INSTITUTUL NAȚIONAL DE CERCETARE - DEZVOLTARE ÎN INFORMATICĂ
- ICI București
B-dul Mareșal Averescu 8-10, sector 1, Cod Poștal 011455, București, ROMÂNIA
Telefon: +40 21 316 07 36, +40 21 316 52 62, Fax: +40 21 316 10 30, E-mail: office@ici.ro
C.U.I. 2785503, Nr. Înregistrare la Registrul Comerțului: J40/11029/1999

Anexa nr. 1

Informații privind
serviciile ICI București privind securitatea datelor,
rețelelor și sistemelor informatice

1. **Descriere:**

Siguranța schimbului de date constituie o provocare majoră care obligă la implementarea modalităților adecvate de prevenție și răspuns la amenințările de natură informatică. Amenințările cibernetice fac ca o entitate responsabilă să realizeze că are nevoie de o protecție continuă și comprehensivă, dar așa ceva se poate realiza fie prin conceperea / construirea unui Security Operations Center (SOC) propriu, fie prin apelarea la servicii externalizate.

În ceea ce privește prima opțiune sunt provocări mixte și uneori greu de depășit, întrucât un SOC propriu presupune, pe lângă etape complexe de implementare, și costuri asociate semnificative cu resursa umană implicată, toate acestea fiind necesar a fi abordate într-o perspectivă de continuitate 24/7/365.

În contrapondere, compartimentul de operațiuni de securitate a informațiilor –SOC, implementat de către Institutul Național de Cercetare-Dezvoltare în Informatică (ICI-București), poate oferi soluții pertinente la costuri semnificativ mai reduse decât cele subsecvente operării unui SOC propriu, având totodată flexibilitate în ceea ce privește nevoile de securitate informatică în principal, dar și pe alte paliere secundare unde este dezvoltată o expertiză adecvată. Diferența de costuri este determinată în principal de translatarea în sarcina ICISOC a costurilor semnificative de infrastructură tehnologică și cele cu resursa umană înalt specializată.

ICISOC furnizează servicii de securitate integrate într-un sistem cu facilități avansate, proactive, pentru detectarea și neutralizarea atacurilor cibernetice, dintre care, cu titlu de exemplificare, menționăm: *Monitorizare și blocare atacuri de tip DDoS; Intrusion Detection Systems (IDS); Intrusion Prevention Systems (IPS); Blocare atacuri Malware, Ransomware, spammers și spam servers;; Blocare TOR Exit Nodes; Blocare atacuri de tipul Layer 7 Regular Expression; Webfiltering etc.*

De asemenea, sunt furnizate servicii de scanare a vulnerabilităților rețelei locale și de alarmare, care, coroborate cu sprijinul pentru implementarea unor politici de securitate informatică (și nu numai) customizate la nivel de detaliu, pot ridica foarte mult nivelul de awareness al angajaților, pot crește nivelul de securitate informatică al organizației la un cost aproape simbolic raportat la gama de servicii asigurate, cât mai ales la creșterea profesionalizării din punct de vedere al securității cibernetice a celei mai vulnerabile verigi, factorul uman. Creșterea proactivă a nivelului de securitate cibernetică prin intermediul serviciilor specializate ICISOC se realizează în condiții minim invazive pentru rețeaua de date și echipamentele informatice, instalarea senzorilor de date fiind facilă și sigură.

În contextul măsurilor inițiate pentru activitatea de telemuncă, senzorul ICISOC instalat la sediul dvs. poate fi facil configurat și pentru securizarea accesului la resursele organizației, concomitent cu scopul principal de protejare a sistemelor informatice interne.

2. Servicii ale ICISOC

Principalele servicii de securitate cibernetică pe care ICI București vi le pune la dispoziție prin intermediul centrului **ICISOC** sunt:

- Servicii integrate de tip SOC;
- Servicii de consultanță privind securitatea cibernetică, elaborarea de proceduri de securitate;
- Servicii de consultanță și soluții profesionale de tip Data Loss Protection și Insider Threat în domeniul protecției datelor cu caracter personal.

Capabilitățile importante ale serviciilor integrate de tip SOC sunt:

1.	Automatizări de securitate prin analiză de indicatori de compromitere	2.	Recomandări automate de politici de securitate
3.	Capabilități de detecție și prevenire a tranzitului fișierelor malițioase	4.	Utilizarea doar de informații anonimizate despre fișierele inspectate, date de telemetrie
5.	Actualizări de semnături pe toată durata contractuală (minim 150 actualizări/zi)	6.	Detecție și carantină a fișierelor malițioase
7.	Monitorizarea și schimbarea statutului unui fișier malițios, rescrierea automată a regulilor IPS și politicilor de securitate	8.	Reguli personalizate pentru anumite fișiere menținute sub strictă supraveghere
9.	Capabilități "machine learning" pentru detectarea de fișiere malițioase	10.	Utilizarea de date de telemetrie anonimizate ale fișierelor, pe baza modului de interacțiune cu sistemul de operare
11.	Recunoașterea infrastructurii de rețea și analizarea continuă a comportamentului acesteia	12.	Monitorizarea continuă a traficului de date util
13.	Trafic de date de management optimizat, cu informațiile de telemetrie incluse	14.	Detectarea mișcărilor laterale a aplicațiilor malițioase prin zone de infrastructură de rețea
15.	Identificarea stațiilor și echipamentelor de calcul cu comportament neconform cu politicile de securitate	16.	Analiza constantă a protocoalelor de comunicații de date utilizate
17.	Detectarea și înregistrarea tentativelor de exfiltrare de date	18.	Identificarea tentativelor de conectare la servere Command & Control
19.	Personalizarea regulilor de detecție a amenințărilor de securitate cibernetică	20.	Clasificarea amenințărilor dupa criterii personalizate
21.	Funcționalități avansate de analiză și raportare	22.	Functionalități avansate de informare și alertare

În urma unui site-survey dedicat veți avea la dispoziție politici precum: Politica de securitate a datelor/informației; Politica de utilizare a mediilor de stocare; CleanDesk Policy; BYOD Policy; Politica securitate stații; Norme de definire/utilizare a parolelor; Procedura de acces la echipamentele IT; Politica de raportare a incidentelor; Procedura de acțiune în caz de defecțiune a echipamentelor; Politica de utilizare a internetului în cadrul companiei; Politica de utilizare a mailului de serviciu; Politica de filtrare a accesului internet (webfiltering); Procedura de organizare a exercițiilor de awareness; Plan de awareness, etc.

De asemenea, serviciile de protecție a datelor cu caracter personal vizează asigurarea conformității cu prevederile legale în domeniu și protejarea efectivă a datelor cu caracter personal prin intermediul unor soluții de tip Data Loss Protection și Insider Threat.

Pentru informații detaliate privind serviciile de securitate cibernetică ale ICI București, vă rugăm să accesați site-ul nostru (www.ici.ro), sau oferta instituției noastre din SICAP.

3. Beneficii ale serviciilor ICI București

Principalele beneficii la nivel profesional pe care urmărim ca dumneavoastră să le obțineți în urma colaborării cu ICI București sunt următoarele:

a) Creșterea nivelului general de securitate și protecție a datelor, rețelelor și sistemelor informatice la nivel de organizație;
b) Asigurarea măsurilor de prevenire și reducere a riscurilor și incidentelor de securitate cibernetică;
c) Gestionarea promptă și conformă a riscurilor și eventualelor incidente de securitate cibernetică ce vă pot afecta organizația;
d) Identificarea timpurie a riscurilor și incidentelor de securitate cibernetică și reacția rapidă în caz de incident;
e) Creșterea nivelului de cunoștințe privind securitatea cibernetică la nivelul organizației, precum și la nivel de angajați;
f) Creșterea nivelului intern de securitate privind rețelele de date, precum și datele și documentele electronice în sine;
g) Creșterea nivelului extern de securitate cibernetică prin impunerea unor cerințe specifice mai stricte și în cunoștință de cauză instituțiilor partener și furnizorilor.

4. Costuri

Costurile estimate ale serviciilor de securitate cibernetică furnizate de către ICI București sunt după cum urmează:

- Pentru servicii integrate de tip SOC:
  - Servicii în regim 24/7/365: 4800 lei lunar (fără TVA).

    Costul este calculat pentru un număr de peste 50 calculatoare / endpoint-uri. Prețul ofertat se majorează procentual cu 20% la fiecare 50 de endpoint-uri suplimentare (spre exemplu, pentru 51-100 de endpoint-uri costul este de 120% din prețul de bază), neputându-se depăși 140% din prețul de bază (care reprezintă echivalentul unei rețele de peste 101 endpoint-uri/dispozitive). Nu sunt incluse în matricea de calcul echipamentele de rețea.

    Pentru a veni în sprijinul organizațiilor cu un număr mai redus de calculatoare/endpoint-uri, ICISOC oferă următoarea grilă de reduceri:

- 70% pentru un număr de calculatoare între 1-10;

- 60% pentru un număr de calculatoare între 11-20;

- 50% pentru un număr de calculatoare între 21-50.

- Prețul pentru instalarea, configurarea și înrolarea unui senzor în nodul central ICISOC este de 4500 lei (fără TVA).

Costurile includ instalarea, configurarea, servicii de training și servicii de mentenanță, intervenție și remediere în perioada contractuală.

- Pentru identificarea costurilor privind serviciile de consultanță în domeniul securității cibernetice și serviciilor privind protecția datelor cu caracter personal vă stăm la dispoziție pentru realizarea unei analize în funcție de particularitățile organizației dumneavoastră.

Date de contact: office@icisoc.ro