

Ofrimi i shërbimeve të sigurisë kibernetike dhe menaxhimit të rrezikut kibernetik

1. Qëllimi i angazhimit

Qëllimi i këtij angazhimi është:

- identifikimi i dobësive teknike në sistemet dhe asetet e teknologjisë informative;
- testimi i efektivitetit të kontrolleve të sigurisë;
- monitorimi dhe analiza e ngjarjeve të sigurisë;
- forcimi i qeverisjes së sigurisë së informacionit;
- krijimi dhe mirëmbajtja e një procesi të strukturuar të menaxhimit të rrezikut kibernetik;
- mbështetja e institucionit për përmbushjen e kërkesave rregullative dhe përgatitjen për auditim.

2. Fushëveprimi i shërbimeve

2.1. Shërbimi i skanimit të dobësive

Operatori ekonomik duhet të ofrojë shërbime të rregullta të skanimit të dobësive për identifikimin e cenueshmërive në sistemet dhe asetet e teknologjisë informative.

Kërkesat minimale

- skanime automatike tremujore të dobësive;
- analizë e konsoliduar tremujore e rezultateve dhe trendeve;
- përfshirje e IP-ve të brendshme dhe të jashtme;
- përfshirje e serverëve dhe sistemeve të ekspozuara në rrjet;
- kontroll i konfigurimeve dhe dobësive të njohura të bazuara në CVE;
- mundësi për skanime shtesë pas ndryshimeve madhore në sisteme.

Dorëzimet minimale

- 4 raporte tremujore të skanimit të dobësive;
- 4 përmbledhje ekzekutive me:
 - trendet e rrezikut;
 - gjetjet kritike;
 - rekomandimet për masa korrigjuese;
- klasifikim i gjetjeve sipas nivelit të rrezikut;

- kritik;
- i lartë;
- i mesëm;
- i ulët.

2.2. Shërbimi i testimit të depërtueshmërisë

Operatori ekonomik duhet të kryejë testim të depërtueshmërisë për të vlerësuar efektivitetin e kontrolleve të sigurisë dhe për të identifikuar dobësitë që mund të shfrytëzohen praktikisht.

Kërkesat minimale

- testim vjetor i depërtueshmërisë;
- qasje hibride:
 - testim automatik;
 - validim manual i gjetjeve kritike;
- përdorim i metodologjive dhe praktikave të njohura ndërkombëtare, përfshirë OWASP dhe praktikat më të mira të industrisë.

Dorëzimet minimale

- raport i detajuar i testimit të depërtueshmërisë;
- përmbledhje ekzekutive jo-teknike;
- gjetje teknike me evidencë;
- vlerësim të rrezikut për secilën gjetje;
- rekomandime të zbatueshme për korrigjim;
- retestim opsional për gjetjet kritike, sipas kërkesës së institucionit.

2.3. Shërbimet SIEM dhe SOC

Operatori ekonomik duhet të ofrojë zgjidhje dhe shërbime për monitorimin e centralizuar të ngjarjeve të sigurisë, korelacionin e logeve, zbulimin e kërcënimeve dhe analizën e alarmeve.

Kërkesat minimale

- përfshirje e serverëve virtualë dhe fizikë;
- mbledhje e centralizuar e logeve;
- zbulim i kërcënimeve dhe alarmim;

- monitorim 8 orë në ditë;
- minimum 2 orë analizë aktive të logeve në ditë;
- përcjellje e alarmeve dhe eskalim sipas kritikalitetit;
- raportim mujor i aktivitetit.

Dorëzimet minimale

- konfigurimi fillestar dhe onboarding i shërbimit;
- konfigurim i monitorimit dhe alarmimit;
- raporte mujore të aktivitetit SOC;
- njoftime dhe eskalime për incidente dhe alarme kritike.

2.4. Shërbimi i menaxhimit të rrezikut kibernetik

Operatori ekonomik duhet të ofrojë shërbim të strukturuar për identifikimin, vlerësimin, trajtimin, monitorimin dhe raportimin e rreziqeve kibernetike.

Kërkesat minimale

Identifikim i rreziqeve që lidhen me:

- sistemet e informacionit;
- aplikacionet dhe shërbimet digjitale;
- infrastrukturën e rrjetit;
- palët e treta dhe shërbimet e jashtme.

Vlerësim periodik i rrezikut duke marrë parasysh:

- gjasat e shfrytëzimit;
- ndikimin operacional;
- ndikimin financiar;
- ndikimin ligjor, reputacional dhe rregullativ.

Gjithashtu kërkohet:

- krijim dhe mirëmbajtje e regjistrit të rrezikut;
- përcaktim i pronarëve të rrezikut;
- definim i masave të trajtimit dhe afateve të korrigjimit;

- raportim periodik tek menaxhmenti.

Dorëzimet minimale

- regjistër i rrezikut kibernetik;
- plan trajtimi dhe korigjimi;
- raporte periodike mbi ekspozimin ndaj rrezikut;
- pasqyrë mbi trendet e rrezikut dhe progresin e masave korigjuese.

3. Kërkesa të përgjithshme funksionale dhe rregullative

Operatori ekonomik duhet të sigurojë që shërbimet e ofruara mbështesin institucionin në:

- monitorimin dhe zbulimin e ngjarjeve kibernetike;
- regjistrimin dhe ruajtjen e evidencave për auditim;
- menaxhimin e incidenteve dhe eskalimin e tyre;
- identifikimin dhe trajtimin e dobësive;
- raportimin menaxherial dhe ekzekutiv;
- menaxhimin e rrezikut teknologjik dhe kibernetik;
- përmirësimin e vazhdueshëm të kontrollit të sigurisë.

4. Kriteret e kualifikimit të operatorëve ekonomikë

Operatorët ekonomikë pjesëmarrës duhet të dëshmojnë së paku:

4.1. Kapaciteti profesional

- përvojë në ofrimin e shërbimeve të sigurisë kibernetike;
- përvojë në vulnerability scanning, penetration testing, SIEM/SOC, qeverisje të sigurisë dhe menaxhim të rrezikut;
- staf profesional me kualifikime dhe certifikime relevante.

4.2. Kapaciteti teknik

- qasje në mjete dhe platforma profesionale për skanim, testim dhe monitorim;
- aftësi për të prodhuar raporte teknike dhe ekzekutive;
- aftësi për të ofruar mbështetje dhe eskalim të strukturuar.

4.3. Përvoja e ngjashme

- referenca nga projekte të ngjashme të realizuara në sektorë të rregulluar, financiarë ose me kërkesa të larta sigurie, nëse disponohen.

5. Përmbajtja e ofertës së operatorit ekonomik

Operatorët ekonomikë duhet të paraqesin:

- profilin e kompanisë;
- përshkrimin e përvojës relevante;
- metodologjinë e punës për secilin shërbim;
- planin e implementimit dhe afatet;
- përbërjen e ekipit dhe CV-të e ekspertëve kyç;
- listën e certifikimeve profesionale;
- ofertën teknike.

6. Kohëzgjatja e kontratës

Kohëzgjatja e kontratës do të jetë 12 muaj, me mundësi vazhdimi sipas nevojave të institucionit dhe në përputhje me dispozitat kontraktuale.

7. Kushtet e përgjithshme

- Ofertat duhet të jenë të vlefshme për së paku 30 ditë nga data e dorëzimit.
- Të gjitha shërbimet duhet të ofrohen në koordinim me personat përgjegjës të institucionit.
- Çdo devijim nga kërkesat e kësaj dosjeje duhet të specifikohet qartë në ofertë.
- Institucioni rezervon të drejtën të kërkojë sqarime shtesë nga operatorët ekonomikë.

8. Kriteret e vlerësimit

Ofertat mund të vlerësohen mbi bazën e:

- përputhshmërisë së ofertës teknike me kërkesat;
- përvojës dhe kualifikimeve të operatorit ekonomik;
- cilësisë së metodologjisë së propozuar;
- kapaciteteve të ekipit të angazhuar.

9. Afati dhe mënyra e dorëzimit të ofertave

Operatorët ekonomikë duhet t'i dorëzojnë ofertat e tyre brenda afatit të përcaktuar në njoftimin e tenderit, në formatin dhe mënyrën e përcaktuar nga autoriteti kontraktues.