gar nur eine Firewall verwenden, sollten sich dringend mit entsprechenden Spezialisten in Verbindung setzen. Nur so kann das eigene Unternehmen vor den Gefahren durch DDoS-Angriffe, die nicht nur an Häufigkeit sondern auch an Größe zunehmen, effektiv und zukunftsgerichtet geschützt werden.

Selbsteinschätzung DDoS-Schutz

Basis: 201 Unternehmen



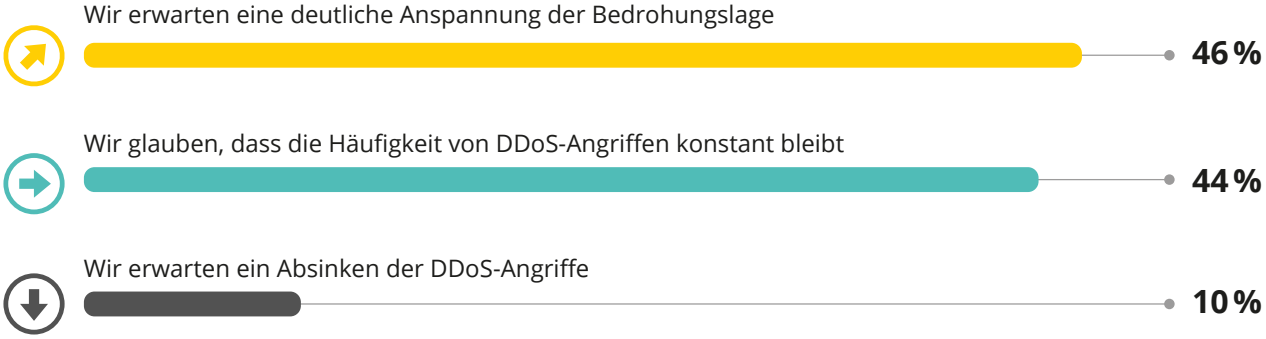
Die Bedrohungslage bleibt angespannt

Und dass es allerhöchste Zeit ist, einen professionellen DDoS-Schutz aufzubauen, zeigt die Zukunftseinschätzung der Unternehmen. Denn mit einer Entspannung der Bedrohungslage rechnen die Unternehmen nicht. Im Gegenteil: Sie erwarten sogar noch eine Verschärfung. 46 Prozent der Unternehmen gehen davon aus, dass sich die Bedrohungslage durch DDoS-Angriffe in den kommenden Jahren noch deutlich mehr anspannen wird.

Weitere 44 Prozent erwarten, dass die Häufigkeit von DDoS-Angriffen auf dem aktuellen Niveau bleiben wird. Nur jedes zehnte Unternehmen geht davon aus, dass die Häufigkeit von DDoS-Angriffen sinken wird. Deutlicher kann die Notwendigkeit für den Bedarf an professionellem DDoS-Schutz gar nicht aufgezeigt werden.

Bedrohungslage durch DDoS-Angriffe

Basis: 201 Unternehmen



Fazit

DDoS-Angriffe sind eine konkrete Gefahr für jedes Unternehmen. Denn jedes Unternehmen, das über eine Online-Infrastruktur verfügt, ist ein potenzielles Ziel von DDoS-Attacken. Zwar verwenden bereits heute viele Unternehmen einen dedizierten DDoS-Schutz, um Angriffe abzuwehren. Jedoch verlassen sich immer noch einige Unternehmen ausschließlich auf ihre Firewall. Dabei ist eine Firewall selbst ein Asset, das vor DDoS-Angriffen geschützt werden muss und dient keineswegs dazu DDoS-Angriffe auf das eigene Netzwerk abzuwehren.

Grundsätzlich können Unternehmen kleinere DDoS-Angriffe erfolgreich abwehren. Größere Angriffe stellen viele Unternehmen jedoch vor Probleme. Denn nur rund 40 Prozent aller Unternehmen sehen sich in der Lage, große DDoS-Attacken abwehren zu können. Die Folgen erfolgreicher DDoS-Angriffe können verheerend sein. Erhöhte interne, wie externe Kosten, Datenverluste oder auch potenzielle existenzbedrohende Schäden sind für Unternehmen zu erwarten.

Und wie sieht die Gefahrenlage in Zukunft aus? Kurzum: alles andere als rosig! Denn die überwiegende Mehrheit geht davon aus, dass es keine Besserung der Bedrohungslage durch DDoS-Angriffe geben wird. Im Gegenteil, 46 Prozent der Unternehmen erwarten sogar eine weitere Anspannung. Kein Wunder, wenn DDoS-Attacken einfach und unkompliziert für wenig Geld beauftragt werden können.

Das sollte für Unternehmen und Institutionen Alarmsignal genug sein, um sich mit den besten verfügbaren Möglichkeiten gegen DDoS-Angriffe zu schützen. Sollte dies mit den internen Mitteln nicht möglich sein, ist die Zuhilfenahme eines Managed Service Providers ein wichtiger Schritt, um das eigene Unternehmen robuster gegen DDoS-Attacken aufzustellen.

Zur Studie

Die Studie "DDoS-Angriffe - Eine Gefahr für jedes Unternehmen" wurde von der techconsult GmbH im Auftrag von EWE konzipiert und durchgeführt. 201 Unternehmen aus Deutschland wurden zu ihrem Einsatzgrad von Abwehrmaßnahmen gegen DDoS-Angriffe, den Konsequenzen erfolgreicher DDoS-Angriffe sowie ihrer Einschätzung zur Bedrohungslage durch DDoS-Attacken befragt. Die Stichprobe umfasste alle Branchen. Ansprechpartner waren in erster Linie IT-Entscheidende.

Branche

- **51 %** Dienstleistung
- **23 %** Industrie
- **15 %** Öffentliche Verwaltungen, Non-Profit, Gesundheits- und Sozialwesen
- **5 %** Banken und Versicherung
- **7 %** Handel

Größenklassen

- **19 %** 10 bis 49 Mitarbeitende
- **17 %** 50 bis 99 Mitarbeitende
- **22 %** 100 bis 249 Mitarbeitende
- **18 %** 250 bis 499 Mitarbeitende
- **10 %** 500 bis 999 Mitarbeitende
- **13 %** 1.000 und mehr Mitarbeitende

Weitere Informationen

Über die EWE TEL GmbH

Die EWE TEL GmbH ist ein deutsches Telekommunikations- und IT-Unternehmen mit Hauptsitz in Oldenburg, Niedersachsen. Das Unternehmen wurde im Jahr 1999 als 100%ige Tochtergesellschaft der EWE AG gegründet und bietet eine breite Palette an Telekommunikations- und IT-Dienstleistungen für Unternehmen, Institutionen und Privatkunden an. Hierzu gehören unter anderem Festnetz- und Mobilfunkdienste, Internet und Datendienste sowie IT- und Sicherheitslösungen. Dabei legt das Unternehmen besonderen Wert auf hohe Qualität und Verfügbarkeit seiner Dienstleistungen.

Die EWE TEL GmbH betreibt ein eigenes Glasfasernetz mit einer Länge von mehr als 40.000 km und ist somit einer der größten Netzbetreiber in Norddeutschland. Zudem betreibt das Unternehmen eigene Rechenzentren und verfügt über eine hoch performante Infrastruktur für seine Kunden. Mit seinen innovativen Lösungen und seinem umfassenden Know-how in der Telekommunikations- und IT-Branche ist die EWE TEL GmbH ein zuverlässiger Partner für Unternehmen jeder Größe und Branche.

EWE TEL GmbH
Cloppenburger Straße 310
26133 Oldenburg
Telefon: 0800 1393835
E-Mail: **business@ewe.de**
Web: **business.ewe.de**

Über die techconsult GmbH

Die techconsult GmbH, gegründet 1992, zählt zu den etablierten Analystenhäusern in Zentraleuropa. Der Schwerpunkt der Strategieberatung liegt in der Informations- und Kommunikationsindustrie (ITK). Durch jahrelange Standard- und Individual-Untersuchungen verfügt techconsult über einen im deutschsprachigen Raum einzigartigen Informationsbestand, sowohl hinsichtlich der Kontinuität als auch der Informationstiefe, und ist somit ein wichtiger Beratungspartner der CXOs sowie der IT-Industrie, wenn es um Produktinnovation, Marketingstrategie und Absatzentwicklung geht.

Impressum

techconsult GmbH
Baunsbergstraße 37
34131 Kassel

E-Mail: **info@techconsult.de**
Tel.: +49 (0) 561 8109 0
Fax: +49 (0) 561 8109 101
Web: **www.techconsult.de**

Autor der Studie

Raphael Napieralski
Analyst
E-Mail: **raphael.napieralski@techconsult.de**