



COMUNICAT DE PRESĂ

Cisco sporește forța soluției Cisco Self-Defending Network

Soluția lansată impulsionează securitatea colaborativă și adaptivă din rețele pentru o protecție mai eficientă și inteligentă

Cisco a anunțat astăzi lansarea unor importante capabilități noi pentru îmbunătățirea colaborării dintre mai multe produse și servicii din portofoliul său de securitate, simplificând capacitatea organizațiilor de a controla și limita amenințările de securitate informațională într-o manieră mai coordonată și mai flexibilă la nivelul rețelelor, precum și administrarea și protejarea comunicațiilor confidențiale cu utilizatorii la distanță.

Îmbunătățirile colective privesc următoarele produse și servicii: Cisco Intrusion Prevention System (IPS), Cisco Security Agent (CSA), Cisco Security Mitigation Analysis and Response System (CS-MARS), Cisco Security Manager (CSM) și Cisco Secure Sockets Layer Virtual Private Network (SSL VPN). Împreună, aceste îmbunătățiri marchează evoluția cea mai recentă a soluției Cisco Self-Defending Network – un cadru complex care încorporează diverse produse de securitate pentru echipamente terminale și rețele într-o soluție de securitate integrată, colaborativă și adaptivă pentru organizațiile de toate mărimile.

Conform celor declarate de Mick Scully (Vice President of Product Management, Security Business, Cisco), pericolul tot mai mare al amenințărilor de securitate informațională – atât din punctul de vedere al profiturilor ilicite, cât și din cel al impactului asupra productivității – transformă controlul și protecția colaborativă a comunicațiilor confidențiale dintr-o simplă cerință IT într-o cerință comercială vitală.

„Pe măsură ce organizațiile devin din ce în ce mai distribuite, abordările tradiționale privind securitatea rețelelor trebuie să facă loc unor soluții mai moderne. În prezent, organizațiile nu se mai pot baza exclusiv pe utilizarea unor produse de securitate autonome sau unidimensionale. Este necesară o unificare a componentelor de securitate individuale – echipamente de rețea, echipamente terminale și instrumente centralizate de analiză și administrare – într-un sistem de securitate integrat. Un astfel de sistem ar trebui să coordoneze constant protecția în toate zonele de extindere a amenințărilor. Securitatea colaborativă permite organizațiilor să extindă disponibilitatea rețelelor, să optimizeze partajarea informațiilor și să sporească eficiența operațională în condițiile unui stres redus.” (Mick Scully)

Controlarea colaborativă a amenințărilor informatice: securizarea întregii rețele

Portofoliul Cisco de soluții de securitate îmbunătățite include Cisco IPS 6.0, CSA 5.2, CS-MARS 4.3 și CSM 3.1 – patru produse care se combină în scopul coordonării vizibilității, al protecției întregii rețele, al simplificării administrării politicilor de securitate și al limitării dinamice a amenințărilor informatice pentru menținerea continuității proceselor comerciale. Aceste produse noi consolidează abordarea Cisco privind protecția coordonată, extinzând-o dincolo de caracterul autonom tipic ale acestor clase

de produse și stabilind o relație vitală între rețele și echipamentele lor terminale. Se asigură astfel protejarea coordonată a tuturor punctelor de intrare potențiale.

De exemplu, partajarea informațiilor între IPS 6.0 și CSA 5.2 minimizează accesările fals pozitive și ajută la blocarea de către dispozitivele IPS a amenințărilor informatice înainte ca acestea să aibă posibilitatea să se prolifereze. IPS 6.0 asigură, de asemenea, detectarea adaptivă a anomaliilor de tipul „ziua zero” și analiza comportamentală pentru identificarea viermilor și a altor activități rău intenționate prin căutarea modelelor suspecte de trafic în rețea; pe de altă parte, IPS 6.0 se integrează cu terțe programe de scanare pentru optimizarea analizei amenințărilor utilizate pentru implementarea de acțiuni protective. Printre alte caracteristici adaptive se numără capacitatea de ajustare a „evaluărilor de risc” bazate pe relevanța atacurilor și instalarea unor filtre automate de evenimente și acțiuni specifice sistemelor de operare.

„Sofisticarea și coordonarea înglobate în IPS 6.0 oferă o soluție inteligentă de controlare a amenințărilor informatice la nivelul rețelelor de companie, care poate contribui la sporirea productivității. Sistemele de securitate colaborativă permit fluidizarea operațiilor, indiferent care ar fi amenințările externe. Acest lucru este foarte reconfortant. La sfârșitul unei zile de lucru, soluția Cisco ne oferă mai mult decât o productivitate sporită – ea ne oferă avantaje concurențiale, materializate în operații comerciale securizate.” (Tami Martin, Intrusion Detection System Engineer, Argonne Labs)

De asemenea, colaborarea optimizată în domeniul securității se extinde, în cazul soluției CSA 5.2, la sporirea calității serviciilor (QoS) și la funcții de control wireless. De exemplu, CSA 5.2 permite politicilor de securitate pentru echipamentele terminale mobile – precum laptop-urile – să restricționeze identificatorii de sistem ai serviciilor *ad hoc* și metodele de criptare și să solicite conexiuni VPN securizate de la locațiile la distanță. Împreună, aceste politici de securitate pot ajuta companiile să protejeze activitățile personalului mobil.

Datorită coordonării strânse dintre IPS 6.0 și CSA 5.2, activitățile rău intenționate din rețea se transmit dispozitivului CS-MARS, care reunește informațiile la nivelul unui echipament unic. CS-MARS efectuează analize comportamentale sofisticate la nivelul rețelei și, după înțelegerea contextului de activități rău intenționate, se coordonează cu CSM 3.1, care aplică modificările adecvate ale politicilor de securitate de la nivelul rețelei companiei.

„Dispuneți altfel de o inteligență de rețea, extrasă din sisteme și echipamente care colaborează și coordonează protecția la nivelul întregii rețele. Această inteligență a rețelei permite clienților noștri să identifice diverse amenințări informatice – violări de politici, vulnerabilități, exploit-uri și comportări anormale – și să simplifice administrarea sistemelor de controlare a amenințărilor informatice. Inteligența colaborativă permite un control simplificat și rentabil, care generează o reacție adaptivă la amenințările informatice în timp real.” (Mick Scully)

„Colaborarea constituie cerința-cheie pentru strategia noastră de securitate, iar abordarea sistemică oferită de Cisco în ceea ce privește securitatea colaborativă este

cea mai bună din domeniu. Ne bazăm pe soluțiile de securitate colaborativă de la Cisco pentru a coordona protecția la nivelul întregii rețele. De asemenea, ne bazăm pe furnizorul de servicii IT administrate HEIT Consulting, un partener strategic în implementarea soluției Cisco. Împreună cu Cisco și HEIT, avem capacitatea să ne securizăm operațiile interne, să ne protejăm clienții și să ne conformăm reglementărilor din domeniu. Pe scurt, Cisco și HEIT ne ajută să eliminăm o mare parte din stresul asociat cu problemele de securitate.” (Carl Goodman, Information Services Manager, Premier Valley Bank, California)

Îmbunătățirile VPN SSL din Cisco ASA consolidează securitatea accesului la distanță

În afara elementelor inovatoare din domeniul controlului colaborativ al amenințărilor informatice, Cisco a anunțat și un val nou de îmbunătățiri VPN SSL ale software-ului instalat pe familia de produse ASA (Adaptive Security Appliance), care oferă firewall integrat, IPS, anti-malware și funcționalitate VPN. Recentul software ASA 8.0 optimizează soluțiile VPN SSL, completând deja verificatele soluții IPsec de la Cisco cu funcții care reduc costurile IT chiar și în contextul sporirii gradului de distribuire a organizațiilor și a mobilității utilizatorilor. Actualizările VPN SSL pentru produsele ASA includ:

- VPN fără client (*clientless VPN*) cu design de portal îmbunătățit pentru activități particularizabile – marcaje personalizate, fluxuri RSS și asistență pentru localizare
- Clientul VPN Cisco de tipul „generația următoare” AnyConnect cu suport extins pentru sistemele de operare Microsoft Vista și Windows, MAC OS X și Linux
- Clientul Cisco Cisco AnyConnect Mobile VPN acceptă Windows Mobile 5.0 Pocket PC Edition
- Acces optimizat în rețea pentru trafic VoIP (Voice over IP) și alte tipuri de trafic sensibil la latență
- Capacitate de crearea a unor „tuneluri inteligente” care asigură acces bazat pe politici la aplicații fără necesitatea alocării de drepturi administrative
- Autoritate de certificare (Certificate Authority – CA) încorporată și opțiuni suplimentare de acreditare a utilizatorilor pentru simplificarea autentificării
- Maparea directă a apartenenței la Windows Active Directory pe accesul VPN simplifică administrarea securității IT prin automatizarea alocării de permisiuni VPN adecvate
- Extensiile de evaluare a nivelului de securizare adaptează mai eficient permisiunile VPN acordate utilizatorilor
- Administrare intuitivă prin intermediul aplicației ASA Adaptive Security Device Manager, CSM 3.1

„Capgemini pune la dispoziția angajaților săi baza de cunoștințe a organizației, iar oferta VPN SSL de la Cisco ne ajută să asigurăm un acces securizat la aplicațiile vitale pentru câteva mii de consultanți răspândiți la sediile clienților noștri. Chiar și atunci când consultanții noștri utilizează PC-uri cu privilegii de acces limitate, le putem oferi un acces particularizat și securizat la resursele esențiale din rețeaua noastră.” (Alex Zuiderwijk, Network and Security Manager, Capgemini, Olanda)

Îmbunătățirile aduse soluției Lifecycle Security Services completează operațiile de controlare a amenințărilor informatice

Soluția Cisco Lifecycle Services maximizează avantajele oferite de aceste îmbunătățiri colaborative, ajutând clienții să eficientizeze instalarea soluțiilor adoptate. Cisco a adăugat capacități suplimentare la portofoliul sau de servicii de securitate, printre care un portal Security Center, Cisco Security IntelliShield Alert Manager Service și Cisco Remote Management Services.

Portalul Security Center asigură o sursă centralizată de informații despre activitățile curente de securitate, furnizând utilizatorilor sugestii privind produsele și serviciile Cisco pentru limitarea amenințărilor informatice. Abonamentele Cisco IPS Signature asigură acces la baza de date Cisco Security IntelliShield Alert Manager pentru informații detaliate despre evenimentele IPS. Această îmbunătățire, combinată cu o caracteristică care va fi disponibilă curând, va permite clienților să coreleze semnăturile IPS cu informațiile de avertizare IntelliShield, accelerând astfel remedierea efectelor atacurilor potențiale. În plus, Cisco IPS Signature Management Service simplifică operațiile cotidiene ale dispozitivelor IPS prin instalarea și adaptarea actualizărilor imediat după ce devin disponibile.

Despre Cisco Systems

Cisco Systems (NASDAQ: CSCO) este liderul mondial în comunicațiile Internet care contribuie la transformarea conectării, comunicării și colaborării interpersonale. Informații despre Cisco se găsesc la adresa Web <http://www.cisco.com>. Pentru știri de ultimă oră, accesați site-ul Web de la adresa <http://newsroom.cisco.com>.

###

Cisco, sigla Cisco, Cisco Systems și sigla Cisco Systems sunt mărci înregistrate ale Cisco Systems, Inc. și/sau ale societăților afiliate din SUA și din alte câteva țări. Toate celelalte mărci menționate în acest document sunt proprietatea firmelor respective. Utilizarea termenului de partener nu implică o relație de parteneriat între Cisco și oricare altă companie. Acest document face parte din Informațiile Publice Cisco.