

SISTEME DE ÎNALTĂ SECURITATE

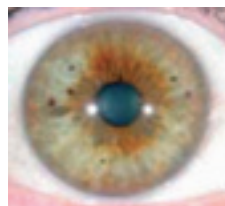
Cristian Șoricuț
SET ALARM INTERNATIONAL

Expresia „sisteme de înaltă securitate” a fost folosită atât de mult în ultimii ani, încât s-a creat falsa impresie că înalta securitate „ne pîndește” de după colț și doar barierele financiare ne împiedică să o atingem sau să o utilizăm în viața de zi cu zi. Nimic mai fals.

Conceptul de înaltă securitate a apărut inițial ca urmare a necesității securizării unor obiective cu caracteristici unice (din punct de vedere dimensional, al valorilor protejate sau al condițiilor de mediu), ce impuneau soluții tehnice deosebite sau utilizarea unor echipamente și sisteme produse la comandă pentru securizarea aceluia obiectiv.



Mai târziu, conceptul de înaltă securitate a fost interpretat de mass media ca fiind legat exclusiv de echipamente și tehnologii de ultimă oră, precum cele necesare identificării biometrice (recunoaștere facială, scanarea irisului, profil vascular al mîinii, cititoare de amprente sau cititoare de amprente palmare, etc.), echipamente de supraveghere video cu amplificatoare de lumină /termoviziune sau safe-uri realizate din materiale exotice (aliaje cu conținut ridicat de iridiu și zincorniu, materiale termorezistente și greu de penetrat, rezistente la acțiunea sculelor așchietoare sau termice uzuale); într-un cuvînt, orice tehnologie nouă a primit acest calificativ.



Nu putem nega avantajele aduse de evoluția tehnologică, dar, de cele mai multe ori, se omite (poate chiar intenționat) veriga slabă a oricărui sistem și anume, factorul uman. Orice sistem de securitate este gândit împotriva amenințărilor externe, cele interne fiind, în multe cazuri, subevaluate.

Să analizăm un caz obișnuit: o societate ce dispune de echipamente pentru controlul accesului, bazate pe identificare cu cartele de proximitate și un dispecerat

propriu. Fără o cartelă validă (presupunînd că echipamentele mecanice de restricționare a accesului sunt corect instalate), pătrunderea în zona securizată este dificilă (copierea unei cartele de proximitate fiind imposibilă la nivel de amator). Însă din interior, unde se află centrala de control al accesului și, în cele mai multe cazuri, softul de gestiune și monitorizare, deschiderea ușii se află la un click distanță. Nu punem în discuție metodele de selectare ale personalului, însă întodeauna există posibilitatea ca, în anumite condiții, factorul uman să cedeze. Am ajuns în acest moment să punem întrebarea fundamentală: „Ce se poate face?”. Răspunsul îl primim analizînd sistemele de securitate ale unor obiective importante din întreaga lume și este foarte simplu: „Proceduri.”. Ce este o procedură? Într-o exprimare mai puțin academică, procedura este o succesiune de pași obligatorii, de parcurs într-o ordine prestabilită, ce include elemente de control și autentificare, făcînd imposibile sau deosebit de dificile operațiuni nepermise.

Evitînd definițiile, consider că un exemplu ar fi mai mult decît elocvent. În domeniul bancar, în perioada interbelică, pentru deschiderea seifului exista o procedură cît se poate de simplă, dar care s-a dovedit eficientă și anume, operarea simultană a două sau mai multe chei. Procedura implică prezența a două sau trei persoane de încredere, posesoare ale unor elemente de identificare (în cazul acesta chei ale seifului). Chiar dacă una dintre persoanele abilitate ar fi intrat în posesia celorlalte chei, distanțele dintre broaștele seifului nu permiteau îndeplinirea condiției de simultaneitate, iar o încercare de deschidere eșuată bloca mecanismul pentru un anumit interval de timp.

Acest exemplu, să spunem „low-tech”, demonstrează că pot fi create, cu mijloace relativ simple, proceduri care pot transforma un sistem vulnerabil într-un sistem de înaltă securitate. Altfel spus, susținem afirmația că un sistem de înaltă securitate nu este neapărat cel realizat cu cele mai noi echipamente și tehnologii, ci acel sistem care are cel mai mic număr de vulnerabilități. Este evident că o tehnologie sau un echipament deosebit de performant ajută foarte mult, îndeplinind condițiile dorite (rata de alarme false redusă, probabilitate de detecție ridicată și posibilități de eludare reduse), însă utilizarea acestuia fără o analiză de risc adecvată și definirea unor proceduri de utilizare eficiente poate conduce la realizarea unui sistem de securitate neperformant și foarte scump.

Este adevărat că, pentru a concepe și realiza un astfel de sistem, este nevoie de îndeplinirea cumulativă a unor condiții importante și respectarea unor etape; totuși, nu este imposibil.

Aceste etape sînt:

a) întocmirea unei analize de risc complete pentru obiectivul protejat și efectuarea unui audit de securitate

prin care să fie relevate riscurile și vulnerabilitățile (atât externe, cât și interne);

b) realizarea proiectului sistemului de securitate și definirea procedurilor de utilizare/intervenție;

c) implementarea proiectului și trainingul personalului utilizator/de intervenție;

d) analiza rezultatelor obținute și verificarea procedurilor;

e) asigurarea mentenanței sistemului și verificarea periodică a respectării procedurilor.

Trebuie menționat faptul că aceste etape se adresează exclusiv sistemelor de înaltă securitate, realizate la comandă, sisteme ce exced cu mult prevederile minimale specificate în normele legale în vigoare. În această categorie de obiective intră obiective militare sau civile unde se asigură protecția bunurilor, a valorilor sau a informațiilor deosebite/ excepționale.



Nu vom insista asupra analizei de risc, pentru aceasta existând reguli bine definite, însă vom puncta celelalte etape.

Astfel, realizarea proiectului trebuie subliniată ca fiind o etapă multidisciplinară la care trebuie să colaboreze

proiectanți din toate ramurile conexe sistemului de securitate (securitate electronică, mecanică, informatică și umană). Spre deosebire de protecția antiincendiu, unde amenințările sunt clar definite și protecția dictată de legile fizicii este, în mare măsură, standardizată, securitatea antifracție lasă o mai mare libertate proiectanților, astfel încât sistemele să răspundă unor varii amenințări. Aparenta libertate a proiectanților impune o responsabilitate deosebită, dublată de o pregătire profesională de top. Numai cunoașterea în amănunt a fiecărui echipament sau dispozitiv propus permite utilizarea sa cu întregul potențial. Sistemele



redundante sau condiționările dintre sisteme sunt un lucru obișnuit, iar „capcanele” în calea infractorilor pot fi extrem de elaborate (detecții multicriteriale coroborate cu reacții by-event sau by-time).

Sistemele de securitate mecanică trebuie să asigure un grad ridicat de protecție fizică și să întârzie cât mai mult posibil un act ostil împotriva zonei de protecție, crescând șansele unei detecții, respectiv intervenții precise și eficiente. Securitatea informatică nu va permite facilitarea unui atac extern sau a unei scurgeri

de informații ce poate crea vulnerabilități. Nu în ultimul rând, pregătirea și antrenarea personalului utilizator/ de intervenție, pentru respectarea cu strictețe a procedurilor, reprezintă un factor cheie în securitatea unui astfel de obiectiv. Chiar dacă procedurile par un mecanism birocratic, cu unele scenarii extrem de puțin probabile, cu cât „acoperă” mai mult din cazuistica posibilă, cu atât mai bine se evită eventualele excepții ce pot deveni amenințări.



În cadrul implementării proiectului, compartimentarea informațiilor pe baza principiului „need to know – nevoie de a cunoaște” face ca deținerea unei imagini de ansamblu asupra sistemului să fie limitată la un grup restrâns de persoane. În mod similar, instruirea compartimentată și alocarea exactă a drepturilor de utilizator va asigura păstrarea interferențelor între compartimentele de securitate la un nivel minim. Tot prin proceduri bine stabilite trebuie asigurată, în mod preventiv, schimbarea codurilor de acces și a elementelor de identificare personală ce pot fi compromise în timpul utilizării.



Pentru analiza rezultatelor, un audit extern poate descoperi eventualele scăpări sau proceduri deficitare și propune măsurile de remediere adecvate. Dacă, în urma verificărilor efectuate, rezultă că nivelul de securitate atins satisface cerințele impuse, se mai pune doar problema păstrării sau îmbunătățirii acestui nivel pe întreaga durată de viață a sistemului.

În final, subliniem că acest scurt ghid nu se dorește a fi exhaustiv, ci încearcă doar sistematizarea informațiilor într-o formă ușor de înțeles, care să permită atât instalatorilor, cât și beneficiarilor să aibă o perspectivă, sper ușor diferită față de cea inițială, asupra sistemelor de înaltă securitate.