SECURITATEA INFORMAȚIEI ŞI CONTROLUL GUVERNAMENTAL

CONF UNIV. ȚARCĂ NAIANA
Universitatea Oradea, ntarca@uoradea.ro
MUREŞAN IOANA-MARIA
Universitatea Oradea

Electronic access to public services offers people a better time schedule. Using the Internet, the greatest world experts „lives" in your computer, because you can „speak" to them. Information is now available for anyone who owns a computer.

Acum câțiva ani, când războiul rece s-a terminat, acesta a fost înlocuit de unul economic. De o parte se situează civilizația agricolă şi industrială, iar de cealaltă parte, civilizația informațională. Politica civilizației agricole este marcată de lupta pentru obținerea simbolurilor modernității: armate, steaguri, monede, independență pe fondul insurecțiilor civile, a celei industriale de naționalism, ideologia statelor-națiuni, iar a civilizației informaționale de globalizarea afacerilor şi finanțelor, de o sfidare a naționalismului şi a granițelor. Delimitarea clară a celor trei este imposibilă şi acest fapt a generat nu numai probleme comune ci şi o luptă continuă pentru stabilirea unei hegemonii globale. De aici, efortul conştient şi coordonat al țărilor dezvoltate de a regândi strategic atât infrastructura cât şi suprastructura civilizației informaționale.

În prezent, civilizația informațională se bazează pe disponibilitatea şi accesibilitatea informației. Comunicarea, transferul şi schimbul de informații se desfăşoară prin intermediul sistemelor tehnice. Milioane de computere sânt interconectate între ele prin rețele complexe terestre sau prin satelit. Punerea la un loc a datelor stocate digital, a textelor, a sunetelor şi imaginilor (multimedia) a condus la răspândirea utilizării sistemelor moderne de comunicații, a calculatoarelor personale şi a serviciilor electronice de informații. Producța de informație, astăzi, este mai mult decât echivalentul fabricilor de ieri, pentru căinformația nu se epuizează. Economii în valoare de trilioane de dolari depind de corectitudinea şi rapiditatea operațiilor efectuate cu ajutorul calculatoarelor. Exporturile mondiale de servicii şi proprietăți intelectuale le-au egalat pe cele de produse electronice şi automobile împreună. Toate acestea s-au întâmplat deoarece informația şi valoarea economică au devenit aproape sinonime. Ca urmare, informația a devenit proprietate națională vitală, cu valoare strategică**;** neprotejată, poate fi cuceritã sau distrusă. Informația stocată nu are o valoare în sine. Valoarea ei se manifestă în momentul în care este folosită sau, mai rău, este pierdută prin nefolosirea rapidă şi eficientă. De aici efortul permanent de reorganizare a producției şi distribuției de informație, de protejare a ei.

Pe plan internațional, marile puteri interpretează diferit acordurile privind informația. Rãzboiul informațional a devenit în timp o posibilitate reală, calculatoarele electronice transformându-se în ținte. Unul dintre câmpurile de luptă este Internetul. Caracterul său deschis oferă statelor posibilitatea să sponsorizeze hackeri care să pătrundă în calculatoarele altor state sau să intercepteze informațiile transmise prin rețea.

Războiul informațional, datorită legislației precare şi spațiului în care se poartă implică riscuri mici si posibile câştiguri mari. Hackerul, ascuns în spatele tastaturii este foarte greu de depistat. Riscul de a fi judecat este foarte mic, iar cel de a fi condamnat este aproape nul.

Acest nou tip de luptă este practicat în competiția economică şi politică şi de marile companii, care atacă bazele de date ale concurenței. Miza o reprezintă banii. Cel care controlează informația controlează banii. Impactul asupra creşterii economice este foarte puternic.

1. Securizarea informației – preocupare a guvernelor

Preocupările guvernelor în domeniul securității informației digitale datează de prin anii 60, când au început să-şi stocheze documentele în format electronic.

Agenția de Securitate Națională (NSA-National Security Agency) reprezenta răspunsul guvernului american la problematica următoare: "să păstrăm codurile noastre secrete şi să le spargem pe ale inamicului". Agenția era atât de bine camunflată încât existența ei a fost negată, acronimul NSA fiind considerat ca derivând din No Such Agency („aceasta agenție nu există"). Cercetătorii aveau sarcina să furnizeze mijloacele pentru protecția comunicațiilor şi sistemelor de informații ale guvernului şi armatei americane.

Tot ce era legat de criptografia modernă era ținut secret.Până prin anul 1975, nimeni nu se ocupa în mod serios de criptografie, cu excepția agențiilor supuse controlului guvernamental. Publicarea cărtilor despre criptografie, participarea angajatilor NSA la simpozioane sau conferinte pe teme de criptografie, exportul de soft specializat, erau interzise. Se aflau sub incidența legii "Arms Regulation" sau pe lista US Munition Tools, unde uneltele criptografice erau enumerate printre tancuri si bombardiere. NSA considera că activitatea criptografică ne-guvernamentală şi publicațiile criptografice reprezintă o amenințare la adresa securității naționale.

Una dintre problemele care trebuia rezolvată era menținerea secretului informației transmisă pe canale nesigure. Modul obişnuit de securizare a informației constă în codarea unui mesaj utilizând o "cheie". Rezultatul este un mesaj cifrat, foarte greu descifrabil pentru un neautorizat. Când mesajul ajunge la destinație, receptorul utilizează aceeaşi cheie pentru a descifra mesajul.

Punctul slab al acestei scheme constă în transmiterea cheii de la emițător la receptor utilizând aceleaşi canale nesigure. Punctul ei forte constă în dimensiunea cheii: cu cât este mai mare cu atât este mai greu de spart codul.

Pentru afaceri sau uz personal, guvernul american a susținut produsul Data Encryption Standard (DES). DES a fost realizat în laboratoarele de cercetări ale IBM si este limitat la o cheie de maximum 56 biti. Introducerea DES a fost însotită de zvonul că NSA a forțat IBM să "slăbească" sistemul pentru ca guvernul să poată sparge mesajele codate, iar NSA să-şi mentină monopolul.

Ultimele decenii, însă, au fost mai puțin blânde cu NSA. Pe lângă faptul că i-a fost deconspirată existența, a pierdut şi monopolul tehnologiilor de criptare. În domeniul comunicațiilor au apărut pe piață telefoane cu o criptare atât de sofisticată încât ridică probleme serioase chiar şi pentru NSA.

Interesele diferitelor grupuri erau divergente. Pe de o parte NSA, CIA şi FBI, jucători majori în politică, ar fi dorit să poată monitoriza orice convorbire telefonică, transmisie fax sau transmisie de date, să poată sparge orice coduri de acces. De cealaltă parte s-au coalizat firme particulare de computere, adepții democrației şi descentralizării din Internet, cei pentru care libertatea înseamnă şi viață personală privată. În ideea de a împăca cele două grupări, politicienii au aruncat în luptă, în aprilie 1993, cipul Clipper, pentru criptarea comunicațiilor: telefon, modem, fax (sponsorizat de NSA). Acest cip care utilizează un foarte puternic algoritm de criptare are un defect major. Există o cheie universală pentru decodare, aflată în posesia agentilor guvernamentali şi care va putea fi folosită atunci când vor fi autorizați să monitorizeze comunicațiile.

2. Proiecția digitală umană

Calculatoarele au devenit arhivele celor mai intime detalii ale vieții oamenilor, când păstrarea documentelor în format digital s-a extins în sectorul privat. .

Progresul tehnologic a facilitat stocarea unui volum tot mai mare de date personale în format electronic şi a simplificat posibilitățile de invadare a vieții personale. În orice moment poate fi reconstruită proiecția digitală a unei persoane pe baza poştei electronice, a grupurilor de discuții la care participă, a soft-urilor pe care le copiază din rețea, a cumpărăturilor electronice pe care le face, etc.

Proiecția digitală este distribuită în baze de date asupra cărora nu avem control: baza de date a companiei aeriene cu care zburăm, a lucrătorilor vamali, a firmei de închiriat maşini, a hotelului la care ne cazăm, a firmei de turism prin care plecăm în concediu, a publicației la care ne abonăm.

Aceste înregistrări care ne definesc pe noi ca si indivizi sânt, din păcate, neprotejate. Pot fi modificate, pot fi, fără autorizatie făcute cunoscute altora. Nu există, deocamdată, viată electronică

privată. Dublura digitală umana poate fi făcută să dispară într-o fracțiune de secundă, acest lucru având implicații multiple asupra vieții personale.

3. Software-ul PGP

Internetul este o anarhie tehnologică si anarhiştii, prin tradiție, au respins controlul guvernamental si solutiile top-down. Aşa, în anul 1991, a început coşmarul agențiilor secrete, atunci când un programator, Philip Zimmerman, a creat un software numit PGP (Pretty Good Privacy) şi l-a oferit gratuit pe Internet. PGP este un program de criptare ce poate fi folosit pentru stocarea documentelor sau pentru trimiterea confidențială a datelor sau a mesajelor e-mail.

Criptografia tip "public domain" creată de Zimmerman, deşi răspândită acum în lume, este considerată ilegală în USA, deoarece acesta nu deține licență pentru algoritmii pe care îi foloseşte. Ceea ce face Zimmermann este considerat ca un fel de apostolat în criptografia publică. Nu poate fi acuzat că a beneficiat material de pe urma cercetărilor lui pentru că rezultatele le-a publicat sub formă de proiect de cercetare pe un BBS si le-a comunicat unui prieten care le-a postat pe Internet. În foarte scurt timp PGP s-a raspândit în întreaga lume. Zimmerman a trecut apoi la realizarea unei versiuni PGP pentru comunicatii analogice, ceea ce reprezintă lovitura de grație dată cipului Clipper.

PGP, prin distribuția liberă a codului sursă a însemnat practic sfârşitul monopolului criptografiei în întreaga lume. Acum, oricine îşi poate cripta profesional mesajele. Prima bătălie pentru viață privată în civilizația informațională a fost câstigată.

BIBLIOGRAFIE:

1. EvghenieV.,-"Implementarea unui sistem de comerț electronic", raport de cercetare, UPB, 1999
2. Rajput W.,-"E-Commerce Systems Arhitecture and Aplications", BookNews, Inc., 2002
3. "Your European Gateway to Electronic Commerce" – An initiative by the European Commission © European Community, 1999