DDoS-RESILIENCY-SCORE

> *Der DDoS Resiliency Score (DRS) ist ein Standard, mit dem Mitigationsstrategien objektiv und quantitativ gemessen und bewertet werden.*

Warum ein DDoS Resiliency Score, und wie wird er verwendet?

Heute sind viele Kenntnisse, Daten und Lösungen verfügbar, mit deren Hilfe Strategien und Vorkehrungen für IT-Netzwerke gegen DDoS-Angriffe aufgebaut werden können.

Obgleich der großen Menge an Daten gibt es keine Messwertskala für die Bewertung und Bemessung der Stärken von Angriffen und der Fähigkeit, diesen zu widerstehen.

Wie viele Organisationen können beispielsweise genau bewerten oder prognostizieren, welcher Art und welchem Umfang von DDoS-Angriffsvektoren ihr System widerstehen kann? Hier setzt der DRS als Instrument an.

Mithilfe des DRS haben Organisationen u.a. folgende Möglichkeiten:

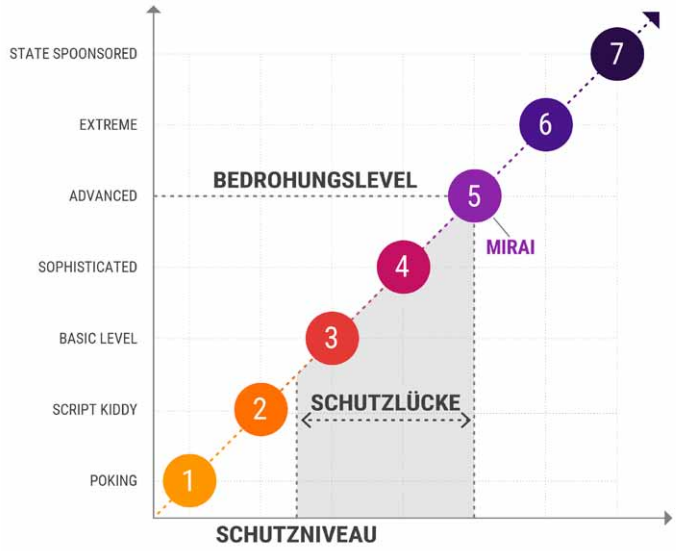
Die Abwehrbereitschaft gegen DDoS-Angriffe bewerten.
Der DRS stellt eine spezifische definierte Liste der Angriffstypen bereit, der eine Organisation widerstehen kann, bevor ein Ausfall erfolgt.

Bessere Entscheidungen bezüglich der Technologie fällen.
Technikteams können die Effektivität unterschiedlicher DDoS-Technologien und Lösungsoptionen vergleichen, indem sie Noten vergeben.

Die Kommunikation zwischen Leitung und Technikteams erleichtern.
Eine Benotung mit 4,7 kann beispielsweise der Leitung vermitteln, dass die Fähigkeiten zur Schadensbegrenzung seit der letzten Benotung mit 3,5 verbessert wurden. Gleichzeitig stellt der DRS eine Liste spezifischer Angriffsvektoren zusammen, die blockiert bzw. nicht blockiert werden; Technikteams können diese Liste analysieren.

Informationen zum Bewertungsmechanismus des DRS

Der Bewertungsmechanismus des DRS basiert auf sieben aufsteigenden Stufen von DDoS-Angriffen. Jede Stufe bringt zusätzliche Angriffsarten, besser ausgereifte Angriffsvektoren und ein größeres Traffic-Volumen mit sich.
Damit steigen auch die Anforderungen für die Verteidigung; jede Stufe erfordert eine kürzere Reaktionszeit zur Schadensbegrenzung und eine geringere Latenz.



Sieben Angriffsstufen:
Welche können Sie abwehren und ab wo steigt Ihre Abwehr aus?

Die nachfolgende Tabelle bietet eine Übersicht der wichtigsten Merkmale der einzelnen DDoS-Angriffsstufen. Weitere Einzelheiten befinden sich in den technischen Daten. Mit jeder der Stufen von 1 bis 7 werden größere Anforderungen bezüglich der folgenden Aspekte gestellt:

Level	Bezeichnung	Volumen	RPS	Vektoren
1	Poking, Anklopfen	100 MBit	1000	1
2	ScriptKiddy, Booter-Services	1 GBit	5000	2
3	Basic Level Professionals	100 GBit	10000	5
4	Sophisticated Professionals	500 GBit	100000	10
5	Advanced Professionals	1000 GBit	1 Mio	no limit
6	Extreme Professionals	no limit	no limit	no limit
7	State Sponsored	no limit	no limit	no limit

Mithilfe des DRS haben Organisationen u.a. folgende Möglichkeiten:

Traffic-Volumen: Das Volumen eines DDoS-Angriffsvektors wird in Bit pro Sekunde (BPS), Paketen pro Sekunde (PPS) und Transaktionen pro Sekunde (TPS) gemessen.

Arten von Angriffsvektoren: Mit jeder Stufe werden neben den bereits auf den vorherigen Stufen vorhandenen Angriffsvektoren weitere eingeführt.
Angriffsniveau: Angriffe werden anspruchsvoller und leistungsstärker. Nicht nur in Bezug auf ihren Umfang oder ihre Angriffsvektoren, sondern auch hinsichtlich der inneren Eigenschaften der einzelnen Angriffe. Mit jeder Stufe werden anspruchsvollere Eigenschaften eingeführt, die effektivere Angriffe charakterisieren, z.B. IP-Adressen-Spoofing, URL-Randomisierung usw.
Anforderungen zur Schadensbegrenzung: Eine Organisation, die in der Lage ist, einen Angriff nach zehn Sekunden vollständig zu entschärfen, ist belastbarer als eine, der dies erst nach zehn Minuten möglich ist. Mit jeder Stufe werden Ansprüche auf kürzere Reaktionszeiten gestellt, die anhand des maximalen Ausfalls infolge von Angriffen gemessen werden. Ein weiterer Parameter zur Messung der Belastbarkeit ist die ‘Maximale Latenz’. Diese wird anhand der zusätzlichen Zeit gemessen, die einem durchschnittlichen Paket bei seiner Rundreise im Vergleich zur normalen Zeit, in der kein Angriff erfolgt, zur Verfügung steht.

Der DRS kann je nach Ihrer Rolle auf verschiedene Weise genutzt werden:

1 Organisationen sollten alle relevanten Beteiligten (Assessoren, Berater und interne Teams) dazu anhalten, Ihre Empfehlungen unter Verwendung des DRS-Standards abzugeben. Dies ermöglicht Bewertung und Vergleich von Mitigation-Strategien sowie die Bezifferung von Entscheidungen und Aktivitäten im Laufe der Zeit.

2 Sicherheitsberatern wird nahegelegt, den Standard anzuwenden, um Endkunden einen besseren Service zu bieten, da die Kommunikation erleichtert wird und Erwartungen mit viel weniger Raum für Missverständnisse abgestimmt werden können.

3 Anbieter von DDoS Stresstests, die DDoS-Angriffe simulieren, wird nahegelegt den DRS-Standard zuverwenden, um zu gewährleisten das Tests im Einklang mit einem objektiven Standard erfolgen, der den Vergleich und die Neubewertung zu jedem Zeitpunkt durch andere Bewerter zulässt.