Südtiroler Informatik AG
Informatica Alto Adige SPA

Marktrecherche für den Ankauf eines Schutzdienstes gegen DDoS-Angriffe für Telecom-Internetverbindungen

Dokument für die Marktrecherche

Südtiroler Informatik AG, Werner-Von-Siemens-Straße 29
39100 Bozen
PEC: supply@pec.siag.it
http://www.siag.it

Bozen

VORWORT

Die Südtiroler Informatik AG (nachfolgend SIAG) erbringt IT-Dienstleistungen für die Provinz Bozen über ihre beiden Data Center in Bozen und Bruneck. Jedes Data Center ist mit einer hochgradig redundanten Internet-Konnektivität ausgestattet und durch modernste Firewall- und IPS-Technologien geschützt, um die Nutzung der eigenen Dienste auch über das Internet und nicht nur über das Landes-Intranet zu ermöglichen.

DDoS-Angriffe stellen ein erhebliches Risiko für das Netz und die Verfügbarkeit der Anwendungen dar. Herkömmliche Sicherheitslösungen auf Perimeter-Ebene, wie Firewalls und IPS (Intrusion Prevention System), lösen dieses Problem nicht, sondern werden selbst zum Ziel von DDoS-Angriffen.

Um Bedrohungen der Verfügbarkeit gezielt entgegenzuwirken, ist ein DDoS-Mitigationssystem erforderlich.

Die vorliegende Markterhebung im Rahmen der Ankaufs des **„Dienstes zum Schutz vor DDoS-Angriffen für Telecom-Internetverbindungen“** gemäß den Art. 25 des L.G. 16/2015 in geltender Fassung und Art. 77 des GvD Nr. 36/2023 verfolgt das folgende Ziel:

- bestmögliche Bekanntmachung der Initiative und eine möglichst umfassende Verbreitung der Informationen zu gewährleisten;
- die bestmögliche Beteiligung aller betroffenen Akteure zu haben und die tatsächliche Existenz mehrerer interessierter Wirtschaftsteilnehmer zu überprüfen;
- die qualitativen und technischen Merkmale der zu analysierenden Waren und Dienstleistungen dieser Marktrecherche optimal bekanntzumachen;
- Stellungnahmen und Anregungen der betroffenen Akteure zur Erlangung einer besseren Marktübersicht zu erhalten.

Es wird darauf hingewiesen, dass für die betreffende Lieferung/Dienstleistung, für die technischen Spezifikationen, die aufgrund der besonderen Anforderungen zu erfüllen sind, eine Situation der Nichtzulässigkeit im Sinne der ANAC-Leitlinien Nr. 8 für die Anwendung von Verhandlungsverfahren ohne vorherige Veröffentlichung einer Bekanntmachung vorliegt. Gemäß den Bestimmungen derselben Leitlinien ist Folgendes zu beachten:

- die Anforderungen und die Mittel, um diese zu erfüllen, finden Sie in Punkt 1 "Anforderungen" dieses Dokuments;

- die voraussichtlichen Gesamtkosten für den Erwerb der Lieferung/Dienstleistung können grob auf € 184.000,00 ohne MwSt. geschätzt werden, wie in Punkt 2 "Erwartete Kosten" dieses Dokuments angegeben;
- der Auftraggeber wird alle vernünftigen Alternativlösungen bewerten, die im Zusammenhang mit den bereitgestellten Beiträgen vorgeschlagen werden;
- die eventuelle Vergabe - wenn nach Abschluss der Beweisaufnahme festgestellt wird, dass die entsprechenden Voraussetzungen gegeben sind und daher die eventuell vorgeschlagenen vernünftigen Alternativlösungen als nicht durchführbar angesehen werden - erfolgt gemäß Artikel 25 L.P. 16/2015 i.g.F. und 76 des Gesetzesdekrets Nr. 36/2023.

Bitte senden Sie Ihren unentgeltlichen Beitrag – nach vorhergehender Einsicht der unten angeführten Datenschutzerklärung – mittels Zusendung des ausgefüllten Fragebogens innerhalb **24.04.2026** an die zertifizierte E-Mail-Adresse supply@pec.siag.it**.**

Alle Informationen, die Sie mit diesem Dokument liefern, werden ausschließlich im Rahmen der Ziele der gegenständlichen Initiative verwendet.

Bitte geben Sie an, ob Ihre Beiträge Informationen und/oder Daten enthalten, die durch Patentrechte geschützt sind oder andere Geschäfts-, Handels- oder Betriebsgeheimnisse offenbaren, sowie sonstige vertrauliche Informationen darlegen, die Rückschlüsse auf Ihre Marktposition und/oder Ihr Fachwissen in dem von dieser Marktrecherche erfassten Tätigkeitsbereich zulassen.

Da auch andere Wirtschaftsteilnehmer Zugang zu den Ergebnissen dieser Marktrecherche haben könnten, möchten wir Sie außerdem bitten anzugeben, ob die in Ihren Beiträgen enthaltenen Informationen in anonymer Form veröffentlicht werden sollen.

Die Zustellung des Dokuments an unsere Adresse beinhaltet die Einwilligung zur Verarbeitung der gelieferten Daten.

Bozen,

Südtiroler Informatik AG
Informatica Alto Adige SPA

Daten des Unternehmens

Name des Unternehmens
St.-Nr.
MwSt-Nr.
Adresse
PEC
Name und Nachname Ansprechperson
Rolle im Unternehmen
Telefon
Fax
E-Mail

DATENSCHUTZERKLÄRUNG NACH ART. 13 DER VERORDNUNG (EU) 2016/679

Gemäß den Artikeln 13 ff. der GDPR - EU-Verordnung 2016/679 sind Sie eingeladen, die Informationen unter folgendem Link einzusehen: https://assets-eu-01.kc-usercontent.com/482bf257-c7e4-01f3-0b5d-5f9ff7229638/47dea7fd-fa1b-4840-b1f3-f0aa1a02f787/informativa-supply-siag-de.pdf.

Kurze Beschreibung der Initiative

SIAG verfügt über ein aktives System zur Mitigation von DDoS-Angriffen auf ihren Internetanbindungen, über die Dienstleistungen für ihre Kundinnen und Kunden bereitgestellt werden, und muss die vertragliche Erneuerung dieses Dienstes vorbereiten.
Die wirksamste Abwehr gegen DDoS-Angriffe kann aufgrund ihrer Natur ausschließlich durch den Schutz der Übertragungsressourcen gewährleistet werden, welche die Internet-Konnektivität bereitstellen. Im Fall von DDoS-Angriffen ist der Schutz umso effektiver, je näher er an den Quellen der Angriffe und damit möglichst weit entfernt von den Zielsystemen umgesetzt wird.

1. Anforderungen

Der von SIAG gesuchte Dienst zum Schutz vor DDoS-Angriffen muss auf verteilten Plattformen basieren, die in den Data Centern und in den Zugangsnetzen des Anbieters vorhanden sind, ohne dass beim SIAG vor Ort dedizierte Geräte für den Dienst installiert oder architektonische Anpassungen an der Infrastruktur der SIAG vorgenommen werden müssen.
Insbesondere wird gefordert, dass der Internetverkehr der SIAG unter normalen Bedingungen keiner Umleitung unterzogen wird und direkt zum Upstream-Provider fließt, um die Kompatibilität des Dienstes

mit der bestehenden Netzarchitektur zu gewährleisten, den getätigten Investitionen Rechnung zu tragen und da diese Architektur für ein direktes Routing zu den Upstream-Providern mit bereits optimierten und im Betrieb getesteten Flüssen ausgelegt und dimensioniert wurde. Diese Infrastrukturen müssen in der Lage sein, den auf die Data Center der SIAG gerichteten Verkehr kontinuierlich zu überwachen und **erst bei Anomalien** eingreifen zu können, indem sie den Verkehr zu Appliances umleiten, die in der Lage sind, legitime Verbindungen zu filtern und als schädlich eingestufte Sessions auszusortieren.

Aus diesem Grund ist dem Verkehrsfluss besondere Aufmerksamkeit zu widmen. Dieser wird zum Autonomous System des Betreibers (AS 3269) angekündigt, soll dem normalen Weg ins Internet folgen und **nur im Fall eines DDoS-Angriffs** zu den Scrubbing-Centern umgeleitet werden.

Die vorgeschlagene Lösung muss Folgendes ermöglichen:

- **Analyse** des aus dem Internet kommenden Verkehrs in Echtzeit;
- **Erkennung** eventueller Unregelmäßigkeiten im Verkehr;
- **Mitigation** der festgestellten Unregelmäßigkeiten durch Eliminieren des schädlichen Verkehrs.

Sie muss außerdem in der Lage sein, die wichtigsten Arten volumetrischer DDoS-Angriffe zu mitigieren, wie die folgende – nicht abschließende – Liste beschreibt:

- **ICMP-Flood-Angriffe:** Diese Angriffe nutzen offene oder falsch konfigurierte Server aus, um große Datenmengen an das Ziel zu senden und dadurch die Intensität des Angriffs zu verstärken (z. B. mittels DNS, NTP, SNMP).
- **UDP-Flood-Angriffe:** Diese Angriffe beinhalten das massenhafte Senden von UDP-Paketen (User Datagram Protocol) an ein Ziel, häufig unter Verwendung von Port-Scanning oder anderen Techniken, um verwundbare Dienste zu identifizieren und auszunutzen.
- **Amplification-Angriffe:** Diese Angriffe nutzen offene oder falsch konfigurierte Server aus, um große Datenmengen an das Ziel zu senden und so die Intensität des Angriffs zu verstärken. Einige Beispiele für Protokolle, die für Amplification-Angriffe verwendet werden, sind DNS (Domain Name System), NTP (Network Time Protocol) und SNMP (Simple Network Management Protocol).
- **SYN-Flood-Angriffe:** SYN-Flood-Angriffe nutzen das TCP-Protokoll (Transmission Control Protocol), indem eine große Anzahl unvollständiger SYN-Verbindungsanfragen an ein Ziel gesendet wird,

wodurch die Ressourcen des Servers überlastet und der legitime Zugang für Benutzerinnen und Benutzer verhindert wird.

- **HTTP/HTTPS-Reflection/Amplification-Angriffe:** Diese Angriffe nutzen offene Webserver aus, um den Verkehr zum Ziel zu reflektieren und zu verstärken, indem fehlerhafte oder manipulierte HTTP/HTTPS-Anfragen verwendet werden.
- **DNS-Reflection/Amplification-Angriffe:**
  Diese Angriffe nutzen offene oder falsch konfigurierte DNS-Server aus, um den Verkehr zum Ziel zu reflektieren und zu verstärken, indem fehlerhafte oder manipulierte DNS-Anfragen ausgenutzt werden.

Der Dienst muss außerdem die folgenden Merkmale aufweisen:

- Fähigkeit zum Bereinigen von Verkehrsvolumen bis zu 10 Gbps
- Unbegrenzte Anzahl an Mitigations
- Punktgenauer Schutz bis hin zur einzelnen IP (auch innerhalb größerer Subnetze)
- Incident Report innerhalb NBD nach Deaktivierung der Diversion
- Breite Auswahl an Serviceprofilen, um mögliche zukünftige Optimierungen zu ermöglichen
- 24x7-Unterstützung mit technischem Support in italienischer Sprache, erbracht aus Italien

Der Anbieter muss den Dienst **proaktiv** durch ein kontinuierliches Monitoring erbringen und – im Fall der Feststellung von Verkehrsanomalien, die auf DDoS-Angriffe zurückzuführen sind – SIAG informieren, um deren Genehmigung für das Einleiten von Eindämmungsmaßnahmen (Anwendung der Diversion) einzuholen. Während der gesamten Dauer des Angriffs wird das Personal des Anbieters fortlaufend mit der Überwachung seiner Entwicklung beauftragt sein.
Die Diversion muss nach Bestätigung von SIAG deaktiviert werden, sobald der Anbieter über das Ende des Angriffs berichtet. Der Anbieter muss SIAG bei jedem Statuswechsel der Dienstkonfiguration informieren.

2. Erwartete Kosten

Die voraussichtlichen Kosten belaufen sich auf 60.000,00 € zuzüglich einer einmaligen Aktivierungsgebühr von 4.000,00 € zzgl. MwSt. für die ersten 12 Monate. Darüber hinaus ist eine optionale Verlängerung um zwei weitere Jahre vorgesehen, die in 12-Monats-Schritten (2. Jahr + 3. Jahr) zu einem Preis von 60.000,00 € zzgl. MwSt. pro zusätzlichem Jahr aktiviert werden kann. Auf der Grundlage der Vorschläge, welche von den an dieser Marktrecherche teilnehmenden Unternehmen eintreffen werden, und unabhängig von den oben genannten Schätzungen, wird die Südtiroler Informatik AG ein Kaufverfahren in Übereinstimmung

mit den Ergebnissen der Umfrage anstrengen, um ein Ergebnis zu erhalten, das ihren Bedürfnissen so gut wie möglich entspricht.

In diesem Zusammenhang ist anzumerken, dass, sobald das Ergebnis dieser Umfrage vorliegt und die in die gemäß Art.25 L. P 16/2015 i.g.F. und 76 des D.Lgs. n. 36/2023 genannten Bedingungen erfüllt sind, die Südtiroler Informatik A.G. sich das Recht vorbehält, den Ankauf als Verhandlungsverfahren ohne Veröffentlichung der Mitteilung fortzusetzen.

Fragen

1. Wie hoch ist der durchschnittliche Jahresumsatz, den das Unternehmen im letzten Zweijahreszeitraum mit dem Verkauf von Anti-DDoS-Schutzdiensten erzielt hat, sowohl auf dem italienischen Markt allgemein als auch speziell im Markt der Öffentlichen Verwaltung?

Antwort:

_____
_____
_____
_____

2. Es wird darum gebeten, die bisherigen und wichtigsten Lieferungen von Anti-DDoS-Schutzdiensten des Unternehmens aufzulisten und deren wesentliche Merkmale zu beschreiben.

Antwort:

_____
_____
_____
_____

3. Beschreibung des Referenzmarktes, der Kundinnen und Kunden sowie der abgedeckten Marktsegmente.

Antwort:

_____
_____
_____
_____

4. Beschreibung der Vertriebsmodalitäten auf dem Markt, Beschreibung der Lieferkette und Angabe, auf welchem Weg das Produkt bzw. der Dienst auf den Markt gelangt (Direktvertrieb, Distributoren, Retail usw.).

Antwort:

_____
_____
_____
_____

5. Welche Stärken weist das Unternehmen im Vergleich zur Konkurrenz auf?

Antwort:

_____
_____
_____
_____

6. Über welche Qualitäts-, Prozess-, Umwelt- usw. Zertifizierungen verfügt Ihr Unternehmen? Welche Elemente Ihrer Produkte und Dienstleistungen werden durch diese Zertifizierungen aufgewertet? Warum?

Antwort:

_____
_____
_____
_____

7. In welcher vertraglichen Rolle beabsichtigt das Unternehmen teilzunehmen? Bitte angeben, ob die Teilnahme als Hersteller, als Vertriebspartner, mit Exklusivität oder ohne Exklusivität erfolgen soll. Für den Fall einer Teilnahme aufgrund exklusiver Rechte muss der Lieferant den Nachweis über das exklusive Recht erbringen (siehe Anlage).
Im Fall einer Teilnahme als Vertriebspartner wird das Unternehmen aufgefordert, Nachweise über eventuelle kommerzielle Vereinbarungen mit dem Hersteller hinsichtlich Verkauf/Vertrieb, Wartung und der damit verbundenen Dienstleistungen in Bezug auf die benötigten Lizenzen vorzulegen.

Antwort:

_____
_____
_____
_____

8. Durchschnittlich angewandte Preisbedingungen (Listenpreise, Art der gewährten Rabatte für Lizenzen, Wartung sowie Preise und Rabatte für alle angefragten Dienstleistungen), detailliert für jeden im vorherigen Kapitel 1 – Bedarf aufgeführten Punkt.

Antwort:

_____
_____
_____
_____

Unterschrift Lieferant

_____