PERICOLUL DE LÂNGĂ NOI, LIPSA SECURITĂȚII IT (I)

Călin M. RANGU,
vicepreşedinte CEO
IIRUC Service

Securitatea IT este un subiect vechi, mult uzitat. Din cauza demonetizării subiectului, lipsa securității IT a devenit practic o obişnuință. Ştim la ce ne putem aştepta: să ne fie furate datele personale, să ne fie instalate software-uri nedorite pe calculatoare, datele să fie extrase neautorizat, traficul să fie interceptat etc.

Companiile româneşti investesc în securitate IT numai când se întâmplă ceva. Se vorbeşte despre outsourcingul dezvoltării software, dar puține companii testează şi verifică împotriva codurilor software ostile. Probabil nici una nu o face încă într-un mod structurat, în primul rând din cauza costurilor mari asociate şi a neştiinței. Iar neştiința nu e cauzată de lipsa de profesionalism, ci de faptul că cei care doresc să penetreze un soft cu un program ostil inovează de fiecare dată, fiind cu un pas înaintea celui care verifică.

Dezvoltările interne sunt şi mai periculoase, deoarece faptele de încălcare a regulilor de securitate sunt de obicei ascunse, pentru a preveni afectarea imaginii corporației. Iar costul certificării dezvoltărilor interne, al aplicării celor mai bune standarde este mult prea mare pentru o firmă care nu are activitatea de dezvoltare soft ca o competență primară.

Ce ar fi de făcut? În primul rând conştientizarea, inventarierea şi crearea unei structuri corporatiste de management al securității IT. Apoi, utilizarea auditării şi certificării sistemelor. Analizarea continuă a vulnerabilităților va limita pericolul.

Sistemele de protecție de bază trebuie respectate. Nu mai poți activa în internet fără programe antivirus, anti-malware, anti tot ce va mai apărea în viitor. Dar protecția va fi doar împotriva atacurilor „normale", obişnuite şi, în general, automatizate.

Atacurile pregătite şi concertate sunt tratate cu măsuri proactive şi reactive, cu soluțiile şi metodele proprii. Dacă, organizațional, se ştie cum să se limiteze accesul la resursele informatice, dându-i-se fiecăruia posibilitatea să acceseze doar ce trebuie, înregistrând continuu accesul la resursele companiei, aspectele tehnice, cum ar fi: nivele de echipamente specializate, programe de detectare a intruziunilor, de monitorizare a traficului, analiza comportamentală a traficului din rețea şi a utilizatorilor, sisteme de autentificare, semnături digitale etc., nu sunt încă foarte cunoscute.

Punctele cele mai nevralgice sunt cele externe acestei structuri tehnice, locul în care se introduc datele şi cel de unde se accesează resursele informatice. Autentificarea şi autorizarea accesului la resurse sunt, de obicei, uşor de interceptat şi de utilizat apoi prin preluarea identității şi a accesului neautorizat. Standardele se perfecționează continuu şi din acest motiv se constată o restrângere a modurilor de autentificare. Pentru a vedea ce trebuie utilizat, trebuie să ne uităm în zonele de risc, acolo unde securitatea înseamnă bani. Majoritatea modurilor de a pierde bani pe internet sunt prin furtul de identitate aferent cardurilor bancare. Marile organizații au impus standarde stricte, permițând însă prea multă vreme laxitate în implementare. Cardurile cu chip au intrat timid pe piața românească, din cauza costurilor de emitere, dar mai ales de acceptare. Iar dacă o bancă emite astfel de carduri şi alții nu le acceptă, universalitatea sistemului de plată cu cardul dispare.

Chipurile de pe carduri asigură nu numai securitatea operațiunii financiare, ci şi securitatea identității personale. Astfel, aceste chipuri se generalizează pentru autentificare. Fie că te autentifici în internet banking, introducând cardul cu chip într-un mic cititor specializat, sau te prezinți cu acel card în fața lucrătorului bancar dintr-o agenție, universalitatea standardelor de securitate este recunoscută. Cardul în sine este însă doar o parte a sistemului. Procesul de autentificare se închide printr-un server, care trebuie să fie echivalent al standardizării cu cel al sistemelor pentru certificatele digitale, în care nerepudierea să fie pe primul loc.