Europol und führende Unternehmen in der Sicherheitsbranche sagen Ransomware den Kampf an

Barracuda und AWS sichern NoMoreRansom.org erfolgreich gegen Tausende Angriffe

NO MORE RANSOM!

Die Koalition „No More Ransom“

- Niederländische Polizei im Bereich Hightech-Kriminalität
- Cybercrime Centre von Europol
- Eine zunehmende Zahl an Unternehmen im Bereich Cybersicherheit

www.NoMoreRansom.org

- Gehostet auf Amazon Web Services (AWS)
- Geschützt durch die Barracuda Web Application Firewall in AWS

Herausforderung

Ein Online-Center mit Ressourcen schaffen für Opfer von Cyberkriminalität, das gegen unvermeidliche Angriffe geschützt ist

Lösung

AWS Security mit der Barracuda Web Application Firewall für vollständige Sicherheit bei millionenfachem Zugriff jeden Tag

Ergebnisse

51.000 Angriffe wurden innerhalb weniger Tage verhindert und mehr als eine Million VPN-basierte Attack Requests wurden bis heute identifiziert und geblockt. NoMoreRansom.org wurde noch nie durch Cyberangriffe lahmgelegt.

Im Sommer 2016 wurde eine einzigartige Koalition gebildet, die auf den rasanten Anstieg von Cyberkriminalität, verursacht durch die Verwendung von Ransomware, reagieren sollte. Das Ziel der Koalition „No More Ransom“ unter der Leitung des European Cybercrime Centre von Europol, der niederländischen Polizei, Kaspersky und Intel Security besteht darin, ein zentrales, öffentliches Repository an Wissen und Ressourcen bereitzustellen, das Einzelpersonen und Unternehmen im Kampf gegen Ransomware unterstützt.

Schätzungen von Behörden zufolge belaufen sich die weltweiten Schäden aufgrund von Ransomware im Jahr 2016 auf mehr als 200 Milliarden US-Dollar. Um dagegen anzukämpfen, stellt„No More Ransom“ online Informationen über die neuesten Ransomware-Varianten einschließlich Entschlüsselung-Keys zur Verfügung, die bei früheren Attacken erfolgreich die Daten wiederherstellen konnten.

Die Entscheidung für die Verwendung von AWS

Ein zentraler Bestandteil der Website von„No More Ransom“ ist eine Anwendung, die stichprobenartig von Benutzern übermittelte Daten analysiert, um bestimmte Ransomware zu identifizieren. Auf der Website wird zudem eine stetig größer werdende Datenbank mit Entschlüsselung-Keys gehostet, mit denen die gekaperten Daten wiederhergestellt werden könnten, ohne die Lösegeldforderung zahlen zu müssen. Die Benutzer werden auf der Website zu den Schlüsseln weitergeleitet, die am wahrscheinlichsten für sie infrage kommen. Darüber hinaus sollen Menschen auf der ganzen Welt über die Gefahren von Ransomware und Möglichkeiten für deren Erkennung und Umgehung informiert werden.

> *AWS und Barracuda haben sich voll und ganz für das Projekt eingesetzt. Ihre Teams haben schnell zusammengearbeitet, um die für uns erforderlichen Sicherheitskontrollen zu planen, und sie haben uns gezeigt, wie wir diese Kontrollen ganz problemlos mithilfe der Barracuda Web Application Firewall konfigurieren können.*
>
> ***Steven Wilson***
> *Leiter des European Cybercrime Centre Europol*

Informationen über die Web Application Firewall

Die Barracuda Web Application Firewall blockiert die ständig länger werdende Liste durchdachter webbasierter Eindringversuche und Angriffe, die auf Webservern gehostete Anwendungen zum Ziel haben – sowie die vertraulichen oder geheimen Daten, auf die sie Zugriff haben. Zwischen Internet und Webserver positioniert, scannt die Barracuda Web Application Firewall jeglichen eingehenden Internetdatenverkehr, um Angriffe zu blockieren. Darüber hinaus überprüft sie den ausgehenden Datenverkehr und bietet so einen hohen und effektiven Schutz vor Datenverlusten.

WAF

Barracuda
Web Application Firewall

Die Koalition „No More Ransom" war sich darüber im Klaren, dass die Website, die sie aufbauen wollte, ein unmittelbares und unwiderstehliches Ziel für Cyberangriffe sein würde, wodurch Sicherheit zu einem Hauptanliegen wurde. Cyberkriminelle würden ja nichts lieber tun, als einer Website zu schaden, die speziell auf die Bekämpfung von Cyberkriminalität abzielt und diese für die Infizierung von Besuchern mit Malware zu nutzen.

Nachdem unterschiedliche Optionen in Erwägung gezogen wurden, wurde Amazon Web Services (AWS) für das Hosting der Website ausgewählt. AWS bot neben einer hervorragenden Basissicherheit höchste Agilität und Flexibilität. Ein weiterer Grund für diese Wahl war die einfache Integration der nativen Security von Amazon in die branchenführende Application-Security der Barracuda Web Application Firewall.

Agilität und Sicherheit

Die Entscheidung für den Einsatz der Barracuda Web Application Firewall in AWS hat sich als richtig erwiesen. Am ersten Tag der Live-Schaltung der Website von „No More Ransom" schätzten führende Mitarbeiter der Koalition, dass ca. 12.000 Besucher pro Tag die Website aufrufen werden. Stattdessen wurde die Website bereits am ersten Tag von mehr als 2.6 Millionen Besuchern aufgerufen.

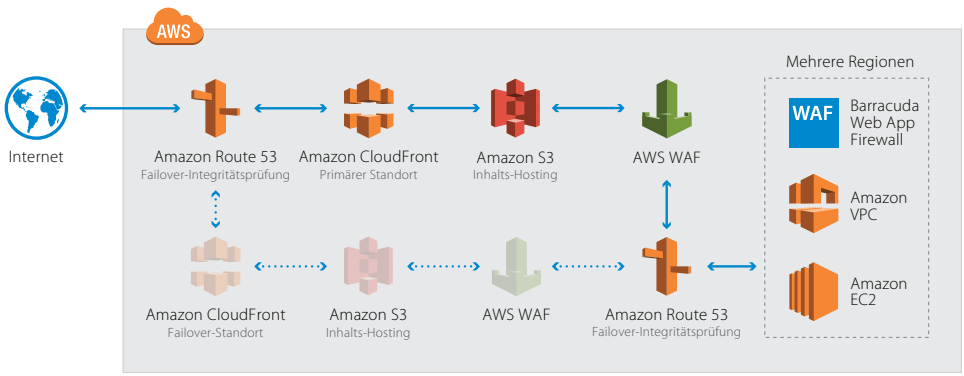
Mit AWS können Ressourcen ganz problemlos angepasst werden, um die unerwartete Nachfrage zu erfüllen, und die Barracuda Web Application Firewall wird automatisch skaliert, um zusätzliche Instanzen bei Bedarf zu schützen – ohne Beeinträchtigung der Leistung.

Ein attraktives Ziel für Cyberkriminelle

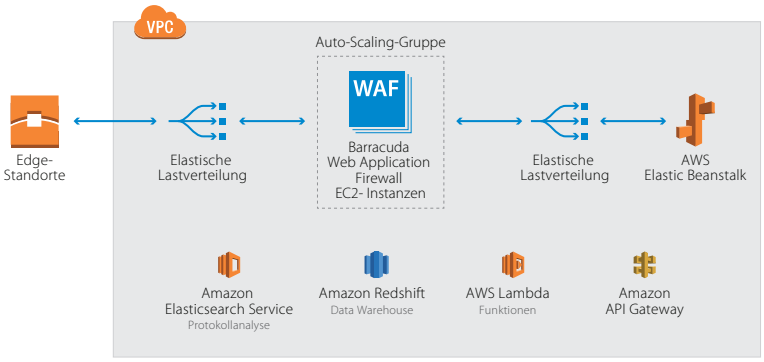
Es war keine Überraschung, dass die Website von „No More Ransom" sofort nach der Live-Schaltung angegriffen wurde. Innerhalb weniger Tage hatte die Barracuda Web Application Firewall mehr als 51.000 Angriffe blockiert, die von standardmäßigen DDoS-Angriffen bis zu ausgefallenen und ausgefeilteren Angriffen auf Teile der Infrastruktur reichten.

Auch VPN-basierte Attack Requests (mit verschleierter Identität) - mehr als eine Million mit steigender Tendenz - wurden erfolgreich identifiziert und blockiert.

Trotz dieser ununterbrochenen Flut von Angriffen – und trotz der enormen Anzahl „anständiger" Besucher – läuft die Website von „No More Ransom" weiterhin reibungslos und wurde noch nie von Angreifern lahmgelegt.



NoMoreRansom.org Edge-Architektur



NoMoreRansom.org Regionale Architektur

Fortlaufender Schutz

Die Initiative „No More Ransom" hat erfolgreich Strafverfolgungs- und Cybersicherheitsressourcen sowie Informationen zusammengestellt, um Einzelpersonen und Unternehmen auf der ganzen Welt beim Kampf gegen Ransomware zu unterstützen. Zukünftig wird die Datenbank der Website immer umfangreicher werden und aller Wahrscheinlichkeit nach immer ausgeklügeltere öffentlich zugängliche Anwendungen aufnehmen.

Während der gesamten Entwicklung und Einführung neuer Anwendungen und Funktionen wird die Barracuda Web Application Firewall verhindern, dass Benutzer durch unerwartete Schwachstellen gefährdet werden. Regelmäßige und bedarfsgesteuerte Schwachstellenüberprüfungen erleichtern den Schutz von Benutzern und optimieren gleichzeitig die Anwendererfahrung beim Kampf gegen Straftaten im Zusammenhang mit Ransomware.

Dieselbe Technologie, die NoMoreRansom.org vor einer Flut von Angriffen schützt, kann auch Ihnen die Sicherheit bieten, die Sie bei der Migration von Anwendungen und Websites zu AWS benötigen. Weitere Informationen erhalten Sie von Ihrem IT-Lösungsanbieter oder unter https://www.barracuda.com/programs/aws/application-security.

Über Barracuda Networks, Inc.

Barracuda (NYSE: CUDA) vereinfacht die IT mit Cloud-Lösungen, mit denen Kunden ihre Netzwerke, Anwendungen und Daten unabhängig von ihrem Speicherort schützen können. Diesen leistungsstarken, benutzerfreundlichen und kostengünstigen Lösungen vertrauen mehr als 150.000 Unternehmen weltweit. Die Implementierung erfolgt in Appliance-, virtuellen Appliance-, Cloud- und Hybrid-Bereitstellungen. Mit seinem kundenorientierten Geschäftsmodell konzentriert sich Barracuda auf die Bereitstellung hochwertiger, abonnementbasierter IT-Lösungen, die umfassende Netzwerk- und Datensicherheit bieten. Weitere Informationen erhalten Sie unter barracuda.com.