UNIVERSITATEA DIN BUCUREȘTI
VIRTUTE ET SAPIENTIA

DEPARTAMENTUL DE ACHIZIȚII PUBLICE
Șoseaua Panduri, nr. 90-92, etaj 5, camera 505, sector 5, București, ROMÂNIA
Tel.: (+40) 21 305 46 20, (+40) 21 305 46 21, (+40) 21 305 46 22, (+40) 21 305 46 23
E-mail: contact@achizitii.unibuc.ro | Website: www.unibuc.ro

Nr. înreg. 12487 / 30.10.2019
(Registratura Achiziții)

APROBAT,
RECTOR,
Prof. Univ. dr. Mircea DUMITRU

INVITAȚIE DE PARTICIPARE

UNIVERSITATEA DIN BUCUREȘTI, cu sediul în Sos.Panduri, nr. 90-92, sector 5, București, are onoarea să vă invite să participați la procedura de atribuire a contractului de achiziție publică de: ***Sistem de securitate avansat de prevenire si protectie impotriva atacurilor cibernetice***

1. Obiectul contractului: ***Sistem de securitate avansat de prevenire si protectie impotriva atacurilor cibernetice***
2. Procedura aplicată pentru atribuirea contractului de achiziție publică: *Achizitie directă.*
3. Sursa de finanțare a contractului de furnizare care urmează sa fie atribuit: *Venituri*
4. Durata contractului: de la data semnării până la data îndeplinirii obligațiilor contractuale reciproce ale părților, dar nu mai târziu de 10.12.2019.
5. Oferta depusă de ofertant trebuie să cuprindă:

Propunerea tehnică

a. Ofertantul va elabora propunerea tehnică astfel încât aceasta să respecte în totalitate cerințele din Caietul de Sarcini.

Propunerea financiară

a. Ofertantul va elabora propunerea financiară astfel încât aceasta să furnizeze toate informațiile solicitate cu privire la preț precum şi la alte condiții financiare şi comerciale legate de obiectul contractului de achiziție publică.

b. Certificatul de înregistrare (copie confom cu originalul) al societății

c. Declarația de eligibilitate.

6. Limba de redactare a ofertei: română
7. Perioada de valabilitate a ofertelor: 30 zile
8. Prețul va fi exprimat în lei, fără TVA.
9. Valoarea maximă estimată, **fără TVA** pentru atribuirea contractului este de: **113220.17 lei**
10. Prețul ofertei este ferm în lei.

NU se acceptă actualizarea prețului contractului

11. Criteriul care va fi utilizat pentru atribuirea contractului de furnizare: *prețul cel mai scăzut în lei, fără TVA.*
12. La oferta de bază:

NU se acceptă oferte alternative

UNIVERSITATEA DIN BUCUREȘTI
VIRTUTE ET SAPIENTIA

DEPARTAMENTUL DE ACHIZIȚII PUBLICE
Șoseaua Panduri, nr. 90–92, etaj 5, camera 505, sector 5, București, ROMÂNIA
Tel.: (+40) 21 305 46 20, (+40) 21 305 46 21, (+40) 21 305 46 22, (+40) 21 305 46 23
E-mail: contact@achizitii.unibuc.ro | Website: www.unibuc.ro

13. Termenul comercial în care se va încheia contractul:
Cheltuielile de manipulare, încarcare, transport, și alte cheltuieli ocazionate de furnizarea produselor vor fi suportate de furnizor.
14. Plata prețului contractului se va face în lei, în maxim 30 zile de la data primirii facturii fiscale.
15. Ofertele se transmit prin e-mail, la: cristina.neagoe@achizitii.unibuc.ro.
16. Data limită pentru transmiterea ofertelor: 06.11.2019, ora 16:00
Pentru informații suplimentare ne puteți contacta la tel. 021.305.46.21.
17. Perioada de derulare a contractului: *de la data semnării până la 10.12.2019.*
Locație: București (Sos.Panduri 90-92, sector 5).

Directia IT&C

Anca Ileana

Întocmit,

Cristina Neagoe

CAIET DE SARCINI

SISTEM DE SECURITATE AVANSAT DE PREVENIRE ȘI PROTECȚIE ÎMPOTRIVA ATACURILOR CIBERNETICE

Cuprins

PREAMBUL

Prevederile cuprinse în prezentul document constituie ansamblul cerințelor pe baza cărora se elaborează propunerea tehnică. Cerințele impuse sunt considerate ca fiind minimale si obligatorii.
In acest sens orice ofertă prezentată care se abate de la aceste prevederi va fi luată în considerare, dar numai în măsura în care propunerea tehnică presupune asigurarea unui nivel calitativ superior cerințelor minimale din prezentul document.
Ofertarea de servicii cu caracteristici inferioare celor prevăzute sau care nu satisfac cerințele va fi declarata ofertă neconformă și va fi respinsă.
Oferta se va prezenta prin raspunsuri explicative la fiecare paragraf în parte.
Toate drepturile asupra documentelor, specificațiilor, planurilor, schemelor și a oricăror alte livrabile care vor rezulta în urma prestării serviciilor de către furnizorul selectat vor fi transferate către Autoritatea contractantă.

Serviciile vor fi prestate cel târziu până la data de 10.12.2019.
La finalul perioadei, furnizorul va preda livrabilele finale, conform cerințelor Autorității contractante.

Capitolul 1 – Obiectul Achizitiei

Obiectul caietului de sarcini îl constituie achiziția infrastructurii de securitate pentru optimizarea nivelului existent de securitate si protectie a infrastructurii. Solutia de securitate va oferi capabilitati de firewall, sistem de prevenire a intruziunilor, protectie antivirus si, de asemenea, va putea bloca in timp real exfiltrarea de date catre servere de comanda si control. Solutia propusa va asigura un nivel ridicat de Securitate , facilitand implementarea tehnologiilor de ultima generatie pentru protectia si controlul datelor pe dispozitivele mobile (laptop-uri) si statii fixe (unitati de tip desktop) precum si protectie si preventie impotriva atacurilor cibernetice asupra aplicatiilor de tip S-a-a-S (Software as a Service)
Pentru delimitarea sarcinilor si responsabilităţilor intre beneficiar si executantul lucrărilor, se fac urmatoarele precizări:
- beneficiarul pune la dispoziţie echipamentele existente in cadrul infrastructurii sistemului existent.
- executantul va furniza echipamentele solicitate, va realiza conexiunile si legaturile necesare, pe infrastructura existenta și va instala, activa și va face setările pentru funcţionarea în bune condiţii a echipamentelor furnizate.

Capitolul 2 – Cerinte Tehnice Solutie de Securitate

2.1 Descriere Generala

a) Solutia va fi instalata in mod bridge –Layer 2 si va rula pe infrastructura virtualizata existenta astfel incat sa nu necesite legaturi fizice suplimentare sau echipamente /hardware noi in infrastructura;
b) Solutia trebuie sa includa un server de management si doua echipamente de tip firewall, fiecare dintre acestea functionand pe cate o masina virtuala, asigurand un nivel avansat de protectie la nivel pe perimetru si capabilitatea de a preveni raspandirea pe orizontala a fisierelor malitioase in interiorul centrului de date al beneficiarului. Masinile virtuale cu capabilitati avansate de securitate si protectie suporta diverse tipuri de hipervizoare, printre care VMware ESX, Microsoft Hyper-V si KVM.
c) Managementul solutiei de securitate se va asigura printr-un server de management dedicat, ce va prezenta de asemenea capabilitati de integrare cu platforme de cloud privat (spre exemplu vCenter, NSX, OpenStack) sau cloud public (AWS,M-Azure,GCP ,ETC) . Astfel, se va asigura posibilitatea importarii de obiecte din aceste platforme terte in serverul de management si vizibilitate in mod dinamic asupra modificarilor ce survin asupra obiectelor, urmand ca acestea sa poata fi folosite in politici de securitate si in activitati avansate de interpretare a logurilor si evenimentelor inregistrate.
d) Masinile virtuale firewall si management sunt destinate rularii in mediul de virtualizare VMware ESX , asigurat de beneficiar. Kitt-ul de instalare pentru masinile de tip firewall este

comun cu componenta de management, livrat in format ISO de furnizor. Imaginea de instalare nu trebuie sa depinda de modul de alocare a resurselor (vCores).

e) Resursele de procesare alocate pentru masinile virtuale firewall vor fi de minim 4 vCores dedicate, cu activare a alocarii prin cheie de licenta, minim 8 GB DRAM cu posibilitate de realocare nerestrictionata de cheia de licenta de activare. Echipamentele firewall permit capacitatea de extindere a resurselor de stocare fara reinstalarea masinii virtuale.

f) Echipamentele firewall vor suporta minim 8 interfete de retea alocabile la nivelul hipervizorului, cu capacitatea de utilizare a mecanismelor de alocare dedicata ale hipervizorului (PCI pass-through, SR-IOV). Echipamentele prezinta un mecanism redundant de prelucrare a traficului, cu replicarea configurabila a informatiilor legate de starea sesiunilor.

g) Solutia de securitate prezinta capabilitati de extindere si scalabilitate, atat pe orizontala, cat si pe verticala. Capacitate de crestere a resurselor de prelucrare (vCores) pana la 16 vCores pentru fiecare nod de prelucrare prin realocarea cheilor de licenta de activare la nivelul componentei de management, fara a necesita reinstalarea masinii virtuale. Capacitate de crestere a performantelor de prelucrare a traficului prin adaugarea la nivelul mecanismului de redundanta a minim 2 noduri suplimentare (in total, un minim de 4 noduri de prelucrare la nivelul mecanismului de redundanta).

h) Toate componentele solutiei de Securitate trebuie sa fie dezvoltate de acelasi producator si gestionate unitar prin intermediul unei singure console de administrare.

i) Serverul de management trebuie sa ofere administratorului IT posibilitatea de realiza managementul infrastructurii de securitate utilizand o singura consola, atat pentru retelele fizice sau virtuale, securizate cu ajutorul echipamentelor de tip firewall, localizate in interiorul retelei beneficiarului sau in cloud public, asigurand astfel consistenta la nivelul politicilor de securitate si vizibilitate completa asupra traficului.

j) Serverul de management trebuie sa permita realizarea unei singure politici ce poate include utilizatori, date, aplicatii, retele, etc facilitand astfel un control sporit, in detaliu, administratorului IT si micsorand totodata timpul necesar administrarii solutiei.

2.2 Cerinte Functionale Generale Echipamente de Securitate

Echipamentele de securitate vor implementa urmatoarele functionalitati la nivelul perimetrului de retea:

a) Firewall la nivelul aplicatiilor – se vor utiliza atat semnaturile cat si comportamentul aplicatiilor pentru a defini politici de firewall per aplicatie

b) Firewall pe baza de continut – se vor identifica tipul de fisiere si categoriile de date in traficul de retea, astfel incat se vor putea defini politici de securitate cu indicarea directiei traficului (download/upload)

c) Identificare URL pe baza de categorii, configurabile, incluzand URL-uri de tip regex, ce permite definirea de politici pentru traficul web pe echipamentele de tip firewall, atat pentru traficul criptat, cat si pentru traficul transmis in clar

d) Decriptarea traficului HTTPS catre internet, dar si a traficului cu destinatie resurse interne nu va fi limitata la porturile implicite ale protocoalelor utilizate

e) Protectia impotriva atacurilor de tip APT(Advanced Persistent Threat) si a comunicatiilor CnC (Command and Control) a resurselor infectate cu Bot se bazeaza pe IP-uri, URL-uri si

reputatia domeniilor DNS, analizand totodata semnaturile si tipurile de comportament ale comunicatiilor de date; se vor putea realiza capturi de pachete, per sesiune, facilitand capabilitatea de a realiza analize detaliata asupra traficului.

f) Preventia impotriva spam bazata pe reputatia IP-ului sursa si detectie pe baza unor mecanisme de identificare utilizand sabloane

g) Preventie anti-virus si anti-malware bazata pe reputatia URL si a semnaturilor, cu posiblitatea de a realiza capturi de pachete, per sesiune.

h) Sistem de prevenire a intruziunilor (IPS), cu activare automata a semnaturilor, ce va lua in considerare impactul de performanta, nivelul de certitudine, severitatea amenintarii, activare mod de functionare doar-detectie si dezactivarea temporara, in mod automat, bazata pe nivelul de utilizarea a resurselor firewall-urilor; solutia trebuie sa fie capabila sa importe semnaturi

i) Preventia impotriva exfiltrarii de date (minim HTTP/S, SMTP,FTP) bazata pe tipuri de date, identificare tipuri de documente si apartenenta documentelor si aplicarea de marcaje criptate, ascunse pe documente si fisiere

2.3 Cerințele pentru modulele de securitate furnizate de Solutia de Firewall

2.3.1 Firewall de tip Stateful Inspection

Trebuie să utilizeze mecanisme de filtrare a conexiunilor bazate pe :

a) informațiile legate de starea acestora. Trebuie să suporte toate specificațiile legate de performanta cerute, lățime de banda, număr total de conexiuni și număr de conexiuni pe secundă.

b) Soluția trebuie să suporte și să controleze accesul la cel puțin 150 de servicii și protocoale de comunicație predefinite.

c) Soluția trebuie să suporte și să controleze accesul la cel puțin 150 de servicii c. și

d) În cadrul soluției de management aferenta modulului, trebuie să existe suport pentru contorizarea accesului la fiecare regula de securitate definita în cadrul soluției, folosind un "hit counter" unic și specific fiecărei reguli de firewall.

e) Trebuie să permită definirea obiectelor de tip timer pentru a permite sau restricționa accesul la anumite reguli de securitate, în funcție de ora și data sistemului, și să ofere capabilități de expirare predefinita a regulilor de securitate.

f) Comunicația dintre firewall și serverul de management trebuie să fie criptata și bazata pe certificate de tip PKI, emise de către o autoritate de certificare locala și integrata cu Soluția de securitate.

g) Firewall-ul trebuie să suporte metode de autentificare a utilizatorilor de tip user, client și sesiune.

h) Următoarele scheme de autentificare trebuie să fie suportate: tokens (exemplu SecureID), TACACS, RADIUS, și certificate digitate emise local, în cadrul soluției, sau de către autorități publice.

i) Soluția trebuie să conțină o bază de date locală a utilizatorilor, pentru a permite autentificare și autorizare, astfel încât să nu fie neapărat necesară o soluție externă de management a acestora.

j) Trebuie să existe suport pentru alocare dinamică de adrese IP folosind protocolul DHCP, server și relay.
k) Soluția trebuie să suporte proxy HTTP și HTTPS.
l) Soluția trebuie să fie capabila să lucreze în mod transparent (bridge mode).
m) Soluția trebuie să ofere suport pentru gateway high availability (cluster HA) m. și distribuție load sharing (cluster LS).

2.3.2 Sistem de detecție și prevenție a intruziunilor (IPS):

a. Trebuie să folosească mecanisme de detecție a atacurilor bazate pe: a. semnături, anomalii de protocol, controlul aplicațiilor și comportamentul acestora.
b. IPS și modulul Firewall de tip Stateful Inspection trebuie să fie integrate pe aceeași platformă.
c. Administratorul soluției trebuie să aibă posibilitatea de a configura modulul IPS să protejeze numai resursele interne.
d. Trebuie să aibă opțiunea de a defini profile IPS pentru client sau pentru server, sau o combinație de amândouă.
e. Trebuie să ofere cel puțin doua profile/politici IPS predefinite.
f. Trebuie să folosească un mecanism software de tip „fail-open", configurabil infuncție de încărcarea procesorului (CPU) și a memoriei (RAM)
g. Trebuie să ofere un mecanism automat pentru activarea și administrarea noilor semnături provenite din update-uri.
h. Trebuie să suporte adăugarea de excepții bazate pe sursa și destinația traficului sau serviciu, indiferent de combinația acestora.
i. Trebuie să includă o metoda de investigare a problemelor, care poate fi activată la nivelul fiecărui profil IPS prin intermediul unui singur buton, aceasta trecând protecțiile din modul preventiv în modul detecție.
j. Trebuie să ofere un mecanism centralizat de corelare și raportare evenimentelor.
k. Administratorul trebuie să fie capabil să activeze noile protecții provenite din update-uri, bazat pe parametrii configurabili (impactul asupra performanței, severitatea amenințărilor, nivelul de încredere, protecția clientului, protecția serverului).
l. Trebuie să poată detecta și preveni următoarele amenințări: folosirea necorespunzătoare a protocoalelor, comunicația folosită în scopuri distructive, atacuri asupra canalelor VPN și atacurile generice care nu au semnături.
m. Pentru fiecare protecție, soluția trebuie să includă tipul protecției (orientată către server sau către client), gradul amenințării, nivelul de încredere și referințe.
n. Trebuie să poată captura pachete de date pentru toate protecțiile active.
o. Trebuie să poată detecta și bloca atacurile la nivel rețea și aplicații, protejând cel o. puțin următoarele servicii: e-mail, DNS, FTP, serviciile Windows (Microsoft Networking), SNMP.
p. IPS trebuie să includă posibilitatea de a detecta sau bloca traficul peer to peer, folosind tehnici evazioniste.
q. Administratorul trebuie să poată defini excluziuni de rețea și host de la inspecția IPS-ului.

r. Soluția trebuie să ofere protecție împotriva DNS Cache Poisoning și să blocheze utilizatorii în a accesa adrese de domeniu blocate.

s. Soluția trebuie să ofere protecție pentru protocoalele VOIP.

t. IPS și/sau Application Control trebuie să detecteze și să blocheze aplicațiile de tip control remote, inclusiv cele care sunt capabile să tuneleze traficul specific prin intermediul protocolului HTTP.

u. IPS trebuie să aibă un mecanism de conversie a semnăturilor SNORT in semnături specifice.

v. Soluția trebuie să permită administratorului să poată bloca ușor traficul inbound și/sau outbound în funcție de zone geografice, țări, fără să fie nevoie să definească grupuri de IP-uri corespunzătoare zonei geografice vizate

2.3.3 Identitatea utilizatorilor:

a. Trebuie să fie în măsură să verifice identitatea utilizatorului, folosind Microsoft Active Directory, pe bază de evenimente de securitate.

b. Trebuie să aibă o metoda de autentificare bazata pe browser WEB pentru obținerea identității unui utilizator sau a obiectelor din afara domeniului AD.

c. Trebuie să aibă client dedicat, instalabil prin politica de securitate pe computerele utilizatorilor care poate dobândi și raporta identități către Soluția de securitate.

d. Trebuie să suporte funcționarea pe infrastructura servere de terminale;

e. Impactul asupra controlerelor de domeniu trebuie să fie mai mic de 4% ;

f. Trebuie să fie în măsură să dobândească identitatea utilizatorului de la Microsoft Active Directory , fără nici un fel de agent instalat pe controlerele de domeniu ;

g. Trebuie să suporte autentificare transparenta Kerberos pentru Single Sign On ;

h. Trebuie să suporte utilizarea de grupuri LDAP imbricate ;

i. Trebuie să poată partaja sau propaga identități de utilizator între mai multe gateway-uri de Securitate .

j. Trebuie să fie capabil de a crea roluri de identitate utilizabile în toate modulele software din cadrul soluției de Securitate .

2.3.4 Anti-Bot și Anti-Virus

a. Soluția trebuie să aibă o componenta Anti-Bot și Anti-Virus integrate pe firewall de generație următoare propus.

b. Aplicația Anti-Bot trebuie să fie capabila de a detecta și a opri un comportament anormal sau suspect în rețea

c. Aplicația Anti-Bot trebuie să utilizeze un motor de detectare pe mai multe niveluri, care include reputația IP-urilor, URL-urilor și adreselor de DNS și să detecteze modele de comunicare specific aplicațiilor de tip bot.

d. Modulul Anti-Bot trebuie să fie capabil să scaneze pentru acțiuni specifice aplicațiilor de tip bot.

e. Politicile Anti-Bot și Anti-Virus trebuie să fie administrate într-o consola centrala .

f. Anti-Bot și Anti-Virus trebuie să folosească un mecanism centralizat de corelare și raportare a evenimentelor de securitate.
g. Aplicația anti-virus trebuie să fie în măsură să prevină accesul la site-uri infectate sau suspectate drept malițioase.
h. Aplicația anti-virus trebuie să fie capabilă de a inspecta trafic criptat SSL .
i. Aplicația Anti-Bot și Anti-Virus trebuie să aibă actualizări în timp real de la un serviciu locat în cloud.
j. Aplicația Anti-Virus trebuie să fie capabilă să opreasca fișiere malware conținute în traficul de intrare în rețeaua locală.
k. Politicile anti-virus și anti-bot trebuie să fie gestionate centralizat cu posibilitate de configurare și aplicare selectivă.

2.3.5 IPsec VPN

a) Solutia trebuie să suporte autorități de certificare interna (proprietara) și externe (publice).
b) Soluția trebuie să suporte criptare 3DES și AES-256 pentru IKE faza I și II, IKEv2 plus "Suite-B-GCM-128" și "Suite-B-GCM-256" pentru faza II ;
c) Soluția trebuie să suporte cel puțin următoarele grupuri Diffie-Hellman: Grup 1 (768 bit), Grup 2 (1024 bit), Grup 5 (1536 bit) , Grup 14 (2048 bit) , Grup 19 si Grup 20.
d) Soluția trebuie să suporte integritatea datelor cu MD5 , SHA1, SHA-256 , SHA-384 și AES – XCBC;
e) Soluția trebuie să includă suport pentru VPN punct la punct în următoarele topologii : Full Mesh, Stea, Hub&spoke.
f) Soluția trebuie să suporte configurarea VPN prin intermediul unei interfețe grafice (GUI) folosind metode de tip drag and drop a obiectelor;
g) Soluția trebuie să suporte SSL VPN fără client pentru acces de la distanta ;
h) Soluția trebuie să suporte VPN L2TP , inclusiv suport pentru client iPhone L2TP ;
i) Soluția trebuie să permită administratorului să aplice normele de securitate pentru a controla traficul în interiorul VPN-ului ;
j) Soluția trebuie să suporte "domain based" și "route based" VPN folosind interfață tunel virtuala (VTI) și protocoale de rutare dinamice;
k) Soluția trebuie să includă posibilitatea de a stabili tunele VPN cu gateway-uri cu IP-uri dinamice publice;
l) Soluția trebuie să includă compresie IP pentru VPN "client-to-site" și "site-to-site".

2.3.6 Sandboxing

a) Sistemul de securitate trebuie sa suporte capabilitati avansate de sandboxing (la nivelul aplicatiilor, sistemului de operare si arhitecturii hardware) pentru prevenirea atacurilor necunoscute ("zero-day" attacks), cu functia de selectie a localizarii geografice unde se realizeaza emularea fisierelor.

b) Solutia ofertata trebuie sa analizeze atat traficul web HTTP/S, cat si traficul SMTP. Solutia trebuia sa poata prelua pentru emulare fisiere rezultate din fluxul de prelucrare a altor solutii de securitate (de exemplu web proxy) folosind protocolul ICAP.

c) Solutia ofertata trebuie sa ruleze in mediu controlat provizionat in cloud (cu posibilitate de executie locala prin achizitie ulterioara a unui echipament specializat) minim urmatoarele tipuri de fisiere: Microsoft Office, Adobe PDF, executabile in arhitectura OS Microsoft (inclusiv cod interpretat Powershell si clase Java), identificate inclusiv prin despachetarea arhivelor. Dimensiunea maxima a fisierelor emulate trebuie sa fie de pana la 100Mb pentru toate tipurile de fisiere cu posibilitatea de configurare a actiunii (acceptare/interzicere la depasirea dimensiunii).

d) Solutia trebuia sa permita configurarea duratei de emulare, numarului si tipului de masini virtuale in cazul "detonarii " fisierului, cu statut necunoscut, pe appliance local, asigurand emularea in urmatoarele medii: Microsoft Windows XP, 7/8/10, Office 2003/7/10/13/16.

e) Solutia va permite incarcarea manuala a fisierelor pentru emulare cu posibilitatea de automatizare a procelui prin REST API.

2.3.7 Sanitizarea documentelor

a) Solutia trebuie sa implementeze mecanisme de sanitizare a documentelor prin excluderea continutului activ (inclusive referinte la URL-uri) si reconstruirea intr-un format imprimabil a urmatoarelor tipuri de fisiere: Microsoft Office (word, excel, powerpoint), Adobe PDF, .png, .gif, .jpeg, .tiff.

b) Mecanismele de sanitizare trebuie sa fie minim aplicabile traficului HTTP/S si SMTP.

c) Solutia ofertata permite posibilitatea recuperarii documentelor originale fara interventia administratorilor de sistem.

2.4 Server de Management

Serverul de management trebuie sa corespunda din punct de vedere tehnic si functional conform cerintelor urmatoare:

a) Aplicația de management de securitate trebuie să fie capabilă să coexiste pe gateway-ul de securitate, dar și independent de acesta.

b) Aplicația de management de securitate trebuie să accepte segregarea atribuțiilor administratorilor în funcție de rolul acestora. De exemplu, rol pentru managementul politicii firewall sau numai rol pentru vizualizare log-urilor .

c) Soluția trebuie să includă un canal sigur criptat de comunicare, bazat pe certificate între toate componentele distribuite de furnizor, și care aparțin unui singur domeniu de gestionare ;

d) Soluția trebuie să includă o Autoritate de Certificare interna X.509, care poate genera certificate de gateway-uri și utilizatori și care permite autentificarea pe VPN ;

e) Soluția trebuie să includă posibilitatea de a folosi autorități de certificare externe care accepta PKCS # 12 , standardele CAPI sau Entrust ;

f) Toate aplicațiile de securitate trebuie să fie gestionate de la consola centrala ;

g) Aplicația de management trebuie să permită monitorizarea accesului la regulile de securitate, pe măsură ce acestea au fost aplicate pentru traficul specific, pe baza unui contor (hit counter);

h) Soluția trebuie să includă o opțiune de căutare pentru a putea interoga cu ușurințăcare obiect din rețea conține o adresa IP specifica sau doar o parte din ea;
i) Soluția trebuie să includă opțiunea de a segmenta baza de reguli cu ajutorul etichetelor sau a titlurilor de secțiune, cu scopul de a organiza mai bine politica de Securitate;
j) Soluția trebuie să aibă un mecanism de verificare prealabila a politicii de Securitate înainte de instalarea politicii ;
k) Soluția trebuie să aibă un mecanism de control de revizuire a politicii de Securitate ;
l) Soluția trebuie să aibă opțiunea de a adăuga un server de management aflat în standby, care se sincronizează automat cu cel activ, fără a fi nevoie de un dispozitiv de stocare extern .
m) Soluția trebuie să includă capacitatea de a distribui și de a aplica centralizat noi versiuni de software de gateway;
n) Soluția trebuie să includă un instrument gestiune centralizată a licențelor de gateway-uri controlate de către stația de management ;
o) Interfață Grafica de Management (GUI) trebuie să aibă capacitatea de a exclude cu usurinta adresa IP de la definiția semnăturii IPS ;
p) Log Viewer ar trebui să aibă capacitatea de a exclude cu ușurință adrese IP vizualizate în log-urile IPS , atunci când sunt depistate ca fals pozitiv .
q) Prin intermediul GUI trebuie să existe posibilitatea de a ajunge cu ușurință la semnătura IPS pornind de la intrările de tip log IPS .
r) Log Viewer ar trebui să aibă capacitatea de a afișa toate log-urile de securitate (FW , IPS, URLF, s.a), într-un un singur panou, pentru a simplifica procesul de depanare a problemelor de conectivitate pentru o adresă IP.
s) Log Viewer ar trebui să aibă capacitatea să creeze filtru folosind obiectele predefinite (clienți, rețele, grupuri, utilizatori, s.a) ;
t) Log Viewer ar trebui să aibă capacitatea de a crea multiple "filtre salvate" personalizate, pentru utilizare la o dată ulterioară.

Capitolul 3 – Solutie de securitate de prevenire si protectie impotriva atacurilor cibernetice asupra terminalelor mobile si statiilor fixe

3.1 Descriere Generala

Solutia de securitate va facilita implementarea tehnologiilor de ultima generatie pentru protectia si controlul datelor pe dispozitivele mobile (laptop-uri) si statii fixe (unitati de tip desktop). Solutia de securitate propusa va include minim urmatoarele componente functionale:
a) Capabilitati avansate de protectie si preventie impotriva atacurilor necunoscute (“zero-day”);
b) Capabilitati avansate de protectie si preventie impotriva atacurilor de tip zero-phising ;
c) Capabilitati avansate de protectie si preventive impotriva atacurilor de tip ransomware ;
d) Capab ilitati avansate de preventie impotriva exfiltrarii de informatii confidentiale ca urmare a compromiterii unui terminal sau statii de lucru (functionalitate “anti-bot”) ;
e) Capabilitati avansate de protectie si preventive de tip “anti-exploit” ;

f) Capabilitati avansate de protectie si preventie a atacurilor cibernetice pe baza analizei de comportament ;

g) Capabilitati avansate de protectie si preventie anti-virus;

h) Capabilitatea de a furniza la cerere rapoarte detaliate pentru investigatii suplimentare derulate dupa finalizarea atacului cybernetic (capabilitati avansate de tip "forensics");

i) Capabilitati avansate de protectie si preventie a statiilor de lucru si a terminalelor portabile prin activarea functiilor de firewall, identificarea si controlul avansat al aplicatiilor si protectia porturilor terminalului;

j) Capabilitati de conectare securizata, de la distanta, la sediul central.

3.2 Cerinte Functionale

3.2.1 Capabilitati avansate de protectie si preventie impotriva atacurilor necunoscute ("zero-day")

- Solutia ofertata trebuie sa suporte capabilitati avansate de sandboxing (la nivelul aplicatiilor, sistemului de operare si arhitecturii hardware) pentru prevenirea atacurilor necunoscute ("zero-day" attacks), cu functia de selectie a localizarii geografice unde se realizeaza emularea fisierelor (cloud);
- Solutia ofertata trebuie sa ruleze in mediu controlat provizionat in cloud (cu posibilitate de executie locala prin achizitie ulterioara a unui echipament specializat) minim urmatoarele tipuri de fisiere: Microsoft Office, Adobe PDF, executabile in arhitectura OS Microsoft (inclusiv cod interpretat Powershell si clase Java), identificate inclusiv prin despachetarea arhivelor;
- Solutia trebuie sa implementeze mecanisme de sanitizare prin excluderea continutului activ (inclusiv referinte la URL-uri) si reconstruirea intr-un format imprimabil a urmatoarelor tipuri de fisiere: Microsoft Office (word, excel, powerpoint), Adobe PDF, .png, .gif, .jpeg, .tiff.
- Solutia ofertata permite posibilitatea recuperarii documentelor originale fara interventia administratorilor de sistem.

3.2.2 Capabilitati avansate de protectie si preventie impotriva atacurilor de tip zero-phising.

- Solutia ofertata implementeaza protectie in timp real impotriva site-urilor necunoscute cu continut potential malitios de tip phising .
- Solutia ofertata ofera capabilitati de detectie statica si euristica a elementelor din site-urile ce solicita informatii personale;

3.2.3 Capabilitati avansate de protectie si preventive impotriva atacurilor de tip ransomware

- Solutia ofertata implementeaza mecanisme avansate de detectie si preventie a atacuriloSolr de tip ransomware pe baza de comportament, conexiunea la internet nu trebuie sa fie necesara ;
- Solutia ofertata faciliteaza detectia si prevenirea activitatilor malitioase de criptare a fisierelor
- Solutia ofertata faciliteaza restaurarea automata a fisierelor criptate, in cazul unui atac de tip ransomware

3.2.4 Capabilitati avansate de preventie impotriva exfiltrarii de informatii confidentiale ca urmare a compromiterii unui terminal sau statii de lucru (functionalitate "anti-bot")

- Solutia ofertata trebuie sa fie capabila sa blocheze comunicatiile catre servere externe CnC (command-and-control), in urma compromiterii unei statii de lucru sau a unui terminal portabil;

3.2.5 Capabilitati avansate de protectie si preventive de tip "anti-exploit"

- Solutia ofertata ofera protectie impotriva atacurilor de tip "exploit", ce pot conduce la compromiterea aplicatiilor legitime ;
- Solutia ofertata poate detecta atacurile de tip exploit prin identificarea actiunilor de manipulare suspicioasa a memoriei statiei de lucru sau a terminalului portabil .

3.2.6 Capabilitati avansate de protectie si preventie a atacurilor cibernetice pe baza analizei de comportament

- Solutia ofertata detecteaza si blocheaza fisierele malitoase, functionand in mod adaptiv, pe baza comportamentului acestora in timp real
- Solutia ofertata poate identifica, clasifica si bloca in timp real forme noi ale unui fisier cunoscut de tip malitios.

3.2.7 Capabilitati avansate de protectie si preventie anti-virus

- solutia ofertata ofera capabilitati de protectie impotriva fisierelor malitoase cu statut deja cunoscut.

3.2.8 Capabilitatea de a furniza la cerere rapoarte detaliate pentru investigatii suplimentare derulate dupa finalizarea atacului cybernetic (capabilitati avansate de tip "forensics")

- Solutia ofertata va include capabilitati avansate de investigare a incidentelor cibernetice.
- Solutia ofertata include capabilitati de generare pe baza de cerere a unui raport ce evidentiaza modul in care s-a desfasurat atacul cibernetic, identifica si evidentiaza in mod automat exfiltrarea de date si manipularea sau criptarea acestora .

3.2.9 Capabilitati avansate de protectie si preventie a statiilor de lucru si a terminalelor portabile prin activarea functiilor de firewall, identificarea si controlul avansat al aplicatiilor si protectia porturilor terminalului .

- Solutia ofertata implementeaza un nivel de securitate ridicata prin activarea functiilor de firewall, identificarea si controlul avansat al aplicatiilor si protectia porturilor terminalului

3.2.10 Capabilitati de conectare securizata, de la distanta, la sediul central .

- Solutia ofertata poate facilita conectarea utilizatorilor de la distanta prin intermediul unei tunel securizat.

3.3 Server de Management si Monitorizare Solutie de Securitate Terminale Portabile si Statii de Lucru

a) Solutia ofertata trebuie sa permita instalarea si configurarea componentei de securitate a terminalelor portabile si statiilor fixe pe acelasi server de management ce deserveste sistemul de securitate avansat de prevenire si protectie impotriva atacurilor cibernetice, ce urmeaza a fi instalat la nivelul perimetrului de retea;
b) Solutia ofertata unifica componentele de management la nivel de perimetru si management al terminalelor portabile si statiilor de lucru, oferind o experienta unifica, unica, administratorului de sistem.

3.4 Licente

a) Solutia ofertata va include licentele necesare pentru protectia a 50 de statii de lucru sau terminale portabile (laptop-uri), pentru o durata de 12 luni.
b) Acces la ultimele versiuni de software in vederea actualizarii acestora pe o perioada de 12 luni.

Capitolul 4 - Solutie de securitate de prevenire si protectie impotriva atacurilor cibernetice asupra aplicatiilor de tip S-a-a-S (Software as a Service).

4.1 Descriere generala .

Solutia ofertata trebuie sa fie capabila sa protejeze datele organizatiei, blocand atacurile cibernetice asupra aplicatiilor de tip SaaS (software as a service) ce au ca tinta organizatia Universitatea Bucuresti.
Solutia ofertata se va livra ca un serviciu in cloud si furnizeaza capabilitati avansate de protectie impotriva atacurilor cibernetice, prin activarea minim a urmatoarelor capabilitati functionale.

- Protectie impotriva atacurilor necunoscute (atacuri "zero-day")
- Protectie impotriva atacurilor de tip phising
- Protectia identitatii utilizatorilor
- Protectie impotriva exfiltrarii de date din cadrul organizatiei

Solutia ofertata include un management intuitiv, in cloud si faciliteaza instalarea, configurarea si managementul cu usurinta a intregii solutii.
Solutia ofertata faciliteaza implementarea mecanismelor avansate de protectie si preventie la nivelul aplicatiilor de tip SaaS, minim urmatoarele : Microsoft Office 365 Email, Microsoft Office 365 OneDrive, Microsoft Office 365 SharePoint, OneDrive, Google Gmail, Google Drive.

4.2 Cerinte functionale .

- Solutia ofertata trebuie sa fie capabila sa detecteze si sa previna atasamentele malitioase receptionate prin email sau situate intr-un spatiu de stocare in cloud public;
- Solutia ofertata faciliteaza executia fisierelor cu statut necunoscut in mediu controlat cu scopul de a detecta si preveni fisierele cu malitoase
- Solutia ofertata este capabila sa furnizeze la cerere rapoarte avansate de tip "forensics" ce includ activitatea potential malitioasa a fisierelor detonate in mediul de sandboxing
- Solutia trebuie sa implementeze mecanisme de sanitizare prin excluderea continutului activ (inclusiv referinte la URL-uri) si reconstruirea intr-un format imprimabil a minim urmatoarelor tipuri de fisiere: Microsoft Office (word, excel, powerpoint), Adobe PDF, .png, .gif, .jpeg, .tiff ; solutia ofertata permite posibilitatea recuperarii documentelor originale fara interventia administratorilor de sistem.
- Solutia ofertata trebuie sa implementeze mecanisme avansate de detectie si preventie a atacurilor de tip phising asupra email-ului sau prin intermediul link-urile web ;
- Solutia ofertata trebuie sa fie capabila sa detecteze un comportament anormal la nivelul contului, ce poate indica compromiterea contului utilizatorului;
- Solutia ofertata trebuie sa fie capabila sa furnizeze informatii cu privirea la incercarile de autentificare, cu success sau esuate, totodata generand o harta dinamica ce faciliteaza identificarea cu usurinta a activitatii potential malitioase la nivelul contului utilizatorului;
- Solutia ofertata trebuie sa fie capabila sa indexeze toate email-urile si fisierele scanate pentru a contrui in timp real rapoarte, ce pot fi salvate la nevoie;
- Solutia ofertata trebuie sa fie capabila sa se integreze cu Microsoft ADFS sau alti furnizori de identitate, in vederea facilitarii capabilitatilor avansate de autentificare prin mijloace multiple (MFA – multi-factor authentication) si a accesului controlat la conturile utilizatorilor;
- Solutia ofertata trebuie sa fie capabila sa restrictioneze accesul la aplicatia SaaS prin utilizarea identitatii utilizatorilor, a locatiei acestora si dupa tipul dispozitivului utizat;
- Solutia ofertata faciliteaza managementul punand la dispozitie un portal de tip web, implementand de asemenea tehnologia SAML pentru accesul administratorului;
- Solutia ofertata va permite administratorului solutiei sa intreprinda actiuni corective asupra oricarui eveniment prezentat in consola de administrare;
- Solutia ofertata va permite administratorului solutiei sa investigheze amanuntit evenimente prezentate in consola de administrare, facilitand posibilitatea de a filtra evenimentele dupa severitate, aplicatie utilizata, etc.

4.3 Licente

Solutia ofertata va include licentele necesare pentru protectia a 50 de conturi de email Office 365 in cloud Microsoft si suport pentru o durata de 12 luni

Capitolul 5 - Servicii de implementare

Furnizorul va asigura o echipa de specialisti formată din minimum 2 experți tehnici pentru implementarea cerințelor de mai sus. Furnizorul va prezenta CV-urile celor doi experți indicând zona de competență pentru care sunt abilitați să deruleze activitățile.

Proiectul de implementare a soluției tehnice va demara cu o analiză ce va avea ca rezultat o documentație de tip Low Level Design însoțită de o prezentare detaliată în fața echipei tehnice a beneficiarului și va fi acceptată de responsabilul tehnic desemnat din partea Autorității contractante.

Furnizorul va asigura instruirea a minimum 2 persoane tehnice din partea Autorității contractante, Direcția IT&C, în administrarea și utilizarea soluției tehnice implementate.

Instruirea va avea o perioadă de min. 3 zile partea teoretică și practică care va fi organizată astfel:

- O zi la începutul implementării proiectului
- 2 zile la sfârșitul implementării proiectului cu activități de tip hands-on pentru operarea și administrarea sistemului implementat

Furnizorul va prezenta un plan de instruire și curricula adecvată.

Cursanții vor primi un document de atestare a participării la cursurile organizate din partea furnizorului.

Furnizorul va pune la dispoziția personalului tehnic al Autorității contractante documentația tehnică specifică soluțiilor implementate.

Capitolul 6 - Operare, mentanță și suport

Furnizorul va prezenta un plan detaliat de escaladare a incidentelor cu responsabil și date de contract.

Capitolul 7 - Livrabile și calendar de prestare a servciilor

Furnizorul va prezenta un plan de implementare a soluției tehnice și de prestare a servciilor care nu va depăși data de 10.12.2019.

Acest plan va fi discutat și acceptat de Autoritatea contractantă la contractare.

Capitolul 8 - Condiții de plată

Furnizorul serviciilor va emite factura numai după ce Autoritatea contractantă va semna documentul de acceptanță pentru livrabilele solicitate în prezentul caiet de sarcini, respectiv după data de 10.12.2019.

NOTĂ: Acolo unde apar specificaţii tehnice care indică o anumită origine, sursă, producţie, un procedeu special, o marcă de fabrică sau de comerţ, un brevet de invenţie, o licenţă de fabricaţie se va citi "sau echivalent"

NOTA: Raspunderea pentru conţinutul caietului de sarcini aparţine persoanei din departamentul/ compartimentul autorităţii contractante ce procedeaza la intocmirea/completarea/actualizarea acestuia şi redactarea fisei de date a achizitiei (dacă este cazul), pe baza necesităţilor asumate de compartimentul respectiv, în funcţie de specificul documentaţiei de atribuire şi de complexitatea problemelor care urmeaza să fie rezolvate în contextul aplicarii respectivei proceduri de atribuire.

Întocmit
Șef Serviciu Infrastructură,

Ing. Marian Ancuța

AVIZAT
Director IT&C,

Dr. Anca ILEANA