Checkliste für den Kampf gegen DDoS-Erpressung

DDoS-Angriffe (Distributed Denial of Service) nehmen immer mehr zu. Können Sie sich wehren? Unternehmen ohne DDoS-Abwehrstrategie haben zwei Möglichkeiten: Lösegeld zahlen oder einen unerwarteten Ausfall riskieren. Gehen Sie die folgenden Schritte durch, um das Risiko eines erpresserischen DDoS-Angriffs auf Ihr Unternehmen zu minimieren.

1. Zahlen Sie nicht (egal wie verlockend es scheint)

Akamai empfiehlt, den Erpressern kein Geld zu geben. Es besteht keine Garantie, dass der Angreifer seine Drohungen wahr machen kann oder dass eine Zahlung einen DDoS-Angriff verhindern würde. Cyberkriminelle versuchen, die „Angst vor dem Unbekannten" zu nutzen, um schnell Geld zu verdienen, bevor sie das nächste Ziel anvisieren.

2. Bitten Sie Abwehrexperten um Hilfe

Ermitteln Sie, ob Ihre geschäftskritischen Ressourcen und die Backend-Infrastruktur geschützt sind. Wenn Sie keine DDoS-Abwehrkontrollen eingerichtet haben, wenden Sie sich an cloudbasierte Anbieter, die schnell Notfalldienste bereitstellen können, damit sich die Risiken für Sie minimieren (kontaktieren Sie die DDoS-Hotline von Akamai). Unsere globalen SOCC-Spezialisten haben über 20 Jahre Erfahrung im Kampf gegen DDoS-Angriffe.

3. Lassen Sie die DDoS-Spiele beginnen

Mit dem richtigen Abwehrpartner und den richtigen Sicherheitskontrollen haben Angreifer keine Chance. Für Akamai wurden fast alle DDoS-Angriffe im Zusammenhang mit dieser Kampagne proaktiv mit unserem Null-Sekunden-SLA abgewehrt. Nur bei einem geringen Prozentsatz war die aktive Abwehr durch unser globales SOCC erforderlich. Tatsächlich wurden ca. 70 % aller Angriffe, die wir 2020 abgewehrt haben, mit dem Null-Sekunden-SLA von Prolexic vollständig blockiert.

4. Optimieren Sie Ihre Sicherheit

Schon ein einziger Angriff macht deutlich, dass DDoS-Abwehrmaßnahmen in der heutigen Bedrohungslandschaft ein Muss sind. Bewerten Sie Ihre Risikotoleranz, um zu ermitteln, ob eine On-Demand- oder eher eine cloudbasierte Always-on-Abwehrlösung am besten geeignet ist, Ihre Internetpräsenz zu schützen.

5. Werfen Sie einen Blick in Ihr DDoS-Playbook

Wenn Sie es noch nicht getan haben, versammeln und informieren Sie Ihre Mitarbeiter aus den Bereichen IT, Betrieb, Sicherheit und Kundenkommunikation, damit alle auf einen möglichen Angriff vorbereitet sind und wissen, was zu tun ist. Bei Akamai erstellen wir mit jedem Kunden ein individuelles Abwehr-Runbook und führen eine Vielzahl theoretischer Angriffsübungen durch. So wissen die Mitarbeiter jederzeit, wer welche Prozesse und Verfahren einsetzen muss, um die Vorfallsreaktion zu optimieren.

Um die geschäftskritischen Ressourcen von heute am Laufen zu halten, benötigen Unternehmen – sowohl große als auch kleine – Zugang zu hochwertigen Abwehrkontrollen, einer Plattformskalierung und dem nötigen Fachwissen, um DDoS-Angriffskampagnen zu stoppen. Besuchen Sie akamai.com/ddos-briefing, um ein individuelles Briefing zu DDoS-Bedrohungen anzufragen und Informationen zu erhalten, mit denen Sie Ihr Unternehmen schützen können.