PERICOLUL DE LÂNGĂ NOI, LIPSA SECURITĂȚII IT (II)

Insecuritatea crescută din cauza virulenței infracționalității IT determină uneori o retragere în cochilia internă, care de fapt creează niște riscuri neașteptate. Proporția lui Pareto este valabilă și în acest domeniu: 80% dintre riscurile de securitate sunt interne, nu externe.

Călin M. RANGU,
vicepreşedinte CEO,
IIRUC Service

Companiile au nevoie de o structură organizatorică, de procese bine definite, de proceduri şi scenarii de combatere a criminalității informatice, care preced tehnologiile. După ce s-au identificat zonele sensibile, sistemele şi datele critice, se identifică metodele de protejare. Soluțiile pot fi interne sau externalizate.

Conceptul Security-In-Depth prezintă cercurile concentrice care trebuie construite. Dar cum comunicațiile, internetul, fac parte din economia globală, nici o companie nu trăieşte izolat. Aceste cercuri trebuie să includă şi zonele de nesiguranță, cele externe şi necontrolate de fapt. Construcția unei protecții interne aproape întotdeauna excede capabilitățile interne ale companiilor, deoarece costurile pentru soluții de securitate sunt mari, iar riscurile se schimbă continuu. Dacă ai implementat o soluție pentru a evita un risc, atacatorii deja au identificat o nişă nouă.

Lupta de unul singur este o luptă pierdută. Este mult mai sigur să te bazezi pe parteneri externi, care au metodologiile şi mijloacele de luptă necesare. Riscurile nu pot fi externalizate, rămân ale fiecărei companii în parte, dar lupta cu aceste riscuri se poate externaliza. Un furnizor de servicii, în cazul externalizării infrastructurii IT, are obligația proprie de a asigura o securitate sporită, lipsa acesteia atrăgând un risc reputațional de neasumat. Cum un client al unei bănci alege banca în primul rând pe baza încrederii pe care o inspiră acea bancă, costul fiind secundar, la fel şi o companie care este un furnizor de servicii trebuie să insufle aceeaşi încredere. Externalizarea ridică întrebările referitoare la accesul datelor confidențiale. Se uită însă că inclusiv specialiştii IT proprii nu ar trebui să aibă acces la datele confidențiale. Riscurile sunt la nivel uman, nu la nivel de companie. Administratorul de server ar trebui să administreze serverul, nu să citească datele. Iar aici, soluțiile IT sunt foarte clare, există şi se pot aplica. Accesul la date ar trebui să îl aibă specialiştii de business, proprietarii datelor, care le-au generat şi le utilizează. Un responsabil de client corporate al unei bănci lucrează cu datele acelui client. Într-adevăr, acesta utilizează un calculator, poate şi un server pe care se află datele. Dar nu administrează serverul. Separarea responsabilităților este esențială pentru un mediu de lucru corect. Altfel, zonele gri vor crea numai semne de întrebare şi neîncredere.

De obicei, sunt atacate punctele slabe ale lanțului. Iar punctul slab este un utilizator care nu şi-a luat măsurile de siguranță necesare. Acest lucru este valabil şi în cadrul companiilor, unde autentificarea doar cu o parolă este o protecție pentru nespecialişti, până la utilizatorul de acasă al unui serviciu de internet-banking, care este expus la maximum. O autentificare sigură, cel puțin în acest moment, este disponibilă la nivel mondial, şi de curând şi în România. Măsurile de securitate trebuie aplicate de la primul punct de acces, de la autentificare. Uneori se securizează prea mult nodul central şi se uită utilizatorii. Tehnologiile smartcard cu chip, care aplică standardele de securitate CAP, EMV, 3DES sunt la îndemâna oricui în acest moment. Cititoarele de carduri cu chip sunt accesibile oricui. Credențialele electronice (userul, parola, amprenta electronică, PIN-ul) sunt deja bunuri de valoare mare, care sunt atacate cel mai frecvent. Nu sunt atacate sistemele principale ale unei bănci, superprotejată, ci credențialele personale, care îl fac pe atacator să preia identitatea celui atacat.