Südtiroler Informatik AG
Informatica Alto Adige SPA

Marktrecherche für den Ankauf von einem Dienst zum Schutz vor DDoS-Angriffen 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

Südtiroler Informatik AG (im Folgenden SIAG) erbringt IT-Dienstleistungen für die Provinz Bozen über ihre beiden Datenzentren in Bozen und Bruneck. Jedes Rechenzentrum ist mit einer hochredundanten Internetanbindung ausgestattet und durch modernste Firewall- und IPS-Technologien geschützt, um die Nutzung der Dienste auch über das Internet und nicht nur über das Intranet der Provinz zu ermöglichen.
DDoS-Angriffe stellen ein großes Risiko für das Netzwerk und die Verfügbarkeit von Anwendungen dar. Herkömmliche Perimeter-Sicherheitslösungen wie Firewalls und IPS (Intrusion Prevention Systems) lösen das Problem nicht, sondern sind selbst Ziel von DDoS-Angriffen.
Um den Verfügbarkeitsbedrohungen gezielt zu begegnen, ist es notwendig, die Sicherheitsinfrastruktur der IAA mit einem DDoS Mitigation System zu integrieren.
Die vorliegende Marktrecherche im Rahmen des Kaufs von einem Dienst zum Schutz vor DDoS-Angriffen für Telecom-Internetverbindungen bezieht sich auf die Notwendigkeit:

- die Initiative so gut wie möglich bekannt zu machen, um eine möglichst weite Verbreitung der Informationen zu gewährleisten;
- eine möglichst fruchtbare Beteiligung der interessierten Kreise zu erreichen und die tatsächliche Existenz mehrerer interessierter Wirtschaftsteilnehmer zu überprüfen;
- die qualitativen und technischen Merkmale der untersuchten Waren und Dienstleistungen so weit wie möglich bekannt zu machen;
- Entgegennahme von Kommentaren und Vorschlägen der interessierten Kreise, um eine bessere Kenntnis des Marktes zu erhalten.

Gemäß Art. 25 L.P. 16/2015 i.g.F. und Art. 77 des Gesetzesdekrets Nr. 36/2023 verfolgt diese Marktrecherche folgendes 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 € 210.000,00 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 **07.06.2024** 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, _____

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

Die SIAG benötigt ein System zur Eindämmung von DDoS-Angriffen auf ihre Internetverbindungen, über die sie ihren Kunden Dienstleistungen anbietet.
Die wirksamste Bekämpfung von DDoS-Angriffen kann naturgemäß nur durch den Schutz der Übertragungsressourcen erreicht werden, die die Internetverbindung bereitstellen. Im Falle von DDoS-Angriffen ist der Schutz umso wirksamer, je näher er an den Quellen der Angriffe und damit von den Zielen entfernt implementiert wird.

1. Anforderungen

Der von der SIAG angestrebte Schutzdienst gegen DDoS-Angriffe muss auf verteilten Plattformen basieren, die in den Rechenzentren und Zugangsnetzen des Anbieters vorhanden sind, ohne dass in den Räumlichkeiten der SIAG spezielle Geräte für diesen Dienst hinzugefügt werden müssen und ohne dass architektonische Änderungen an der Infrastruktur der SIAG vorgenommen werden müssen. Diese Infrastrukturen müssen in der Lage sein, den an die SIAG-Rechenzentren gerichteten Verkehr ständig zu überwachen, und nur im Falle von Anomalien die Möglichkeit haben, einzugreifen, indem sie den Verkehr

zu Geräten umleiten, die in der Lage sind, rechtmäßige Verbindungen zu filtern und als bösartig angesehene Sitzungen umzuleiten.
Aus diesem Grund muss dem Verkehrsfluss besondere Aufmerksamkeit gewidmet werden, der in Richtung des autonomen Systems des Betreibers (AS 3269) angekündigt wird, dem normalen Fluss in Richtung Internet folgen muss und nur im Falle eines DDoS-Angriffs in Richtung der Scrubbing-Zentren umgeleitet wird.

Die vorgeschlagene Lösung muss Folgendes ermöglichen

- **Analyse** des aus dem Internet kommenden Datenverkehrs in Echtzeit;
- **Erkennung** von Anomalien im Datenverkehr;
- **Entschärfung** der festgestellten Anomalien durch Beseitigung des bösartigen Datenverkehrs.

Sie muss auch in der Lage sein, die wichtigsten Arten von volumetrischen DDoS-Angriffen zu entschärfen, die in der folgenden Liste beschrieben sind, z. B:

- **ICMP-Flood-Angriffe**: Bei diesen Angriffen wird das Internet Control Message Protocol (ICMP) ausgenutzt, um eine große Anzahl von ICMP-Paketen zu senden, wodurch die Bandbreite überlastet und Netzwerkressourcen verbraucht werden.
- **UDP-Flood-Angriffe**: Bei diesen Angriffen wird eine große Anzahl von UDP-Paketen (User Datagram Protocol) an ein Ziel gesendet, wobei häufig Port-Scans oder andere Techniken eingesetzt werden, um anfällige Dienste zu identifizieren und auszunutzen.
- **Amplifikationsangriffe**: 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. Beispiele für Protokolle, die für Amplifikationsangriffe 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 Transmission Control Protocol (TCP) aus, indem sie eine große Anzahl unvollständiger SYN-Verbindungsanfragen an ein Ziel senden, wodurch die Serverressourcen überlastet werden und der legitime Zugriff der Benutzer verhindert wird.
- **HTTP/HTTPS-Reflection/Amplification-Angriffe:** Diese Angriffe nutzen offene Webserver aus, um den Datenverkehr zum Ziel zu reflektieren und zu verstärken, indem sie missgestaltete oder manipulierte HTTP/HTTPS-Anfragen verwenden.

- **DNS-Reflexions-/Verstärkungsangriffe:** Diese Angriffe nutzen offene oder falsch konfigurierte DNS-Server aus, um den Datenverkehr zum Ziel zu reflektieren und zu verstärken, indem sie missgebildete oder manipulierte DNS-Anfragen ausnutzen.

Der Dienst muss außerdem die folgenden Merkmale aufweisen

- Kapazität zur Bereinigung von Verkehrsvolumen von 2 Gbit/s
- Große Auswahl an Granularität der gesäuberten/wiederhergestellten Bandbreite, um eine mögliche künftige Optimierung von bis zu 10 Gbps gesäuberter Bandbreite vorhersehen zu können
- Unbegrenzte Anzahl von Entschärfungen
- Punkt-für-Punkt-Schutz bis hin zu einer einzelnen IP (auch innerhalb größerer Subnetze)
- Vorfallsbericht innerhalb von NBD bei Deaktivierung der Umleitung
- Große Auswahl an Service-Profilen, um mögliche zukünftige Optimierungen vorhersehen zu können
- Unterstützung h24x7 mit technischem Support in italienischer Sprache von Italien aus

Der Lieferant erbringt den Dienst proaktiv durch ständige Überwachung und informiert bei Feststellung von Verkehrsanomalien, die auf DDoS-Angriffe hinweisen, die SIAG, um deren Genehmigung zur Durchführung von Eindämmungsmaßnahmen (Anwendung von Umleitungen) einzuholen. Während der gesamten Dauer des Angriffs wird das Personal des Lieferanten dessen Entwicklung ständig überwachen. Die Umleitung wird deaktiviert, sobald die SIAG die Rückkehr des Angriffs durch den Lieferanten bestätigt. Der Lieferant muss die SIAG stets über jede Änderung des Status der Dienstkonfiguration informieren. Darüber hinaus wird die Bewertung eines möglichen anderen wirtschaftlichen Wertes des Dienstes für den Fall verlangt, dass die SIAG im Falle eines vermuteten Angriffs ohne Bestätigung durch das SIAG-Personal außerhalb der üblichen Arbeitszeiten (Samstage, Sonntage, Feiertage und von Montag bis Freitag in den Abendstunden von 17:30 Uhr bis 8:00 Uhr des folgenden Morgens) die selbständige Anwendung von Gegenmaßnahmen durch den Lieferanten verlangt.

2. Erwartete Kosten

Die voraussichtlichen Kosten belaufen sich auf 70.000,00 € zzgl. MwSt. für 12 Monate. Es gibt auch eine optionale Verlängerung für zwei weitere Jahre, die in 12-Monats-Tranchen (2. Jahr + 3. Jahr) zu Kosten von 70.000,00 € zzgl. MwSt. für jedes weitere 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 in den letzten zwei Jahren mit dem Verkauf von DDoS-Schutzdiensten sowohl auf dem italienischen Markt als auch speziell auf dem Markt der öffentlichen Verwaltung erzielt hat?

Antwort:

_____
_____
_____
_____

2. Bitte führen Sie die bisherigen und wichtigsten DDoS-Schutzdienste des Unternehmens auf und beschreiben Sie deren Hauptmerkmale.

Antwort:

_____
_____
_____
_____

3. Beschreiben Sie den Zielmarkt, wer die Kunden sind und welche Marktsegmente abgedeckt werden.

Antwort:

_____
_____
_____
_____

4. Beschreiben Sie, wie das Produkt/die Dienstleistung auf den Markt kommt (Direktverkauf, Vertriebshändler, Einzelhandel usw.)

Antwort:

_____
_____
_____
_____

5. Was sind die Stärken im Vergleich zur Konkurrenz?

Antwort:

_____
_____
_____
_____

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

Antwort:

_____
_____
_____
_____

7. In welcher vertraglichen Eigenschaft beabsichtigt das Unternehmen, sich zu beteiligen? Geben Sie an, ob Sie beabsichtigen, als Hersteller, Händler, mit oder ohne Ausschließlichkeitsrecht teilzunehmen. Im Falle einer Teilnahme auf der Grundlage ausschließlicher Rechte muss der Lieferant das ausschließliche Recht nachweisen. Im Falle einer Teilnahme als Händler wird das Unternehmen aufgefordert, Nachweise für Geschäftsvereinbarungen mit dem Hersteller über den Verkauf/Vertrieb, die Wartung und damit verbundene Dienstleistungen für die Lizenzen, die Gegenstand der Anforderung sind, vorzulegen?

Antwort:

_____
_____
_____
_____

8. Durchschnittliche Preiskonditionen (Listenpreise, Art der Rabatte für Lizenzen, Wartung, Preise und Rabatte für alle erforderlichen Dienstleistungen) für jede in Kapitel 1 - Anforderungen aufgeführte Anforderung?

Antwort:

_____
_____
_____
_____

Unterschrift Lieferant

_____