LINK11

CASE STUDY

WISAG

www.link11.com

WISAG Case Study

DDoS-Schutz für Firmennetzwerke und VPN: Sicherer Zugriff von allen Standorten

Wer ist die WISAG?

Das Kerngeschäft der WISAG sind vielfältige Dienstleistungen für Büro-, Gewerbe-, und Wohnimmobilien, für die Industrie sowie für Fluggesellschaften und Flughäfen. Die Geschäftsbereiche und Produktwelten werden zunehmend durch digitale Technologien unterstützt und erweitert. Das Unternehmen verfügt über rund 1.400 Standorte, die per VPN (Virtual Private Network) mit der Zentrale verbunden sind, um auf die Internetanbindung, Software und Dokumente zuzugreifen.

Was war die Problemstellung und die Aufgabe?

Im Rahmen einer Neuausrichtung der zentralen IT Infrastruktur wechselte man von einem gemanagten VPN zu IP-VPN, das neben mehr Flexibilität und einer höheren Abdeckung auch geringere Betriebskosten bedeutet. Das Netzwerk, für das von den Außenstandorten zur Zentrale VPN-Tunnel aufgebaut werden, wird vom IT-Team der WISAG in Eigenregie betrieben. Damit liegt auch die Absicherung gegen Angriffe auf die Internetanbindung in der Verantwortung des Unternehmens. Der Anspruch lautet dabei: Die zentrale Infrastruktur hochverfügbar machen, damit Remote-Mitarbeiter arbeitsrelevante Dokumente rund um die Uhr abrufen können und die Betriebssteuerung störungsfrei läuft – in allen der zahlreichen Dienstleistungsbereiche des Unternehmens. So beschreibt Michael Futterer, Leiter Informationssysteme bei der WISAG, die Anwendungsbereiche. Aber auch der Datenaustausch zwischen den verschiedenen Standorten der WISAG erfolgt über VPN und muss ständig verfügbar sein. Das VPN-Gateway ist dabei wie ein Nadelöhr zu sehen, das durch Angriffe gezielt überlastet werden kann. Angreifer können die verfügbare Bandbreite oder Ressourcen aufbrauchen, mit dem Ergebnis, dass keine Daten mehr zwischen dem Firmennetzwerk und den Außenstandorten ausgetauscht werden können.

„Die zentrale Infrastruktur hochverfügbar machen, damit Remote-Mitarbeiter arbeitsrelevante Dokumente rund um die Uhr abrufen können und die Betriebssteuerung störungsfrei läuft“

Michael Futterer,
Leiter Informationssysteme

Was wurde benötigt?

Angesichts der zunehmenden Cyberrisiken hat das Unternehmen proaktiv nach einem Schutz seiner zentralen Firmeninfrastruktur gesucht, um etwaige Angriffe frühzeitig zu erkennen und Betriebsunterbrechungen zu verhindern.

Die beste Absicherung gegen diese Ausfälle der geschäftskritischen Komponente stellte nach Einschätzung der WISAG eine Lösung gegen Distributed-Denial-of-Service-Angriffe (kurz: DDoS-Angriffe) dar. Schädlicher DDoS-Datenverkehr wird dabei erkannt und mitigiert, was Überlastungen in der VPN-Verbindung verhindert. Dafür wird ein kundenspezifisches Datenverkehrsprofil erstellt, anhand dem der ankommende Datenverkehr automatisiert als gutartig oder bösartig identifiziert wird. Nur der gewünschter Traffic fließt an das Kundennetzwerk weiter. Technisch wird dem VPN-Gateway für die Analyse des Datenverkehrs ein DDoS-Filtercluster sowie die Router eines externen Schutzanbieters vorgeschaltet.

Warum fiel die Entscheidung auf Link11?

Bei der Entscheidung für den DDoS-Schutz durch Link11 spielten neben den technischen Möglichkeiten und der Zuverlässigkeit der Schutzlösung auch Betreuung und Kommunikation eine große Rolle. Gute und schnelle Erreichbarkeit, kompetente Ansprechpartner und muttersprachlicher Support gehören zu den Dienstleistungsversprechen, in denen sich die WISAG selbst wiederfindet. Auch der Umstand, dass es sich beim Schutzanbieter um ein deutsches Unternehmen handelt, zählte dazu, so Futterer. Das erleichterte es, schnell ein Vertrauensverhältnis zu schaffen, das besonders wichtig ist, wenn es sich bei der IT-Sicherheit um ein zentrales Thema des Geschäftsbetriebs handelt. So begann Anfang 2020 eine konstruktive Partnerschaft.

Welche Erfahrungen wurden gemacht?

Im Rahmen der Zusammenarbeit während des Implementierungsprozesses aufgetretene unvorhergesehene Schwierigkeiten konnten aufgrund der guten Beziehung schnell, unkompliziert und nachhaltig gelöst werden. So wurde seitens Link11 generell die Unterstützung der Kunden bei der Einbindung der Lösung in die bestehende Infrastruktur über die Standardprozesse hinaus noch weiter ausgebaut. Je vorausschauender Kunden über technische Anforderungen an ihre Infrastruktur informiert sind, desto effizienter können die Prozesse laufen, bilanziert der IT-Leiter der WISAG. Link11 hat aus dieser Erfahrung die Einbeziehung von Experten aus dem eigenen Network Operations Center zum festen Bestandteil seines Onboardings bei Kunden gemacht.

„Link11 gibt uns ein gutes Sicherheitsgefühl“

Michael Futterer,
Leiter Informationssysteme

Letztendlich konnte die Integration des Link11 Infrastruktur-DDoS-Schutzes erfolgreich abgeschlossen werden, der Schutz ist aktiv und das Netzwerk der WISAG zuverlässig gegen Angriffe abgesichert. Die Filterung des Datenverkehrs erfolgt dank moderner Technologien wie maschinellem Lernen und vollständiger Automatisierung in Echtzeit und verhindert so menschliche Fehler bei der Erkennung und Abwehr von Angriffen. Auch neue, bisher nicht aufgetretene Angriffsmuster werden in Sekundenbruchteilen abgewehrt. „Eine überzeugende Sache“, findet Futterer. Das sorgt für eine effiziente Risikominimierung von DDoS-Attacken und entlastet das IT-Team der WISAG in seiner Arbeit. „Link11 gibt uns ein gutes Sicherheitsgefühl“, so Futterer. Zudem haben er und sein Team mit dem Link11 Online-Dashboard den Netzwerkverkehr und mögliche Anomalien immer im Blick.

Für die WISAG haben sich auch die Erwartungen an die Kommunikation mit dem DDoS-Schutzanbieter erfüllt. Falls man Fragen habe, liefere Link11 eine schnelle Antwort, so der IT-Leiter. Wichtige Informationen zum Netzwerkbetrieb fließen zudem proaktiv.

Was lässt sich zusammenfassend sagen?

Das Fazit über die bisherige Zusammenarbeit fällt entsprechend positiv aus: „Unser Netzwerk ist gegen DDoS-Attacken nun umfassend abgesichert“, bilanziert Futterer. Damit könne man sich beruhigt anderen Themen zuwenden. Er ist sich sicher, dass der Schutz außerdem eine abschreckende Wirkung hat. Zeigt er möglichen Angreifern doch, dass sich das Unternehmen ernsthaft mit dem Thema beschäftigt hat und ein Angriff voraussichtlich nichts bringen wird.

Link11 GmbH | Lindleystr. 12 | 60314 Frankfurt | info@link11.com | +49 69 26492977