Cybersäkerhetsprogram för svenska SMF:er

1. Namn på offertförfrågan:

Cybersäkerhetsprogram för SMF

2. Förfrågan ställs av:

Kista Science City AB som en del av projektet Sweden Secure Tech Hub (hädanefter SSTH) i samarbete med fem andra science parks: Linköping Science Park, Lindholmen Science Park (Gothenburg), Ideon Science Park (Lund), Luleå Science Park och Blue Science Park (Karlskrona).

3. Syfte:

Att erbjuda mindre tech-bolag ett program med utbildning, anpassat stöd och test inom cybersäkerhet. Målet är att stärka bolagens kompetens och medvetenhet om cybersäkerhetsfrågor, identifiera och åtgärda sårbarheter samt stödja en säker digitalisering. SSTH planerar att erbjuda cirka 60 bolag tjänster för test och validering fram till och med september 2026 och som levereras av flera leverantörer.

4. Avtalet avser:

Moduler för ett cybersäkerhetsprogram riktat till svenska SMF inom EDIH-ramverket. Modulerna ska kunna avropas var för sig. Fler än en leverantör kan tilldelas avtal för att säkerställa konkurrens, kvalitet och mångfald i erbjudna tjänster. Modulerna erbjuds till företag baserat på efterfrågan och projektet resurser. Avtalet har således inget fast antal moduler eller företag.

5. Målgrupp:

Ramavtal för Cybersäkerhetsprogramet är riktat mot svenska tech-SME (små och medelstora företag) som verkar inom både hård- och mjukvarusektorerna. Dessa företag har behov av att stärka sin kompetens och medvetenhet kring cybersäkerhetsfrågor för att säkerställa en trygg och säker digitalisering. Programmet är särskilt utformat för att stödja företag som kvalificerar sig inom EDIH-ramverket (European Digital Innovation Hubs), och som har potential att dra nytta av företagspecifikt stöd, penetrationstester samt avancerad testning. Deltagarna består av tech-bolag som kanske ännu inte har identifierade sårbarheter men som behöver rådgivning och stöd för att upptäcka och åtgärda sådana, samt förbättra sina säkerhetsåtgärder för att skydda sina digitala tillgångar och system

6. Längd på avtalet:

Avtalet löper i ett år från avtalets startdatum.

7. Värde, storleksordning och frekvens:

Omfattningen kan variera beroende på bolagens behov och regionala förutsättningar. Det finns inget garanterat minimumvärde utan bygger löpande på bolagens identifierade behov.

8. Antal leverantörer:

Fler än en leverantör kan väljas för att säkerställa leveranssäkerhet och kvalitet i erbjudna tjänster.

9. Beskrivning av efterfrågade tjänster

9.1. Företagsspecifikt stöd inom cybersäkerhet

Format: 1-dag på distans eller hos företaget

Exempel på innehåll:

- **Företagsspecifikt stöd:** Rådgivning och praktiska lösningar baserade på internationella och branschspecifika säkerhetsstandarder (t.ex. ISO 27001, NIST).
- **Avancerade hot och attacker:** Djupgående analys och förståelse för aktuella cyberhot som APTs (Advanced Persistent Threats), ransomware, och zero-day-sårbarheter.
- **Säkerhetsarkitektur och design:** Implementering av säkerhetsprinciper i systemarkitektur, inklusive nätverkssegmentering, säker kodning och användning av säkerhetsramverk.
- **Incidentrespons och hantering av intrång:** Utveckling av incidenthanteringsplaner, identifiering och begränsning av intrång, samt återställning av system efter säkerhetsincidenter.
- **Anpassad rådgivning och stöd:** Skräddarsydd hjälp för att förbättra företagets säkerhetsställning, inklusive workshops och interaktiva övningar för att stärka organisationens motståndskraft mot cyberattacker.

Genomförande: På distans, i företagets eller leverantörens lokaler

9.2. Penetrationstester och teknisk utvärdering

Format: Penetrationstest (Grey box eller White box)

Exempel på innehåll:

- **Systemgranskning:** Utför en omfattande analys av företagets IT-infrastruktur, inklusive nätverksarkitektur, servrar, och databaser för att identifiera potentiella säkerhetsbrister.

- **Penetrationstest:**

    - **Grey box:** Tester där begränsad kunskap om systemet används för att simulera en intern attack.
    - **White box:** Tester med fullständig systeminsikt för att simulera en attack från en insider eller en mycket informerad angripare.

- **Kodgranskning:** Analysera källkoden för webbapplikationer, mobilappar, och API för att upptäcka säkerhetsbrister som SQL-injektioner, XSS, och andra kodbaserade sårbarheter.

- **Teknisk utvärdering:** Testning av specifika teknologier såsom IoT-enheter, industriella kontrollsystem (ICS), och SCADA-system för att säkerställa att de uppfyller högsta säkerhetsstandard.

- **Åtgärdsrapport:** Utförlig rapport med detaljerade rekommendationer och åtgärdsplaner för att åtgärda identifierade sårbarheter, anpassade efter branschspecifika krav.

- **Intyg/slutrapport:** Formell dokumentation som sammanfattar testresultaten och ger konkreta rekommendationer för förbättringar, inklusive en bedömning av åtgärdseffektivitet och riskminskning.

Genomförande: På distans, i företagets eller leverantörens lokaler

9.3. Fördjupad testning av särskilt skyddsvärd teknik

Format: Testmiljö motsvarande skyddsklass 3, med experter på plats för stöd

Exempel på innehåll:

- **Anpassade tester:** Utför skräddarsydda säkerhetstester som exakt matchar företagets specifika behov och säkerhetskrav.

- **Genomförande av tester:** Utför omfattande och rigorösa tester med stöd från erfarna cybersäkerhetsexperter för att identifiera och åtgärda sårbarheter.

- **Utförlig rapport:** Skapa detaljerade rapporter med rekommenderade åtgärder som följer branschspecifika krav och standarder.

- **Intyg eller slutrapport:** Tillhandahåll formella intyg eller slutrapporter som redovisar resultatet av testerna och ger konkreta rekommendationer för förbättringar och riskminskning.

Genomförande: I särskilt avsedd testmiljö

10. Krav på utförare

Skall-krav:

- Anbudsgivaren ska uppfylla lagligt ställda krav avseende registrerings-, skatte- och avgiftsskyldigheter i Sverige och eventuellt anlitade underleverantörer ska uppfylla samma krav och måste godkännas av uppdragsgivaren enligt särskild ordning.

- Flera namngivna och bakgrundskontrollerade personer med relevanta specialistområden ska kunna utföra ett eller samtliga steg i programmet.

- Förmåga att koordinera leveransen av respektive steg direkt med företagen.

Bör-krav:

- Utförarens metodik bör baseras på långvarig erfarenhet och forskning, med särskild hänsyn till hållbarhet, jämställdhet och samhällsnytta.

10. Offerten ska inkludera:

10.1. Skall-krav:

- Mandagspris och uppskattning av antal timmar för att genomföra respektive modul i programmet.

- Namn på personer med relevanta specialistområden och erfarenhet av arbete med kommunalt ägda aktörer och europeiska projekt.

- Relevanta referenser, inklusive tidigare erfarenheter av samverkan i projekt med kommunalt ägda och offentliga aktörer.

- Leveranstid från beställning för respektive aktivitet/steg.

10.2. Bör-krav:

- Genomförandeupplägg som möter uppdragsbeskrivningen och kraven, med en tydlig plan för samverkan mellan de sex science parks.

- Möjlighet att erbjuda genomförande för samtliga fyra steg med särskilt fokus på att maximera hållbarhet, jämställdhet och samhällsnytta.

11.3. Option:

Möjlighet att förlänga projektet och erbjuda tjänsterna till fler företag. Offerten bör tydliggöra enhetspris för förlängning.

11. Utvärdering av anbud:

11.1. Kompetens och erfarenhet: Max 30 poäng

- Dokumenterad erfarenhet av test och validering av avancerad teknik.

11.2. Genomförande och metodik: Max 30 poäng

- Tydlighet och kvalitet i genomförandeplanen.

11.3. Pris: Max 30 poäng

- Kostnadseffektivitet i förhållande till erbjuden kvalitet.
- Referenser och tidigare resultat.
- Tidigare prestationer och kundnöjdhet

11.4. Samverkansförmåga: Max 10 poäng

Förmåga att samarbeta och samordna insatser över flera geografiska områden och aktörer (Skall-krav)

12. Relevanta certifieringar:

12.1. Leverantörens personal skall inneha relevanta certifieringar inom cybersäkerhet och penetrationstestning, såsom t.ex. Certified Information Systems Security Professional (CISSP), Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH), CREST, och/eller GIAC Penetration Tester (GPEN) (Skall-krav).

12.2. Företaget ska vara certifierat enligt ISO/IEC 27001 för informationssäkerhet och ha implementerat best practice från ISO/IEC 27002 (Skall-krav).

13. Språk för anbudsinfordran:

13.1. Anbudet ska lämnas på svenska.

14. Språk för leverans:

14.1. Leveransen av tjänsterna ska kunna genomföras på svenska och engelska.

14.2. Leverantören förbinder sig att kunna kommunicera och utföra tjänsterna på båda språken.

15. Språk för kommunikation:

15.1. All kommunikation mellan parterna under avtalets löptid ska ske på svenska eller engelska beroende på vad som kommes överens om.

15.2. Eventuella undantag från detta krav ska godkännas skriftligen av den upphandlande parten.

16. Språk för dokumentation och rapporter:

16.1. All dokumentation, rapporter och andra skriftliga material som genereras under avtalets löptid ska vara på svenska eller engelska.

16.2. Leverantören ansvarar för att översätta sådan dokumentation vid behov.

17. Anbudets avlämnande:

Anbudet skall inkomma senast den 8 augusti 2024 och vara giltigt till minst 8 augusti 2025. Anbudet skall vara undertecknat och inlämnat/inskickat i PDF-format till karin.bengtsson@kista.com.

18. Frågor:

Frågor om förfrågningsunderlaget skickas skriftligt till karin.bengtsson@kista.com samt sakarias.strand@kista.com senast 25 juli 2024.