Outsourcing as a solution for IT security

Lect.dr. Emil BURTESCU
Universitatea „Constantin Brâncoveanu”

A company's quest for minimum data security is often hindered when, following thorough risk analysis, the budgetary requirement is too large or the availability and/or skills of internal staff are inadequate for the task. This faces management with a difficult decision. One option to consider in such cases is outsourcing the service to a specialised IT security provider.
Keywords: *outsourcing, IT security, management security service, management security service providers, 24/7.*

Asigurarea securității datelor din calculatoarele proprii trebuie să fie o preocupare constantă pentru conducerea firmei. Securitatea nu este o destinație, securitatea este un proces continuu. Aceasta presupune asigurarea şi menținerea **confidențialității**, **integrității**, **disponibilității** şi **nerepudierii** datelor firmei. O firmă trebuie să fie capabilă să **prevină**, să **detecteze** şi să **răspundă** la atacurile informatice care-i pun in pericol datele şi care-i pot periclita afacerile.

Sunt situații în care asigurarea securității presupune apelarea la firme specializate. Acestea pot face atât studiul necesar implementării măsurilor de securitate, cât şi implementarea acestor măsuri care rezultă în urma studiului sau pot face doar studiul urmând ca implementarea să fie făcută cu forțe proprii. De regulă, se apelează la firme specializate atunci când fie firma este mică şi nu are personal specializat, fie când cheltuielile cu menținerea nivelului de calificare al personalului cu asigurarea securității sunt mari.

Încercarea de a implementa şi de a supraveghea sistemul de securitate din interior poate fi un proces complicat şi costisitor. Recrutarea şi angajarea de personal specializat este foarte dificilă, şi păstrarea acestuia este şi mai dificilă, datorită cererii şi valorii de pe piața de muncă a specialiştilor din domeniul securității. Costurile de instruire permanentă cu asemenea personal sunt de asemenea ridicate din cauza profunzimii de cunoştințe necesare în domeniu. Dacă mai adăugăm la acestea cerința de a păstra un complex software şi hardware actualizat, vom vedea că acest lucru nu este la îndemâna multor firme şi din această cauză se recurge la **externalizarea serviciilor de securitate** ca modalitate de a întruni cerințele de securitate.

Externalizarea serviciilor de securitate reprezintă opțiunea firmei pentru asigurarea serviciilor de securitate de către o altă firmă[1]. În acest caz, se poate vorbi despre un **Furnizor de Management Servicii de Securitate (FMSS)**[2]. Acesta va furniza nu numai serviciile de securitate, ci şi managementul acestora. **Managementul Serviciilor de Securitate** (MSS)[3] nu va mai fi făcut de către firmă, ci de către furnizorul de servicii. Majoritatea FMSS oferă o serie de servicii pentru o taxă lunară care implică un anumit nivel de instalare, consultanță, control 24 de ore pe zi, şapte zile din şapte[4], astfel încât, aşa cum se spune şi în reclame, „să te poți concentra asupra afacerii în timp ce noi ne îngrijim de securitate“. Aceste servicii nu sunt o soluție perfectă, dar ele pot fi cu siguranță folosite pentru a reduce riscurile şi pentru a impune multe cerințe de securitate de bază. În multe cazuri FMSS nu face decât să implementeze elemente de securitate de bază pe care multe firma le-a încercat şi fie a eşuat în implementarea lor adecvată în interiorul acesteia, fie nu a putut să le mențină actualizate la cerințele impuse.

Serviciile principale ale celor mai multe ofer-

[1] În literatura de specialitate, în limba engleză, se foloseşte termenul de *outsourcing*.
[2] În literatura de specialitate, în limba engleză, sunt întâlnite sub denumirea de *MSSP – Management Security Service Providers*.
[3] *MSS – Management Security Service.*
[4] Servicii întâlnite şi sub denumirea de „24/7“.

te de FMSS sunt centrate pe servicii de management de firewall şi pe furnizarea următoarelor facilităţi:

- Managementul firewall/router;
- Controlul şi autentificarea perimetrului de acces;
- Reţele private virtuale;
- Filtru de conţinut de web;
- Detectarea intruziunii;
- Scanarea de viruşi;
- Evaluarea vulnerabilităţii/testul de penetrare;
- Răspunsul în caz de incident.

Aceste facilităţi sunt interconectate în timp real şi permit raportări şi analize la cerere pentru a proteja atât serviciile de reţea din interior, cât şi din exterior. Informaţiile suplimentare pot fi disponibile din analiza de trafic, având în vedere faptul că tot traficul de reţea este filtrat de serviciul de management.

În majoritatea cazurilor, externalizarea serviciilor de securitate, presupune instalarea şi folosirea de dispozitive hardware, inclusiv unul sau mai multe dispozitive de securitate sau aplicaţii similare. Se poate opta pentru dispozitive standard create de furnizor cu renume în domeniu, dar de cele mai multe ori se poate opta pentru un amestec de software şi hardware cumpărate de la furnizori. Aceste aplicaţii pot fi instalate la firmă sau la furnizor pentru a se oferi securitate şi alte servicii de management de reţea. Implementarea poate afecta sensibil balanţa securităţii.

Elementele de securitate furnizate din exterior pot fi de mare importanţă pentru firmă. Există multe beneficii obiective principale care pledează pentru externalizare şi care au ca efect reducerea costurilor necesare asigurării securităţii din interiorul firmei. Se pot în acest fel evita costurile mari ale dezvoltării şi menţinerii unui sistem de securitate – inclusiv găsirea şi angajarea personalului specializat necesar pentru a conduce şi administra politica de securitate a firmei. Se poate reduce costul total pentru menţinerea unei infrastructuri de securitate, inclusiv cheltuielile asociate cu monitorizarea şi păstrarea securităţii 24 de ore pe zi, şapte zile din şapte.

Furnizorii de management de servicii de securitate au avantajul mărimii şi specializării, făcând ca serviciile de securitate din firmă să fie mai eficiente şi mai puţin costisitoare dacă le asigură ei decât dacă ar fi asigurate de personalul specializat al firmei beneficiare.

Folosindu-se de instrumente de acces la distanţă, un FMSS se poate ocupa de managementul firewall-ul firmei fără să fie prezent tot timpul la firma beneficiară, prin urmare deserveşte mai multe sedii de birouri fără să mai implice şi cheltuieli de deplasare care pot sa cadă in sarcina beneficiarului.

Să luăm în considerare următoarea analiză a costurilor/beneficiilor în cazul în care se optează pentru asigurarea securităţii de către personalul specializat al firmei, comparativ cu cazul în care se optează pentru externalizarea serviciilor de securitate. Să presupunem că este vorba de o companie cu o singură conectare la Internet, cazul cel mai des întâlnit la firmele mici şi medii, şi că aceasta cere să se creeze un firewall şi să se monitorizeze conectarea 24 de ore pe zi şapte zile din şapte.

Servicii de securitate din interior. Luăm în considerare o firmă medie. Pentru a crea un firewall pentru această conectare trebuie cumpărat hardware şi software pentru firewall la preţul de aproximativ 10.000 USD. Această sumă poate să fie mai mare dacă firma are mai multe conexiuni la Internet sau este o firmă mai mare. Cheltuielile în acest caz pot ajunge între 50.000 USD şi 75.000 USD. Gestionarea şi monitorizarea firewall-ului trebuie făcute de o persoană calificată. Salariul unui specialist în domeniu variază între 40.000 şi 60.000 USD anual. Achiziţionarea unui dispozitiv firewall scump nu suplineşte slaba pregătire a administratorului. Având în vedere faptul că se cere o acoperire permanentă (serviciu 24/7), este nevoie de cel puţin trei oameni, cu cheltuieli anuale medii de aproximativ 150.000 USD. Instruirea (minimă) a personalului de deservire va costa 15.000 USD per total anual. Această ultimă categorie de cheltuieli este necesară pentru ca personalul de deservire să fie la curent cu noutăţile în domeniu.

Făcând un total, vom avea:

Componenta/cheltuiala	Suma (USD)
Software şi hardware	10.000
Salarii	150.000

Instruire	15.000
Costuri totale	**175.000**

Servicii de securitate din exterior (MSSP). Costurile de hardware şi de software sunt tot aceleaşi, dispozitivul firewall/router şi software-ul sunt achiziţionate de către beneficiar – în jur de 10.000 USD. Cheltuielile cu salariile celor trei angajaţi care să gestioneze firewall-ul vor fi nule, dar vor fi înlocuite de cheltuielile lunare de management extern care sunt în jur de aproximativ 2.000 USD. Aceasta duce la cheltuieli anuale de 24.000 USD. Costul iniţial al instalării (plătibil o singură dată) este de aproximativ 15.000 USD. Nu mai sunt costuri de instruire.
Făcând un total vom avea:

Componenta/cheltuiala	Suma (USD)
Software şi hardware	10.000
Costuri management	24.000
Instalare	15.000
Costuri totale	**49.000**

Făcând acum o diferenţă vom avea:

Componenta/cheltuiala	Suma (USD)
Costurile anuale din interior	170.000
Costurile din exterior	49.000
Economii anuale	**121.000**

O economie substanţială. Numai că această economie depinde de mărimea firmei. Dacă firma este mare, se poate să fie mai rentabil ca serviciile de securitate să fie asigurate din interior. Externalizarea serviciilor de securitate se adresează în general firmelor mici şi medii care ori nu dispun de suficiente fonduri pentru asigurarea serviciului, ori nu au personal specializat în domeniu. Calculele au fost făcute la nivelul de preţuri actuale de pe piaţa românească. La nivel mondial, un firewall cu software-ul aferent costă în jur de 50.000 USD, salariul anual al unui angajat în domeniu este cuprins între 75.000 USD şi 100.000 USD, instruirea este aproximativ 10.000 USD de persoană anual, administrarea din afara firmei a serviciului poate să coste între 75.000 USD şi 90.000 USD, iar taxa de instalare este de 20.000 USD.
Din punct de vedere financiar, mai ales pentru firmele mici, apelarea la furnizorii de servicii de securitate este o alegere bună. Dar nu numai factorul financiar poate să conteze în alegere. Alte elemente care pot să determine firma să apeleze la furnizori de servicii de securitate sunt:

- neprofesionalismul personalului intern;
- profesionalismul furnizorului;
- experienţa furnizorului;
- timpul.

Personalul intern însărcinat cu securitatea datelor este, de regulă, în cadrul anumitor firme, administratorul de reţea. Acesta are pe lângă sarcinile curente şi pe cele de asigurare a securităţii. Din cauza acestora, timpul alocat pentru activitatea de securitate, dar mai ales pentru documentarea în acest domeniu este destul de redus.
Furnizorul extern, în schimb, cu asta se ocupă. Sarcina lui este asigurarea securităţii. Personalul acestuia, pe domeniul respectiv, este mult mai bine pregătit ca un angajat propriu.
Experienţa furnizorului, care se va concretiza în timpul de răspuns la anumite incidente, este şi ea foarte mare. Cu cât numărul de firme aflate în administrarea furnizorului de servicii de securitate este mai mare, cu atât experienţa acestuia este mai vastă. Timpul de răspuns la un incident poate fi redus la minimum deoarece acel incident a fost foarte bine documentat la o experienţă anterioară la un alt client.
Timpul este poate unul dintre factorii care creează cea mai mare bătaie de cap. De ce să pierd eu timp, ca manager sau ca proprietar de firmă, cu găsirea unor soluţii de securitate la care nu mă pricep, în detrimentul afacerilor pe care trebuie să le conduc, când pot să apelez la o firmă specializată?
Totuşi, trebuie luat în calcul cât de mult dintr-un proces vital, precum securitatea, se doreşte să fie încredinţat cuiva care nu este un angajat al firmei.
Nici un furnizor nu poate să-şi asume în întregime responsabilitatea cerinţelor de securitate ale firmei, şi nici nu este de dorit lucrul acesta. Va fi nevoie de membri ai personalului care să înţeleagă afacerea şi politicile care guvernează securitatea firmei. Este de preferat să se apeleze la asigurarea securităţii de către firme specializate doar pentru lucruri

tehnice simple la început, lăsând politicile şi mecanismele vitale în grija oamenilor din interior. Aceasta explică lista de servicii de obicei disponibilă de aceşti furnizori. Aceste firme nu-şi asumă o responsabilitate globală. Ele acceptă contracte pentru sarcini cu privire la securitate şi la procesele operaţionale. Orice FMSS care propune să preia responsabilitatea întregului program de securitate al firmei trebuie tratat cu prudenţă.

Furnizorii de management servicii de securitate vor putea oferi o varietate de elemente de securitate de care firma să beneficieze. Unele dintre acestea sunt procesele operaţionale continue, iar furnizorul este capabil să facă acest lucru, asigurând o acoperire 24/7. Alte elemente sunt mai degrabă orientate spre proiecte sau sarcini, iar avantajele furnizorului constau în capacitatea de a instrui şi de a menţine un personal extrem de specializat care ar fi dificil de justificat (sau de păstrat) de către firmă.

Printre elementele de securitate pe care firma le poate da în administrare unui furnizor extern de servicii de securitate se numără:

- analiza riscurilor;
- analiza arhitecturii;
- protecţia perimetrului;
- configurare şi implementare;
- firewall;
- detecţia viruşilor;
- VPN;
- filtrarea Web;
- detectarea şi monitorizarea intruziunilor;
- răspunsul la incidente;
- evaluarea şi testarea vulnerabilităţii;
- conducerea serviciilor de securitate.

Selecţionarea unui furnizor de management de servicii securitate reprezintă o operaţie dificilă. Un FMSS reprezintă un „partener de securitate“ care trebuie să se integreze unora dintre procesele IT&C şi de afaceri ale firmei. Dacă furnizorul eşuează în a oferi nivelul de servicii asupra căruia s-a căzut de acord, ar trebui să existe penalităţi.

Trebuie avut în vedere în primul rând dacă oferta furnizorului se potriveşte cerinţelor de securitate ale firmei. Alegerea furnizorului de management de servicii de securitate trebuie făcută ţinând seama de nevoile de securitate ale firmei şi de ofertele existente. Se va respinge din start oferta care este sub nevoile firmei. Alegerea ideală este aceea în care oferta este mai mare sau cel mult egală cu cerinţele de securitate ale firmei. Poziţia pe piaţă a furnizorului de servicii este foarte importantă. Referinţele luate de la alţi beneficiari de astfel de servicii sunt binevenite în luarea deciziei. Încrederea în furnizorul care va avea acces indirect la datele firmei va cântări mult în alegerea sau nu a acestuia.

Pe plan internaţional piaţa furnizorilor de management de servicii de securitate este in continua creştere, ajungând la valori de miliarde de dolari anual. La nivel naţional această piaţă este, deocamdată, în stadii incipiente. Unele firme, iniţial furnizoare de programe antivirus, livrează deja management al serviciilor de securitate la diferite firme. La această etapă s-a ajuns în unele cazuri destul de uşor deoarece în prealabil se livrau deja servicii de securitate sau de asistenţă tehnică în domeniu.

Bibliografie

📖 L. McCarthy, *IT Security: Risking the Corporation*, Prentice Hall PTR, 2003.

📖 M. Miller, *Absolute PC Security & Privacy – Defending Your Computer Against Outside Intruder*, SYBEX Inc., 2002.

📖 P.E. Proctor, F.C. Byrnes, *The Secured Enterprise*, Prentice Hall PTR, 2002.

📖 D. Russel, G.T. Gangemi Sr., *Computer Security Basics*, O'Reilly & Associates, Inc., 1991.

📖 M. Strebe, C. Perkins, *Firewalls 24seven*, SYBEX Inc., 2002.

📖 M. Strebe, *Windows 2000 Server 24seven*, SYBEX Inc., 2002.