Securitatea cibernetică

Lumea în care trăim devine din ce în ce mai interdependentă, iar acest lucru se datorează în mare parte evoluţiilor din domeniul tehnologieiinformaţiei şi comunicaţiilor. Această interdependenţă crescândă generează numeroase avantaje, cât şi dezavantaje, având în vedere faptul că instituţii publice şi companii private au devenit aproape în totalitate dependente de sistemeleinformatice pentru a îndeplini activităţi importante. Aşadar, guvernele de peste tot în lume trebuie să se pregătească pentru a face faţă unor provocări noi care pot apărea în spaţiul cibernetic, deoarece viaţa de zi cu zi a oricărui cetăţean, economia naţională, precum şi securitatea naţională a oricărui stat depind în prezent de stabilitatea şi securitatea spaţiul cibernetic.

Aceste provocări sunt incluse în conceptul de “securitate cibernetică” care se referă la ameninţări, vulnerabilităţi şi necesitatea ca guverne şi structuri supra-statale să dezvolte o strategie de securitate cuprizătoare pentru reţeaua lor digitală. Acest lucru implică crearea şi finanţarea unor instituţii care să se ocupe doar de securitatea cibernetică, realizând planuri pentru prevenirea atacurilor cibernetice, pentru posibilitatea de a avea un răspuns rapid în cazul în care asemenea evenimente au lor, pentru abilitatea de a descoperi .

persoanele sau organizaţiile responsabile pentru acestea astfel încât să fie aduse în faţa justiţiei şi, nu în ultimul rând, pentru abilitatea de a înlocui sau repara în cel mai scurt timp componentele afectate ale reţelei digitale.Securitatea cibernetică este starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și non-repudierea informațiilor în format electronic, a resurselor și serviciilor publice sau private, din spațiul cibernetic.

Infrastructura oricarei natiuni este compusa din institutii publice si private din sectoarele agricol, alimentar, apa, sanatate publica, transport, finante si banci, industria chimica si a altor substante speciale, servicii postale si maritime. Sistemul central al acestei infrastructuri îl constituie spatiul cibernetic - de mii de calculatoare interconectate, servere, rutere, comutatoare (switch-uri), precum si din cablurile de fibra optica

Ce vizează acţiunile ostile

Acestea vizează, în principal:
– perturbarea, dezactivarea, distrugerea, degradarea sau controlarea în mod malițios a unui sistem sau a unei infrastructuri informaționale;
– afectarea integrității datelor sau sustragerea informațiilor restricționate.

De exemplu, date sensibile (contracte, proiecte etc.) pot fi exfiltrate de atacatori informatici sau recuperate de aceștia în cazul pierderii sau furtului unui dispozitiv portabil (telefon inteligent, tabletă, laptop etc.).

Securitatea cibernetică este o prioritate pentru buna funcționare a sistemelor guvernamentale sau de control industrial (producția și distribuția de energie electrică, distribuția de apă) etc. Pentru statul român, securitatea cibernetică este „starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic, a resurselor și serviciilor publice sau private, din spațiul cibernetic“.

Un atac cibernetic asupra unui sistem de control industrial (Supervisory Control and Data Acquisition System – SCADA) poate determina pierderea controlului, oprirea sau deteriorarea instalațiilor. Aceste incidente grave de securitate sunt însoțite adeseori de pierderi economice, financiare și de afectarea imaginii organizației.

Aceste pericole pot fi totuși reduse semnificativ prin folosirea unui set de bune practici, puțin costisitoare, chiar gratuite, și ușor de aplicat. Conștientizarea riscurilor de către angajați este foarte eficientă pentru a limita o mare parte din vulnerabilități.

Surpriza din ataşament

E-mail-urile și atașamentele acestora au un rol foarte important în realizarea atacurilor informatice.

În momentul în care primiți un e-mail, acordați atenție următoarelor aspecte:
– identitatea expeditorului nu este garantată: verificați coerența între expeditor și conținutul mesajului;
– nu deschideți atașamente provenind de la persoane necunoscute. Acestea pot conține software realizat în scopuri nelegitime sau malițioase (malicious software sau malware, cum ar fi viermi, troieni, spyware, forme de adware etc.);
– nu răspundeți e-mail-urilor conținând solicitări de date personale sau confidențiale (de exemplu codul PIN și numărul cardului bancar).

Rețelele de criminalitate informatică, prin acțiuni de manipulare a persoanelor (inginerie socială), distribuie către mai mulți utilizatori mesaje electronice nesolicitate (spam), cu un conținut aparent comercial, de publicitate pentru produse și servicii, pentru infectarea utilizatorilor. În urma infectării sistemului informatic, de exemplu, acesta poate deveni parte a unui botnet – o rețea de calculatoare infectate prin diverse metode de către o persoană sau entitate rău-intenționată. Odată infectate, calculatoarele sunt folosite de cel care controlează rețeaua (botmaster), pentru sustragerea de date confidențiale sau bancare, pentru inițierea de atacuri de tip DdoS, pentru spargerea parolelor sau pentru căutarea și exfiltrarea de informații.

Componenta software a unui botnet este formată din 2 părți: clientul și serverul de comandă și control (C&C). În general,

modulele client au implementate rutine de asigurare a persistenței în sistemul infectat prin autocopierea în zona de start-up a sistemului de operare. Botmasterul este cel care controlează, prin intermediul serverului C&C, mașinile infectate. El poate, în funcție de tipul botnet-ului, să administreze, monitorizeze și să obțină diverse statistici privind activitatea boților prin intermediul unui panou de comandă și control.