ตลาดหลักทรัพย์แห่งประเทศไทย

ประกาศเชิญชวนประกวดราคา

โครงการจัดหาบริการ Web Application Firewall และ DDoS Protection

ตลาดหลักทรัพย์แห่งประเทศไทย (“ตลาดหลักทรัพย์”) มีความประสงค์คัดเลือกผู้ประกอบกิจการให้บริการ Web Application Firewall และ DDoS Protection (“ผู้เสนองาน”) โดยมีรายละเอียดข้อมูลโครงการฯ ขอบเขตงานตามสัญญา คุณสมบัติของผู้ยื่นข้อเสนองาน กำหนดการและข้อมูลอื่นที่เกี่ยวข้องตามที่แสดงไว้ในข้อกำหนดและขอบเขตของงาน (Term of Reference) (ซึ่งต่อไปในเอกสารนี้จะเรียกว่า “ข้อกำหนดการเสนองาน”)

ข้อกำหนด

1. งานตามสัญญา

1.1 ความต้องการด้านเทคนิค

1) เป็นระบบที่ให้บริการ Web Application Firewall (WAF) และ DDoS Protection รวมถึงบริการ Content Delivery Network (CDN) ในรูปแบบ Global Cloud Platform (Always-on mode) เพื่อป้องกันการโจมตี Web Application และ DDoS ไปยังเว็บไซต์โดยเฉพาะ และสามารถป้องกันการโจมตีอัตโนมัติได้ตลอด 24 ชั่วโมง ไม่จำกัดจำนวนครั้ง และขนาดของการโจมตี
2) ผู้เสนอให้บริการจะต้องเป็น Leader ของ Gartner ด้าน Web Application Firewall ปี 2021 หรือเป็นกลุ่ม Leader ของ The Forrester Wave DDoS Mitigation Solutions ปี 2021
3) ระบบที่ให้บริการจะต้องได้รับรองมาตรฐาน PCI-DSS, ISO 27001 และ SOC 2 Type II เป็นอย่างน้อย (โปรดระบุ)
4) สามารถป้องกันเว็บไซต์ให้ตลาดหลักทรัพย์ อย่างน้อย 20 Domains
5) สามารถรองรับการใช้งานสำหรับ Clean Bandwidth ไม่ต่ำกว่า 250 Mbps (เมื่อคำนวนแบบ 95 percentile ต่อเดือน) หรือแบบ Data Transfer ไม่ต่ำกว่า 81 TB ต่อเดือน[1] (โปรดระบุขนาดที่เสนอ)
6) สามารถทำ Health check และ Load balance ไปยัง Origin web server ในรูปแบบ IP Address/CNAME เพื่อกระจายการทำงานของ Server/Data Center ได้ (โปรดระบุวิธีหรือ mode) และสามารถทำงานแบบ Active/Standby และ Active/Active ได้
7) สามารถตรวจสอบสถานะ Web Service ของแต่ละ server และแจ้งเตือนเมื่อ server UP หรือ DOWN ผ่าน Email ได้เป็นอย่างน้อย
8) ระบบที่ให้บริการจะต้องมี Network Uptime ไม่ต่ำกว่า 99.99% ต่อปี (Downtime ไม่เกิน 50 นาที)
9) ผู้ให้บริการมี Site Reference ในประเทศไทยที่ใช้บริการ Web Application Firewall และ DDoS Protection สำหรับเว็บไซต์ ในรูปแบบ On-cloud (Always-on mode)
10) สามารถใช้งานเว็บไซต์ผ่านช่องทาง HTTP และ HTTPS บน TCP 80, 443 และ Custom Port ทั้ง Frontend และ/หรือ Backend ได้ และสามารถป้องกันการโจมตี Website Attack และ DDoS ได้ (โปรดระบุ)
11) สามารถป้องกันการโจมตี DDoS มายัง Cacheable และ Uncacheable object ในระดับ Layer 7 ได้โดยอัตโนมัติ

[1] อ้างอิงการคำนวณค่าจาก http://www.kylesconverter.com/data-bandwidth/megabits-per-second-to-terabytes-per-month

12) มีศูนย์ Scrubbing Center ที่สามารถป้องกันการโจมตี DDoS ได้จากทั้งในประเทศและต่างประเทศ รวมทั้งรองรับการโจมตี DDoS แบบ HTTP Request per second ได้อย่างน้อย 3 เท่าของเหตุการณ์ที่เคยเกิดขึ้นใหญ่ที่สุด[2]
13) สามารถป้องกันการโจมตีทั้งในระดับ Layer 3-4 (Volumetric Attack หรือ Network Level) และในระดับ Layer7 (Application Attack หรือ Application Level) เช่น HTTP flood, SYN Flood และ ICMP Flood, TCP Fragmentation และ Slow-rate attack ได้เป็นอย่างน้อย
14) ระบบสามารถป้องกัน โดยมีความสามารถของ Web Application Firewall ในการตรวจจับและป้องกันเว็บไซต์ เช่น SQL injection, File inclusion, Cross-site Scripting เป็นอย่างน้อย (โปรดระบุชนิดของการโจมตีที่ตรวจจับได้)
15) ผู้เสนอจะต้องแนบเอกสารผลการทดสอบ Web Application Firewall และ DDoS Protection โดยใช้ Tool ที่แตกต่างกันอย่างน้อย 5 ชนิด โดยให้ระบุขนาดการโจมตี เทคนิคที่ใช้ และความเร็วในตรวจจับและป้องกันอย่างชัดเจน
16) มี POP Node ในประเทศเพื่อให้บริการรับ-ส่งข้อมูลระหว่างผู้ให้บริการ และผู้ใช้งานเว็บไซต์ภายในประเทศ
17) สามารถส่งค่าหมายเลข IP Address ของ Client ต้นทางที่เชื่อมต่อเข้ามายังเว็บไซต์ได้ (X-Forwarded-Proto) ผ่านช่องทาง HTTP และ HTTPS ได้ (โปรดระบุรูปแบบที่ใช้)
18) สามารถรองรับการใช้งาน IPv4 และ IPv6
19) ระบบที่ให้บริการสามารถเก็บข้อมูลการโจมตี (Attack log) และข้อมูลการวิเคราะห์การโจมตี (Attack Analytic Log) อย่างน้อย 30-90 วัน (โปรดระบุจำนวนวันสูงสุด)
20) ระบบสามารถส่ง Access log, Attack log และ Attack Analytic Log มาให้กับระบบจัดเก็บข้อมูลภายนอกทั้งแบบ real-time หรือ off-line (โปรดระบุวิธีการ)
21) สามารถทำ API Security ตามมาตรฐานของ OpenAPI Specification document (โปรดระบุเครื่องมือที่ใช้ในการ Export/Import เช่น Swagger เป็นต้น)
22) สามารถทำ Bot Management หรือ Bot Access Control ได้ตามประเภทและชนิดของ client application โดยสามารถทำ Bad bot และ good bot list ได้
23) สามารถกำหนดเงื่อนไขให้ตรวจสอบต้นทางหรือผู้ใช้งานด้วยเทคนิคต่างๆ (โปรดระบุ) เช่น Cookie, Java และ CAPTCHA support
24) สามารถ Application Delivery Rule ได้ เช่น การทำ URL Rewrite, การทำ Header parameter & value Remove และ Add, การทำ Redirect URL และ การทำ Rate Limited เป็นต้น
25) สามารถกำหนดการเข้าถึงหน้า Management Console ผ่านเว็บไซต์ด้วยระบบ 2-factor authentication ได้
26) สามารถกำหนด Caching Static Content ในระดับวินาทีได้ (โปรดระบุเวลาที่น้อยที่สุดที่สามารถทำได้)
27) มีระบบการแสดงผลการวิเคราะห์ภัยคุกคามที่เกิดขึ้นได้ (Dashboard) ในด้านต่างๆ ผ่านทาง Web Portal
28) มีหน้าจอแสดงปริมาณการใช้งาน และการโจมตีที่เกิดขึ้นแบบ Real-time ทั้งในระดับ Layer 3/4 และ Layer 7
29) มีระบบ Machine Learning ที่สามารถวิเคราะห์การโจมตีที่เกิดขึ้นเพื่อสรุปเป็นเหตุการณ์โดยระบุ รูปแบบการโจมตี, รายละเอียดข้อมูลผู้โจมตี, เวลาที่เกิดและระยะเวลา, ปริมาณของการโจมตี, เว็บที่ถูกโจมตี, อัตราการป้องกัน, ระดับความรุนแรง เป็นต้น
30) สามารถแจ้งเตือนการโจมตี DDoS ในรูปแบบ E-mail ได้เป็นอย่างน้อย
31) มี Technical Support Team ที่สามารถให้คำปรึกษาและแก้ไขปัญหาตลอด 24*7 ตลอดระยะเวลาการใช้บริการ ผ่านทางช่องทาง E-mail และมีระบบขอความช่วยเหลือผ่าน Web Portal ของเจ้าของผลิตภัณฑ์

---

[2] อ้างอิงข้อมูล ณ เดือนกันยายน 2564 22,000,000 packets/second (https://www.reuters.com/technology/russias-yandex-says-it-repelled-biggest-ddos-attack-history-2021-09-09/)

32) มีผู้ประสานงานทางเทคนิคในประเทศไทยผ่านช่องทาง Email, โทรศัพท์ และ LINE เป็นอย่างน้อย ตลอด 24*7 ตลอดระยะเวลาการใช้บริการ

33) ระบบสามารถจัดทำรายงานสรุป ในรูปแบบ PDF หรือ HTML ที่มีเนื้อหาครอบคลุมรายละเอียดการป้องกันการโจมตี เช่น จำนวนครั้งที่ถูกโจมตี, โจมตีมาจากที่ใด, ประเภทการโจมตี และ Threshold ที่ถูกโจมตี เป็นอย่างน้อย พร้อมรายละเอียดหรือคำแนะนำให้ปรับปรุง Configuration ให้มีประสิทธิภาพ

34) มีรายงานการป้องกันอ้างอิงตามหมายเลข CVE ที่สามารถตรวจสอบได้ด้วยตนเองผ่านเว็บไซต์เจ้าของผลิตภัณฑ์ (ถ้ามี)

ทั้งนี้ผู้เสนองานจะต้องปฏิบัติงานหรือส่งมอบงานให้เป็นตามมาตรฐานของกฎหมายหรือข้อกำหนดอื่นใดที่เกี่ยวข้อง

1.2 การดำเนินงาน และสิ่งที่ต้องส่งมอบ

a) การสนับสนุนการติดตั้งให้เว็บไซต์ได้รับบริการ Web Application Firewall และ DDoS Protection รวมถึง Content Delivery Network

b) มีระบบให้บริการ Web Application Firewall และ DDoS Protection รวมถึง Content Delivery Network แบบ 24x7x365 (ตลอดเวลา)

1.3 การส่งมอบและการติดตั้ง

a) License และ Features ที่ได้รับ

b) ระยะเวลาในการใช้บริการ

1.4 การรับประกันและบำรุงรักษา

ให้บริการการดูแลและบริหารจัดการระบบ แก่ตลาดหลักทรัพย์ได้ตลอด 24 ชั่วโมง โดยหากพบปัญหา ทางผู้เสนองานจะต้องเข้ามาดำเนินการแก้ไขตลอดระยะเวลาของสัญญา

2. ระยะเวลาของสัญญา

ระยะเวลาของสัญญาให้บริการ 3 ปี 6 เดือน โดยเริ่มตั้งแต่วันที่ 1 มกราคม 2565 ถึงวันที่ 30 มิถุนายน 2568

กำหนดการ

ลำดับ	รายละเอียด	กำหนดการ
1	ประกาศเชิญชวน	11 พฤศจิกายน 2564
2	สอบถามข้อมูลเพิ่มเติมเป็นลายลักษณ์อักษร ITProcurementUnit@set.or.th	16 พฤศจิกายน 2564
7	กำหนดตอบคำถามเป็นลายลักษณ์อักษร ITProcurementUnit@set.or.th	18 พฤศจิกายน 2564
8	ยื่นข้อเสนองาน	24 พฤศจิกายน 2564
10	ประกาศรายชื่อผู้ชนะการประกวดราคา	20 ธันวาคม 2564

หมายเหตุ ตลาดหลักทรัพย์ขอสงวนสิทธิในการเปลี่ยนแปลงกำหนดการดังกล่าวข้างต้นได้ตามความเหมาะสม

ติดต่อสอบถามข้อมูลเพิ่มเติม

Email: itprocurementunit@set.or.th

ฝ่ายบริหารเทคโนโลยีสารสนเทศ ส่วนจัดหาเทคโนโลยีสารสนเทศ
ชั้นที่ 10 อาคารตลาดหลักทรัพย์แห่งประเทศไทย ถนนรัชดาภิเษก ดินแดง กรุงเทพฯ Visit us at http://www.set.or.th