SECURITATEA INFORMATIONALA IN REPUBLICA MOLDOVA VS SECURITATEA INFORMATIONALA LA NIVEL MONDIAL

IAVORSCHI INGA
Universitatea Tehnică din Moldova

Securitatea informaţională reprezintă un domeniu cu mai multe intrebări decît răspunsuri. Am avansat considerabil în ultimii 30 de ani datorită progresului înregistrat în domeniul tehnologiilor informaţionale. Suntem într-un proces de transformare continuu, unde în fiecare zi apar funcţii noi ale roboţilor, maşini cu autopilot, drone pe post de chelneri şi lista poate fi suplinită cu multe alte inovaţii atractive. Totodată, împreună cu progresele fascinante din domeniul TIC simetric cresc şi ameninţările la securitatea cibernetică.

Impactul economic acestor ameninţări se apropie la un **miliard (rusa – miliasd)** de dolari SUA pe an. Analiştii aşteaptă în 2018 o creştere a pieţei securitatii informaţionale cu încă 8% - în total 96,3 miliarde de dolari.[1]

Suntem dependenţi de tot ce ne economiseşte timpul. Am ajuns să facem schimb de date pe timp. Un exemplu elocvent ar fi o casa inteligentă, care are nevoie de date personalizate, cu care operează acest sistem electronic inteligent, pentru a reduce din propriile responsabilităţi ce ţin de menaj, prepararea bucatelor sau alte mofturi inteligente specifice unei persoane ce face parte din societatea modernă. Odată cu evoluţia acestei societăti am ajuns sa fim usor controlabili.

Dacă ai fi fost întrebat în trecut pe cineva din serviciile secrete care este dispozitivul ce oferă informaţie suficientă pentru filarea unei persoane, ar fi răspuns simplu ceva care are coordonate geografice şi oferă cît mai multe date personale. Astăzi practic toate device-urile au încorporate camere video, gps şi respectiv o serie de date ce determină posesorul acestuia.

Pornind de la afirmaţia că cine e posesor de informaţie acela deţine lumea subînţelegem valoarea neestimabilă a informaţiei. În data de 26 mai 2018 intra în vigoare un Regulamentul european privind protecţia datelor cu caracter personal. Acest regulament vine cu o serie strictă de recomandări pentru operatorii de date. Aceste rigori sunt necesare pentru a preveni, a proteja si înlătura incidentele de securitate.

Cu toate că în Moldova legislaţia impune rigori mai drastice în sectorul informaţional, organul abilitat de control nu deţine resurse umane pentru a face faţă fluxului mare de lucru. Datorită acestui fapt avem o mare diferenţă atunci cînd se operează cu datele la noi în ţară comparativ ce restul ţărilor. Cu toate că avem o ţară dezvoltată la capitolul IT cu cele mai mari viteze de internet şi accesibile ca preţ, putine persoane cunosc noţiunea de audit informaţional.

Din experimentul efectuat de mine personal 90% din personele juridice nu dispun de cadre calificate care documentează setările, politicile, ajustările

sistemului informațional a companiei în care activează. Auditului în țările Europene este o practică obișnuită, de aceea incidentele de securitate la ei sunt reduse.Pentru a argumenta opinia vizavi de securitatea datelor cu caracter personal am efectuat urmatorul experiment. Pentru descrierea exercițiului efectuat am folosit 3 parametri.

D (Disponibilitatea)- presupune că în procesul de operare cu datele, utilizatorii autorizați au accesul la informație atunci cînd este necesar.

I (Integritate) - implementarea protocoalelor interne de securizare a informațiilor conform standartului ISO 27001.

C (Confidențialitate) - presupune că accesul la date îl dețin doar persoanele autorizate.

Am evaluat protecția datelor la cîteva companii din domenii diferite (IT, producere, contabilitate, prestări servicii, medicină) cu ajutorul sistemului **DIC**. Verificării au fost supuse toate bazele operaționale de date existente în companiile unde am efectuat experimentul.

Astfel am obtinut urmatoarele rate

I. pentru parametru D-80%.

II. pentru parametru C -50%(rata cea mai ridicata fiind la companiile din medicină).

III. pentru prametru I - 20%(rata cea mai ridicată la firmele IT).

În concluzie- puțini pot avea siguranța că datele personale odată oferite voluntar sau involuntar vor fi prelucrate în mod discret,corect și sigur de operatorul de date.

De aceea pentru sporirea parametrilor DIC este necesar de implimentat o serie de politici de securitate adecvate, cu practici și structuri bine organizate, cu resurse software licentionate și nu în ultimul rînd de personal competitiv, pentru a spori performanța obiectivelor de securitate.Pentru a garanta protecția datelor e necesar să se ea în calcul urmatoarele aspecte.

1. Riscurile potențiale rezultate în urma auditului informațional care descriu amenințările asupra resurselor, vulnerabilitațile sistemelor la amenințări de securitate sau probabilitatea de producere a unui incident de securitate.

2. Legislația Republicii Moldova privind protecția datelor cu caracter personal pe care trebuie să o respecte organizațiile.

3. Stabilirea unor obiective legate de securitatea datelor,a organizațiilor ce vizează resursele necesare pentru a fi protejate, potențialele riscuri ce țin de aceste resurse, ierarhizarea riscurilor, efectuarea periodică a auditului pentru a înlătura și a diminua potențialii factori de risc.

Poziționarea Moldovei într-o zonă de risc. Necesitatea de a proteja datele apare in urma incidentelor de securitate care se produc zilnic fie ca e vorba de fraudele bancare, escrocherii sau alte scurgeri de informație. Conform practicii din anul 2017 cînd s-a produs cel mai mare atac hacker din lume, prezent în cel puțin

99 de ţări care a infectat peste 100.000 de calculatoare din intreaga lume cum ar fi Rusia, China, SUA, Spania, Germania, Franta.

Atacul de tip „cerere de rascumparare”, a fost unul care avea dublu scop. Pe de o parte, cerea de bani, în aceasta fiind similar cu multe tipuri de atac din trecut, dar de data asta cu o eficacitate şi viteza de implantare la nivel de sisteme cu relevanţa internaţională. Conform datelor oferite de site-ul malwaress.com putem vedea impactul global al virusului in figurile de mai jos.

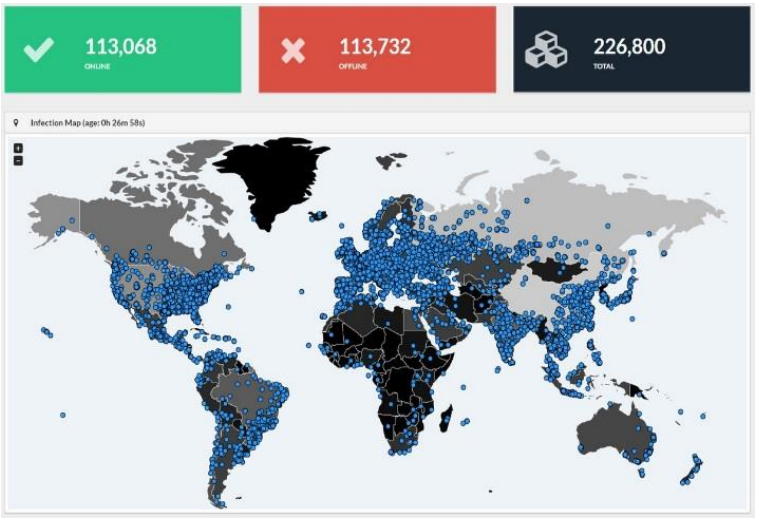

Figura 1. Calculatoarele on-line in timpul atacului.

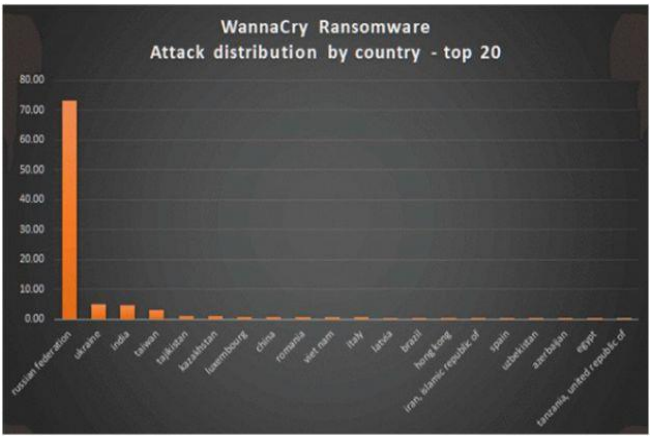

Figura 2 Ţările cele mai afectate de virus conform statisticii oferite de Kaspersky.

Din statistica de mai sus rezultă că ţările vecine cu Moldova sunt în topul preferinţelor atacatorilor. Ceea ce ne induce la ideea ca ne aflăm într-o zona critică. Inspiraţi de acest tip de atac au fost şi hackerii din Moldova care acţionau cu o schemă mai simpla în felul următor, la calculatoarele unde era instalată baza contabilă apărea urmatorul mesaj (recuperarea datelor pentru suma de 300 de $). În cazul celor ce au fost ţinta WannaCry oamenii urmau să plătească cu bitcoini atunci în Moldova era mai simplu de urmărit răufăcătorii pentrucă se cereau bani reali.

Totusi oamenii au ales să plătească deoarece aveau programe nelicenţionate, de copii de rezerve nu dispuneau şi cel mai impresionant nici specialişti sau organe specializate în domeniu securităţii informaţionale nu cunoşteau. Să fi avut statut de operator cu parametri DIC=100% atunci la sigur nu deveneau ţinta escrocilor.

Seriile de scurgeri de date pot continua spre exemplu recent gigantul Facebook a fost ţinta atacurilor cibernetice in urma cărora 300000 de conturi au fost sparse. Ceea ce rezultă ca să poţi proteja datele cu caracter personal trebuie sa respecţi anumite reguli de utilizare, special concepute pentru a opera cu datele, sa nu faci abuz de încredere a personalului tehnic, să documentezi orice proces nou iniţiat în cadrul companiei, să faci audit informaţional conform unui grafic personalizat, să fii informat despre soluţiile noi ce apar pe piaţă şi nu în ultimul rînd să foloseşti programe licenţionate.

Nu există un regulament unic valabil pentru toate domeniile existente de activitate, în schimb poţi să iţi personalizezi propria politică de scuritate, reeşind din speificul de lucru, pentru a obţine siguranţa că informaţia nu va fi vulnerabilă din punct de vedere a securităţii.

Referințe bibliografice:

1. https://ro.wikipedia.org/wiki/Gartner
2. Informații proprii din cadru procesului de activitate a firmei DATA PROTECTION CONSULTING.
3. https://malwareless.com/wannacry-ransomware-massively-attacks-computer-systems-world/