

Acum și în România



# De la criza economică la securitatea datelor

hacker român, prezentată pe softpedia.com, care a reușit să spargă site-ul binecunoscutei companii de securitate informatică Kaspersky, iar apoi a pătruns în site-ul Bitdefender printr-o vulnerabilitate identificată la serverul SQL al respectivei pagini de internet. Astfel, nici măcar creatorii unora dintre cele mai apreciate programe antivirus nu mai sunt la adăpost de tehnicile actuale ale hackerilor.

Conform unui studiu al Universității Carnegie Mellon, 99% din numărul total de network intrusions sunt realizate prin exploatarea unor vulnerabilități sau a unor erori de configurare care ar fi putut fi contracarate, dacă ar fi fost puse în evidență la timp. De aceea, singura metodă de apărare cu adevărat eficientă o reprezintă testarea permanentă a sistemului pentru identificarea acestor vulnerabilități și eliminarea lor ulterioară.

Multe analize internaționale avertizează că nici înăsprirea și perfecționarea instrumentelor de urmărire și pedepsire legală a hackerilor, chiar dacă sunt necesare și binevenite, nu pot rezolva problema, pentru că ele reprezintă, în ultimă instanță, o provocare suplimentară de a căuta noi subterfugii de a păcăli legea. Concluzia fiind iarăși că departamentele IT trebuie să fie mereu mai proactice și mai eficiente în prevenirea atacurilor.

Trebuie, de asemenea, avut în vedere că pericolul nu vine doar de la atacurile din exterior, ci inclusiv din interiorul sistemului.

În același timp, noțiunea de network este astăzi puternic extinsă, odată cu creș-

tierea tendinței de externalizare a datelor, cu creșterea popularității ofertelor de social networking și de cloud computing, precum SaaS (software-as-a-service). Astfel, activitatea curentă presupune mult mai multe treceri de intrare și de ieșire din pro-

prul sistem, oferind un plus de oportunități pentru hackeri. Tradițional, pentru protejarea sistemelor s-au folosit metode reactive de protecție, precum firewall, anti-virus sau intrusion detection systems. Astăzi, aceste sisteme nu mai sunt suficiente. În loc să așteptăm atacul trebuie să luăm măsuri proactice, să utilizăm sisteme capabile să identifice sursele de risc. Testarea manuală utilizată în general până acum este greoaie și se efectuează la intervale mari de timp, care lasă sistemul descoperit pe durate apreciabile, durate pe parcursul cărora riscul crește la cote inacceptabile. Este esențial ca sistemul proactiv să realizeze o testare automată care poate avea loc cu o frecvență perfect adaptată necesităților. În plus, rapoartele oferite de aceste sisteme trebuie să fie disponibile atât inginerilor de sistem, cât și managerilor, deoarece, de multe ori, complexitatea problemelor privește simultan ambele departamente. Multe situații impun, datorită complexității lor, apelarea rapidă la o consultanță de specialitate.

Cei care au rezolvat cu succes toate aceste probleme, putându-se considera The Technology Leader In Vulnerability Assessment and Management, Outpost24, sunt prezenți acum și în România. Ei oferă reale soluții proactice, eficiente, simplu de utilizat și cu un suport tehnic de excepție, ce este operațional 24 de ore din 24, timp de 7 zile pe săptămână.

Cu headquarterul în Suedia, Outpost24 s-a extins deja practic în toată lumea, operând cu un network global bazat pe birouri locale plasate în peste 25 de țări, precum SUA, Rusia, majoritatea țărilor europene, precum Anglia, Germania sau Franța, pentru a ajunge în Turcia, Australia, Thailanda sau Brazilia. Sunt peste 1.000 de clienți din lumea întreagă, de la mari organizații multinaționale până la mici afaceri locale, corporații sau structuri guvernamentale, universități, firme din domeniul financiar, bancar, juridic, al asigurărilor, din transport, industrie, tehnologie, sănătate, educație, media, comerț, servicii etc. Toate acestea beneficiază de un suport permanent 24 de ore din 24, timp de 7 zile pe săptămână. În permanență, specialiștii Outpost24 sunt gata să rezolve prompt orice probleme cu care se confruntă un client. Este un aspect extrem de important pe care îl apreciază toți clienții, promptitudinea, sollicitudinea și competența specialiștilor Outpost24.

Firme importante, precum Traveler, cel mai mare provider de servicii de business-payment non-bancar din lume, cu peste 700 de retail branches și 16.000 de business customers, acoperind majoritatea aeroporturilor, porturilor și gărilor importante din întreaga lume, deservind astfel peste 40% din utilizatorii liniilor aeriene mondiale, apelează la serviciile Outpost24. Soluția încercată anterior era greoaie, greu de folosit, iar rapoartele furnizate erau prea complicate. Coșmarul acestor bătaii de cap a dispărut imediat ce au apelat la serviciile Outpost24, cu rapoarte clare, extrem de simple și precise pentru manageri și detaliate, cuprinzând toate informațiile necesare pentru departamentul tehnic. Traveler a fost surprins de promptitudinea, sollicitudinea, competența și de expertiza tehnică a serviciului de suport tehnic, gata oricând să rezolve orice problemă. S-a remarcat imediat eficiența în identificarea vulnerabilităților,

dar și capacitatea de înlăturare extrem de rapidă a acestora.

Declarații similare au făcut și reprezentanții celei mai mari firme olandeze de asigurări, Lloyd Group, cu peste 6.500 de angajați, care consideră că sistemul corespunde perfect propriei politici de securitate, fiind extrem de performant, cu rapoarte clare, perfect adaptabile cerințelor proprii. Testarea permanentă a sistemului și suportul echipei tehnice, care permite înlăturarea rapidă a vulnerabilităților evidențiate, le-a dat aceleași satisfacții ca și celor de la Traveler. Aprecierile sunt unanime, toți evidențiind diferențele imense față de soluțiile utilizate anterior.

Universitatea din Helsinki, lider în cercetarea în domeniul tehnologiei informației, a hotărât și ea să apeleze la serviciile Outpost24, considerând sistemul excelent ca performanțe și eficiență în determinarea vulnerabilităților interne și externe pe care le detectează automat, cu maximă promptitudine și acuratețe. Datorită calităților rapoartelor furnizate, eliminarea acestora se poate realiza simplu și rapid.

Outpost24 oferă două produse: Outscan-Perimeter Vulnerability Assessment și HIAB-Hacker In A Box. Cele două sisteme pot fi folosite independent, dar împreună oferă o protecție perfectă a sistemului. Outscan nu necesită nici instalare și nici întreținere, fiind imediat operațional. El scanează perimetrul format din exact aceleși elemente pe care le vizează și hackerii, detectează vulnerabilitățile și dirijează remediile necesare, pentru a preveni orice încercare a hackerilor de a penetra sistemul din afară.

Dar protecția exterioară nu este, de cele mai multe ori, suficientă. Toate studiile și statisticile arată că majoritatea problemelor sunt produse din interiorul sistemului, de către persoane care au deja acces la sistem. Din acest motiv, se impun măsuri speciale de securitate, pentru a te putea apăra chiar și de persoanele considerate de încredere. Pentru prevenirea acestor pericole a fost creat HIAB, care este livrat sub forma unui server preinstalat care acționează din interiorul sistemului. El caută și identifică toate vulnerabilitățile prezente pe diferitele servere, stații de lucru sau alte device-uri din interiorul sistemului, le semnalează și ajută la rezolvarea lor.

Pentru networkuri restrânse pentru care se presupune că nu există amenințări din interior este suficient Outscan-ul. Dar pentru majoritatea network-urilor mari este recomandată utilizarea simultană a ambelor sisteme.

Outpost24 oferă cele mai sigure și mai eficiente soluții de protecție pentru orice network, de la cele mai mici la cele mai mari. Mulți clienți au abandonat alți provideri, pentru a apela la Outpost24, dar nici unul nu a părăsit Outpost24.

Outpost24 se bazează integral pe o tehnologie proprie. Soluțiile sale sunt aplicabile pentru orice sistem de operare utilizat în mod normal, pentru orice aplicații și tip de network. Dar, cel mai important, sistemul este disponibil astăzi și în România. Cei interesați pot găsi lămuriri complete pe [www.outpost24.com](http://www.outpost24.com), dar cel mai bine apelând direct la Sales Office Manager România - Rodica Neagu - la [rodica.neagu@outpost24.com](mailto:rodica.neagu@outpost24.com).

Cecilia Caragea

5



**Un audit din decembrie 2008 al companiei Gecad Net pune în evidență faptul că 90% dintre site-urile românești au vulnerabilități cu grad ridicat de risc. Nu este o joacă, pentru că orice vulnerabilitate critică poate fi exploatată pentru a determina întreruperea activității site-ului respectiv sau chiar preluarea totală a controlului asupra aplicației sau chiar a serverului, modificarea paginilor, pierderea, utilizarea sau furtul datelor existente în bazele de date. Pericolele menționate nu privesc însă doar site-urile, ci orice server conectat la internet.**

Aspectul cel mai grav îl reprezintă tendința generală de creștere a insecurității, agravată, în momentul de față, și de criza economică. Un raport recent al firmei de securitate McAfee arată că rece-

scopuri criminale clare, premeditate și bine pregătite. Pierderile nu privesc doar drepturile intelectuale. De la furturile de cash la pierderea reputației și a încrederii clienților sunt nenumărate formele prin care pot fi prejudiciate firmele supuse acestor atacuri. Un studiu ce cuprinde 800 de responsabili IT estimează doar costurile de reparații la peste 400 de milioane de dolari, iar pe cele referitoare doar la proprietate intelectuală și la datele pierdute, la peste 3 miliarde de dolari. Mult mai greu de estimat sunt pierderile legate de scăderea cifrei de afaceri și, în special, de scăderea valorii de brand. În majoritatea țărilor precum Marea Britanie sau Germania costurile cauzate de o intruziune se întind de la 100.000-200.000 de euro la 5-6 milioane de euro, cu o valoare medie în jur de 2 milioane de euro.

Noua provocare cu care se confruntă serverele din lumea întreagă constă în faptul că metodele clasice de apărare, de tipul fire-wall, programe antivirus etc., nu mai

## Metodologia utilizată de Outpost24



siunea globală crește dramatic vulnerabilitatea informației, care a ajuns astăzi la un nivel neatins vreodată până în prezent, necesitând acțiuni urgente de securizare. Este alarmantă în special creșterea numărului de atacuri targetate, întreprinse în

sunt nici pe departe suficiente. Fără un sistem proactiv de testare a sistemului și de detecție a vulnerabilităților în vederea eliminării lor rapide, serverul este efectiv la cheremul hackerilor. Un exemplu grăitor în acest sens îl reprezintă acțiunea unui

terea tendinței de externalizare a datelor, cu creșterea popularității ofertelor de social networking și de cloud computing, precum SaaS (software-as-a-service). Astfel, activitatea curentă presupune mult mai multe treceri de intrare și de ieșire din pro-