Q-EAST SOFTWARE
Smart Systems Management

ÎNDRUMAR DE PLANIFICARE A SECURITĂȚII CIBERNETICE

**Traducere în limba română după documentul "Cyber Security Planning Guide"*

întocmit de FCC - Federal Communications Commission, SUA

Federal Communications Commission

CUPRINS

CUVÂNT ÎNAINTE

În contextul unui mediul informațional dinamic și predispus atacurilor cibernetice de amploare, este important ca fiecare organizație, fie că vorbim de companii mai mari sau mai mici sau de instituții publice si agenții guvernamentale, să adere la implementarea unor acțiuni bine puse la punct de securitate cibernetică.

Astfel, devine o misiune în sine identificarea responsabilă a vulnerabilităților sistemelor informatice, atât pentru protecția datelor cu valență strategică, cât și pentru asigurarea unei bune funcționări a infrastructurilor critice organizației.

În sprijinul efortului de consolidare la nivel instituțional a *Strategiei de securitate cibernetică a României*, Q-East Software furnizează soluții de ultimă generație pentru managementul și securitatea sistemelor informatice, a bazelor de date și a aplicațiilor companiilor și instituțiilor din sectorul privat sau public.

Q-East Software face de peste un deceniu pionierat în promovarea soluțiilor de securitate cibernetică și este alături de companiile vizionare care conştientizează nevoia stringentă de a situa managementul şi protecţia datelor pe primul plan în politicile lor de dezvoltare.

„Îndrumarul de planificare a securității cibernetice” este un document util în elaborarea planurilor de acțiune personalizate în materie de securitate cibernetică, fiind realizat pe baza traducerii în limba română a documentului *“Cyber Security Planning Guide”,* întocmit de prestigioasa organizație Federal Communications Commission (FCC), agenție independentă a Guvernului Statelor Unite ale Americii, supravegheată de Congres, care reglementează domeniul telecomunicațiilor și cel al inovațiilor tehnologice de peste Ocean.

Acest ghid de planificare este conceput pentru a întâmpina nevoile companiei dumneavoastră, utilizând instrumentul personalizabil Cyber Planner al FCC. Instrumentul este conceput pentru organizațiile cărora le lipsesc resursele de angajare a personalului dedicat pentru a-şi proteja afacerea, informaţiile şi clienţii împotriva ameninţărilor cibernetice. Chiar şi o societate cu un computer sau un terminal de carduri de credit poate beneficia de acest instrument important.

În general, recomandăm ca societăţile care utilizează reţele mai sofisticate cu zeci de computere să consulte un expert în securitatea cibernetică, pe lângă utilizarea planificatorului cibernetic. FCC nu oferă garanţii cu privire la respectarea orientărilor oferite de acest instrument şi nu este responsabilă de niciun prejudiciu care poate apărea ca rezultat al folosirii sale dacă nu sunt respectate modalitățile de utilizare.

Prezentele orientări au fost dezvoltate de FCC, la acestea contribuind şi partenerii din sectorul public şi privat, inclusiv Departamentul de Securitate Naţională, Alianţa Naţională de Securitate Cibernetică şi Camera de Comerţ a Statelor Unite ale Americii. La sfârșitul materialului, veți găsi un glosar de termeni utilizați frecvent în securitatea cibernetică, care vă vor fi de folos pentru întocmirea materialelor proprii de abordare a acestui vast domeniu.

I. CONFIDENȚIALITATEA ŞI PROTECȚIA DATELOR

Securitatea datelor este crucială pentru toate organizațiile. Informaţiile despre consumatori şi clienţi, informaţiile despre plăţi, dosarele personale, detaliile conturilor bancare - toate acestea sunt adesea imposibil de înlocuit în cazul în care sunt pierdute şi devin periculoase dacă ajung în mâinile infractorilor. Pierderea de date cauzată de dezastre precum inundaţiile sau incendiile este devastatoare, însă dacă acestea ajung la hackeri sau sunt contaminate de software-uri rău intenţionate, aceasta poate avea consecinţe mult mai mari. Modul în care dumneavoastră manipulaţi şi vă protejaţi datele este esenţial pentru securitatea afacerii dumneavoastră şi pentru asigurarea confidențialității clienţilor, angajaţilor şi partenerilor.

ELEMENTELE DE ACŢIUNE ALE PLANULUI CIBERNETIC

1.1 REALIZAŢI UN INVENTAR AL DATELOR

Puteți realiza acest inventar răspunzând pe rând la următoarele întrebări:

Ce fel de date deține afacerea dumneavoastră?

O afacere obişnuită va deține toate tipurile de date, unele dintre ele mai valoroase şi mai sensibile decât altele, însă toate datele au valoare pentru cineva. Datele afacerii dumneavoastră pot include date ale clienţilor precum înregistrări contabile, contabilitatea tranzacţiilor şi informaţii financiare, detalii de contact şi adrese, istoricul cumpărăturilor, obiceiurile de cumpărare şi preferinţele, precum şi informaţii despre angajaţi precum dosarele de salarizare, informaţiile despre plata directă a salariilor în conturile bancare, numerele de securitate socială, adresele de domiciliu şi numerele de telefon, adresele de email de serviciu şi personale. De asemenea, acestea pot include informaţii despre afaceri proprietare şi sensibile precum evidenţele financiare, planurile de marketing, design-urile produselor, şi informaţiile despre impozitele statale, locale şi federale.

Cum sunt manipulate şi protejate acele date?

Experţilor în securitate le place să spună că datele sunt supuse riscului atunci când sunt transferate. Dacă toate datele legate de afacerea dumneavoastră s-ar afla într-un singur computer sau server care nu este conectat la internet, şi nu ar părăsi niciodată acel computer, ar fi probabil foarte uşor de protejat.

Însă majoritatea activităţilor necesită ca datele să fie transferate şi utilizate în întreaga companie. Pentru a fi înţeleşi, datele trebuie să fie accesate şi utilizate de angajaţi, analizate şi cercetate în scopuri de marketing, utilizate pentru a contacta clienţii, şi chiar utilizate împreună cu partenerii cheie. Ori de câte ori datele sunt transferate, acestea pot fi expuse diferitelor pericole.

În calitate de proprietar al unei organizaţii sau angajat al unei instituţii publice, trebuie să aveţi un plan şi o politică clară – un set de linii directoare, dacă doriţi – despre cum trebuie manipulat, validat şi protejat fiecare tip de date, în funcţie de unde se deplasează şi cine le va utiliza.

Cine are acces la date şi în ce circumstanţe?

Nu orice angajat trebuie să aibă acces la toate informaţii. Personalul de marketing nu ar trebui să aibă nevoie sau nu ar trebui să fie lăsat să vizualizeze datele despre salarizarea angajaţilor şi personalul administrativ nu trebuie să acceseze toate informaţiile cu privire la clienţi.

În momentul în care faceţi un inventar al datelor şi ştiţi exact ce date deţineţi şi unde sunt păstrate, este important să desemnaţi atunci drepturile de acces la acele date. Să faceţi acest lucru înseamnă pur şi simplu să creaţi o listă a anumitor angajaţi, parteneri sau contractanţi care să aibă acces la anumite date, în ce circumstanţe, şi cum vor fi acele privilegii de acces gestionate şi urmărite.

Este posibil ca afacerea să aibă o varietate de date cu potential confidential, inclusiv:

- Înregistrările privind vânzările către clienţi
- Creditele şi tranzacţiile clienţilor
- Corespondenţa clienţilor şi listele de emailuri
- Informaţii despre suportul oferit clienţilor
- Informaţii despre garanţiile clienţilor
- Registrele medicale sau privind sănătatea pacienţilor
- Înregistrările privind salarizarea angajaţilor
- Liste cu adresele de email ale angajaţilor
- Registrele medicale şi privind sănătatea angajaţilor
- Evidenţele financiare ale organizatiei
- Planurile de marketing

- Prospecte de afaceri şi chestionare
- Design produse şi planuri de dezvoltare
- Corespondenţă juridică, cu privire la impozite şi financiară

1.2 ORGANIZAȚI DATELE ÎN LOCAȚII ADECVATE

După ce ați identificat datele, înregistrați locația acestora și mutați-le în locații mai adecvate, în funcție de necesități.

1.3 DEZVOLTAŢI O POLITICĂ DE CONFIDENȚIALITATE

Confidențialitatea este importantă pentru afacere şi pentru clienţi. Încrederea continuă în practicile de afaceri, produsele companiei şi manevrarea sigură a informaţiilor unice ale clienţilor are impact asupra profitabilităţii. Politica de confidențialitate este o garanţie pentru clienţi că veţi utiliza şi proteja informaţiile acestora în baza temeiului legal.

Politica de confidențialitate începe cu o afirmaţie simplă şi clară care descrie informaţiile pe care vreți sa le colectați despre clienţi (adrese fizice, adrese de email, istoric navigare, etc), şi ce doriți să faceţi cu acestea. Clienţii, angajaţii şi chiar proprietarii de afaceri se aşteaptă din ce în ce mai mult să faceţi din confidențialitatea informațiilor lor o prioritate.

Există de asemenea un număr din ce în ce mai mare de reglementări care protejează confidențialitatea clientului şi a angajatului şi adesea, penalizări costisitoare pentru nerespectarea confidențialității. Veţi fi răspunzător pentru ceea ce solicitaţi şi oferiţi în politica de confidențialitate.

De aceea este important să creaţi propria politică de confidențialitate cu grijă şi să o afişaţi pe site-ul dumneavoastră web. De asemenea, este important să împărtășiți politicile, regulile şi aşteptările dumneavoastră despre confidențialitate cu toţi angajaţii şi partenerii care pot veni în contact cu acele informaţii. Angajaţii dumneavoastră trebuie să fie familiarizați cu politica de confidențialitate cerută prin lege şi cu ceea ce înseamnă pentru activitatea lor obişnuită zilnică.

Politica de confidențialitate trebuie să se refere la următoarele tipuri de date:

Informaţii personale identificabile: Adesea denumite IPI, aceste informaţii includ numele şi prenumele, adresele de domiciliu şi sediile, adresele de email, numerele cardurilor de credit şi de conturi bancare, numerele de identificare fiscală, codurile pacienților şi

numerele de securitate socială. Acestea pot, de asemenea, să includă genul, vârsta şi data naşterii, oraşul naşterii sau de reşedinţă, numărul permisului de conducere, numerele de telefon fix şi celular.

Informaţii personale cu privire la sănătate: Fie că sunteţi un furnizor de servicii medicale cu multe informaţii sensibile despre pacienţi sau pur şi simplu gestionaţi informaţii medicale sau cu privire la sănătate pentru un număr mic de angajaţi, este vital să protejaţi acele informaţii. Anumite studii au constatat că majoritatea consumatorilor sunt foarte preocupaţi de confidențialitatea şi protecţia dosarelor lor medicale. Aceştia nu vor ca informaţiile cu privire la sănătatea lor să ajungă în mâinile hackerilor sau ale hoţilor de identitate care ar putea să abuzeze de acestea în scopul câştigului financiar.

Informaţii despre clienţi: Acestea includ informaţii despre plăți, cum ar fi numerele cardurilor de credit sau de debit şi codurile de verificare, adresele de facturare şi livrare, adresele de email, numerele de telefon, istoricul cumpărăturilor, preferinţele de cumpărare şi comportamentul de cumpărare.

1.4 PROTEJAŢI DATELE COLECTATE PE INTERNET

Site-ul web poate fi un loc excelent pentru colectarea de informaţii – de la tranzacţii şi plăţi până la istoricul achiziţiei şi cel al navigării, şi chiar abonările la buletinele informative, interogările online şi solicitările clienţilor.

Aceste date trebuie protejate, fie că vă găzduiți propriul site web şi astfel vă administraţi propriile servere, fie că site-ul web şi bazele de date sunt găzduite de un terţ cum ar fi o companie de găzduire web.

În cazul în care colectaţi datele prin intermediul unui site web găzduit de un terţ, asiguraţi-vă că terţul protejează complet acele date. Pe lângă implementarea tuturor celorlalte măsuri de precauţie care au fost descrise, precum clasificarea datelor şi controlul accesului, trebuie să vă asiguraţi că orice date colectate prin intermediul site-ului web şi stocate de terţ sunt suficient de sigure. Acest lucru asigură protecţie împotriva hackerilor şi a terţilor, precum şi a angajaţilor respectivei companii de găzduire.

1.5 CREAŢI STRATURI DE SECURITATE

Protecția datelor, ca şi orice altă provocare de securitate, înseamnă crearea straturilor de protecţie. Ideea de a stratifica securitatea este simplă: nu puteţi şi nu trebuie să vă bazaţi

doar pe un mecanism de securitate – cum este o parolă - pentru a proteja ceva sensibil. Dacă acel mecanism de securitate cedează, nu vă mai rămâne nimic care să vă protejeze.

În ceea ce priveşte securitatea datelor, există un număr de straturi procedurale şi tehnice cheie pe care trebuie să le aveţi în vedere:

Inventariaţi datele

Am menţionat mai sus necesitatea de a realiza un inventar al datelor astfel încât să aveţi o imagine completă a tuturor datelor pe care afacerea dumneavoastră le deţine şi le controlează. Este esenţial să realizaţi un inventar complet, astfel încât să nu treceţi cu vederea anumite date sensibile care ar putea fi expuse.

Identificaţi şi protejaţi datele sensibile şi valoroase

Clasificarea datelor este unul dintre cei mai importanţi paşi în securitatea datelor. Nu toate datele sunt create egale, şi puţine organizaţii au timpul sau resursele pentru asigurarea protecţiei maxime a tuturor datelor pe care le deţin. De aceea, este important să vă clasificaţi datele în funcţie de cât de sensibile sau de valoroase sunt – astfel încât să ştiţi care sunt cele mai sensibile date, unde se află şi cât de bine sunt protejate.

Clasificările uzuale ale datelor includ următoarea terminologie:

EXTREM DE CONFIDENŢIALE: Această clasificare se aplică celor mai sensibile informaţii despre afaceri care au scopul de a fi utilizate strict în cadrul companiei dumneavoastră. Divulgarea lor neautorizată ar putea să aibă un impact grav şi advers asupra companiei, partenerilor de afaceri, vânzătorilor şi/sau clienţilor pe termen scurt, mediu şi lung. Acestea pot include date cu privire la tranzacţiile cu cardurile de credit, numele şi adresele clienţilor, conţinutul benzii magnetice a cardurilor, parole şi coduri PIN, dosarele despre salarizarea angajaţilor, numerele de securitate socială, informaţiile despre pacienţi (dacă sunteţi o companie de servicii medicale) şi date similare.

SENSIBILE: Această clasificare se aplică informaţiilor sensibile despre afaceri, care au scopul de a fi utilizate în cadrul companiei dumneavoastră şi informaţiilor pe care dumneavoastră le consideraţi a fi private. Exemplele includ evaluările performanţelor angajaţilor, rapoartele de audit intern, diverse rapoarte financiare, propuneri de design ale produselor, contracte de parteneriat, planurile de marketing şi listele de emailuri pentru marketing.

DOAR PENTRU UZ INTERN: Această clasificare se aplică informaţiilor sensibile care sunt în general accesibile unui public larg şi al căror scop este de a fi utilizate doar în cadrul companiei dumneavoastră.

Controlaţi accesul la datele dumneavoastră

Indiferent de tipul de date pe care le deţineţi, trebuie să controlaţi accesul la acestea. Cu cât sunt mai sensibile datele, cu atât este mai restrictiv accesul. Ca regulă generală, accesarea datelor trebuie să fie pe baza principiului nevoii de cunoaştere. Doar indivizii care au o nevoie specifică de a accesa anumite date trebuie să fie lăsaţi să facă acest lucru.

După ce aţi clasificat datele, începeţi procesul de atribuire a privilegiilor şi a drepturilor de acces. Acest lucru presupune întâi crearea unui document cu numele persoanelor care pot accesa datele şi specificarea categoriilor de date care pot fi accesate şi în ce circumstanţe. Aici se adaugă regulile de utilizare şi modul în care se solicită să se facă protecţia datelor. Ca parte din acest proces, o afacere ar trebui să aibă în vedere dezvoltarea unui plan şi a unei politici concrete – un set de linii directoare – despre cum trebuie manevrat şi protejat fiecare tip de date, în funcţie de cine are nevoie de acces la acestea şi de nivelul clasificării lor.

Securizaţi datele

Pe lângă măsurile de securitate administrativă care determină cine are acces şi la ce date, măsurile de securitate tehnică sunt esenţiale. Două măsuri de securitate primară pentru date sunt parolele şi criptarea.

Parolele implementate pentru a vă proteja cele mai sensibile date trebuie să fie cât mai solide posibil. Acest lucru înseamnă că parolele alese trebuie să fie aleatorii, complexe şi lungi (cel puţin 10 caractere), schimbate cu regularitate şi păzite îndeaproape de cei care le-au setat. Instruirea angajaţilor cu privire la principiile unor parole sigure şi importanţa acestora reprezintă o necesitate.

Este posibil ca parolele sigure să nu fie suficiente pentru protejarea datelor sensibile. Este posibil ca organizațiile să dorească să aibă în vedere autentificarea cu doi factori, care combină adesea o parolă cu o altă metodă de verificare, cum ar fi un cod numeric personal dinamic sau codul PIN.

Unele metode populare ale identificării cu doi factori includ:

- Un element pe care solicitantul îl cunoaşte în mod individual ca pe un secret, cum ar fi o parolă sau un cod PIN.
- Un element care doar solicitantul, cum ar fi un paşaport, un simbol fizic sau o carte de identitate.
- Un element pe care doar solicitantul îl poate furniza ca date biometrice, cum ar fi amprentele proprii sau geometria feţei.

O altă tehnologie esenţială de protejare a datelor este criptarea. Criptarea a fost utilizată pentru a proteja datele sensibile şi comunicaţiile timp de decenii, iar criptarea actuală este foarte rezonabilă ca preţ, uşor de utilizat şi extrem de eficientă în protecția datelor.

Criptarea codifică informaţiile la un grad atât de avansat ca acestea să nu poată fi citite şi utilizate de nimeni care nu are cheia potrivită pentru a debloca datele. Cheia este ca o parolă, astfel că este foarte important ca această cheie să fie protejată în mod corespunzător în orice moment.

Criptarea este rezonabilă ca preţ chiar şi pentru cele mai mici organizații, iar unele software-uri de criptare sunt gratuite. Puteţi folosi criptarea pentru a cripta sau proteja un întreg hard disk, un folder specific sau o unitate sau doar un singur document. De asemenea, puteţi utiliza criptarea pentru a vă proteja datele pe o unitate USB şi pe orice alt suport detaşabil.

Deoarece nu toate nivelurile de criptare sunt create egale, organizațiile ar trebui să aibă în vedere utilizarea unei metode de criptare a datelor care este certificată FIPS (Standardul Federal de Prelucrare a Informaţiei), ceea ce înseamnă că aceasta a fost certificată pentru conformitatea cu protocoalele federale ale securităţii guvernamentale.

Creaţi copii de rezervă pentru datele dumneavoastră

Crearea copiilor de rezervă este la fel de importantă ca protecția datelor dumneavoastră. În cazul în care datele dumneavoastră sunt furate de hoţi sau hackeri sau chiar şterse accidental de un angajat, cel puţin veţi avea o copie pe care să vă bazaţi.

Implementaţi o politică care să specifice pentru care date este nevoie de copii de rezervă şi cum; cât de des se fac copii de rezervă ale acestora; cine este responsabil de crearea copiilor de rezervă; unde şi cum sunt stocate copiile de rezervă şi cine are acces la acele copii de rezervă.

Organizațiile au multe opţiuni pentru realizarea unor copii de rezervă rezonabile ca preţ, fie că se fac copii de rezervă ale acestora pe o unitate externă din biroul dumneavoastră, sau că se fac copii de rezervă automat şi online astfel încât toate datele dumneavoastră să fie stocate într-un centru de date la distanţă şi sigur.

Reţineţi că suporturile fizice precum un disc sau o unitate utilizată pentru stocarea copiilor de rezervă a datelor, sunt vulnerabile indiferent de tip, astfel că trebuie să vă asiguraţi că protejaţi orice copii de rezervă stocate în biroul dumneavoastră sau în afara locaţiei şi, că sistemele de stocare a datelor pentru copiile de rezervă sunt criptate.

1.6 PLANUL PENTRU PIERDEREA SAU FURTUL DATELOR

Orice organizație trebuie să-şi facă un plan pentru situaţiile neaşteptate, care includ pierderea sau furtul de date. Pierderea sau furtul de date nu vă prejudiciază doar afacerea, brandul şi încrederea clienţilor, acestea vă expun, de asemenea, la reglementările statale şi federale adesea costisitoare care acoperă protecţia datelor şi confidențialitatea. Pierderea datelor poate, de asemenea, expune afacerile la un risc semnificativ de litigii.

De aceea, este esenţial să se înţeleagă exact care date sau reglementări cu privire la încălcarea securităţii vă afectează afacerea şi cât de pregătiţi sunteţi să le faceţi faţă. Acest lucru ar trebui să înceapă de la un plan de intervenţie în caz de încălcare a securităţii datelor care va face mai uşoară lansarea unui răspuns rapid şi coordonat în cazul pierderilor sau a furtului de date.

Cel puţin, toţi angajaţii şi contractanţii ar trebui să înţeleagă că trebuie să raporteze imediat orice pierdere sau furt de informaţii responsabilului companiei. Şi întrucât confidenţialitatea datelor şi încălcarea legilor în această privință sunt chestiuni foarte stricte, nicio pierdere nu trebuie ignorată. Un angajat care nu-şi aminteşte unde a lăsat un suport de rezervă, poate totuşi reprezenta un caz de încălcare a securităţii datelor şi în acest caz trebuie să acţionaţi în mod corespunzător.

Dacă nu credeţi că o încălcare a securităţii datelor ar putea avea loc în organizația dumneavoastră, gândiţi-vă la următoarea situație. În 2010, Serviciul Secret al S.U.A. şi Unitatea de analiză criminalistică a Verizon Communications Inc. a răspuns la 761 de încălcări combinate a securităţii datelor. Din acestea, 482, sau 63 la sută, erau companii cu 100 de angajaţi sau mai puţin. Iar în anul 2011, Visa a estimat că aproximativ 95 la sută din

încălcările securităţii datelor cardurilor de credit pe care le-a descoperit se refereau la clienţii organizațiilor mici.

Online Trust Alliance are un ghid comprehensiv pentru pregătirea unei organizații în vederea securităţii datelor, disponibil la https://otalliance.org/resources/data-breach-protection

Comisia Federală pentru Comerţ are de asemenea materiale pentru a ajuta organizațiile să-şi securizeze datele aflate în grija lor şi pentru a proteja confidențialitatea datelor clienţilor, inclusiv un tutorial video interactiv, la adresa http://business.ftc.gov/privacy-and-security.

II. ESCROCHERIILE ŞI FRAUDA

Noile tehnologii de telecomunicaţii pot oferi nenumărate oportunităţi pentru organizații, însă acestea oferă, de asemenea, infractorilor cibernetici multe modalități noi de a vă prejudicia afacerea, de a vă înşela clienţii şi de a vă strica reputaţia. Organizațiile de toate mărimile trebuie să fie conştiente de cele mai obişnuite înşelătorii comise online.

Pentru a vă proteja afacerea împotriva înşelătoriilor online, fiţi precauţi în momentul în care vizitaţi linkurile web sau când deschideţi ataşamente primite de la expeditori necunoscuţi, asiguraţi-vă că păstraţi toate software-urile actualizate şi că protejați cardurile de credit împotriva activităţii neautorizate.

ELEMENTELE DE ACŢIUNE ALE PLANULUI CIBERNETIC

2.1 INSTRUIŢI ANGAJAŢII PENTRU A RECUNOAŞTE INGINERIA SOCIALĂ

Ingineria socială, cunoscută şi ca „pretexting” (folosirea de pretexte), este utilizată de mulţi infractori, atât online, cât şi offline, pentru a amăgi persoanele vizate să ofere informaţii personale şi/sau să instaleze software-uri rău intenționate pe computerele, dispozitivele sau reţelele lor. Ingineria socială are succes, întrucât atacatorii cibernetici fac tot ce pot pentru ca lucrarea lor să pară şi să sune legitimă, uneori chiar utilă, ceea ce face mai uşoară înşelarea utilizatorilor.

Mare parte din ingineria socială offline are loc prin telefon, însă aceasta are loc frecvent și online. Informaţiile adunate din reţelele sociale sau afişate pe site-urile web pot fi suficiente pentru a crea un şiretlic convingător. De exemplu, profilurile de LinkedIn, postările pe Facebook şi mesajele pe Twitter pot permite unui infractor să întocmească dosare detaliate despre angajaţi. Instruirea personalului cu privire la riscurile implicate în publicarea detaliilor personale sau de afaceri pe internet poate să prevină pierderile personale şi organizaţionale.

Mulţi infractori utilizează tactica ingineriei sociale pentru a determina utilizatorii să instaleze în mod voluntar software-uri rău intenționate pentru computere, cum ar fi falsul antivirus, crezând că fac ceva care îi va ajuta. Falsul antivirus este conceput pentru a fura informaţii mimând un software legal de securitate. Utilizatorii care sunt păcăliţi să încarce programe rău intenționate pe computerele lor, pot să furnizeze posibilitatea controlului de la distanţă unui atacator, instalând fără să ştie software-uri care pot fura informaţii financiare sau care pot încerca pur şi simplu să le vândă software-uri de securitate false.

Software-ul rău intenţionat poate de asemenea să facă modificări de sistem care fac dificilă terminarea programului. Prezenţa pop-up-urilor care afişează avertismente de securitate neobişnuite şi care solicită informaţii despre cardurile de credit este cea mai evidentă metodă de identificare a contaminării cu antivirus fals.

2.2 PROTEJAŢI-VĂ ÎMPOTRIVA FRAUDEI ONLINE

Frauda online ia multe înfăţişări care pot afecta pe oricine, inclusiv organizațiile şi angajaţii acestora. Este utilă menţinerea transmiterii de mesaje online constante şi previzibile în timpul comunicării cu clienţii, pentru a-i împiedica pe alţii să se dea drept reprezentanți ai organizației.

Asiguraţi-vă că nu solicitaţi niciodată informaţii personale sau detalii despre conturi prin email, reţele sociale sau alte mesaje online. Informaţi-vă clienţii că nu veţi solicita niciodată acest tip de informaţii prin astfel de canale şi instruiţi-i să vă contacteze direct în cazul în care au întrebări.

2.3 PROTEJAŢI-VĂ ÎMPOTRIVA PHISHING-ULUI (ÎNŞELĂTORIEI)

Phishing-ul (înşelătoria) este tehnica utilizată de infractorii online pentru a înşela persoanele, făcându-le să creadă că au de-a face cu un site web sau cu o altă entitate de încredere. Organizațiile înfruntă această ameninţare din două direcţii - hoţii de identitate pot să imite angajații pentru a obţine avantaje de la clienţii instituției şi pot încerca să le fure angajaţilor credențialele online. Atacatorii profită adesea de evenimente actuale şi anumite perioade ale anului, precum:

- Dezastrele naturale (Uraganul Katrina, tsunami-ul indonezian)
- Alertele de epidemii şi sanitare (H1N1)
- Problemele economice
- Alegerile politice majore
- Sărbătorile

Organizațiile trebuie să se asigure că sistemul lor de comunicaţii online nu solicită niciodată clienţilor să trimită informaţii sensibile prin email, în timpul vizitelor personale sau prin telefon. Este important să faceţi o afirmaţie clară în comunicările organizației în care să subliniaţi că nu veţi solicita niciodată informaţii prin email, astfel încât, în cazul în care cineva are drept ţintă clienţii dumneavoastră, aceştia să poată realiza că solicitarea este o înşelătorie.

Sensibilizarea angajaților este cea mai bună apărare împotriva situațiilor în care utilizatorii sunt păcăliţi să-şi furnizeze numele de utilizatori şi parolele infractorilor cibernetici. Explicaţi tuturor că nu trebuie să răspundă mesajelor primite care solicită informaţii personale. Dacă un străin susţine că este dintr-o organizaţie legală, verificaţi identitatea sa înainte de a-i împărtăşi orice informaţie personală sau clasificată. De asemenea, pentru a evita atragerea lor pe un site fals, angajaţii ar trebui să ştie să nu apese click pe un link transmis prin email de la o sursă nesigură. Angajaţii care trebuie să acceseze un link de pe un site web dintr-o sursă îndoielnică trebuie să deschidă o fereastră a unui browser de internet şi să tasteze manual adresa web a site-ului pentru a se asigura că linkul transmis prin email nu redirecţionează în mod intenționat către un site periculos.

Acest sfat este critic în special pentru protecția online a conturilor bancare, care aparţin organizaţiei. Infractorii au drept ţintă conturile bancare ale organizațiilor mai mult decât orice altceva. În cazul în care consideraţi că aţi dezvăluit informaţii sensibile despre organizaţie, asiguraţi-vă că:

- Raportaţi acest lucru persoanelor responsabile din cadrul organizaţiei
- Contactaţi instituţia financiară de care aparţineți şi închideţi orice conturi compromise (în cazul în care consideraţi că datele financiare sunt în pericol)
- Schimbaţi orice parole pe care le-aţi dezvăluit şi dacă aţi utilizat aceeaşi parolă pentru mai multe resurse, asiguraţi-vă că aţi schimbat-o pentru fiecare cont.

2.4 NU VĂ LĂSAŢI PĂCĂLIŢI DE OFERTELE DE FALȘI ANTIVIRUȘI

Falsul antivirus, „scareware” şi alte înşelătorii online împotriva securităţii au fost în spatele câtorva dintre cele mai de succes fraude online din ultima vreme. Asiguraţi-vă că organizaţia dumneavoastră are implementată o politică care explică care este procedura de urmat în cazul în care computerul unui angajat este infectat cu un virus.

Instruiţi-vă angajaţii să recunoască un mesaj legal de avertizare (utilizând un fişier de testare de pe eicar.org, de exemplu) şi să notifice în mod corespunzător echipa dumneavoastră IT dacă s-a întâmplat ceva rău sau suspect.

Dacă este posibil, configuraţi-vă computerele astfel încât să nu permită utilizatorilor obişnuiţi să aibă acces administrativ. Acest lucru va minimiza riscul ca aceştia să instaleze

software-uri rău intenționate şi va condiţiona utilizatorii, întrucât adăugarea unui software neautorizat să lucreze pe computere este împotriva politicii organizației.

2.5 PROTEJAŢI-VĂ ÎMPOTRIVA SOFTWARE-URILOR RĂU INTENŢIONATE

Organizațiile pot experimenta o situație de criză în urma introducerii nedorite a software-urilor rău intenţionate, care pot intra în dispozitive de pe internet, prin descărcări, ataşamente, email, rețele sociale şi alte platforme. Software-ul rău intenţionat specific de care trebuie să fim conştienţi este key-logging, care urmăreşte apăsarea tastelor unui utilizator.

Multe organizații devin victimele instalării de software-uri rău intenţionate de tip key-logging în sistemele computerelor din mediul lor informatic. Odată instalate, software-urile rău intenţionate pot înregistra apăsările tastelor realizate la un computer, permiţând atacatorilor să vadă parolele, codurile cardurilor de credit şi alte date confidenţiale. Păstrarea software-urilor de securitate actualizate şi repararea computerelor dumneavoastră cu regularitate va face mai dificilă infiltrarea acestui tip de software rău intenţionat în reţeaua dumneavoastră.

2.6 DEZVOLTAŢI O ABORDARE STRATIFICATĂ PENTRU A VĂ PROTEJA ÎMPOTRIVA SOFTWARE-URILOR RĂU INTENȚIONATE

În ciuda progresului înregistrat în crearea unei conştientizări mai mari a ameninţărilor la adresa securităţii pe internet, autorii software-urilor rău intenţionate nu se dau bătuţi. Rapoartele de cercetare privind software-urile rău intenţionate ale firmei SophosLabs văd peste 100.000 de mostre unice în fiecare zi.

Protecţia eficientă împotriva virusurilor, cailor troieni şi a altor software-uri rău intenționate necesită o abordare stratificată pentru apărarea dumneavoastră. Software-ul antivirus este o necesitate, însă nu trebuie să fie singura linie de apărare a unei companii. În schimb, utilizaţi o combinaţie de tehnici pentru a vă păstra mediul sigur.

De asemenea, aveţi grijă cu utilizarea unităţilor UB și a altor suporturi detaşabile. Acestea ar putea avea pre-instalate software-uri rău intenționate care vă pot infecta computerul, astfel că trebuie să vă asiguraţi că aveţi încredere în sursa dispozitivelor cu suporturi detaşabile înainte de a le utiliza.

Combinând ca metode utilizarea filtrării web, protecţia semnăturii antivirus, protecţia proactivă împotriva software-urilor rău intenţionate, paravanele de protecţie, politicile solide de securitate şi instruirea angajaţilor, scade semnificativ riscul de infecţie. Păstrând protecţia software actualizată crește siguranţa sistemelor dumneavoastră.

2.7 FIŢI CONŞTIENŢI DE SPYWARE (PROGRAMELE SPION) ŞI ADWARE

Programele spyware şi adware, în momentul instalării, vor trimite reclame pop-up, vor redirecţiona către anumite site-uri web şi vor monitoriza site-urile web pe care le vizitaţi. Versiunile extreme pot urmări ce taste sunt apăsate. Programele spion pot determina încetinirea computerului dumneavoastră şi, de asemenea, vă pot face susceptibili în ceea ce priveşte furtul datelor confidenţiale. Dacă sunteţi supus ferestrelor pop-up care apar continuu sau dacă sunteţi redirecţionat cu regularitate către alte site-uri web decât cele pe care le tastaţi în browserul dumneavoastră, computerul dumneavoastră este posibil să fi fost infectat cu programe spion.

Pentru a elimina programul spion, executaţi imediat o scanare completă a computerului dumneavoastră cu software-ul antivirus şi, dacă este cazul, folosiți un produs legal, conceput special pentru a elimina programele spion. Pentru a evita infectarea cu programe spion, limitaţi cookie-urile din preferinţele browserului dumneavoastră, nu dați click niciodată pe linkuri cu ferestre pop-up şi fiţi atenţi la software-urile care pot fi descărcate gratis din surse nesigure.

2.8 VERIFICAŢI IDENTITATEA SOLICITANŢILOR DE INFORMAŢII PRIN TELEFON

Mare parte din ingineria socială offline are loc prin telefon. Informaţiile adunate din reţelele sociale şi informaţiile afişate pe site-urile web, pot fi suficiente pentru a crea un şiretlic convingător menit să înșele angajaţii.

Asiguraţi-vă că vă instruiţi angajaţii să nu dezvăluie niciodată apelanţilor, informaţii despre clienţi, numele de utilizatori, parole sau alte detalii sensibile. Atunci când cineva solicită informaţii, contactaţi întotdeauna persoana din nou utilizând un număr de telefon cunoscut sau un cont de email pentru a verifica identitatea solicitantului.

Legături utile

- Utilizaţi resursele Campaniei Opreşte-te.Gândeşte.Conectează-te.™ a Departamentului de Securitate Internă, create special pentru organizațiile care doresc să-și instruiască angajaţii: www.dhs.gov/stopthinkconnect
- Găsiţi cele mai actualizate patch-uri pentru computer şi aplicaţii software necesare: http://www.softwarepatch.com/
- Instrumente gratuite de scanare a securităţii computerelor pentru computerul sau reţeaua dumneavoastră: https://www.staysafeonline.org/stay-safe-online
- Fiţi la curent cu cele mai noi înşelătorii, fraude şi ameninţări la adresa securităţii pe măsură ce au loc: http://nakedsecurity.sophos.com/
- Topuri suplimentare pentru prevenirea phishing-ului: http://www.fraud.org/scams/internet-fraud/phishing
- Învăţaţi cum să faceţi faţă tehnicilor de phishing cu acest joc interactiv: http://cups.cs.cmu.edu/antiphishing_phil/

III. SECURITATEA REŢELELOR

Securizarea reţelei companiei dumneavoastră constă din: (1) identificarea tuturor dispozitivelor şi conexiunilor din reţea; (2) stabilirea limitelor dintre sistemele companiei şi altele; şi (3) impunerea controalelor pentru a vă asigura că accesul neautorizat, abuzul sau evenimentele de refuz de servicii pot fi contracarate sau incluse rapid şi recuperate dacă au loc într-adevăr.

ELEMENTELE DE ACŢIUNE ALE PLANULUI CIBERNETIC

3.1 SECURIZAŢI REŢEAUA INTERNĂ ŞI SERVICIILE CLOUD

Reţeaua companiei dumneavoastră trebuie separată de internetul public prin mecanisme solide de autentificare a utilizatorilor şi sisteme de impunere a politicilor precum paravanele de protecţie şi proxy-urile de filtrare web. Soluţiile suplimentare de monitorizare şi securitate, cum ar fi programele antivirus şi sistemele de detecţie a intruziunilor, trebuie să fie de asemenea utilizate pentru a identifica şi opri încercările rău intenționate de accesare a codurilor sau de accesare neautorizată.

Reţeaua internă

După identificarea punctelor limită din reţeaua companiei dumneavoastră, fiecare limită trebuie evaluată pentru a determina ce tipuri de controale de securitate sunt necesare şi cum pot fi acestea utilizate cel mai bine. Routerele marginale trebuie să fie configurate doar la traficul căilor spre şi de la adresele IP publice ale companiei dumneavoastră, paravanele de protecţie trebuie utilizate pentru a restricţiona traficul doar către şi de la setul minimum de servicii necesare, iar sistemele de prevenire a intruziunilor trebuie configurate pentru a monitoriza activitatea suspectă care trece prin perimetrul reţelei dumneavoastră. Pentru a preveni blocajele, toate sistemele de securitate pe care le utilizaţi în perimetrul reţelei organizației, trebuie să poată partaja lungimea de bandă pe care o oferă furnizorul de servicii internet.

Servicii bazate pe cloud

Consultaţi cu atenţie termenii contractuali stabiliți cu furnizorii de servicii cloud pentru a vă asigura că informaţiile şi activităţile companiei sunt protejate cu acelaşi grad de securitate pe care l-aţi furniza singuri. Solicitaţi securitate şi auditare din partea furnizorilor dumneavoastră de servicii cloud. Analizaţi şi înţelegeţi acordurile privind asigurarea

nivelului de calitate a serviciilor, sau SLA, timpii prevăzuți pentru restaurarea sistemelor şi restabilirea conexiunilor.

De asemenea, trebuie să vă informaţi cu privire la serviciile suplimentare pe care le poate furniza un serviciu cloud. Aceste servicii pot include serviciile de backup şi restaurare şi serviciile de criptare, care pot fi foarte atractive pentru organizații.

3.2 DEZVOLTAŢI POLITICI SOLIDE CU PRIVIRE LA PAROLE

În general, metodele de autentificare cu doi factori, care necesită două tipuri de dovezi că sunteţi cine susţineţi, sunt mai sigure decât simpla utilizare a parolelor statice pentru autentificare. Un exemplu obişnuit poate fi un simbol de securitate personală care afişează coduri de acces în schimbare, pentru a fi utilizate împreună cu o parolă stabilită. Cu toate acestea, sistemele cu doi factori nu pot fi întotdeauna posibil de implementat sau practice pentru o organizație.

Politicile cu privire la parole trebuie să-i încurajeze pe angajaţi să utilizeze cele mai solide parole posibile, fără a crea nevoia sau tentaţia de a reutiliza parolele sau de a le scrie.

3.3 SECURIZAŢI ŞI CRIPTAŢI WI-FI-UL COMPANIEI DUMNEAVOASTRĂ

Controlul accesului wireless

Compania dumneavoastră poate alege să opereze o Reţea locală fără fir (WLAN) pentru utilizarea internetului de către clienţi, invitaţi şi vizitatori. În acest caz, este important ca o astfel de WLAN să fie păstrată separat de reţeaua principală a companiei, astfel încât traficul din reţeaua publică să nu poată traversa sistemele interne ale companiei în orice punct.

Accesul intern, WLAN nepublic trebuie restricţionat la dispozitive specifice şi utilizatori specifici în cea mai mare măsură posibilă, îndeplinind în acelaşi timp necesităţile de afaceri ale organizației. În cazul în care reţeaua WLAN are controale de acces mai puţin stricte decât reţeaua prin cablu a organizației, conexiunile duble - în cazul în care un dispozitiv se poate conecta atât la reţelele fără fir şi cu fir simultan - trebuie interzise prin controale tehnice asupra fiecărui astfel de dispozitiv (de ex., setările comutatorului LAN/WLAN la nivelul BIOS). Tuturor utilizatorilor le trebuie credențiale unice cu date de expirare presetate pentru utilizare în momentul accesării reţelei WLAN interne.

Criptarea wireless

Din cauza defectelor de securitate demonstrabile care sunt cunoscute în vechile forme de criptare fără fir, reţeaua WLAN internă a companiei trebuie să utilizeze doar criptarea Acces protejat Wi-Fi 2 (WPA2).

3.4 CRIPTAŢI DATELE SENSIBILE ALE COMPANIEI

Criptarea trebuie utilizată pentru a proteja datele pe care compania dumneavoastră le consideră sensibile, pe lângă îndeplinirea cerinţelor regulatorii aplicabile cu privire la protecţia informaţiilor. Diferite scheme de criptare sunt potrivite în diferite circumstanţe. Cu toate acestea, aplicaţiile care respectă standardul OpenPGP, cum ar fi PGP (Pretty Good Privacy - Confidențialitate destul de bună) şi GnuPG (Gnu Privacy Guard), oferă o gamă largă de opţiuni pentru securizarea datelor pe disc şi în tranzit. Dacă alegeţi să oferiţi tranzacţii sigure prin intermediul site-ului web al companiei, consultaţi-vă cu furnizorul de servicii cu privire la opţiunile disponibile pentru achiziționarea unui certificat SSL.

3.5 ACTUALIZAŢI CU REGULARITATE TOATE APLICAŢIILE

Toate sistemele şi software-urile, inclusiv echipamentele din reţea, trebuie să fie actualizate la timp întrucât actualizările patch-urilor şi microprogramelor devin indisponibile în timp. Utilizaţi servicii de actualizare automată ori de câte ori este posibil, în special pentru sistemele de securitate precum aplicaţiile împotriva software-urilor rău intenţionate, instrumentele de filtrare web şi sistemele de prevenire a intruziunilor.

3.6 STABILIŢI REGULI SIGURE DE NAVIGARE PE WEB

Reţeaua internă ar trebui să pună la dispoziția angajaților doar acele servicii şi resurse de pe internet care sunt esenţiale pentru activitatea şi nevoile lor de zi cu zi. Utilizaţi caracteristicile sigure de navigare incluse cu software-ul modern de navigare pe web şi un proxy web pentru a vă asigura că site-urile rău intenționate sau neautorizate nu pot fi accesate din reţeaua dumneavoastră internă.

3.7 DACĂ ACCESUL DE LA DISTANŢĂ ESTE PERMIS, ASIGURAŢI-VĂ CĂ ESTE SIGUR

În cazul în care compania dumneavoastră trebuie să ofere accesul de la distanţă la reţeaua internă a companiei dumneavoastră prin internet, o opţiune populară şi sigură este de a

utiliza un sistem sigur al unei Reţele Private Virtuale (VPN) însoţit de autentificarea solidă cu doi factori, utilizând dispozitive simbol hardware sau software.

3.8 CREAŢI O POLITICĂ CU PRIVIRE LA UTILIZAREA SIGURĂ A UNITĂŢII FLASH

Asiguraţi-vă că angajaţii nu introduc niciodată nicio unitate necunoscută sau USB-uri în computerul lor. Aşa cum menţionează *Bazele Securităţii pe internet pentru Afaceri 2.0 a Camerei de Comerț S.U.A*., organizațiile trebuie să stabilească o politică astfel încât angajaţii să ştie că nu trebuie să deschidă niciodată un fişier de pe o unitate flash cu care nu sunt familiarizaţi şi că trebuie să ţină apăsată tasta Shift în momentul în care introduc unitatea flash, pentru a bloca software-urile rău intenţionate.

Legături utile

- Sistemul Microsoft de verificare a tăriei parolelor: https://www.microsoft.com/security/pc-security/password-checker.aspx
- Philip Zimmerman, Unde să obţinem PGP: http://philzimmermann.com/EN/findpgp/
- Publicaţiile despre securitate US-CERT: http://www.us-cert.gov/reading_room/
- Publicaţia specială NIST 800-153, Proiect de directive pentru securizarea reţelelor locale fără fir (WLAN): http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf
- Camera de Comerţ a S.U.A.: *Bazele Securităţii pe internet pentru Afaceri 2.0* https://www.uschamber.com/sites/default/files/issues/technology/files/ISEB-2.0-CyberSecurityGuide.pdf

IV. SECURITATEA SITE-URILOR WEB

Securitatea site-urilor web este mai importantă decât oricând. Serverele web, care găzduiesc datele şi alt conţinut disponibil clienţilor pe internet, sunt adesea cele mai vizate şi atacate componente ale reţelei unei companii. Infractorii cibernetici caută permanent site-uri web securizate în mod necorespunzător pentru a le ataca, în timp ce mulţi clienţi spun că securitatea site-urilor web este un criteriu de top în momentul în care aleg să facă cumpărături online. Drept rezultat, este esenţială securizarea serverelor şi a infrastructurii reţelelor care le susține. Consecinţele unei nerespectări a securităţii sunt mari: pierdere de profituri, prejudicierea credibilităţii, răspunderea judiciară şi pierderea încrederii clienţilor.

În continuare, puteți găsi câteva exemple de ameninţări specifice la adresa securităţii pentru serverele web:

- Infractorii cibernetici pot exploata bug-urile software din serverul web, care stau la baza sistemului de operare, sau conţinutul activ pentru a obţine accesul neautorizat la serverul web. Exemplele de acces neautorizat includ obţinerea accesului la fişiere sau foldere care nu aveau scopul de a fi accesate public şi capacitatea de a executa comenzi şi/sau instala software-uri rău intenționate pe serverul web.
- Atacurile de tip refuz serviciu pot fi direcţionate către serverul web sau infrastructura de suport a reţelei pentru a preveni sau împiedica utilizatorii site-ului web să utilizeze serviciile acestuia. Acest lucru poate include imposibilitatea utilizatorului de a-și accesa emailul, site-urile web, conturile online sau alte servicii. Cel mai obişnuit atac are loc atunci când atacatorul inundă o reţea cu informaţii, astfel încât aceasta să nu poată procesa solicitarea utilizatorului.
- Informaţiile sensibile de pe serverul web pot fi citite sau modificate fără autorizare.
- Informaţiile sensibile despre bazele de date back-end care sunt utilizate pentru a sprijini elementele interactive ale unei aplicaţii web pot fi compromise prin injectarea de comenzi software neautorizate. Exemplele includ injectarea limbajului de interogare structurat (SQL), injectarea LDAP şi a scripturilor inter-site (XSS).
- Informaţiile sensibile necriptate transmise între serverul web şi browser pot fi interceptate.
- Informaţiile de pe serverul web pot fi modificate în scopuri rău intenționate. Desfigurarea site-urilor web este un exemplu raportat în mod obişnuit al acestei ameninţări.

- Infractorii cibernetici pot obţine accesul neautorizat la resurse din altă parte a reţelei organizaţiei printr-un atac de succes asupra serverului web.
- Infractorii cibernetici pot, de asemenea, să atace entităţile externe după ce compromit un server web. Aceste atacuri pot fi lansate direct (de ex., de pe serverul compromis împotriva unui server extern) sau indirect (de ex., de exemplu plasarea de conţinut rău intenționat pe serverul web compromis care încearcă să exploateze vulnerabilităţile din browserele utilizatorilor care vizitează site-ul).
- Serverul poate fi utilizat ca un punct de distribuţie pentru instrumentele de atac, pornografie sau software-uri copiate ilegal.

ELEMENTELE DE ACŢIUNE ALE PLANULUI CIBERNETIC

4.1 PLANIFICAŢI ŞI ABORDAŢI CU GRIJĂ ASPECTELE DE SECURITATE ALE UTILIZĂRII UNUI SERVER WEB PUBLIC.

Întrucât este mult mai dificilă abordarea securităţii după ce utilizarea şi implementarea au avut loc, securitatea trebuie avută în vedere din faza iniţială de planificare. Organizațiile au mai multe şanse să ia decizii despre configurarea computerelor în mod corespunzător şi constant dacă dezvoltă şi utilizează un plan de implementare detaliat, bine conceput. Dezvoltarea unui astfel de plan va sprijini administratorii serverelor web în luarea deciziilor inevitabile de compromis între utilitate, performanţă şi risc.

Organizațiile trebuie, de asemenea, să aibă în vedere cerinţele de resurse umane pentru implementarea şi operarea continuă a serverului web şi a infrastructurii de suport. Următoarele puncte dintr-un plan de implementare:

- Categoriile de personal necesar -- de exemplu, administratorii sistemelor şi cei ai serverelor web, administratorii site-urilor web, administratorii de reţea şi personalul pentru securitatea sistemelor de informaţii.
- Abilităţi şi instruire necesare pentru personalul numit.
- Cerinţele de personal individuale (şi anume, nivelul de efort necesar al categoriilor specifice de personal) şi colective (şi anume, nivelul global de efort).

4.2 IMPLEMENTAŢI PRACTICI ŞI CONTROALE CORESPUNZĂTOARE DE MANAGEMENT AL SECURITĂŢII ÎN CAZUL MENŢINERII ŞI OPERĂRII UNUI SERVER WEB SIGUR

Practicile adecvate de management sunt esenţiale pentru operarea şi menţinerea unui server web sigur. Practicile de securitate includ identificarea resurselor sistemului de informaţii al companiei dumneavoastră şi dezvoltarea, documentarea şi implementarea politicilor, şi a liniilor directoare pentru a ajuta la asigurarea confidenţialităţii, integrităţii şi disponibilităţii resurselor sistemului de informaţii. Sunt recomandate următoarele practici şi controale:

- O politică largă de securitate a sistemului de informaţii în afaceri.
- Configurarea serverului şi controlul şi managementul schimbărilor.
- Evaluarea şi managementul riscurilor.
- Configuraţii standardizate ale software-urilor care să satisfacă politica de securitate a sistemului de informaţii.
- Conştientizarea nevoii de securitate cibernetică şi instruirea personalului.
- Planificarea intervenţiilor, continuitatea operaţiilor şi planificarea recuperării.
- Certificarea şi acreditarea.

4.3 ASIGURAŢI-VĂ CĂ SISTEMELE DE OPERARE ALE SERVERULUI WEB ÎNDEPLINESC CERINŢELE DE SECURITATE ALE ORGANIZAŢIEI DUMNEAVOASTRĂ.

Primul pas în securizarea unui server web este asigurarea sistemului de operare pe care se bazează. Serverele web disponibile operează pe un sistem de operare cu scop general. Pot fi evitate multe probleme de securitate dacă sistemele de operare pe care se bazează serverele web sunt configurate în mod corespunzător. Configuraţiile hardware şi software implicite sunt de obicei setate de producători pentru a scoate în evidenţă caracteristicile, funcţiile şi uşurinţa utilizării în detrimentul securităţii. Întrucât producătorii nu sunt conştienţi de nevoile de securitate ale fiecărei organizaţii, fiecare administrator de server web trebuie să configureze noi servere pentru a reflecta cerinţele de securitate ale afacerii şi să le reconfigureze pe măsură ce aceste cerinţe se schimbă. Utilizarea ghidurilor de configurare a securităţii sau listele de verificare pot ajuta administratorii în securizarea sistemelor în mod constant şi eficient. Securizarea iniţială a unui sistem de operare include, în general, următorii paşi:

- Peticiţi şi upgradaţi sistemul de operare.
- Schimbaţi toate parolele implicite.
- Eliminați sau dezactivaţi serviciile şi aplicaţiile inutile.

- Configuraţi autentificarea utilizatorilor la sistemul de operare.
- Configuraţi verificarea resurselor.
- Instalaţi şi configuraţi verificări suplimentare de securitate.
- Realizaţi testarea securităţii sistemului de operare.

4.4 ASIGURAŢI-VĂ CĂ APLICAŢIA SERVERULUI WEB ÎNDEPLINEŞTE CERINŢELE DE SECURITATE ALE ORGANIZAŢIEI DUMNEAVOASTRĂ.

În multe privinţe, instalarea şi configurarea sigură a aplicaţiei serverului web va oglindi procesul sistemului de operare discutat mai sus. Principiul primordial este instalarea cantităţii minime de servicii necesare ale serverului web şi eliminarea oricăror vulnerabilităţi cunoscute prin patch-uri sau upgradări. Dacă programul de instalare instalează orice aplicaţii, servicii sau scripte inutile, acestea trebuie să fie eliminate imediat după încheierea procesului de instalare. Securizarea aplicaţiei serverului web include în general următorii paşi:

- Peticiţi şi upgradaţi aplicaţia serverului web.
- Eliminaţi sau dezactivaţi serviciile, aplicaţiile şi conţinutul probei care sunt inutile.
- Configuraţi autentificarea utilizatorului la serverul web şi comenzile de acces.
- Configuraţi comenzile resurselor serverului web.
- Testaţi securitatea aplicaţiei serverului web şi conţinutul web.

4.5 ASIGURAŢI-VĂ CĂ DOAR CONŢINUTUL CORESPUNZĂTOR ESTE PUBLICAT PE SITE-UL DUMNEAVOASTRĂ WEB.

Site-urile web ale companiilor sunt adesea unul dintre primele locuri în care infractorii cibernetici caută informaţii valoroase. Cu toate acestea, multor organizaţii le lipseşte un proces sau o politică de publicare web care să determine ce tip de informaţii să publice în mod deschis, ce informaţii să publice cu acces restricţionat şi ce informaţii ar trebui să nu fie publicate în orice depozit accesibil publicului. Unele exemple general acceptate a ceea ce nu trebuie publicat sau cel puţin a ceea ce ar trebui să fie examinat şi analizat cu atenţie înainte de a fi publicat pe un site web public includ:

- Informaţii de afaceri clasificate sau proprietare.
- Informaţii sensibile legate de securitatea afacerii.
- Dosarele medicale.
- Măsurile de securitate fizice şi informatice detaliate ale unei companii.

- Detaliile despre reţeaua şi infrastructura sistemului de informaţii a unei companii - de ex., intervalele de adrese, convenţiile privind denumirile şi codurile de acces.
- Informaţii care specifică sau implică vulnerabilităţi de securitate fizică.
- Planuri detaliate, hărţi, diagrame, fotografii aeriene şi desene arhitecturale ale clădirilor de afaceri, proprietăţilor sau instalaţiilor.
- Orice informaţii sensibile despre persoane fizice care pot fi supuse legilor federale, de stat, sau, în anumite cazuri, legilor internaţionale cu privire la confidențialitate.

4.6 ASIGURAŢI-VĂ CĂ AU FOST LUATE MĂSURILE CORESPUNZĂTOARE PENTRU PROTEJAREA CONŢINUTULUI WEB ÎMPOTRIVA ACCESULUI SAU A MODIFICĂRILOR NEAUTORIZATE.

Deşi informaţiile disponibile pe site-urile web publice au scopul de a fi publice (presupunând că sunt implementate după un proces şi o politică de revizie solidă), este totuşi important să vă asiguraţi că informaţiile nu pot fi modificate fără autorizare. Utilizatorii unor astfel de informaţii se bazează pe integritatea acestora chiar şi dacă informaţiile nu sunt confidenţiale. Conţinutul de pe serverele web accesibile publicului este în mod natural mai vulnerabil decât informaţiile care nu sunt accesibile de pe internet, şi această vulnerabilitate înseamnă că organizațiile trebuie să protejeze conţinutul web public prin configurarea corespunzătoare a comenzilor resurselor serverelor web. Exemplele de practici de control al resurselor includ:

- Instalați sau activaţi doar serviciile necesare.
- Instalaţi conţinutul web pe un hard disk dedicat sau o partiţie logică.
- Limitaţi încărcările în directoare care nu pot fi citite de serverul web.
- Definiţi un singur director pentru toate scripturile externe sau programele executate ca parte din conţinutul web.
- Dezactivaţi utilizarea legăturilor simbolice.
- Definiţi o matrice completă de acces la conţinutul web care să identifice care foldere şi fişiere din directorul de documente de pe serverul web sunt restricţionate, care sunt accesibile şi de către cine.
- Dezactivaţi listele de directoare.
- Implementaţi autentificarea utilizatorilor pentru a identifica utilizatorii aprobaţi, semnăturile digitale şi alte mecanisme criptografice după caz.

- Utilizaţi sistemele de detectare a intruziunilor, sistemele de prevenire a intruziunilor şi sistemele de verificare a integrităţii fişierelor pentru a identifica intruziunile şi a verifica conţinutul web.
- Protejaţi fiecare server back-end (şi anume, serverul bazei de date şi severul directoarelor) împotriva atacurilor prin injectare de comenzi.

4.7 UTILIZAŢI CONŢINUTUL ACTIV ÎN MOD RAŢIONAL DUPĂ ANALIZAREA BENEFICIILOR ŞI A RISCURILOR.

Informaţiile statice s-au aflat pe serverele celor mai vechi site-uri web, de obicei în forma documentelor bazate pe text. Curând după aceea, elementele interactive au fost introduse spre a oferi noi oportunităţi pentru interacţiunea utilizatorilor.

Din păcate, aceleaşi elemente interactive au introdus noi vulnerabilități legate de web. Acestea implică în mod obişnuit un cod de executare în mod dinamic care utilizează un număr mare de input-uri, de la parametrii URL ai paginii web până la conţinutul protocolului de transfer hipertext (HTTP) şi, mai recent, conţinutul limbajului de marcare extensibil (XML). Diferite tehnologii cu conţinut activ prezintă diferite vulnerabilităţi aferente, iar riscurile acestora trebuie cântărite faţă de beneficiile lor. Deşi majoritatea site-urilor web utilizează o anumită formă de generatoare de conţinut activ, multe furnizează de asemenea o parte sau întregul lor conţinut într-o formă statică.

4.8 UTILIZAŢI TEHNOLOGIILE DE AUTENTIFICARE ŞI CRIPTOGRAFICE, DUPĂ CAZ, PENTRU A PROTEJA ANUMITE TIPURI DE DATE SENSIBILE.

Serverele web publice vin adesea în sprijinul tehnologiilor pentru identificarea şi autentificarea utilizatorilor cu diferite privilegii pentru accesarea informaţiilor. Unele dintre aceste tehnologii se bazează pe funcţiile criptografice care oferă un canal sigur între un client al browserului web şi un server web care suportă criptarea. Serverele web pot fi configurate astfel încât să utilizeze diferiţi algoritmi criptografici, oferind niveluri variate de securitate şi performanţă.

Fără implementarea autentificării corespunzătoare a utilizatorilor, organizațiile nu pot restricţiona în mod selectiv accesul la informaţii specifice. Toate informaţiile care se află pe un server web public pot fi apoi accesate de oricine are acces la server. În plus, fără anumite procese de autentificare a severului, utilizatorii serverului web public nu vor

putea determina dacă serverul este „autentic” sau o versiune contrafăcută operată de un infractor cibernetic.

Chiar şi cu un canal criptat şi un mecanism de autentificare, este posibil ca atacatorii să încerce să acceseze site-ul prin forţă brută. Tehnicile de autentificare necorespunzătoare pot permite atacatorilor să adune nume de utilizatori valide sau eventual să obţină accesul la site-ul web. Mecanismele puternice de autentificare pot de asemenea să vă protejeze împotriva atacurilor de tip phishing, în care hackerii pot păcăli utilizatorii să-şi dea credențialele personale, şi atacul de tip pharming, în care traficul către un site web legal poate fi redirecţionat către unul ilegal. Un nivel corespunzător de autentificare trebuie implementat pe baza sensibilităţii utilizatorilor şi a conţinutului serverului web.

4.9 UTILIZAŢI INFRASTRUCTURA REŢELEI PENTRU A AJUTA LA PROTEJAREA SERVERELOR WEB PUBLICE.

Infrastructura reţelei (de ex., paravanele de protecţie, routerele, sistemele de detecţie a intruziunilor) care sprijină serverul web joacă un rol critic de securitate. În majoritatea configuraţiilor, infrastructura reţelei va fi prima linie de apărare între un server web public şi internet. Însă designul reţelei nu poate proteja singur un server web. Frecvenţa, complexitatea şi varietatea atacurilor asupra serverelor web comise până în prezent sprijină ideea că securitatea serverului web trebuie implementată prin mecanisme de protecţie stratificate şi diversificate, o abordare denumită uneori „apărare în profunzime”.

4.10 ASUMAŢI-VĂ UN PROCES CONTINUU DE MENŢINERE A SECURITĂȚII SERVERULUI WEB.

Menţinerea în siguranţă a unui server web necesită efort, resurse şi vigilenţă constante. Administrarea în siguranţă a unui server web zilnic este esenţială. Menţinerea securităţii unui server web va implica de obicei următorii paşi:

- Configurarea, protejarea şi analiza fişierelor jurnal.
- Crearea de copii de rezervă a informaţiilor critice în mod frecvent.
- Păstrarea unei copii autorizate protejate a conţinutului web.
- Stabilirea procedurilor pentru recuperarea dintr-o situație de compromis.
- Testarea şi aplicarea patch-urilor la timp.
- Testarea periodică a securităţii.

V. EMAILUL

Emailul a devenit o parte critică a activităţii noastre de zi cu zi, începând de la managementul intern până la asistenţa directă a clienţilor. Beneficiile asociate cu emailul ca un instrument de afaceri primar sunt mult mai mari decât aspectele negative. Cu toate acestea, organizațiile trebuie să rămână vigilente, întrucât o platformă de email de succes începe cu principiile de bază ale securităţii emailului, pentru a asigura confidențialitatea şi protecţia clientului şi a informaţiilor de afaceri.

ELEMENTELE DE ACŢIUNE ALE PLANULUI CIBERNETIC

5.1 CREAŢI UN FILTRU PENTRU EMAILURILE SPAM

S-a documentat foarte bine că spam-urile, încercările de phishing şi alte emailuri nesolicitate şi nedorite constituie adesea peste 60 la sută din toate emailurile pe care le primeşte o persoană fizică sau juridică. Emailul este metoda primară pentru răspândirea virusurilor şi software-urilor rău intenţionate şi este una dintre cele mai uşoare pentru a ne apăra împotriva acestora. Aveţi în vedere să utilizaţi serviciile de filtrare ale emailurilor pe care furnizorul dumneavoastră de servicii, de găzduire sau alţi furnizori cloud vi le oferă. O aplicaţie locală de filtrare a emailurilor este de asemenea o componentă importantă a unei strategii solide antivirus. Asiguraţi-vă că actualizările automate sunt activate pe aplicaţia dumneavoastră de email, filtrul de emailuri şi programele antivirus. Asiguraţi-vă că filtrele sunt analizate cu regularitate astfel că emailurile şi/sau domeniile importante nu sunt blocate din greşeală.

5.2 INSTRUIŢI-VĂ ANGAJAŢII SĂ UTILIZEZE EMAILUL ÎN MOD RESPONSABIL

Ultima linie de apărare pentru toate eforturile dumneavoastră împotriva riscurilor cibernetice revine angajaţilor care utilizează instrumente precum emailul şi utilizarea şi managementul responsabil şi adecvat al informaţiilor care sunt sub controlul acestora. Doar tehnologia nu poate face o afacere sigură. Angajaţii trebuie instruiţi să identifice riscurile asociate cu utilizarea emailului, cum şi când să utilizeze emailul corespunzător cu activitatea lor, şi când să solicite asistenţa profesioniştilor. Instruirea angajaților este disponibilă în multe forme, inclusiv prin presa scrisă, videoclipuri şi chestionare online.

Aveţi în vedere să solicitaţi instruirea de securitate pentru toţi angajaţii noi şi urmarea cursurilor de perfecţionare în fiecare an. Eforturile simple precum buletinele informative

lunare, buletinele de urgenţă în momentul în care sunt detectaţi viruşi şi chiar postere în spaţiile comune de lucru pentru a le reaminti angajaţilor despre securitatea cibernetică şi lista de verificare a confidențialității creează un mediu de lucru educat în protejarea afacerii dumneavoastră.

5.3 PROTEJAŢI INFORMAŢIILE SENSIBILE TRIMISE PRIN EMAIL

Cu proliferarea sa ca şi instrument primar pentru a comunica pe plan intern şi extern, emailul de serviciu include adesea informaţii sensibile. Fie că este vorba despre informaţiile companiei care ar putea să vă prejudicieze afacerea sau date precum informaţiile personale cu privire la sănătate (PHI) sau informaţiile personale identificabile (PII), este important să vă asiguraţi că astfel de informaţii sunt transmise şi accesate doar de cei care au dreptul să le vadă.

Întrucât emailul în forma sa iniţială nu este conceput pentru a fi sigur, incidentele de adresare greşită sau altă redirecţionare accidentală obişnuită pot duce la scurgerea de date. Organizațiile care manipulează astfel de informaţii trebuie să se gândească dacă astfel de informaţii trebuie transmise prin email, sau cel puţin să aibă în vedere utilizarea criptării emailurilor. Criptarea este procesul de convertire a datelor în format care nu poate fi citit pentru a preveni dezvăluirea către personalul neautorizat. Doar persoanele fizice sau organizaţiile cu acces la cheia de criptare pot citi informaţiile. Alte servicii cloud oferă “Secure Web Enabled Drop Boxes” care permit transferul sigur al datelor pentru informaţiile sensibile, fiind adesea o abordare mai bună de transmitere a comunicărilor între companii sau clienţi.

5.4 STABILIŢI O POLITICĂ DE RETENȚIE A EMAILURILOR SENSIBILE

O altă consideraţie importantă este managementul emailului care se găsește în sistemele de mesagerie ale companiei şi computerele utilizatorilor dumneavoastră. De la costul de stocare şi backup până la cerinţele legale şi de reglementare, companiile trebuie să se documenteze asupra modului în care vor gestiona retenția emailurilor şi implementa controalele de bază pentru a ajuta angajații să atingă acele standarde. Multe industrii au reguli specifice care dictează cât de mult pot sau ar trebui să fie reţinute emailurile, însă regula de aur este doar atât timp cât susțin eforturile dumneavoastră de afaceri. Multe companii implementează un standard de retenție de 60-90 de zile, dacă nu se specifică altfel din punct de vedere legal.

Pentru a asigura conformitatea, companiile trebuie să aibă în vedere arhivarea obligatorie la o dată limită de retenție aleasă şi ştergerea automată și definitivă a emailurilor după un alt punct stabilit, cum ar fi 180-360 de zile în arhive. În plus, organizaţiile ar trebui să descurajeze utilizarea folderelor personale pe computerele angajaţilor (cel mai adesea configurabile de la nivelul sistemului de emailuri), întrucât acest lucru va face mai dificilă gestionarea standardelor companiei.

5.5 DEZVOLTAŢI O POLITICĂ DE UTILIZARE A EMAILURILOR

Politicile sunt importante pentru stabilirea aşteptărilor cu angajaţii sau utilizatorii dumneavoastră, şi pentru dezvoltarea standardelor pentru a asigura adeziunea la politicile dumneavoastră publicate.

Politicile dumneavoastră trebuie să fie uşor de citit, înţeles, definit şi aplicat. Ariile cheie la care se face referire includ ce sistem de email ar trebui sau nu ar trebui utilizat pentru companie, şi ce date sunt permise pentru a fi transmise. Alte arii ale politicii ar trebui să facă referire la retenția, confidențialitatea şi utilizarea acceptabilă.

În funcţie de activitatea dumneavoastră şi de jurisdicţie, este posibil să aveţi nevoie de monitorizarea emailurilor. Drepturile companiei şi ale utilizatorului trebuie să fie precizate şi în politica de utilizare, care trebuie să facă parte din instruirea generală a utilizatorului final. Politica de utilizare trebuie analizată anual și actualizată conform celor mai noi reglementări în domeniu.

Ca şi mostră de politică de utilizare a emailului, vezi: http://www.sans.org/security-resources/policies/Email_Policy.pdf

VI. DISPOZITIVELE MOBILE

În cazul în care compania dumneavoastră utilizează dispozitive mobile pentru a desfăşura activitatea companiei, cum ar fi accesarea emailului companiei sau date sensibile, acordaţi o atenţie specială securităţii mobile şi potenţialelor ameninţări care pot expune şi compromite reţelele globale ale activităţii dumneavoastră. Această secţiune descrie mediul cu ameninţări mobile şi practicile pe care organizaţiile le pot utiliza pentru a ajuta la securizarea dispozitivelor precum telefoanele inteligente, tabletele şi laptopurile cu Wi-Fi activat.

Multe organizaţii constată că angajaţii sunt mai productivi atunci când utilizează dispozitivele mobile, iar beneficiile sunt prea mari pentru a fi ignorate. Chiar dacă mobilitatea poate creşte productivitatea la locul de muncă, a permite angajaţilor să-şi aducă propriile dispozitive mobile în cadrul întreprinderii poate crea provocări semnificative în ceea ce priveşte securitatea şi managementul datelor.

Pierderea de date şi încălcările securităţii datelor cauzate de pierderea sau furtul telefoanelor generează provocări mari, întrucât dispozitivele mobile sunt în prezent utilizate pentru a stoca informaţii confidenţiale de afaceri şi pentru a accesa reţeaua corporaţiei. Conform unui studiu privind securitatea mobilă realizat de Symantec în decembrie 2010, 68 la sută din respondenţi au clasat pierderea şi furtul ca principala problemă privind securitatea dispozitivelor mobile, în timp ce 56 la sută au declarat că software-urile rău intenţionate pentru dispozitive mobile reprezintă a doua lor grijă. Este important să amintim că în timp ce angajatul individual poate fi răspunzător de un dispozitiv, compania este totuşi răspunzătoare pentru date.

CELE MAI IMPORTANTE AMENINŢĂRI CARE VIZEAZĂ DISPOZITIVELE MOBILE

- **Pierderea de date** – Un angajat sau un hacker accesează informaţiile sensibile din dispozitiv sau din reţea. Acest lucru poate fi fără intenţie sau rău intenționat, şi este considerat cea mai mare ameninţare pentru dispozitivele mobile
- **Atacurile de tip inginerie socială** – Încercările unui infractor cibernetic de a păcăli utilizatorii să dezvăluie informaţii sensibile sau să instaleze software-uri rău intenţionate. Metodele includ phishing-ul şi atacurile ţintite.
- **Software-uri rău intenţionate** – Software-uri rău intenționate care includ viruşi tradiţionali informatici, viermi informatici şi programe de tip cal troian. Exemplele specifice includ viermele Ikee, care vizează dispozitivele care se bazează pe iOS; şi

software-urile rău intenţionate Pjapps care pot înscrie dispozitivele Android infectate într-o colecţie de dispozitive „zombie” controlate de hackeri, cunoscute sub denumirea de „botnet”.

- **Amenințările la adresa integrităţii datelor** – Încercările de a corupe sau de a modifica datele pentru a perturba operațiunile unei activităţi în scopul câştigului financiar. Acestea pot, de asemenea, să aibă loc fără intenţie.
- **Abuzul de resurse** – Încercările de a abuza reţeaua, dispozitivele sau resursele. Exemplele includ transmiterea de spam-uri de pe dispozitive compromise sau atacurile de tip refuz servicii utilizând resursele de calcul ale dispozitivelor compromise.
- **Atacurile bazate pe web şi reţea** – Lansate de site-uri web rău intenționate sau site-uri legale compromise, acestea vizează browserul unui dispozitiv şi încearcă să instaleze software-uri rău intenţionate sau să fure datele confidenţiale care trec prin acesta.

ELEMENTELE DE ACŢIUNE ALE PLANULUI CIBERNETIC

Câţiva paşi simpli pot ajuta la asigurarea faptului că informaţiile companiei sunt protejate. Aceştia includ necesitatea ca toate dispozitivele mobile care se conectează la reţeaua întreprinderii să fie echipate cu software de securitate şi protecţie prin parolă; şi asigurarea instruirii privind securitatea generală pentru a face angajaţii să fie conştienţi de importanţa practicilor de securitate pentru dispozitivele mobile. Practicile mai specifice sunt detaliate mai jos.

6.1 UTILIZAŢI SOFTWARE-URI DE SECURITATE PE TOATE TELEFOANELE INTELIGENTE

Software-urile de securitate concepute special pentru telefoanele inteligente pot opri hackerii şi împiedica infractorii cibernetici să vă fure informaţiile sau să vă spioneze atunci când utilizaţi reţelele publice. Acestea pot detecta şi elimina viruşii şi alte ameninţări mobile înainte să vă cauzeze probleme. Acestea pot de asemenea să elimine textul supărător şi mesajele spam multimedia.

6.2 ASIGURAŢI-VĂ CĂ TOATE SOFTWARE-URILE SUNT ACTUALIZATE

Dispozitivele mobile trebuie tratate ca şi computerele personale în sensul că toate software-urile de pe dispozitive trebuie actualizate, în special software-urile de securitate.

Acest lucru va proteja dispozitivele împotriva noilor versiuni ale software-urilor rău intenţionate şi a viruşilor care ameninţă informaţiile critice ale organizației.

6.3 CRIPTAŢI DATELE DE PE DISPOZITIVELE MOBILE

Informaţiile de afaceri şi personale stocate pe dispozitivele mobile sunt adesea sensibile. Criptarea acestor date reprezintă o necesitate. Dacă un dispozitiv este pierdut şi cartela SIM furată, hoţul nu va putea accesa datele dacă pe dispozitiv este încărcată tehnologia corespunzătoare de criptare.

6.4 OFERIŢI UTILIZATORILOR ACCES LA DISPOZITIVELE MOBILE CU PROTECŢIE PRIN PAROLĂ

Pe lângă criptare şi actualizările de securitate, este importantă utilizarea parolelor puternice pentru a proteja datele stocate pe dispozitivele mobile. Acest lucru va ajuta la împiedicarea accesării datelor sensibile în caz că dispozitivul este pierdut sau ajunge în mâinile hackerilor.

6.5 ÎNDEMNAŢI UTILIZATORII SĂ FIE CONŞTIENŢI DE ÎMPREJURIMI

Fie că introduc parole sau vizualizează date sensibile sau confidenţiale, utilizatorii trebuie să fie precauţi la cei care se pot uita peste umărul lor.

6.6 UTILIZAŢI ACESTE STRATEGII PENTRU EMAIL, TRANSMITEREA MESAJELOR ŞI REŢELELE DE SOCIALIZARE

Evitaţi deschiderea mesajelor text neaşteptate din partea expeditorilor necunoscuţi– Ca şi în cazul emailului, atacatorii pot utiliza mesaje text pentru a răspândi software-uri rău intenţionate, înşelătorii de tip phishing şi alte ameninţări printre utilizatorii de dispozitive mobile. Aceeaşi precauţie trebuie aplicată pentru deschiderea mesajelor text nesolicitate cu care utilizatorii s-au obişnuit în cazul emailului.

Nu vă lăsaţi ademeniţi de spammeri şi phisheri. Pentru a proteja reţelele organizației împotriva infractorilor cibernetici, ar trebui să implementați soluţii corespunzătoare de securitate a emailurilor, inclusiv prevenirea spamurilor. Astfel puteți proteja reputaţia şi gestiona mai precis riscurile.

Daţi click cu precauţie. Exact ca pe computerele staţionare, comunicarea pe reţelele de socializare pe dispozitivele mobile şi laptopuri trebuie realizată cu grijă şi precauţie. Utilizatorii nu trebuie să deschidă linkuri neidentificate. Nu durează mult ca un utilizator să fie păcălit să compromită un dispozitiv şi informaţiile de pe acesta.

6.7 STABILIŢI PROCEDURI DE RAPORTARE PENTRU ECHIPAMENTELE PIERDUTE SAU FURATE

În cazul unei pierderi sau a unui furt, angajaţii şi managementul trebuie să ştie ce să facă în continuare. Trebuie să fie implementate procesele de dezactivare a dispozitivului şi de protejare a informaţiilor sale împotriva intruziunii. De asemenea, sunt disponibile produse pentru automatizarea unor astfel de procese, permiţând companiilor de orice mărime să respire mai uşor după astfel de incidente.

6.8 ASIGURAŢI-VĂ CĂ TOATE DISPOZITIVELE SUNT CURATE ÎNAINTE DE ARUNCARE

Majoritatea dispozitivelor mobile au o funcţie de resetare care permite ca toate datele să fie şterse. Cartelele SIM trebuie, de asemenea, să fie şterse şi distruse.

Legături utile:

- Instruiți-vă angajaţii cu privire la aplicaţiile mobile: http://onguardonline.gov/articles/0018-understanding-mobile-apps
- Păstraţi-vă laptopurile sigure: http://onguardonline.gov/articles/0015-laptop-security

VII. ANGAJAŢII

Companiile trebuie să stabilească o politică oficială şi procese de recrutare consistente pentru a controla şi păstra calitatea angajaţilor lor. Multe organizații au învăţat din greu că angajarea unei persoane cu cazier judiciar, recomandări falsificate sau un istoric indezirabil poate crea un coşmar legal şi financiar.

Dacă nu fac verificări în procesul de angajare, angajatorii riscă să facă alegeri nechibzuite de angajare care pot duce la violenţă la locul de muncă, furt, delapidare, procese pentru angajare neglijentă şi numeroase alte probleme.

ELEMENTELE DE ACŢIUNE ALE PLANULUI CIBERNETIC

7.1 DEZVOLTAŢI UN PROCES DE RECRUTARE CARE EXAMINEAZĂ ÎN MOD CORESPUNZĂTOR CANDIDAŢII

Procesul de recrutare trebuie să fie un efort de colaborare între diferite grupuri din cadrul organizaţiei dumneavoastră, incluzând echipele de recrutare, resurse umane, de securitate, juridice şi de management. Este important să aveţi un proces solid de depunere candidaturi, reluare, intervievare şi verificare a referinţelor, pentru a identifica potenţialele lipsuri şi probleme care pot apărea, printr-o verificare a antecedentelor.

O resursă de screening pentru angajările online denumită „Curs online de certificare a recrutării sigure” vă poate ajuta să stabiliţi bazele pentru un proces de recrutare sigur. Cursul va învăţa echipele dumneavoastră ce să caute în diferite stagii ale procesului de recrutare, cum să intervieveze şi cum să stabilească un program sigur, pentru a evita recrutarea unui angajat care poate fi problematic. Cursul este disponibil la adresa: http://www.esrcheck.com/ESRonlineSafeHiringCourse.php .

7.2 REALIZAŢI VERIFICĂRILE ANTECEDENTELOR ŞI ALE RECOMANDĂRILOR

Verificările antecedentelor sunt esenţiale şi trebuie să fie consecvente. Utilizarea unei companii de verificare a antecedentelor este extrem de recomandată. Verificarea standard a antecedentelor trebuie să includă următoarele:

- Verificarea locurilor de muncă
- Verificarea studiilor
- Cazierele judiciare

- Testul antidoping
- Oficiul Trezoreriei Afacerilor Externe şi de Control din S.U.A.
- Registrele cu infractori de natură sexuală
- Istoricul şi validarea securităţii sociale

În funcţie de tipul afacerii dumneavoastră, alte criterii de verificare pot consta în verificarea creditelor, verificările civile şi verificările penale federale. De asemenea, se recomandă şi efectuarea verificărilor post-angajare pentru toţi angajaţii o dată la doi - trei ani, în funcţie de domeniul dumneavoastră de activitate.

Dacă realizaţi verificări ale antecedentelor, dumneavoastră, în calitate de angajator, aveţi obligaţii conform Legii Raportării Corecte a Creditelor. Pentru mai multe informaţii despre obligaţiile angajatorului conform FCRA, vizitaţi http://business.ftc.gov/documents/bus08-using-consumer-reports-what-employers-need-know.

7.3 AVEŢI GRIJĂ ÎN COLABORAREA CU TERŢII

Angajatorii trebuie să analizeze în mod corespunzător companiile partenere prin care organizaţia dumneavoastră angajează consultanţi terţi. Pentru a vă asigura că sunt îndeplinite criteriile de verificare pentru consultanţii terţi, trebuie să stabiliţi în mod explicit cerinţele de acreditare în contractul dumneavoastră de servicii. Menţionaţi în contract că cerințele de acreditare ale companiei trebuie urmate.

7.4 STABILIŢI CONTROALE DE ACCES CORESPUNZĂTOARE PENTRU ANGAJAŢI

Atât datele clienţilor, cât şi datele interne ale companiei sunt considerate confidenţiale şi necesită o grijă specială atunci când sunt vizualizate, stocate, utilizate, transmise sau aruncate. Este importantă analiza rolului fiecărui angajat şi stabilirea controlului accesului la date în funcţie de rol. Dacă un rol nu necesită ca angajatul să utilizeze vreodată date sensibile, accesul angajaţilor la date trebuie să fie strict interzis. Cu toate acestea, dacă rolul necesită ca angajatul să lucreze cu date sensibile, nivelul de acces trebuie analizat în profunzime şi atribuit într-o manieră controlată şi stratificată, urmând principiile „minimului de privilegii”. Acesta permite angajatului să acceseze doar datele necesare pentru a-şi realiza sarcinile de serviciu.

Dacă organizaţia nu are implementat un sistem pentru a controla accesul la date, sunt recomandate cu tărie următoarele precauţii. Fiecare angajat trebuie să:

- Evite accesul sau vizualizarea datele clienţilor fără un motiv valabil legat de activitate. Accesul trebuie să se facă pe baza necesităţii de a cunoaşte.
- Evite furnizarea datelor confidenţiale oricui altuiva, fie că vorbim de reprezentanţi ai clienţilor, partenerii de afaceri sau chiar alţi angajaţi – decât dacă este sigur de identitatea şi autoritatea acelei persoane.
- Evite utilizarea datelor clienţilor pentru dezvoltarea, testarea, prezentările de instructaje sau în niciun alt scop decât cel de a furniza servicii de producţie, testarea specifică a clienţilor sau diagnosticare. Doar datele curăţate în mod corespunzător, care nu pot fi urmărite până la un client, angajat al clientului, cumpărător sau angajatul organizaţiei dumneavoastră trebuie utilizate în aceste scopuri.
- Utilizeze întotdeauna metode sigure de transmitere precum emailul sigur, transferul sigur de fişiere (de la aplicaţie la aplicaţie) şi suporturile electronice criptate (de ex., CD-uri, unităţi sau benzi USB).
- Păstreze întotdeauna datele confidenţiale (exemplare tipărite şi electronice) doar atât cât este necesar.
- Urmeze o politică de „birou curat”, menţinând spaţiile de lucru ordonate şi securizând documentele sensibile, astfel încât informaţiile confidenţiale să nu ajungă pe mâini greşite.
- Utilizeze întotdeauna doar serviciile aprobate de eliminare a documentelor sau să distrugă toate documentele tipărite care conţin informații confidenţiale după finalizarea utilizării lor. În mod similar, să utilizeze doar metode aprobate care elimină complet toate datele în momentul aruncării, trimiterii pentru reparaţii sau pregătirii pentru reutilizarea suporturilor electronice.

7.5 OFERIŢI INSTRUIRE DE SECURITATE PENTRU ANGAJAŢI

Instruirea pentru conştientizarea securităţii învaţă angajaţii să înţeleagă vulnerabilităţile sistemului şi ameninţările care planează asupra activității organizației în momentul utilizării unui computer dintr-o reţea.

Un program IT puternic de securitate trebuie să includă instruirea utilizatorilor IT cu privire la politica, procedurile şi tehnicile de securitate, precum şi diversele controale de management, operaţionale şi tehnice necesare şi disponibile pentru a păstra sigure resursele IT. În plus, administratorii infrastructurii IT trebuie să aibă abilităţile necesare pentru a-şi realiza sarcinile atribuite în mod eficient. Dacă nu se acordă atenţie ariei de

instructaj de securitate, organizația este supusă unui risc mare întrucât securitatea resurselor este mai mult o problemă umană decât una tehnologică.

Utilizatorii de tehnologii sunt cel mai larg public în orice organizaţie şi reprezintă singurul şi cel mai important grup de persoane care pot ajuta la reducerea erorilor accidentale şi a vulnerabilităţilor IT. Utilizatorii pot include angajaţii, contractanţii, cercetătorii invitaţi străini sau locali, vizitatorii, oaspeţii şi alţi colaboratori sau asociaţi care au nevoie de acces. Utilizatorii trebuie:

- Să înţeleagă şi să respecte politicile şi procedurile de securitate.
- Să fie instruiţi în mod corespunzător cu privire la regulile de conduită în sistemele şi aplicaţiile la care au acces.
- Să lucreze cu managementul pentru a îndeplini necesităţile de instruire.
- Să păstreze software-ul şi aplicaţiile actualizate cu patch-uri de securitate.
- Să fie conştienţi de acţiunile pe care le întreprind pentru a proteja mai bine informaţiile companiei. Aceste acţiuni includ: utilizarea parolelor adecvate, folosirea copiilor de rezervă a datelor, protecţia adecvată antivirus, raportarea oricăror incidente suspecte sau a încălcărilor politicii de securitate, şi urmărirea regulilor stabilite pentru a evita atacurile de tip inginerie socială şi pentru a împiedica răspândirea spam-urilor sau a viruşilor şi a viermilor.

O organizare clară a tot ceea ce înseamnă date sensibile versus date nesensibile este de asemenea necesară. De obicei, următoarele date sunt considerate informaţii sensibile care ar trebui manipulate cu precauţie:

- Numerele de identificare emise de guvern (de ex., numerele de securitate socială, numerele permisului de conducere)
- Informaţii financiare despre conturi (numerele conturilor bancare, numerele cardurilor de credit)
- Dosarele medicale
- Informaţii despre asigurările de sănătate
- Informaţii despre salarii
- Parolele.

Instruirea trebuie să acopere politicile de securitate pentru toate căile de acces şi metodele de transmitere, inclusiv bazele de date sigure, email, transferul de fişiere, suporturile electronice criptate şi copiile tipărite.

Angajatorii trebuie să sublinieze în mod constant natura critică a securităţii datelor. Trebuie stabilite cu regularitate cursuri de perfecţionare pentru a inocula cultura securităţii datelor organizaţiei dumneavoastră. În plus, distribuiţi articole de ştiri despre confidențialitatea şi securitatea datelor în cadrul instructajului dumneavoastră şi trimiteți comunicări la nivelul organizaţiei despre ştirile legate de confidențialitatea datelor importante, ca şi memento-uri pentru angajaţii dumneavoastră.

7.6 IMPLEMENTAŢI O LISTĂ DE VERIFICARE CU ANGAJAŢII CARE PĂRĂSESC COMPANIA

Creaţi o listă de verificare a ieşirilor de securitate pentru angajații care nu mai lucrează în cadrul companiei, indiferent de motivul plecării acestora (voluntar sau involuntar). Este recomandat de Camera de Comerţ a S.U.A. şi alte instituţii ca toate organizațiile să se asigure că sunt şterse imediat conturile angajaţilor ale căror contracte au încetat, de pe toate dispozitivele şi unităţile din reţea. Acest lucru este valabil pentru orice dispozitive care este posibil să fi fost scoase în afara unităţii precum laptopuri şi telefoane inteligente.

Legături utile

- Opriţi-vă. Gândiţi. Conectaţi-vă. Materiale interne despre dezvoltarea angajaţilor http://www.dhs.gov/stopthinkconnect
- Prezentare PowerPoint despre securitatea internetului la locul de muncă
- http://go.microsoft.com/?linkid=9745638
- Cartele cu ponturi: Topul ponturilor pentru securitatea internetului la locul de muncă
- http://go.microsoft.com/?linkid=9745642
- Video: „Fii vigilent cu privire la securitatea internetului la locul de muncă”
- http://go.microsoft.com/?linkid=9745640
- Camera de Comerţ a S.U.A.: *Bazele Securităţii pe internet pentru Afaceri 2.0* https://www.uschamber.com/sites/default/files/issues/technology/files/ISEB-2.0-CyberSecurityGuide.pdf

VIII. SECURITATEA FACILITĂŢILOR

Protejarea angajaţilor şi a membrilor publicului care vă vizitează facilitatea este o responsabilitate complexă şi grea. De asemenea, aceasta este una dintre principalele priorităţi ale companiei dumneavoastră.

ELEMENTELE DE ACŢIUNE ALE PLANULUI CIBERNETIC

8.1 RECUNOAŞTEŢI IMPORTANŢA SECURIZĂRII FACILITĂŢILOR COMPANIEI DUMNEAVOASTRĂ

Securitatea fizică a unei facilităţi depinde de un număr de decizii de securitate care pot fi identificate printr-un proces comprehensiv de management al riscurilor. Obiectivul managementului riscurilor este de a identifica un nivel de protecţie la care se poate ajunge pentru compania dumneavoastră, care să corespundă cât mai mult cu nivelul de risc, fără a depăşi riscul.

Este uşor să ne gândim la securitatea fizică a facilităţii companiei dumneavoastră doar ca la un exerciţiu de a menţine controlul punctelor de acces şi a ne asigura că există o vizibilitate completă în ariile care sunt stabilite ca fiind cu risc ridicat – fie din cauza ameninţării accesului uşor al publicului, fie din cauza valorii informaţiilor localizate în apropriere. Cu toate acestea, menţinerea securităţii facilităţii companiei dumneavoastră include şi mediul fizic al spaţiilor publice. De exemplu:

- Angajaţii ale căror computere au acces la informaţii sensibile nu trebuie să aibă monitoarele computerelor orientate spre spaţiile accesibile publicului cum ar fi zonele de recepţie, birourile de check-in şi sălile de aşteptare. Angajaţii trebuie instruiţi să nu scrie datele de conectare şi parolele pe bucăţi mici de hârtie lipite pe echipamentele computerelor care pot fi văzute în spaţiile publice.
- Echipamentele uşor de apucat care pot conţine informaţii sensibile sau informaţii personale identificabile – cum ar fi laptopurile, tabletele electronice şi telefoanele celulare – trebuie amplasate în afara zonelor publice. Dacă aveţi un mediu în care angajaţii lucrează într-o sală de aşteptare sau arie de recepţie, instruiţi-i să nu lase aceste dispozitive pe birourile lor nesecurizate.
- Aveţi în vedere blocajele de cablu ca o metodă uşoară de a spori securitatea pentru computerele de tip laptop. Majoritatea laptopurilor prezintă un port de blocare pentru un cablu care poate fi conectat la biroul utilizatorului. Asiguraţi-vă că

depozitaţi cheia la blocajul de cablu într-o locaţie sigură, departe de biroul la care este blocat computerul.

- În cazurile în care informaţii extrem de sensibile sunt stocate pe un laptop, aveţi în vedere adăugarea unui sistem cu software Lojack. Software-ul rulează neobservat şi permite aplicarea legii pentru a localiza mai uşor computerele furate şi permite, de asemenea, unui administrator să şteargă hard diskul de la distanţă, dacă este cazul.
- Aveți în vedere implementarea unui sistem de identificare a legitimaţiilor pentru toţi angajaţii şi instruiţi angajaţii să se oprească şi să întrebe pe oricine se află în aria operaţională a întreprinderii fără o legitimaţie sau care pare a fi un vizitator neînsoţit.

8.2 MINIMIZAŢI ŞI PROTEJAŢI MATERIALELE TIPĂRITE CU INFORMAŢII SENSIBILE

Probabil cea mai eficientă modalitate de a minimiza riscul de a pierde controlul asupra informaţiilor sensibile de pe materialele tipărite este de a minimiza cantitatea de materiale tipărite care conţin informaţii sensibile. Procedurile de management trebuie să limiteze numărul existent de cazuri şi copii ale memorandumurilor rapoartelor tipărite şi a altor materiale care conţin informaţii personale identificabile.

Protejaţi copiile materialului care conţin informaţii sensibile, furnizând angajaţilor dulapuri sau seifuri în care să încuie dosarele. Faceţi din încuierea informaţiilor importante o procedură standard de operare. Instruiţi angajaţii să înţeleagă că simplul fapt de a lăsa un material tipărit greşit pe un birou, la vederea publicului general, poate duce la impactul asupra întregii companii şi asupra clienţilor dumneavoastră.

8.3 ASIGURAŢI SECURITATEA CORESPONDENŢEI

Centrul dumneavoastră de corespondenţă poate introduce o gamă largă de potenţiale ameninţări în cadrul întreprinderii dumneavoastră. Procesele de verificare şi utilizare ale centrului dumneavoastră trebuie să poată identifica ameninţările şi farsele şi să elimine sau să combată riscul pe care îl aduc facilităţilor, angajaţilor şi operaţiunilor zilnice. Compania dumneavoastră trebuie să se asigure că administratorii corespondenței înțeleg gama de proceduri de verificare şi că le evaluează conform cerințelor dumneavoastră operaţionale specifice.

8.4 ASIGURAȚI GOLIREA COȘULUI DE GUNOI ÎN SIGURANȚĂ

Prea des, informaţiile sensibile - inclusiv informaţiile personale identificabile ale clienţilor, datele financiare ale întreprinderii şi alte date, şi informaţiile de acces la sistemul companiei – sunt disponibile pentru oricine în coşul de gunoi. Investiţi în dispozitivele de distrus documente profesionale şi cumpăraţi destule pentru a le face disponibile angajaţilor. Alternativ, vă puteţi abona la o companie de încredere pentru distrugerea documentelor care va furniza containere cu încuietoare pentru stocare până când sunt distruse documentele. Dezvoltaţi proceduri standard şi programe de instruire a angajaţilor pentru a vă asigura că orice persoană din compania dumneavoastră este conştientă ce tipuri de informaţii trebuie distruse.

8.5 ASIGURAȚI ELIMINAREA ECHIPAMENTELOR ELECTRONICE ÎN SIGURANȚĂ

Trebuie să fiţi conştienţi că golirea coşului de gunoi de pe desktop-ul dumneavoastră sau ştergerea documentelor din folderele de pe computerul dumneavoastră sau alt dispozitiv electronic este posibil să nu şteargă informaţiile pentru totdeauna. Persoanele care au competenţe avansate de utilizare a calculatorului pot încă să vă acceseze informaţiile chiar şi după ce credeţi că le-aţi distrus.

Eliminarea echipamentelor electronice necesită specialişti calificaţi pentru a asigura securitatea informațiilor sensibile din acel echipament. În cazul în care ajutorul din exterior, cum ar fi o firmă de reciclare cu experienţă în reciclarea echipamentelor electronice şi un vânzător de securitate a datelor, nu este disponibil sau este prea scump, trebuie ca o măsură minimă, să scoateţi hard-diskurile din computere şi să le distrugeţi. De asemenea, fiţi atenţi la riscurile pe care le prezintă celelalte tipuri de echipamente asociate cu echipamentele informatice, inclusiv CD-uri şi unităţile USB.

8.6 INSTRUIŢI-VĂ ANGAJAŢII ÎN PRIVINȚA PROCEDURILOR DE SECURITATE A FACILITĂŢILOR

O încălcare a securităţii informaţiilor despre clienţi sau nerespectarea securităţii informaţiilor interne ale companiei poate duce la o pierdere a încrederii publicului în compania dumneavoastră şi poate fi la fel de devastatoare ca un dezastru natural. Pentru a aborda astfel de riscuri, trebuie să devotaţi timpul, atenţia şi resursele (inclusiv cu instruirea angajaţilor) necesare pentru identificarea potenţialelor vulnerabilităţi în

infrastructura IT. Procedurile şi practicile politicii de securitate trebuie apoi să fie o parte standard a zilei de lucru pentru fiecare angajat.

În timp ce instruirea oficială este importantă pentru menţinerea securităţii, procedurile de rutină pe care le stabiliţi atât în desfăşurarea obişnuită a activităţii, cât şi în modul în care vă modelaţi comportamente şi practici bune de securitate sunt la fel de importante. Pe scurt, instructajul de securitate trebuie să fie accentuat ca fiind critic, şi consolidat prin proceduri de rutină şi impunerea sa ca valoare a leadership-ului.

IX. SECURITATEA OPERAŢIONALĂ

Deşi securitatea operaţională (OPSEC) îşi are originile în securizarea informaţiilor importante pentru operaţiunile militare, aceasta deține acum reprezentări în întreaga comunitate de afaceri.

În context comercial, OPSEC este procesul de refuzare a accesului hackerilor la orice informaţie despre capabilitățile sau intenţiile unei organizații, prin identificarea, controlul şi protejarea dovezilor planificării şi a desfăşurării activităţilor care sunt esenţiale pentru succesul operaţiunilor.

OPSEC este un proces continuu care constă în cinci acţiuni distincte:

- Identificarea informaţiilor care sunt critice pentru afacerea dumneavoastră.
- Analiza ameninţării la adresa informaţiilor critice.
- Analiza vulnerabilităţilor pentru afacerea dumneavoastră, care ar putea permite unui infractor cibernetic să acceseze informaţiile critice.
- Evaluarea riscului pentru afacerea dumneavoastră în cazul în care sunt exploatate vulnerabilităţile.
- Aplicarea contramăsurilor pentru diminuarea factorii de risc.

Pe lângă faptul că este un proces în cinci paşi, OPSEC reprezintă şi o mentalitate pe care toţi angajaţii ar trebui să o adopte. Prin auto-educare cu privire la metodologiile OPSEC, protejarea informațiilor sensibile care sunt critice pentru succesul afacerii dumneavoastră trece pe planul întâi.

Această secţiune explică procesul OPSEC şi oferă câteva linii directoare generale care sunt aplicabile pentru majoritatea societăților. Este necesară înţelegerea următorilor termeni înainte ca procesul să poată fi explicat:

- **Informaţii critice** – Anumite date despre strategiile şi operaţiunile afacerii dumneavoastră, care sunt necesare infractorilor cibernetici pentru a prejudicia organizația dumneavoastră.
- **Indicatori OPSEC** – Operaţiuni ale companiei şi informaţiile disponibile publicului larg care pot fi interpretate sau puse cap la cap de un infractor cibernetic pentru a extrage informaţii critice.

- **Vulnerabilitatea OPSEC** – O situație posibilă în care operaţiunile companiei oferă indicatori OPSEC care pot fi obținuți şi evaluaţi cu precizie de un infractor cibernetic pentru a prejudicia operaţiunile de succes ale companiei.

ELEMENTELE DE ACŢIUNE ALE PLANULUI CIBERNETIC

9.1 IDENTIFICAȚI TIPURILE DE INFORMAŢII CRITICE

Identificarea informaţiilor critice este importantă mai degrabă pentru că centrează restul procesului OPSEC pe protejarea informaţiilor vitale decât că încearcă să protejeze toate informaţiile relevante pentru operaţiunile companiei. Având în vedere că orice întreprindere are un timp limitat, personal şi bani pentru dezvoltarea practicilor sigure de afaceri, este esenţială concentrarea acestor resurse limitate pe protejarea informaţiilor critice pentru operaţiunile de succes ale companiei. Exemple de informaţii critice includ, însă nu trebuie să se limiteze la următoarele:

- Liste de clienţi şi informaţii de contact
- Contracte
- Patente şi proprietate intelectuală
- Contracte de închiriere şi înscrisuri
- Manuale de politici organizaționale
- Acte constitutive
- Documente corporatiste
- Notebook-uri de laborator
- Casete audio
- Casete video
- Fotografii şi diapozitive
- Planuri strategice şi minute ale şedinţelor consiliului de administraţie.

Ceea ce este important de reținut este faptul că informaţiile considerate critice pentru o întreprindere este posibil să nu fie critice pentru altă întreprindere. Folosiţi misiunea companiei dumneavoastră ca ghid în a determina care date sunt cu adevărat vitale.

9.2 ANALIZAŢI AMENINŢĂRILE

Această acţiune implică cercetare şi analiză pentru a identifica posibilii infractori cibernetici care pot încerca să obţină informaţii critice cu privire la operaţiunile

organizației dumneavoastră. Indicatorii OPSEC din trebuie să răspundă la următoarele întrebări privind informaţiile critice:

- Cine poate fi un infractor cibernetic (de ex. concurenţii, hackerii motivaţi politic, etc.)?
- Care sunt scopurile infractorului cibernetic?
- Ce acţiuni poate întreprinde infractorul cibernetic?
- Ce informaţii critice deţine deja infractorul cibernetic despre operaţiunile organizației noastre? (şi anume, ce este deja disponibil publicului?)

9.3 ANALIZAŢI VULNERABILITĂŢILE

Scopul acestei acţiuni este de a identifica vulnerabilităţile existente în vederea protejării informaţiilor critice. Acest lucru necesită examinarea fiecărui aspect al securităţii, care urmăreşte să vă protejeze informaţiile critice şi apoi compararea acelor indicatori cu ameninţările identificate la pasul anterior. Vulnerabilităţile obișnuite pentru organizații nclud următoarele:

- Dispozitivele mobile slab securizate care au acces la informaţii critice.
- Lipsa politicii cu privire la ce echipament informatic, conectat la reţea poate fi luat acasă de la locul de muncă sau luat în străinătate în deplasare.
- Stocarea informaţiilor critice în conturile personale de email sau alte reţele din exteriorul companiei.
- Lipsa politicii cu privire la ce informaţii de afaceri pot fi postate pe sau accesate de site-urile reţelelor de socializare.

9.4 EVALUAŢI RISCUL

Această acţiune are două componente. Prima, în care managerii OPSEC trebuie să analizeze vulnerabilităţile identificate în acţiunea precedentă şi să identifice posibilele măsuri OPSEC pentru dimnuarea lor. A doua, în care trebuie selectate măsurile OPSEC specifice pe baza evaluării riscurilor realizată de conducere. Evaluarea riscurilor necesită compararea costului estimat asociat implementării fiecărei măsuri OPSEC cu potențialele efecte negative asupra operaţiunilor companiei care rezultă din exploatarea unei anumite vulnerabilităţi.

Măsurile OPSEC pot implica anumite costuri în timp, resurse, personal sau interferenţă cu operaţiunile obişnuite. În cazul în care costul pentru obţinerea protecţiei OPSEC depăşeşte

costul prejudiciului pe care l-ar putea cauza un intrus, atunci aplicarea măsurii este necorespunzătoare. Întrucât decizia de a nu implementa o anumită măsură OPSEC implică riscuri, acest pas necesită aprobare din partea managementului organizației.

9.5 APLICAŢI MĂSURILE OPSEC CORESPUNZĂTOARE

În cadrul acestei acţiuni, conducerea firmei analizează şi implementează măsurile OPSEC selectate în acţiunea de evaluare a riscului. Înainte ca măsurile OPSEC să poată fi selectate, trebuie cunoscute obiectivele de securitate şi informaţiile critice, apoi identificaţi indicatorii şi evaluate vulnerabilităţile.

Legături utile

Aceste resurse oferă informaţii suplimentare despre originile, scopul şi implementarea securităţii operaţionale.

- Agenţia Naţională de Securitate/Serviciul Central de Securitate, *PURPLE DRAGON: Originea şi dezvoltarea programului OPSEC în Statele Unite (1993)*: http://www.nsa.gov/public_info/_files/cryptologic_quarterly/purple_dragon.pdf
- Joint Publication 3-13.3, *Securitatea operaţională* (29 iunie 2006): Disponibilă prin Sistemul de informaţii electronice despre educaţia şi instruirea cu doctrină comună (JDEIS). http://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C2_JP_3-13-3_OPSEC_Process.pdf
- Programul naţional OPSEC: https://www.iad.gov/ioss/
- Societatea experţilor OPSEC: http://opsecsociety.org/
- Asociaţia experţilor în securitate operaţională: http://www.opsecprofessionals.org/
- Departamentul securităţii interne. Protecţia infrastructurii critice: http://www.dhs.gov/criticalinfrastructure

X. UTILIZAREA CARDURILOR BANCARE

În cazul în care organizația acceptă plata prin carduri de credit sau debit, este important să aveţi implementate etapele de securitate pentru a vă asigura că informaţiile despre clienţii dumneavoastră sunt în siguranţă. De asemenea, este posibil să aveţi obligaţii cu privire la securitate conform contractelor încheiate cu banca sau cu procesorul de servicii de plată. Aceste entităţi vă pot ajuta să preveniţi frauda. În plus, sunt disponibile resurse şi ponturi generale de securitate gratuite pentru a învăţa cum să păstraţi în siguranţă informaţiile sensibile.

ELEMENTELE DE ACŢIUNE ALE PLANULUI CIBERNETIC

10.1 ÎNŢELEGEŢI ŞI CLASIFICAŢI DATELE PE CARE LE PĂSTRAŢI DESPRE CLIENŢI ŞI CARDURI

- Faceţi o listă cu tipul informaţiilor despre clienţii şi datele cardurilor pe care le colectaţi şi păstraţi – nume, adrese, informaţii de identificare, numere ale cardurilor bancare, date de pe benzile magnetice – codurile CVC sau CVV, detalii ale conturilor bancare şi numerele de securitate socială. Infractorii nu vor doar numerele cardurilor; aceştia caută toate tipurile de informaţii personale, în special dacă acestea îi ajută să comită fraude cu privire la identitate.
- Înţelegeţi unde să păstraţi astfel de informaţii şi cum trebuie acestea protejate.
- Stabiliţi cine are acces la aceste date si dacă acele persoane trebuie să aibă acces.

10.2 EVALUAŢI DACĂ TREBUIE SĂ PĂSTRAŢI TOATE DATELE PE CARE LE STOCAŢI

- După ce aflaţi ce informaţii colectaţi şi stocaţi, evaluaţi dacă chiar trebuie să le păstraţi. Adesea, este posibil ca organizațiile să nu realizeze că se conectează la sau că păstrează date inutile, până când nu efectuează un audit. Dacă nu păstraţi date sensibile, este mai greu pentru infractori să le fure.
- Dacă aţi utilizat numerele cardurilor în alte scopuri decât pentru tranzacţiile de plată, cum ar fi un program de fidelitate clienţi, întrebaţi procesatorul dacă puteţi utiliza date alternative. Tokenizarea, de exemplu, este o tehnologie care maschează numerele cardurilor şi le înlocuieşte cu un număr alternativ care nu poate fi utilizat pentru fraudă.

10.3 UTILIZAȚI INSTRUMENTE ŞI SERVICII SIGURE

- Industria plăţilor păstrează liste de furnizori hardware, software şi servicii care au fost validate conform cerinţelor de securitate ale industriei.
- Organizațiile care utilizează sisteme de plată integrate, în care terminalul de carduri este conectat la un sistem mai vast de computere, pot verifica lista de aplicaţii validate pentru plăţi pentru a se asigura că orice software pe care îl utilizează a fost testat.
- Aveţi o discuţie despre securitate cu furnizorul dumneavoastră în cazul în care produsele sau serviciile pe care le utilizaţi în momentul de faţă nu se află pe aceste liste.

10.4 CONTROLAŢI ACCESUL LA SISTEMELE DE PLATĂ

- Fie că utilizaţi un sistem de plată mai complicat sau un terminal simplu autonom, asiguraţi-vă că aţi controlat în siguranţă accesul.
- Izolaţi sistemele de plăţi de celelalte programe mai puţin sigure, în special de cele conectate la internet. De exemplu, nu utilizaţi acelaşi computer pentru a procesa plăţile şi pentru a naviga pe internet.
- Controlaţi sau limitaţi accesul la sistemele de plăţi, doar pentru angajaţii care au nevoie de acces.
- Asiguraţi-vă că utilizaţi un sistem sigur pentru accesul de la distanţă sau eliminaţi accesul de la distanţă dacă nu aveţi nevoie de acesta, astfel încât infractorii să nu se poată infiltra în sistemul dumneavoastră de pe internet.

10.5 UTILIZAŢI INSTRUMENTE ŞI RESURSE DE SECURITATE

Lucraţi cu banca sau procesatorul de plăți şi întrebaţi care sunt măsurile, instrumentele şi serviciile anti-fraudă pe care le puteţi utiliza pentru a vă asigura că infractorii nu pot utiliza informaţiile de pe cardurile furate din organizația dumneavoastră.

- Pentru retailerii de comerţ electronic:
    - Codul CVC/CVV este codul din trei cifre de pe spatele cardului care însoțește semnătura și care poate ajuta să se verifice dacă clientul este în posesia fizică a cardului şi nu doar a numărului de cont.

  - Retailerii pot utiliza, de asemenea, serviciul de verificare a adreselor pentru a se asigura că titularul cardului a furnizat adresa de facturare corectă asociată contului.
  - Serviciile precum *Verificat de Visa* îndeamnă titularul cardului să introducă parola personală confirmându-şi identitatea şi oferind un strat suplimentar de protecţie.
- Pentru retailerii offline:
  - Folosiţi cardul şi obţineţi o autorizare electronică pentru tranzacţie.
  - Verificaţi dacă semnătura se potriveşte cu cardul.
  - Asiguraţi-vă că terminalul dumneavoastră de plăţi este sigur şi în siguranţă împotriva falsificării.

10.6 REŢINEŢI PRINCIPIILE DE BAZĂ ALE SECURITĂŢII

- Utilizaţi parole puternice, unice şi schimbaţi-le frecvent.
- Utilizaţi tehnologii firewall şi antivirus actualizate.
- Nu daţi click pe linkurile suspecte pe care le puteţi primi prin email sau pe care le întâlniţi online.

Legături utile

Nu trebuie să abordaţi securitatea singuri. Lucraţi cu banca dumneavoastră sau cu procesatorul de plăți pentru a vă asigura că obţineţi suportul şi expertiza de care aveţi nevoie.

- Visa oferă informații utile despre folosirea tokenurilor, precum și alte materiale despre securitatea tranzacțiilor cu cardul: https://usa.visa.com/dam/VCOM/Media%20Kits/PDF/visa-security-tokenization-infographic.pdf
- Informaţii despre standardele de securitate din industrie sunt disponibile la Consiliul PCI pentru standardele de securitate: https://www.pcisecuritystandards.org
- Blogul Paysimple.com oferă o postare utilă despre securitatea cardurilor de credit: https://paysimple.com/blog/5-tips-for-proper-handling-of-customer-credit-card-account-information/
- American Express oferă sfaturi legate de securitatea datelor pentru comercianţi: https://www.americanexpress.com/us/content/fraud-protection-center/home.html?inav=footer_fraud_protection_center

- MasterCard oferă resurse pentru protecţia informaţiilor despre clienţi: http://www.mastercard.com/us/business/en/smallbiz/resources/industry/e-commerce/articles/0802CustomerData.html

XI. REACŢIA LA INCIDENTE

Chiar şi structurile şi planurile de securitate cibernetică bine implementate este posibil să nu prevină toate încălcările mecanismelor de apărare ale datelor organizației dumneavoastră, astfel că trebuie să vă asiguraţi că aveţi implementate proceduri care să răspundă la încălcările securităţii în momentul în care acestea au loc.

TIPURI DE ÎNCĂLCĂRI

Încălcările fizice includ infracţiunile din lumea reală precum spargerile şi furtul de echipamente, precum şi orice eveniment în care echipamentele organizației sunt rătăcite sau pierdute în tranzit. Dispozitivele neautorizate pot fi instalate pe un sistem sau într-o reţea, permiţând alte compromiteri ale confidenţialităţii şi integrităţii datelor. Încălcările fizice pot, de asemenea, rezulta din revânzarea, donarea sau reciclarea echipamentelor vechi care nu au fost curăţate în mod corespunzător de informaţiile sensibile potenţiale.

Încălcările de securitate din reţea şi sisteme includ evenimentele în care computerele sunt infectate cu un cod rău intenționat, sunt accesate de indivizi neautorizaţi de la distanţă sau sunt utilizate de indivizi neautorizaţi pentru a desfăşura activităţi infracționale. Acestea pot include şi abuzurile faţă de routerele şi paravanele de protecţie din reţea, atât în cadrul, cât şi în afara limitelor şi controlului organizaţiei dumneavoastră.

Încălcările securităţii datelor, însemnând scurgerea informaţiilor sensibile prin canale nesigure, pot fi generate de oricare dintre tipurile de evenimente descrise mai sus. Încălcările securităţii datelor pot avea loc şi dacă informaţiile sensibile sunt expuse în mod neadecvat, din greşeală.

ELEMENTELE DE ACŢIUNE ALE PLANULUI CIBERNETIC, ÎN CAZ DE ÎNCĂLCARE

11.1 NOTIFICAŢI APLICAREA LEGII, DACĂ ESTE CAZUL

În funcţie de tipul de încălcare şi tipul de activitate, organizației dumneavoastră i se poate solicita să notifice autorităţile locale de aplicare a legii sau autorităţile guvernamentale la descoperirea unei încălcări a securităţii datelor. În cazul expunerii informaţiilor despre clienţi, trebuie să notificaţi clientul/clienţii despre incident, să înregistraţi datele care au fost pierdute sau expuse şi să notaţi măsurile luate pentru a vă asigura împotriva unei alte expuneri.

11.2 LUCRAŢI ÎN COLABORARE STRÂNSĂ CU ECHIPELE TEHNICE ŞI DE CONDUCERE PENTRU A LIMITA PREJUDICIUL

După ce organizația devine conştientă că a avut loc o încălcare, personalul tehnic şi factorii de decizie trebuie să lucreze împreună pentru a decide asupra celui mai practic şi eficient plan de restricţionare. Planurile de restricţionare vor varia de la un set de circumstanţe la altul şi pot deveni rapid intensive în termeni de timp şi resurse, atât din perspectiva impactului tehnologic, cât şi din perspectiva impactului de afaceri. În orice caz, restricţionarea încălcărilor securităţii datelor trebuie focalizată pe determinarea măsurii compromisului şi păstrării confidenţialităţii şi integrităţii datelor sensibile care nu au fost încă furate sau divulgate.

Alte probleme care afectează selectarea şi executarea planului de restricţionare includ strategia managementului reputaţiei - riscului companiei dumneavoastră şi decizia cu privire la solicitarea sau nu a asistenţei din exterior – fie de la o firmă locală sau federală de aplicare a legii, o firmă de consultanţă privată sau o organizaţie care se ocupă cu reacţia la incidente precum US-CERT.

11.3 ÎNCEPEŢI EFORTUL DE RECUPERARE

După stabilirea unui plan de restricţionare şi după ce executarea sa a început, începeţi eforturile de eradicare şi de recuperare. În cazul încălcărilor de securitate din reţea şi sisteme, eradicarea înseamnă de obicei eliminarea tuturor cazurilor de software neautorizat din reţea şi invalidarea tuturor privilegiilor de acces asociate cu utilizatorii care au comis o activitate neconformă.

Curăţarea unei reţele sau a unui sistem de toate urmele de cod rău intenționat poate duce uneori la necesitatea de a şterge complet toate suporturile de stocare şi realizarea unei „instalări curate”. Astfel, recuperarea după o astfel de încălcare poate fi intensivă din punct de vedere al resurselor şi poate necesita restaurarea precaută a datelor de pe copiile de rezervă. Reţineţi că acest copii de rezervă pot, de asemenea, să conţină cod maliţios şi trebuie verificate cu atenţie să nu fie compromise; în caz contrar, încălcarea securităţii va fi perpetuată după faza de recuperare.

11.4 PRINCIPII CHEIE DE RECUPERARE DUPĂ DEZASTRE

- **Nu aşteptaţi până este prea târziu** – Organizațiile nu ar trebui să aştepte până după un dezastru pentru a se gândi la ceea ce ar fi trebuit să facă pentru a-şi proteja

datele. Inactivitatea nu este doar costisitoare din perspectivă financiară, ci ar putea însemna şi desfiinţarea întreprinderii. Organizațiile trebuie să-şi traseze din timp planuri în ceea ce priveşte gradul de pregătire pentru dezastre, inclusiv identificarea sistemelor-cheie, a datelor şi a altor resurse care sunt critice pentru desfăşurarea activităţii.

- **Protejaţi complet informaţiile** – Pentru a reduce riscul de pierdere a informaţiilor critice de afaceri, organizațiile trebuie să implementeze soluţii corespunzătoare de securitate şi backup pentru a arhiva fişierele importante, cum ar fi evidenţele despre clienţi şi informaţiile financiare pe termen lung. Dezastrele naturale, furtul şi atacurile cibernetice pot duce la pierderea de date şi pierderi financiare, astfel că organizațiile trebuie să se asigure că fişierele importante sunt salvate nu doar pe hard diskul extern şi/sau reţeaua companiei, ci şi într-o locaţie sigură, în afara unităţii.
- **Implicaţi angajaţii** – Angajaţii joacă un rol cheie în a ajuta la prevenirea inactivităţii. Aceştia trebuie educaţi cu privire la cele mai bune practici de securitate informatică şi cu privire la ce să facă în cazul în care informațiile sunt şterse accidental sau nu pot fi găsite cu uşurinţă în fişierele lor. Organizațiile au adesea resurse limitate, toţi angajaţii ar trebui să ştie cum să recupereze informaţiile întreprinderilor în perioade de dezastru.
- **Testaţi în mod frecvent** – Perioada de după lovitura unui dezastru reprezintă cea mai grea perioadă pentru a învăţa ce înseamnă să nu fie făcute copii de rezervă pentru fişierele critice aşa cum a fost planificat.
- Testarea regulată de recuperare după dezastru este de nepreţuit. **Testaţi planul** ori de câte ori ceva se schimbă în mediul dumneavoastră.
- **Analizaţi planul** – Dacă testarea frecventă nu este fezabilă din cauza resurselor şi a lungimii de undă, organizațiile ar trebui cel puţin să analizeze semestrial planul cu privire la gradul de pregătire în caz de dezastru.
- **Fiţi pregătiţi** – Întotdeauna este cel mai bine şi mai puţin costisitor să investiţi în securitatea adecvată dinainte, decât să treceţi printr-o reacţie la incidente costisitoare, care ar putea duce la reconstruirea întregii infrastructuri a reţelei.

11.5 ŢINEŢI O REUNIUNE DESPRE „LECŢIILE ÎNVĂŢATE”

În final, organizația dumneavoastră ar trebui să ţină întotdeauna o reuniune despre „lecţiile învăţate” după finalizarea cu succes a etapei de recuperare, pentru a descoperi, a se documenta şi a-şi rafina cunoştinţele acumulate pe durata procesului de control al incidentelor.

XII. DEZVOLTAREA ŞI MANAGEMENTUL POLITICILOR

Toate companiile ar trebui să dezvolte şi să menţină politici clare şi robuste pentru protejarea datelor critice de afaceri şi a informaţiilor sensibile, protejându-şi reputaţia şi descurajând comportamentul necorespunzător al angajaţilor.

Multe dintre aceste tipuri de politici există deja în situaţiile din „lumea reală”, însă este posibil să trebuiască să fie personalizate pentru organizaţia dumneavoastră şi să fie actualizate pentru a reflecta impactul tot mai mare al spațiului cibernetic asupra tranzacţiilor zilnice, atât profesionale cât şi personale. Ca şi în cazul oricărui alt document de afaceri, politicile de securitate cibernetică trebuie să urmeze bunele practici de design şi guvernare - nu atât de mult încât să devină neutilizabile, nu atât de vagi încât să devină fără sens, şi mai ales trebuie analizate cu regularitate pentru a se asigura că rămân pertinente pe măsură ce nevoile dumneavoastră de afaceri se schimbă.

Vă rugăm să aveţi în vedere că în acest document nu se abordează toate cerinţele politicilor pentru organizațiile care se încadrează în actele sau directivele legislative, precum *Legea portabilităţii şi contabilităţii asigurărilor sociale*, *Legea Sarbanes-Oxley* sau alte reglementări federale, statale sau locale.

ELEMENTELE DE ACŢIUNE ALE PLANULUI CIBERNETIC

12.1 STABILIŢI ROLURI ŞI RESPONSABILITĂŢI CU PRIVIRE LA SECURITATE

Unul dintre cele mai eficiente şi mai puţin costisitoare mijloace de prevenire a incidentelor grave legate de securitatea cibernetică este de a stabili o politică care să definească clar separarea rolurilor şi a responsabilităţilor cu privire la sistemele şi informaţiile pe care le conţin. Multe sisteme sunt concepute pentru a furniza un control puternic al accesului bazat de roluri (RBAC), însă acest instrument este de o utilitate redusă, fără proceduri şi politici bine definite pentru atribuirea rolurilor şi a constrângerilor asociate acestora. O astfel de procedură trebuie să menţioneze clar, cel puţin următoarele aspecte:

- Identificaţi clar drepturile de proprietate asupra datelor companiei şi rolurile angajaţilor pentru supravegherea securităţii şi a privilegiilor inerente ale acestora, inclusiv:
  - Rolurile necesare şi privilegiile şi constrângerile aferente acestor roluri.

- Categoriile de angajaţi care ar trebui să primească permisiunea de a-şi asuma diverse roluri.
- Cât de mult poate un angajat să deţină un rol înainte ca drepturile sale de acces să fie reanalizate.
- În cazul în care angajaţii pot deţine roluri multiple, circumstanţele care definesc când să adopte un rol în detrimentul altuia.

În funcţie de tipurile de date utilizate cu regularitate de întreprinderea dumneavoastră, poate avea sens, de asemenea, crearea de politici separate care să guverneze cine este responsabil de anumite tipuri de date. De exemplu, o întreprindere care utilizează volume mari de informaţii personale identificabile (IPI) de la clienţii săi poate beneficia de identificarea unui administrator şef pentru informaţiile legate de confidențialitatea clienţilor. Administratorul ar putea servi nu numai ca expert în toate problemele de confidențialitate, dar ar servi şi ca apărător pentru îmbunătăţirile proceselor tehnice pentru utilizarea IPI.

12.2 STABILIŢI O POLITICĂ DE UTILIZARE A INTERNETULUI DE CĂTRE ANGAJAŢI

Limitele privind utilizarea internetului de către angajaţi la locul de muncă variază foarte mult de la o întreprindere la alta. Liniile dumneavoastră directoare trebuie să permită angajaţilor gradul maximum de libertate de care au nevoie pentru a fi productivi (pauzele scurte pentru a naviga pe internet sau pentru a efectua anumite sarcini personale online s-au dovedit a spori productivitatea). De asemenea, regulamentul de conduită este necesar pentru a se asigura că toţi angajaţii sunt conştienţi de limite, atât pentru a le menţine siguranţa cât şi pentru continuarea succesului companiei. Unele reguli care trebuie avute în vedere:

- Pauzele personale pentru a naviga pe internet trebuie să fie limitate la o durată rezonabilă şi la anumite tipuri de activităţi.
- Dacă utilizaţi un sistem de filtrare web, angajaţii trebuie să deţine cunoştinţe clare cu privire la cum şi de ce activităţile lor pe web vor fi monitorizate, şi ce tipuri de site-uri sunt considerate inacceptabile de către politica dumneavoastră.
- Regulamentul de conduită la locul de muncă trebuie să fie clar, concis şi uşor de urmat. Angajaţii trebuie să se simtă confortabil în timpul realizării sarcinilor personale şi profesionale online fără să se întrebe ce este sau nu este considerat corespunzător.

Organizațiile pot dori să includă un avertisment de tip splash la autentificarea în rețea care să avizeze angajaţii cu privire la politicile de utilizare a internetului ale întreprinderilor, astfel încât toţi angajaţii să fie avizaţi.

12.3 STABILIŢI O POLITICĂ PRIVIND SOCIAL MEDIA

Aplicaţiile de pe reţelele sociale prezintă anumite riscuri care sunt dificil de abordat utilizând soluţiile tehnice sau procedurale. O politică puternică privind social media este crucială pentru orice întreprindere care urmăreşte să utilizeze reţelele sociale pentru a-şi promova activităţile şi a comunica cu clienţii săi. Politica privind social media ar trebui să includă în mod clar următoarele:

- Îndrumare specifică despre când să se dezvăluie activităţile companiei utilizând social media şi ce tipuri de detalii pot fi discutate pe un forum public.
- Reguli de conduită suplimentare pentru angajaţii care utilizează conturile personale din reţelele de socializare pentru a clarifica ce tipuri de subiecte de discuţie sau postări ar putea genera riscuri pentru companie.
- Îndrumare cu privire la acceptabilitatea utilizării adresei de email a companiei pentru a se înregistra la, sau a primi notificări de pe site-urile social media.
- Îndrumare cu privire la selectarea parolelor lungi şi puternice pentru conturile de pe reţelele de socializare, întrucât foarte puţine site-uri social media aplică politici puternice de autentificare pentru utilizatori.

În cele din urmă, toţi utilizatorii social media trebuie să fie conştienţi de riscurile asociate cu instrumentele reţelelor sociale şi tipurile de date care pot fi dezvăluite automat online în timpul utilizării social media. Acordarea timpului necesar pentru a vă educa angajaţii despre potenţialele capcane ale utilizării social media, în special în tandem cu serviciile de geolocalizare, poate fi cea mai benefică practică de securitate privind reţelele sociale dintre toate.

12.4 IDENTIFICAŢI POTENŢIALELE RISCURI REPUTAŢIONALE

Toate organizaţiile trebuie să-şi facă timp să identifice potenţialele riscuri pentru reputaţia lor şi să dezvolte o strategie pentru a minimiza aceste riscuri prin politici sau alte măsuri, în funcţie de disponibilități. Tipurile specifice de riscuri reputaţionale includ:

- A fi imitat online de o organizaţie criminală (de ex., un site web ilegal care falsifică denumirea companiei dumneavoastră şi copiază designul site-ului dumneavoastră,

încercând apoi să înşele potenţialii clienţi prin înșelătorii de tip phishing sau prin altă metodă).

- Scurgerea de informaţii sensibile despre companie sau despre clienţi către public prin internet.
- Publicarea acţiunilor sensibile sau necorespunzătoare ale angajaţilor prin intermediul internetului sau site-urilor social media.

Toate organizațiile ar trebui să stabilească o politică pentru gestionarea acestor tipuri de riscuri şi planuri pentru a aborda astfel de incidente în cazul în care şi atunci când au loc. O astfel de politică trebuie să acopere un proces zilnic pentru identificarea potenţialelor riscuri privind reputaţia companiei în spaţiul cibernetic și măsurile practice pentru prevenirea acestor riscuri care să ajute la recuperarea datelor din potenţialele incidente imediat ce acestea au loc.

Legături utile

- Campania Protejaţi-vă forța de muncă a US-CERT: http://www.us-cert.gov/reading_room/distributable.html
- Socializarea în siguranţă: Utilizarea serviciilor reţelelor de socializare: http://www.us-cert.gov/reading_room/safe_social_networking.pdf
- Guvernare pentru securitatea întreprinderii: http://www.cert.org/governance/
- Ghidul FFIEC privind definiţia riscului reputaţional: http://ithandbook.ffiec.gov/it-booklets/information-security.aspx
- Ce activităţi se pot desfăşura pentru securitate cibernetică: http://staysafeonline.org/business-safe-online

XIII. GLOSAR DE TERMENI UTILIZAȚI ÎN SECURITATE CIBERNETICĂ

Access Control

În general, se referă la un fișier individual sau la un director de fișiere. Fiecare fișier dispune de un atribut de securitate care își verifică prezența pe respectiva listă de control a accesului. Lista de control diferă de la utilizator la utilizator și validează operațiunile pe care utilizatorul este îndreptatit să le execute (citire, scriere, executare, transfer etc.).

Active Content

Un conținut activ este scris în trei scripturi diferite: Active X, Java sau JavaScript. Prin intermediul acestuia se pot produce pagini web animate, care conțin fluxuri (streaming) video sau alte obiecte multimedia. Cu toate acestea, conținutul activ este adesea asociat cu diferite vulnerabilități sau probleme de securitate.

ActiveX

Termenul a fost dat de compania Microsoft pentru a identifica propriul set de tehnologii de programare orientată pe obiecte. Cu ajutorul unui control ActiveX, tehnologia Microsoft orientata pe obiecte poate rula aplicatii în diferite sisteme de operare. Un control ActiveX poate fi creat utilizând multiple limbaje de script, cum ar fi: Visual Basic, PowerBuilder sau VBScript. Beneficiilor aduse de controalele ActiveX li se opun probleme de securitate intens exploatate de hackeri.

Administrator

Este persoana care deține cele mai multe drepturi sau privilegii în cadrul sistemului de operare. În general, în cadrul unei mașini de calcul sub Windows, administratorul sau ”deținătorul contului principal” poate acorda drepturi de acces celorlalți utilizatori. Toate calculatoarele care rulează sistemul de operare Windows au același Identificator de Securitate (SID) – parolă sau combinație de litere și cifre care determină sistemul să aloce unui utilizator acces la anumite resurse. Modul de administrare a conturilor utilizatorilor are o mare importanță în prevenirea apariției unor eventuale breșe de securitate în cadrul sistemului.

Advanced Persistent Threat-APT

Amenințare avansată și persistentă este o formă complexă de atac informatic caracterizată prin două trăsături definitorii:

- nivelul avansat al metodelor de evitare a detecției (ex. prin utilizarea exploit-urilor de tip "zero-day"), al instrumentelor de comunicare/legătură cu centrele de comandă-control (ex. instrucțiunile centrelor de comandă către resursele controlate sunt criptate și transmise în grupuri mici de pachete de date, disimulate în traficul normal TCP), precum și al mijloacelor de exfiltrare a datelor (informatice) de interes (ex. datele sunt "ascunse" iar algoritmii de criptare nu trebuie să atragă atenția în cadrul procesului de transmisie);
- persistența, întrucât amenințarea / atacul trebuie să poată continua pe o durată cât mai mare, în detrimentul organizației / resursei informaționale compromise.

Adware

Orice aplicaţie software care afişează bannere publicitare în timpul derulării programului. Adware-ul include adesea un cod care urmăreşte informaţiile personale ale utilizatorului şi le pasează terţilor fără autorizarea sau cunoştinţa utilizatorului. Şi dacă se adună destul de multe, adware-urile încetinesc computerul semnificativ. În timp, performanţa poate fi atât de deteriorată încât pot apărea probleme în a lucra productiv. Vezi şi Spyware şi Software-uri rău intenţionate.

AH, Authentication Protocol

Adesea numit AH Protocol, headerul de autentificare certifică integritatea datelor transmise/recepționate prin verificarea unei sume de control (checksum) asociată fiecărui mesaj de către un cod de autentificare.

Amenințare combinată

Un atac în reţeaua de computere care caută să maximizeze gravitatea prejudiciului şi viteza de contagiune prin combinarea metodelor—de exemplu, utilizând atât caracteristici ale viruşilor cât şi ale viermilor. Vezi şi Infecţie electronică.

Antivirus

Aplicații special create pentru a identifica, gestiona, curăța sau elimina conținutul infectat sau malițios existent într-un sistem de calcul sub formă de viruși, viermi, Cai Troieni, rootkit, etc. Cele mai multe astfel de aplicații examinează fișier cu fișier în raport cu propriile liste de infecții cunoscute și, după caz: încearcă să remedieze problema prin îndepărtarea infecției din fișierul suspect, neutralizează fișierul respectiv astfel încât acesta să nu fie accesibil și altor programe pe care le-ar putea infecta, respectiv elimină complet fișierul suspect. Vezi şi Virus şi Infecţii electronice.

Aplicaţie

Program care execută funcţii automate pentru un utilizator, cum ar fi prelucrarea în Word, foi de calcul, grafice, prezentări şi baze de date—spre deosebire de programul sistemului de operare (SO).

Applet

Termen introdus în 1993 odată cu aplicația AppleScript. Un applet oferă elemente grafice interesante și chiar interacționează cu utilizatorul. Cel mai adesea, rulează împreună cu alte programe oferind facilități care, luate individual, nu au nicio aplicabilitate directă. Applet-urile sunt scrise în limbaje de programare diferite de HTML sau Script, ceea ce le oferă o mai bună funcționalitate atunci când sunt rulate.

ARP, Address Resolution Protocol

Datorită extinderii conexiunilor Ethernet și IPv4, acest protocol de rezolvare a adreselor este în general folosit pentru translatarea adreselor de tip IP (Internet Protocol) în adrese MAC Ethernet (adrese fizice).

Atac cibernetic (informatic)

Formă violentă de manifestare virtuală la adresa unuia sau mai multor sisteme de calcul. Un atac reușit va oferi celui care l-a inițiat posibilitatea de a controla sistemul țintă prin compromiterea funcțiilor administrative ale acestuia. Atacurile informatice pot fi derulate în mod direct de către hacker sau prin angrenarea de la distanță a altor sisteme aflate (dinainte) sub control.

Atac de tip forţă brută

O procedură exhaustivă de spargere a parolelor care încearcă toate posibilităţile, una câte una. Vezi şi **Atac de tip dicţionar** şi **Atac hibrid**.

Ataşament

Un fişier care a fost adăugat la un email—adesea o imagine sau un document. Acesta ar putea fi ceva folositor sau ceva dăunător pentru computer. Vezi şi Virus.

Autentificare

Confirmarea corectitudinii pretinsei identităţi a unui utilizator persoană fizică, maşină, componentă software sau a oricărei alte entităţi. Atât în cazul rețelelor publice, cât și al celor private, autentificarea este procesul prin care un utilizator sau o stație de lucru se identifică în mod corect în raport cu o altă stație de lucru sau rețea, prin intermediul mai multor elemente de siguranță, cum ar fi: nume_utilizator, parolă, certificat digital etc.

Autorizare

În cazul sistemelor de operare multi-utilizator, administratorul va decide care utilizator va avea acces în sistem, tipul de privilegii în ceea ce priveste folosirea resurselor sistemului (ex. ce tip de fișiere pot fi accesate, pentru cât timp, operațiile care pot fi efectuate asupra fișierelor etc.). În acest context, autorizarea ar putea fi definită drept configurarea inițială a drepturilor utilizatorilor unui sistem informatic de către administratorul acestuia și verificarea respectivelor drepturi cu ocazia accesării sistemului.

Backdoor (uşă secretă)

Software ascuns sau mecanism hardware utilizat pentru a înşela controalele de securitate. Este unul dintre cei mai periculoși Cai Troieni. Adesea, este transmis ca un atașament atractiv pentru utilizatorul vizat, putând fi „camuflat” drept joc video, aplicație multimedia sau documente. În general, se instalează automat la vizitarea unui website infectat și oferă celui care l-a trimis posibilitatea de a accesa de la distanță sistemul de operare al mașinii de calcul atacate și de a intra în posesia datelor personale ale utilizatorului, mesajelor de email, documentelor stocate etc. Specialiștii apreciază destul de dificilă eliminarea din sistem a acestui tip de Troian.

Backup (copie de rezervă)

Copii ale fişierelor care sunt salvate ca protecţie împotriva pierderii, deteriorării sau indisponibilităţii datelor primare. Metodele de salvare includ banda de înaltă capacitate, sub-sisteme de discuri separate sau aplicațiile dedicate pe internet. Stocarea copiilor de rezervă în afara unităţii este ideală, destul de departe pentru a reduce riscul deteriorării de mediu cum ar fi inundaţia, care ar putea distruge atât datele primare cât şi copiile de rezervă, dacă ar fi păstrate în apropiere.

Badware

Vezi Software-uri rău intenţionate, Adware şi Spyware.

Bandwidth

În telecomunicații, lărgimea de bandă reprezintă spațiul (valoarea exprimată în Hertzi) dintre limita minimă și cea maximă a unei benzi de frecvență. în cazul internetului, lărgimea de bandă reprezintă capacitatea maximă a transferului de date pentru o anumită infrastructura de transport (cablu coaxial, fibră optică, radio etc.) și se măsoară în bps (bytes per second – octeți pe secundă).

Blacklisting Software (Program de adăugare în lista neagră)

O formă de filtrare care blochează doar site-urile web specificate ca fiind dăunătoare. Părinţii şi angajatorii utilizează uneori astfel de programe pentru a împiedica copiii şi angajații să viziteze anumite site-uri web. Puteţi adăuga şi şterge site-uri de pe lista “nepermise”. Această metodă de filtrare permite utilizarea mai completă a internetului, însă este mai puţin eficientă în prevenirea accesului pentru orice material dăunător care nu este pe listă. Vezi şi Whitelisting Software.

BIOS

Basic Input / Output System este o componentă integrală, preinstalată, a unui sistem informatic. La pornirea sistemului, BIOS-ul execută o verificare a existenței / bunei funcționări a tuturor componentelor hardware apoi procedează la încărcarea sistemului de operare în memoria RAM din discul dur (HDD) sau unitatea externă (Floppy, CD, DVD etc.).

Blog

Prescurtarea pentru “jurnal web”, un blog este de obicei definit ca o agendă sau un jurnal online. De obicei este actualizat frecvent şi oferit într-un format de jurnal datat cu cea mai recentă intrare în partea de sus a paginii. Acesta conţine adesea linkuri spre alte site-uri web împreună cu comentariul despre acele site-uri sau subiecte specifice cum ar fi politică, noutăţi, cultură populară sau computere.

Bandă largă

Termen general utilizat pentru a face referire la conexiunile reţelelor de înaltă viteză cum ar fi modemul de cablu şi Linie digitală de abonat (DSL). Aceste tipuri de conexiuni internet “întotdeauna activate” sunt de fapt mai susceptibile de anumite ameninţări la adresa securităţii decât computerele care accesează web-ul prin intermediul serviciului de apelare.

Browser

Un software pentru clienţi care poate regăsi şi afişa informaţii de pe serverele World Wide Web. Adesea cunoscut ca un “Browser web” sau “Browser internet”, exemplele incluzând Microsoft Internet Explorer, Google Chrome, Safari al Apple şi Mozilla Firefox.

Bluetooth

Tehnologie care implică folosirea undelor radio de frecvență scurtă între dispozitive PDA, telefoane celulare, computere și orice alte instrumente cu conectare fără fir.

Bot Worm

Este un tip de aplicație scrisă cu scopul de a transforma computerele infectate în platforme virtuale de atac, denumite în literatura de specialitate zombi sau botnets, care vor fi implicate în distribuirea de mesaje nesolicitate (spam), viruși, Cai Troieni etc. Mai nou, aceste aplicații atacă în special programele anti-virus, exploatându-le acestora anumite vulnerabilități recunoscute sau nu. Principala metodă de protecție o reprezintă actualizarea permanentă a pachetelor anti-virus și anti-spyware.

Botnet

Acronim al expresiei robot NETwork. Reprezintă o colecție de calculatoare infectate și aflate sub controlul unei mașini de calcul denumită Master Unit, prin intermediul cărora sunt lansate atacuri informatice de tipul Denial of Service (refuzul serviciului), scanarea neautorizată a porturilor asignate protocolului de poștă electronică, distribuirea de mesaje nesolicitate (spam), furt de date confidențiale, obținerea de parole, date financiare etc. în general, aceste rețele comunică între ele, ceea ce le sporește periculozitatea.

Bot Herder

Este denumirea folosită pentru a identifică pe autorul / creatorul unei rețele de tip Botnet. Acesta menține și exploatează rețeaua în scopul obținerii de beneficii materiale sau de altă natură (ex. politice). Odată creată rețeaua Botnet, autorul adesea o închiriază (pune la dispoziția) cercurilor criminale organizate în vederea desfășurării atacurilor planificate. Se mai regăsește și sub denumirea de Bot Master.

Broadband

Rețea capabilă de transmisii de date cu viteze mari. De asemenea, termenul „bandă largă” se poate referi și la tipul de tehnologie utilizată pentru transferul datelor, cum este cazul DSL (Digital Subscriber Line).

Brute Force

Metoda forței brute este adesea folosită în decodarea (decriptarea, spargerea etc.) unor mesaje sau parole prin încercarea tuturor codurilor sau combinațiilor alfanumerice posibile. Atacul prin forță brută își pierde din valoare odată cu creșterea dimensiunii cheii de criptare sau a codului folosit de utilizator. Multe aplicații de securitate sunt capabile, în prezent, să identifice și să blocheze atacuri informatice de acest tip.

Buffer

Zonă de memorie (tampon) folosită pentru stocarea temporară a datelor aflate în tranzit. Folosirea bufferului împiedică un anumit sistem să încetinească activitatea celorlalte sisteme, dacă acestea operează la viteze diferite.

Bug

Denumire atribuită unei erori dintr-un program informatic, care îl împiedică pe acesta să ruleze în modul pentru care a fost creat. Apare adesea ca urmare a unor greșeli de programare sau de executare a codului sursă, respectiv de instalare a respectivului pachet software pe o mașină de calcul. Multe astfel de erori pot rămâne nedetectate o lungă perioadă de timp, provocând doar o încetinire în funcționarea sistemului, în timp ce altele sunt mult mai grave și pot conduce la întreruperea rulării aplicației ori chiar la paralizarea întregului sistem (ex. Denial of Service).

Cache

Este în general privit ca un depozit temporar și definit drept o colecție de date duplicate stocate într-o locație diferită de cea a datelor originale. Tehnic, poate fi mult mai convenabil ca datele să fie accesate din locația (depozitul) duplicat decât din cea inițială. Este folosită pentru accesarea repetată a anumitor date într-un interval de timp redus (ex. date temporare din Internet).

Cache Poisoning

Formă de atac informatic ce constă în pătrunderea într-un server nume de domeniu (DNS) și înlocuirea unei adrese reale de Internet cu una falsă ori aflată sub controlul atacatorilor, care redirectează traficul de date al mașinii de calcul vizate către pagini web infectate cu viruși, viermi, Cai Troieni ori alte aplicații nocive.

Certificate

Termen aflat în conjuncție cu domeniul criptografiei, desemnează un document electronic ce conține o semnătura digitală asociată unei chei publice, drept sursă de identificare (și veridicitate) a unei pagini web, mesaj de poștă electronică, formular electronic etc. Vezi explicațiile de la infrastructura de chei publice.

Certificat digital

Echivalentul electronic al unei cărţi de identitate care stabileşte credenţialele dumneavoastră în momentul în care desfăşuraţi activităţi comerciale sau alte tranzacţii pe web. Acesta conţine numele dumneavoastră, un număr de serie, datele de expirare, o copie a cheii publice a titularului certificatului (utilizat pentru

criptarea mesajelor şi semnăturile digitale) şi semnătura digitală a autorităţii care a emis certificatul astfel încât destinatarul să poată verifica dacă certificatul este real.
Criptare

O tehnică de securitate a datelor utilizată pentru a proteja informaţiile împotriva inspectării neautorizate sau alterării. Informaţiile sunt codate astfel încât să apară ca un şir fără înţeles de litere şi simboluri în timpul livrării sau transmiterii. La primire, informaţiile sunt decodate utilizând o cheie de criptare.

Chat Room

Desemnează o zonă de discuții pe un server dedicat schimbului de mesaje scurte care folosește protocolul Internet Relay Chat și o aplicație specializată (ex. Yahoo Messenger, Google Talk, mIRC etc.). Camerele de discuții sunt create automat de sistem sau de către utilizatori în funcție de subiectul de interes sau preocupările comune ale acestora. Odată intrat într-o cameră de discuție, utilizatorul autentificat poate observa care utilizatori sunt prezenți sau nu și poate iniția discuții de grup sau private. În general, discuțiile sunt monitorizate de administratorii site-ului sau ai serverului gazdă, iar comportamentul antisocial ori infracțional este pedepsit prin decuplarea sau interzicerea (banarea) utilizatorului "vinovat".

Clickjacking (orig. User Interface Redress Attack)

Descrie o tehnică de inducere în eroare a unui utilizator care vizitează o pagină web, cu scopul de a-l determina să efectueze o operațiune de tip "click" pe un anumit obiect (link) din pagină, care, în realitate, este diferit de cel vizualizat și ales de către vizitator. Tehnic, pagină web vizitată conține un cod (script) care se execută fără știrea utilizatorului (vizitatorului). De exemplu, un "buton" care pare să genereze o cu totul altă operațiune în pagină. Termenul "clickjacking" a fost folosit prima dată în anul 2008 de specialiștii Jeremiah Grossman și Robert Hansen.

Cloud Computing (sau Remote Computing Services)

Reprezintă un nou concept de relație server-aplicație, o arhitectură emergentă de rețea în care aplicațiile se găsesc pe terțe servere (neutre), deținute și întreținute de companii private care furnizează acces (eventual securizat), la distanță, prin intermediul unor instrumente bazate pe tehnologia web. Acest nou model

contrastează cu actualul, în care datele și aplicațiile se găsesc, tipic, pe servere sau computere aflate sub controlul utilizatorilor finali. În marea lor majoritate, utilizatorii finali pierd controlul asupra propriilor informații atunci când plasează date sau aplicații pe servere centralizate. Informațiile critice (sensibile), Gcare odată erau stocate securizat în sistemele informatice personale, se găsesc acum pe serverele unor companii online, ceea ce face ușor de imaginat scenarii de tip "data hostage", ținând cont de posibilitatea ca, într-o bună zi, utilizatorul să nu mai poată dispune de propriile date decât în schimbul unor ori diverse compensații în beneficiul "gazdei".

Content Spoofing

Formă de atac informatic care vizează "ademenirea" utilizatorilor neprevăzători și determinarea acestora să acceseze website-uri clonate. În legislația română se regăsește sub denumirea de fals informatic. Cea mai cunoscută modalitate de falsificare a conținutului web este Phishing-ul. Cea mai periculoasă formă de Content Spoofing se realizează cu ajutorul surselor DHTML (Dynamic Hyperterminal Markup Language) prin care atacatorii pot crea formulare online sau aplicații de autentificare (login) cu scopul de a induce în eroare utilizatorii legitimi și obține neautorizat datele personale sau de logare ale acestora.

Cookie

Un fişier de mici dimensiuni care este descărcat de anumite site-uri web pentru a stoca un pachet de informaţii pe browser. Companiile şi organizaţiile utilizează cookies pentru a memora datele de identificare ale autentificării sau înregistrării, preferinţele cu privire la site-uri, paginile vizualizate şi “coşul de cumpărături’ online astfel încât la următoarea vizită, informaţiile stocate pot fi extrase automat. Un cookie este evident comod însă prezintă şi potenţiale probleme de securitate. Browserul poate fi configurat să informeze ori de câte ori este trimis un cookie. Utilizatorul poate refuza să accepte toate cookie-urile sau să şteargă toate cookie-urile salvate pe browser.

Cookie Poisoning

În mediul Internet, metodă este cunoscută ca fiind operațiunea de schimbare a informațiilor personale stocate în format electronic în calculatorul unui utilizator.

Cookies sunt mici fișiere stocate în hard drive-ul unui computer ce conțin detalii care ajută la o mai rapidă autentificare a identității unui utilizator pe paginile web recent vizitate, cresc viteza de tranzacționare, monitorizează obiceiurile de navigare și chiar personalizează conținutul unui site pentru fiecare utilizator. Deși benefice, Cookies sunt totuși capabile să lase un sistem deschis pentru o largă varietate de aplicații de tip exploits și aceasta din cauza că pot fi cu ușurință accesate de utilizatori neautorizați. Dacă aplicațiile de securitate nu sunt bine configurate pe o mașină de calcul, atacatorii pot examina cu atenție conținutul acestor fișiere Cookies și pot insera propriul conținut, efectuând "ajustări" de pe urma cărora să poată ulterior beneficia. Cea mai bună protecție împotriva modificării conținutului Cookies este eliminarea frecventă a acestora din sistem. Pe de altă parte, administratorii website-urilor folosesc aplicații dedicate care protejează fișierele de tip Cookie prin criptare.

"Copy-Paste" Scam

Formă de inginerie socială prin care utilizatorii sunt "invitați" (ademeniți) să copieze și să însereze cod dăunător Java în bara de adrese a propriului browser, fiind induși în eroare de către atacatori că, astfel, vor primi cupoane-cadou sau alte beneficii online.

Computer zombie

Un cal troian cu acces de la distanţă instalează un cod ascuns care permite controlul de la distanţă a computerului dumneavoastră. Hoţii digitali utilizează apoi reţele robot de mii de computere zombie pentru a-şi desfăşura atacurile asupra altor persoane şi pentru a-şi ascunde urmele. Autorităţile au o perioadă de timp mai dificilă în urmărirea infractorilor când aceştia trec prin computere zombie.

Criptanalysis

Criptanaliza este procesul de descoperire a cheii secrete de codificare a unui mesaj. În jargonul de specialitate se mai numește și spargere de cod. În cele mai multe situații, criptanaliza nu are nimic de-a face cu alte modalități de obținere a unor informații secrete, precum ”darea de mită”, ”înregistrarea textului introdus de la tastatură” ori ”ingineria socială”.

Cybercrime

Termen generic ce încearcă să definească paleta largă de infracțiuni ce sunt comise asupra datelor informatice ori sistemelor informatice și de comunicații, pe de o parte, sau cu ajutorul acestora, pe de altă parte.

Cybersurveillance / Cybermonitoring

Activitatea de supraveghere electronică a activității unei persoane în spațiul cibernetic (PC, rețea, Internet).

Cyberslacking

Practică de zi cu zi a foarte multor angajați ce implică folosirea Internetului pentru o serie de activități online care nu au legătură cu procesul de muncă stabilit prin fișa postului: verificarea poștei electronice personale, navigarea pe site-uri de știri sau divertisment, jocuri online, descărcarea de muzică și filme etc.

Cyberbullying

Formă agresivă de comportament în spațiul virtual, manifestată prin transmiterea de mesaje electronice, postarea de conținut digital nepotrivit sau prin efectuarea de apeluri telefonice, cu scopul de a intimida ori controla o persoană.

Cyberharassment

"Hărțuirea online" presupune utilizarea Internetului, a sistemelor informatice ori a mijloacelor de comunicații electronice, în mod repetat, intenționat și abuziv, cu scopul de a controla, intimida, manipula, discredita, umili, deranja sau supăra o persoană, de a-i produce acesteia o teamă ori a-i afecta initimitatea în spațiul cibernetic.

Cyberstalking

Utilizarea Internetului sau a altor mijloace de comunicare electronică, în mod repetat, pentru a urmări/monitoriza/supraveghea în spațiul cibernetic activitățile ori comportamentul unei persoane, unui grup de persoane sau a unei organizații, cu scopul de a le intimida pe acestea, de a le hărțui ori de a le provoca un sentiment de insecuritate. Adesea, se confunda cu Cyberharassment-ul sau Cyberbullying-ul.

Data Corruption

În timpul tranzitului (transportului), datele informatice pot fi alterate din multiple cauze. De exemplu, vremea nefavorabilă (ploi, ninsori, nori etc.) poate interfera cu trasmisia de date prin intermediul satelitului. Dispozitivele wireless pot, de asemenea, conduce la o alterare a integrității datelor transmise din cauza interferenței produse de aparatura generatoare de microunde (ex. cuptor cu microunde). La nivel de aplicație, datele pot fi alterate (corupte) de erorile de programare (bug-uri) sau de acțiunea virușilor informatici.

Dos Attack

Un atac de tipul refuzul serviciului (Denial of Service) poate fi lansat deopotrivă de pe o singură mașină de calcul sau dintr-o rețea (și atunci avem de-a face cu Distributed Denial of Service). Scopul acestui atac este generarea și transmiterea unui volum semnificativ de date (sau solicitări) spre un anumit calculator / server ceea ce are ca efect blocarea sau indisponibilizarea acestuia. Pentru ca atacul să reușească este însă necesar ca atacatorul să dispună de o conexiune mai rapidă (lățime de bandă mai mare) decât cea a mașinii de calcul vizate. Deși este simplu de realizat, atacul este destul de dificil de evitat.

DDoS

În condițiile unui refuz al serviciului în mod distribuit (Distributed Denial of Service), mai multe mașini de calcul atacă simultan computerul țintă. Numărul covârșitor de mesaje (date) primite determină blocarea sistemului atacat și respingerea drepturilor de acces ale utilizatorilor legitimi. Un atacator poate iniția un atac DDoS exploatând vulnerabilitățile unui singur computer, pe care îl transformă în unitate principală, iar cu ajutorul acestuia caută și comunică cu alte computere vulnerabile pe care ulterior instalează anumite aplicații dedicate. După crearea grupului de computere controlate la distanță (BotNet) atacatorul poate, printr-o singură comandă, să lanseze un atac distribuit asupra mașinii de calcul țintă.

Diversion DDoS

Situații în care acțiuni de tip Dos sau DDoS sunt utilizate în scop diversionist, pentru a induce în eroare specialiștii IT ai organizației atacate și a le abate acestora atenția

de la metodele reale de intruziune, aflate în desfășurare ori care urmează a fi lansate.

Defacement

O formă de atac informatic al cărui scop este batjocorirea unei anumite pagini web, prin plasarea (postarea) de mesaje, adesea cu conținut defăimător sau obscen. În cele mai multe cazuri însă, atacatorii se mulțumesc să își posteze numele (poreclele) sau mesaje către cunoscuți ori să comunice indirect cu administratorul site-ului atrăgându-i acestuia atenția asupra problemelor de securitate pe care ar trebui să le gestioneze. Nu se puține ori, batjocorirea paginilor web ascunde în fapt acțiuni mult mai periculoase, cum ar fi instalarea de aplicații nocive. Cele mai atacate website-uri sunt, în general, cele guvernamentale sau ale unor organizații de interes public sau privat, însă active în viața socială ori economică.

Dictionary Attack

În domeniul securității IT sau al criptanalizei, atacul prin dicționar este definit drept modalitatea de a descoperi un cod sau de a trece cu succes printr-un proces de autentificare folosind o mare varietate de combinații alfabetice (cuvinte). De cele mai multe ori, acest tip de atac reușește datorită ignoranței sau nepriceperii utilizatorilor care aleg să implementeze parole foarte simple sau cu semnificații personale, de până la 7 caractere ceea ce le face extrem de ușor de găsit.

DNS

Sistemul Nume de Domeniu (Domain Name System) inițiază procesul care permite unui utilizator să se conecteze la un server web (pagină de web) prin tastarea în bara de adrese a numelui unui anumit site. Computerele conectate la Internet comunică între ele exclusiv pe baza adreselor IP, iar dispozitivele care permit translatarea bidirecțională a numelor de domenii în adrese IP sunt denumite servere DNS. Aceste servere conțin baze de date cu detalii (nume de domeniu, adresă IP asociată etc.) ale numeroaselor rețele active în Internet și au capacitatea de a memora noi conexiuni, facilitând, astfel, accesul rapid al utilizatorului la paginile web dorite. Serverele DNS sunt organizate pe o structură ierarhică, cele mai importante dintre acestea (root – rădăcină) fiind denumite generic de la „A” la

„M" și găzduite de importanți furnizori de servicii Internet din SUA, Japonia, Marea Britanie și Suedia.

Deturnarea de domenii

Un atac în care atacatorul preia un domeniu blocând prima dată accesul la serverul DNS al domeniului şi instalându-şi apoi propriul său server.

Dumpster Diving (Căutarea prin fişierele şterse)

Recuperarea fişierelor, scrisorilor, notelor, fotografiilor, codurilor de identificare, parolelor, verificărilor, extraselor de cont, ofertelor de carduri de credit şi a multor altor lucruri din coşurile de gunoi şi din coşurile de reciclare. Aceste informaţii pot fi apoi utilizate pentru a comite furtul de identitate.

DNS Spoofing

Formă de atac informatic prin care informațiile dintr-un server Nume de Domeniu sunt modificate de persoane interesate, astfel încât traficul Internet (http, ftp, smtp, pop3 etc.) al unui computer țintă să fie în realitate redirectat către pagini web false (contrafăcute) sau servere aflate sub controlul lor. Scopul acestui atac este inducerea în eroare a utilizatorilor legitimi și determinarea acestora să divulge date personale ori financiare.

Domain

Domeniul reprezintă numele dat unei colecții de adrese IP organizate în mod ierahic în funcție de anumite criterii. Exemplu: în domeniul rădăcină .ro, domeniul de nivel înalt (engl. Top Level Domain) exemplu.ro desemnează întreaga structură de adrese IP corespunzatoare resurselor asociate (pagini web, servere DNS, servere http, servere mail etc.).

Drive-by Download

Definește două modalități prin care un utilizator descarcă în propriul computer un program de pe un website. în prima ipostază, utilizatorul execută conștient sau autorizat operațiunea de descărcare (download) a unui fișier executabil, însă fără a fi pe deplin informat ori să realizeze consecințele descaracrii (instalării) respectivului program (ex. o componentă de tip ActiveX, un applet Java etc.). în a

doua situație, acțiunea de descărcare are loc fără ca utilizatorul / vizitatorul website-ului să fie informat ori fără ca acesta să aibă posibilitatea de a-și exprima consimțământul cu privire la acest fapt.

Tehnic, un drive-by download are loc odată cu vizitarea unui website, prin deschiderea (attachment-ului) unui email ori prin accesarea (click) a unei ferestre pop-up înșelătoare. De cele mai multe ori, atacatorii se apără invocând existența consimțământului utilizatorului / vizitatorului (prin simpla deschidere a email-ului ori prin click efectuat în fereastra pop-up), însă, în realitate, acesta nu este în măsură să conștientizeze operațiunea de descărcare ori nu cunoaște efectele descărcării (și, eventual, instalării) programului în propriul computer.

E-commerce

Comerțul electronic reprezintă totalitatea afacerilor, schimburilor comerciale și tranzacțiilor financiare derulate prin Internet. De asemenea, comerțul electronic poate să implice și activități de publicitate, acceptarea de carduri de credit sau tranzacționarea online de acțiuni.

Evil Twins (Gemenii malefici)

Un punct de atracţie fals pe internetul wireless care este asemănător unui serviciu legitim. În momentul în care victimele se conectează la reţeaua wireless, un hacker poate lansa un atac spion asupra tranzacţiilor acestora de pe internet, sau poate doar să solicite informaţiile de pe cardul de credit în înţelegerea standard plată pentru acces.

Ethernet

Standard (protocol) utilizat pentru conectarea calculatoarelor într-o rețea.

Exploit

Vulnerabilități ale sistemelor informatice, în special ale programelor și aplicațiilor, care sunt cu succes exploatate de atacatorii informatici. Aceștia reușesc să obțină controlul asupra resurselor mașinii de calcul țintă, adesea fără știrea utilizatorului legitim. Atunci când sunt descoperite și raportate, exploit-urile sunt remediate de producătorii de software prin așa-numitele patch-uri de securitate.

False Alarm

Este situația în care o aplicație anti-virus semnalizează în mod eronat un program sau o aplicație care rulează corespunzător drept o amenințare pentru sistem. Aceasta cauzează adesea utilizatorilor finali probleme, întrucât, bazându-se pe fiabilitatea pachetelor anti-virus, aceștia tratează alarmele false ca amenințări reale la adresa securității mașinilor de calcul și aleg să elimine aplicațiile sau programele corespunzătoare asumându-și implicit și costurile (implicațiile) acestor acțiuni.

Fake Offering

Formă a "furtului de identitate" realizată prin aplicarea metodelor specifice "ingineriei sociale", prin care utilizatorii unei platforme online de socializare sunt "îndemnați" să se alăture virtual unor evenimente sau grupuri în schimbul primirii de cadouri. În majoritatea situațiilor, afilierea online la un astfel de grup se face doar în schimbul furnizării de date personale ori chiar credențiale de acces în cont.

Fake Plug-in Scams

Metodă de inginerie socială ce constă în inducerea în eroare utilizatorilor rețelelor de socializare online cu scopul de a îi determină să descarce false extensii de browser în propriile sisteme informatice. Respectivele false extensii se prezintă adesea ca fiind legitime, dar odată instalate sunt capabile să exfiltreze informații sensibile/personale etc. din memoria (spațiul de stocare al) sistemului infectat.

Fast Flux

Metodă de ascundere (mascare) a unui atac informatic ce se bazează pe schimbarea rapidă (de mai multe ori într-un interval scurt de timp) a locației unei pagini web, a unui email, a unei înregistrări DNS sau, în general, a oricărui serviciu distribuit (din Internet) dintr-un sistem informatic în altul, cu scopul de a întârzia semnificativ sau de a evita detectarea (localizarea). Exemplu: se folosește în cazul paginilor web cu conținut pornografic infantil sau defăimător, al mesajelor email între participanții la o infracțiune sau în cazul atacurilor de tip Phishing sau Pharming.

Firewall

Dispozitiv hardware sau aplicație software care protejează un sistem informatic împotriva acțiunilor dăunătoare din exterior (încercări de exploatare, scanare de porturi, introducerea de viruși, viermi sau Cai Troieni, conectarea ascunsă la diferite resurse etc.).

FTP

Protocolul de Transfer Fișiere (File Transfer Protocol) reprezintă acel set de standarde și reguli utilizate în Internet pentru trimiterea și primirea de fișiere. Atunci când se utilizează FTP, în fapt sunt folosite aplicații client FTP, iar transferul se execută prin intermediul unui server dedicat (de FTP).

Furnizor de servicii internet (ISP)

O companie care oferă clienţilor acces la internet.

Hacker

Un individ care încearcă să intre într-un computer fără autorizare.

Hacker Tools

Reprezintă acele utilitare, aplicații sau programe informatice (uneori chiar și dispozitive hardware) cu ajutorul cărora atacatorii informatici reușesc să acceseze neautorizat și să controleze resursele unei mașini de calcul sau ale unei rețele. Multe dintre acestea se găsesc fără costuri pe Internet, dar cele mai sofisticate sunt disponibile numai prin intermediul legăturilor directe sau la distanță (prin intermediul subteranei informatice) cu creatorii de software sau hackerii cu experiență.

Hijacking

Formă de atac informatic prin care o persoană interesată poate obține controlul unui sistem informatic. Cea mai populară formă de deturnare este „man-in-the-middle”, atunci când atacatorul reușește să controleze o conexiune chiar în timpul unui proces de comunicație (transport de date). Această formă de atac este destul de sofisticată întrucât necesită o interceptare a schimbului de chei publice între două sisteme și introducerea cheilor atacatorului. Atacul deschide posibilitatea

accesului neautorizat la mesaje și chiar efectuarea de modificări în conținutul acestora.

Hoax

Tip de mesaje nesolicitate, adesea cu conținut publicitar, pornografic sau de natură să distragă atenția în mod supărător. În marea lor majoritate nu afectează securitatea sistemului, însă au un efect psihologic negativ semnificativ asupra utilizatorilor.

HTML

Limbaj de Marcare în Hipertext (engl. Hypertext Markup Language) este utilizat pentru scrierea de documente în vederea postării pe Internet (World Wide Web). Deși dificil de utilizat, HTML oferă o protecție sporită a paginilor web comparativ cu alte programe sau editoare.

HTTP, Hypertext Transfer Protocol

Reprezintă un set de reguli (protocoale) folosit de browserele și de serverele web pentru transferul datelor (încărcarea și afișarea paginilor web etc.) in Internet Intranet

HTTPS

Absolut identic cu protocolul http, folosește un alt port TCP. Securitatea conexiunii invocând un nivel superior de securitate prin criptare autentificare. Criptarea este furnizată de Palierul Securitatea Transportului (TSL – Transport Layer Security) sau de SSL (Secured Socket Layer). Aceasta reprezintă o protecție împotriva interceptării traficului de către o terță parte, chiar și prin atacul „man-in-the-middle”.

HUB

Punct de conectare pentru dispozitivele dintr-o rețea (inclusiv în cazul Internetului).

ID Theft

Furtul datelor de identitate – contextul în care atacatorii informatici obțin informațiile personale sau financiare ale unei persoane și pe care le folosesc pentru a se prezenta cu identitatea victimei și / sau pentru a accesa finanțele acesteia.

Infecţii electronice

Adesea denumite „viruşi”, aceste programe şi coduri rău intenționate vă afectează negativ computerul şi vă compromit confidențialitatea. Pe lângă viruşii tradiţionali, alte tipuri obişnuite includ viermi şi cai troieni. Aceştia lucrează uneori în tandem pentru a realiza prejudiciul maxim.

Inference Attack

Atacul prin deducție este în fapt o metodă de căutare avansată de date informatice (data mining). Scopul este obținerea a cât mai multe date de pe un anumit nivel de securitate și determinarea unui rezultat cu un nivel de securitate superior prin analiza (deducția) acestor date.

Ingineria socială

Un eufemism pentru mijloacele netehnice sau cu tehnologie redusă—cum ar fi minciunile, personificarea, şiretlicurile, mita, şantajul şi amenințările—utilizate pentru a ataca sistemele de informaţii. Uneori, furnizorii de bunuri sau servicii prin telefon sau angajaţii lipsiţi de etică utilizează astfel de tactici.

Internet

Colecție uriașă de calculatoare aflate în toată lumea și conectate între ele în diferite moduri. Calculatoarele și rețelele comunică între ele prin protocolul TCP/IP, putând fi accesate pagini web, transmise și recepționate mesaje de poștă electronică, derulate conversații prin intermediul mesageriei instant, transferate fișiere prin ftp etc.

IMAP, Internet Message Access Protocol

Protocol folosit pentru stocarea și transferarea mesajelor de poștă electronică direct din serverul dedicat.

Internet Relay Chat (irc)

Sistem destinat discuțiilor care folosește un anumit set de reguli și convenții, precum și o aplicație software client/server.

Internet Service Provider (ISP)

Companie (organizație, firmă, persoană) care furnizează sistemul de calcul, aplicațiile necesare, precum și alte modalități de suport pentru conectarea la Internet.

Intranet

Rețea de calculatoare din interiorul unei organizații.

IP Address

Adresă a Protocolului Internet – este numărul unic asociat fiecărui site web. Adresele IP sunt o serie de patru numere, separate între ele prin puncte. Acest număr este ulterior convertit într-un nume de domeniu, corespunzător paginii web asociate.

IP Spoofing

Metodă avansată de atac informatic utilizată frecvent pentru deturnarea browserelor web în vederea obținerii accesului neautorizat într-o rețea. Atacatorul obține adresa IP reală a unui anumit sistem informatic și modifică antetele pachetelor de date, disimulând astfel adevărata origine (sursă) a pachetelor (datelor). Mașina de destinație va răspunde trimițând propriile pachete către adresa IP falsificată, comunicația fiind controlată de atacator. Această tehnică se folosește mai ales în cazul atacurilor Denial of Service, atunci când atacatorul este mult mai interesat să redirecționeze traficul pachetelor inundând o anumită stație de lucru, fără să acorde importanță răspunsurilor primite.

JavaScript

Limbaj de scriptare (programare) dezvoltat de companiile Sun și Netscape. Deși deține multe dintre caracteristicile limbajului Java, JavaScript a fost dezvoltat independent cu scopul de a crea website-uri cu conținut interactiv.

Keylogger

Aplicație special creată pentru a capta și interpreta codurile generate de apăsarea butoanelor de la tastatură. în acest fel, atacatorii sunt capabili să obțină o varietate de date pe care utilizatorul legitim le introduce de la tastatură, cum ar fi: documente, comenzi, parole, numere de cont etc. Unele programe tip keylogger sunt mult mai performante putând efectua capturi de imagini de pe monitor, memora paginile web vizitate, precum și ferestrele de mesagerie instantă, pe care, ulterior, le transmite atacatorului prin Internet, folosind fără știrea utilizatorului legitim protocoalele SMTP sau POP3.

LAN

Acronim pentru rețea informatică locală (Local Area Network).

Likejacking (LIKE-jacking)

Variantă a ingineriei sociale în rețelele de socializare, prin care atacatorul ademenește utilizatorul să apese false butoane LIKE, ce instalează, în realitate, conținut dăunător (malware) computerul acestuia. De aceea, contaminanții informatici au capacitatea de a se răspândi prin forțarea postării de "noutăți" profilele (timeline-urile) utilizatorilor aflați în lista de contacte a victimei.

Log

Un tip aparte de fișier care stochează date relevante privind acțiunile / procesele care au loc la nivelul unui sistem informatic sau al unei pagini web. În cazul paginilor web, spre exemplu, fișierul memorează numărul de vizite pe pagină, locul de unde a avut loc vizita și alte date statistice. Conținutul unui astfel de fișier poate fi vizualizat prin intermediul unui simplu editor de text. Din punct de vedere al securității sistemului, fișierul de log este extrem de util în identificarea și remedierea erorilor.

Logon / Login

Procedura prin care un utilizator accesează autorizat un sistem informatic sau o aplicație (inclusiv un sistem de operare). În mod obișnuit, în fereastra de autentificare (logon) numele de utilizator va fi afișat, în timp ce parola sau codul de

identificare vor fi afișate sub formă mascată (steluțe) pentru a nu fi observate de persoane interesate.

MAC Address

Este un unic identificator atribuit din fabricație fiecărui adaptor de rețea (Media Access Control). Translatarea adreselor MAC (de nivel 2) în adrese IP (de nivel 3) este efectuată prin Protocolul de Rezolvare a Adreselor (ARP – Address Resolution Protocol).

Malicious Code

Este, în general, descris ca un fișier sau tip de program care interferează cu funcționarea normală a sistemului de operare. Poate fi folosit pentru preluarea controlului resurselor unui sistem informatic, pentru furtul de date confidențiale ori pentru instalarea de aplicații dăunătoare (malware). În literatura de specialitate, codul malițios este menționat ca virus, vierme sau Cal Troian.

Malware

Cod răuvoitor – orice program de calculator sau cod care a fost creat (dezvoltat) cu scopul de a „invada” sisteme de calcul și de a cauza probleme.

Malvertising

Modalitate de atac ce constă în inserarea pe website-ul țintă a unei reclame sau anunț publicitar/de interes, contra-cost, care conține în realitate un contaminant informatic. Acest atac se derulează "silențios", fără ca website-ul afectat să fie în vreun fel accesat neautorizat ori compromis prin alte metode. La accesarea "reclamei", sistemul informatic al vizitatorului se infectează automat cu aplicații dăunătoare (malware) create dinamic și pe care soluțiile antivirus nu le detectează. Cele mai afectate website-uri sunt cele aparținând agențiilor de publicitate, comerț electronic sau media.

Man-in-the-Browser (MitB) Attack

O formă de atac cibernetic orientat pe banking online, ce vizează infectarea browserului unui computer personal cu un troian de tip proxy. Prin intermediul acestuia, atacatorii au posibilitatea să modifice conținutul paginilor web, conținutul

tranzacțiilor financiare ori să insereze tranzacții noi, fără știrea utilizatorului de drept și fără ca aplicația web accesată să sesizeze acest lucru. Un atac de tipul MitB poate avea loc indiferent dacă browserul "victimei" utilizează ca măsuri de securitate protocoalele SSL, TSL sau autentificarea în doi factori.

Manual Sharing Scam

Metodă de răspândire a încărcăturii virale prin intermediul rețelelor sociale, care se bazează pe acțiunea voluntară a "victimelor" de a distribui (prin butonul Share) în lista de contacte fotografii, videoclipuri, oferte sau alte tipuri de mesaje electronice anterior infectate cu contaminanți informatici.

Mobile Code

Cod mobil – categorie de cod scris și încadrat într-un document HTML. Când browserul încarcă pagina web, codul mobil este descărcat și executat de către acesta. Numele său provine din faptul că poate fi trecut cu ușurință de pe un sistem informatic pe altul. Java, JavaScript sau ActiveX sunt toate exemple de limbaje de programare în care poate fi scris codul mobil.

Modem

Termen provenit din unirea cuvintelor Modulare – Demodulare și se referă la un dispozitiv care pune la dispoziție o interfață între calculator și liniile de comunicație, care pot fi cabluri sau linii telefonice.

Netiquette

Abreviere din limba engleză a sintagmei "Network Etiquette" care se referă la un set de convenții/reguli de ordin social care guvernează modul de interacțiune virtuală între utilizatori.

Online Identity

Nume sau pseudonim folosit de o persoană cu ocazia interacțiunii sau activității sale virtuale pe website-uri, forum-uri, platforme sociale online, portaluri ori în cazul comunicărilor efectuate prin mijloace electronice (email, chat etc.). Această identitate virtuală poate fi asumată (reală) sau una inventată (alias) ori falsă.

Parolă

O succesiune secretă de caractere care este utilizată ca un mijloc de autentificare pentru a vă confirma identitatea într-un program de computer sau online.

Patch

Un patch este o mică actualizare de securitate lansată de un producător software pentru a repara greşelile programelor existente. Programele şi/sau sistemele de operare ale computerului dumneavoastră pot fi configurate pentru a verifica automat patch-urile, sau este posibil să trebuiască să vizitaţi periodic site-urile web ale producătorilor pentru a verifica dacă există actualizări.

Packet Filtering

În cadrul aplicațiilor de tip Firewall, operațiunea de filtrare este realizată de utilitare dedicate numite filtre de pachete. Acestea evaluează antetele pachetelor de date care solicită intrarea în sistem și le verifică prin prisma anumitor criterii, înainte de a decide dacă le acceptă sau le resping.

Packet Sniffing

Este un tip de atac informatic derulat cu ajutorul unui dispozitiv electronic sau o aplicație care captează și analizează (monitorizează) toate pachetele de date care tranzitează un anumit punct dintr-o rețea, oferindu-i atacatorului posibilitatea de a obține date confidențiale, personale sau financiare.

Pharming

Una dintre cele mai periculoase metode de atac din sfera falsului informatic. Se realizează prin accesarea și modificarea anumitor fișiere ale sistemului de operare sau a bazelor de date cu adrese IP din cadrul serverelor Nume de Domeniu (DNS), cu scopul de a obține neautorizat date personale, nume de utilizator, parole etc. ale utilizatorilor legitimi.

Phishing

Binecunoscuta metodă de atac informatic care se realizează în trei etape, astfel: (1) Atacatorul creează un site web perfect asemănător cu cel al unei anumite instituții financiare și îl găzduieste pe un server, apoi (2) creează un mesaj de poștă

electronică pretinzând a fi din partea respectivei instituții financiare, prin care anunță existența unei situații deosebite din punct de vedere al securității sistemului și îl ademenește, astfel, pe utilizatorul legitim să acceseze o legătură (link) către web site-ul controlat; (3) odată intrat pe site-ul clonat, utilizatorul (indus în eroare) introduce propriile date personale, financiare, de autentificare etc., care sunt în realitate stocate și mai apoi extrase și folosite neautorizat de către atacator.

Piggybacking

Definește accesarea, cu intenție, a unei conexiuni Internet wireless prin plasarea unui dispozitiv echipat Wi-Fi în raza de acoperire a unui punct de acces (Access Point) și utilizarea serviciilor Internet fără cunoștința ori permisiunea expresă a posesorului (deținătorului legal, abonatul etc.) respectivei conexiuni.

Ping of Death

Atac informatic de tip Dos (Denial of Service-refuzul serviciului) în care un calculator (stație de lucru, sistem informatic etc.) trimite un număr foarte mare de solicitări PING (tehnic cunocute sub denumirea de ICMP Echo Requests), cu conținut exagerat de mare sau chiar ilegal, unui alt calculator (de lucru, server etc.) în încercarea de a-i bloca funcționarea sau de a-l obliga să răspundă solicitărilor (ICMP Echo Replies), astfel încât să nu mai poată furniza corespunzător servicii către clienții (utilizatorii) săi.

PKI, Public Key Infrastructure

În domeniul criptografiei, infrastructura de chei publice este folosită pentru a proba (autentifica) identitatea electronică a unui utilizator sau a unei organizații. Sistemul PKI se bazează pe existența a două certificate digitale (denumite chei), una publică – ce poate fi cunoscută de orice persoană și este folosită pentru criptarea mesajelor adresate unui anumit utilizator, iar alta privată – cunoscută doar de utilizator, cu ajutorul căreia acesta decriptează mesajele ce îi sunt adresate și cu ajutorul căreia poate semna mesajele transmise.

Politica biroului curat

O politică care îndrumă întreg personalul să-şi cureţe birourile la încheierea fiecărei zile lucrătoare şi să arhiveze totul în mod corespunzător. Birourile trebuie curăţate

de toate documentele şi hârtiile, inclusiv conţinutul de pe rafturi —nu doar în scopul ordinii, ci şi pentru a se asigura de faptul că hârtiile şi documentele sensibile nu sunt expuse persoanelor neautorizate în afara orelor de lucru.

Politica ecranului curat

O politică care îndrumă toţi utilizatorii de computere să se asigure că conţinutul ecranului este protejat împotriva privirilor indiscrete şi încălcărilor oportuniste ale confidenţialităţii. De obicei, cel mai uşor mijloc de conformitate este de a utiliza economizorul pentru ecran care se activează fie la cerere sau după o perioadă de timp scurtă specificată. Vezi şi Shoulder Surfing.

POP3, Post Office Protocol

Protocolul Oficiului Poștal – versiunea 3 este principalul protocol utilizat pentru stocarea și primirea mesajelor de la serverele de mail aflate la distanță. Interfața cu utilizatorii o reprezintă programele sau aplicațiile client de mail.

Port Scan

Scanarea porturilor este o metodă populară de exploatare a vulnerabilităților, prin care atacatorul trimite (direcționează) mesaje (pachete de date) fiecărui port al sistemului informatic vizat în vederea identificării celor inactive sau vulnerabile.

PDF, Portable Document Format

Format universal care păstrează în orice document caracterele și culorile folosite inițial, indiferent de platforma sau aplicația cu care au fost editate sau dezvoltate. Adobe Acrobat Reader și Adobe Acrobat sunt cele mai cunoscute aplicații care utilizează formatul PDF.

Promiscuous Mode

Într-o rețea locală (LAN), sintagma definește modul de operare în care fiecare pachet de date poate fi interceptat și „citit” de către adaptorul de rețea. Este necesar, însă, ca acest mod să fie acceptat de adaptorul de rețea, iar driverul specific (de intrare/ieșire) să fie încărcat pe computerul gazdă.

Protocol

Set de reguli sau standard care specifică modul de comunicare al calculatoarelor în cadrul unei rețele, de exemplu în Internet (http, ftp, pop3, imap, smtp etc.).

Proxy Server

Tip de server care, din anumite rațiuni (ex. de securitate), se interpune între un utilizator și restul rețelei (ex. internet), procesând în numele utilizatorului toate solicitările de resurse din afara sistemului (sau rețelei de bază) și cu un timp de răspuns mult diminuat. Un tip aparte de server proxy este cel de anonimizare folosit de persoanele care doresc să nu lase „urme”, navigând pe Internet sau transmițând mesaje de email.

Reţea

Două sau mai multe sisteme de computere care sunt grupate împreună pentru a distribui informaţii, software şi hardware.

Reverse Engineering

Ingineria inversă este intens aplicată în prezent pentru aflarea codului sursă al unui anumit program sau unei aplicații de interes, cu scopul de a afla cum funcționează programul, de a perfecta funcționarea programului, de a repara erorile, de a identifica inserțiile de cod malițios sau de a adapta programul astfel încât să poată fi utilizat și de alte aplicații sau platforme.

Rootkit

Program sau combinație de programe cu ajutorul cărora un atacator poate prelua de la distanță controlul sistemului de operare al unei mașini de calcul. Aplicațiile oferă posibilitatea ascunderii sau disimulării fișierelor sau sarcinilor în execuție (tasks), dar și de a bloca memoria sau intrările în registrele sistemului de operare pentru alte aplicații sau programe de administrare.

Round Robin DNS

Tehnică în care echilibrarea "încărcăturii" virtuale într-o rețea este realizată de un server DNS în locul unei mașini de calcul dedicate (așa cum este normal). Această metodă este folosită în rețele mari și funcționează răspunzând solicitărilor DNS cu o

listă de adresă IP în locul unei singure astfel de adrese (ceea ce înseamnă că toate aceste adrese pot hosta conținutul respectiv). Ordinea în care adresele IP din listă sunt returnate se bazează pe principiul virtual "round robin", adică vor fi afișate (puse la dispoziție) ciclic. Asignarea (atribuirea) de adrese este, însă, secvențială, începând cu prima adresă furnizată în urma primei solicitări, a doua adresă IP după a doua solicitare ș.a.m.d. Odată lista de IP-uri epuizată, din nou prima adresă de IP va fi alocată următoarei solicitări din lanț și ciiclul se repetă. Această metodă este folosită în atacuri informatice, alături de tehnica de Fast Flux.

Router

Dispozitiv care dirijează traficul pachetelor de date în Internet, evaluând căile posibile de ajungere la destinație și identificând cea mai eficientă rută în funcție de nivelul de trafic.

Server

Dispozitiv (sau aplicație software) care pune la dispoziția unui client servicii, distribuind, de exemplu, mesaje de email sau afișând pagini web.

Session Hijacking

Este procesul prin care un atacator deturnează sesiunea web a unui utilizator legitim, obținând în mod neautorizat identificatorul de acces al utilizatorului iar mai apoi drepturile acestuia în cadrul rețelei. În general, identificatorul unei sesiuni web este stocat într-un director de URL (Uniform Resource Locator) sau într-un fișier de tip Cookie. în funcție de nivelul de securitate implementat și de natura atacului, acest tip de intruziune poate sau nu poate fi detectată.

Sexting

Comportament online care o transmite alteia conținut electronic sexual explicit ori sugestiv (text, foto, video, audio etc.).

Sistem de operare (SO)

Programe care gestionează toate funcţiile şi programele de bază de pe un computer, cum ar fi alocarea resurselor în sistem, oferirea accesului şi controalele de securitate, menţinerea sistemelor de fişiere şi gestionarea comunicaţiilor între

utilizatorii finali şi dispozitivele hardware. Exemplele includ Microsoft Windows, Apple Macintosh şi Red Hat Linux.

Smart Card

Tip de card care are posibilitatea de a stoca în chip-ul încorporat o mai mare cantitate de date în format electronic decât un card obișnuit cu bandă magnetică. Cardul Inteligent poate fi programat pentru a deservi mai multe aplicații și are o paletă largă de utilizări (ex. pentru decontări, pentru apeluri telefonice, pentru autentificări în sisteme informatice sau de acces etc.).

SMiShing (SMS Phishing)

Este un nouă formă de atac informatic de tip inginerie socială în care victimei i se prezintă pe telefonul mobil, sub formă de SMS, anumite oferte sau oportunități de a câștiga bani, fiind ulterior "ademenită" să apeleze anumite numere de telefon către (să contacteze) sisteme cu răspuns automat cu scopul de a furniza date și informații personale, financiare sau confidențiale. Cel mai adesea, aceste sisteme automate solicită coduri PIN sau coduri de verificare CVC ale cardurilor bancare.

SMTP, Simple Mail Transfer Protocol

Protocolul pentru Transmiterea Simplă a Mesajelor – protocol responsabil numai cu trimiterea de mesaje de poștă electronică.

Smurfing (Smurf Attack)

Formă de atac informatic, similar unui refuz al serviciului (Denial of Service), prin care atacatorul reușește să falsifice o adresă de IP (a computerului țintă) și să creeze pachete de rețea conținând mesaje ping de tip ICMP (Internet Control Message Protocol) pe care le trimite către toate adresele de IP dintr-o anumită rețea (broadcast). Aceste mesaje ping vor genera răspunsuri (echo) ce vor fi direcționate spre presupusul transmițător, prin aceasta reușindu-se o paralizare a traficului de date în rețea, în special către/de la adresa de IP falsificată.

Sniffer

Dispozitiv electronic sau program informatic ce permite captarea pachetelor de date într-o rețea de calculatoare. În general, este utilizat în scopul unei mai bune

administrări a rețelei, însă din ce în ce mai mult de către atacatorii informatici pentru interceptarea neautorizată de date.

Social Engineering

Ingineria socială poate fi definită ca o colecție de metode sau strategii de comunicare prin care o persoană este indusă în eroare și manipulată în vederea furnizării de informații cu caracter personal, financiare sau confidențiale ori pentru a acționa în sensul dorit de atacator. În acest caz, persoanele interesate exploatează exclusiv vulnerabilitățile persoanei vizate (utilizatorul legitim al sistemului informatic) și nicidecum ale sistemului în sine.

Social Network

Platformă online creată cu scopul de a (inter)conecta utilizatori ori de a dezvolta comunități de persoane în jurul unor idei, pasiuni sau preocupări de orice fel.

Software de monitorizare

Produse software care permit părinţilor să monitorizeze sau să urmărească site-urile web sau mesajele de email pe care le vizitează sau le citeşte un copil. Vezi şi Blacklisting Software şi Whitelisting Software.

Shoulder Surfing (Uitatul peste umăr)

Privitul peste umărul unei persoane pentru a obţine informaţii confidenţiale. Este o modalitate eficientă de a obţine informaţii în locuri aglomerate întrucât este relativ uşor să stai lângă cineva şi să priveşti în timp ce aceştia completează un formular, introduc un cod PIN la un ATM sau în timp ce tastează o parolă. Acest lucru poate fi efectuat de la distanţă mare cu ajutorul unui binoclu sau alte dispozitive de mărire a vizualizării. Pentru a combate acest lucru, experţii recomandă să protejaţi documentele sau tastatura împotriva vizualizării prin utilizarea corpului dumneavoastră sau cu mâna. De asemenea, asiguraţi-vă că vă protejaţi ecranul computerului cu parolă atunci când trebuie să-l lăsaţi nesupravegheat şi că vă faceţi curat pe birou la final de zi. Vezi şi Politica biroului curat şi Politica ecranului curat.

Skimming

O metodă de înaltă tehnologie prin care hoţii capturează informaţiile dumneavoastră personale şi despre conturi de pe cardul dumneavoastră de credit, permisul de conducere sau chiar paşaport utilizând un dispozitiv electronic denumit „skimmer”. Astfel de dispozitive pot fi achiziţionate online la un preţ sub 50$. Cardul dumneavoastră este trecut prin skimmer şi informaţiile conţinute în banda magnetică de pe card sunt citite apoi şi stocate pe dispozitiv sau pe un computer ataşat. Skimming-ul este predominant o tactică utilizată pentru a perpetua fraudarea cardurilor de credit, însă aceasta devine mai populară printre hoţii de identitate.

Spam

Mesajele comerciale nesolicitate sunt, de regulă, mesaje de poștă electronică trimise unui număr mare de utilizatori, fără consimțământul ori aprobarea prealabilă a acestora, cu conținut informativ, publicitar, distractiv, de alertă etc. Nu au un efect direct asupra securității unui sistem informatic, însă irită utilizatorul legitim și, uneori, transmise în număr prea mare, pot afecta traficul Internet în porturile de mail sau chiar bloca căsuțele poștale electronice.

Spear Phishing

Variantă de Phishing având ca țintă o anumită organizație sau instituție (în principal prin utilizarea angajaților/partenerilor/clienților acestora). într-un exemplu folosit pe scară largă, în loc să colecteze un număr foarte mare de adrese email și apoi să expedieze mesajele înșelătoare folosind aplicații de tip Email Mass Sender, făptuitorii concentrează efortul infracțional doar asupra adreselor de email gen prenume.nume@companie.com (care pot fi deduse/generate cu ajutorul unor aplicații simple care generează aleatoriu perechi Nume-Prenume posibile).

Spoof Site

Website-ul clonă este o pagină web special creată după aspectul uneia reale (legitime) cu scopul de a induce în eroare utilizatorii.

Spyware

Programe introduse deliberat pe computerele țintă pentru a capta și transmite diferite date către o persoană din exteriorul sistemului. Acestea pot intercepta o gamă largă de activități, care includ, de exemplu, înregistrarea tastelor apăsate, citirea mesajelor email, înregistrarea siteurilor web vizitate sau detaliile cărților de credit.

SSL (Secure Socket Layer)

Protocol criptografic ce oferă servicii de securitate și integritate a datelor comunicate prin intermediul rețelelor TCP/IP (Internet). Un sistem de criptare care protejează confidențialitatea datelor schimbate între un site web şi utilizatorul individual. Utilizat de site-urile web ale căror URL-uri încep cu https în loc de http.

TCP/IP, Transmission Control Protocol / Internet Protocol

Reprezintă setul de standarde și protocoale de transmitere a datelor în rețeaua Internet și de corectare a erorilor. Protocolul TCP verifică transportul datelor de la client la server, în timp ce protocolul IP este responsabil pentru mutarea pachetelor de date între calculatoare.

TCP SYN Flood

Atac informatic de tip Dos care are avantajul stabilirii unei conexiuni, pe 3 căi, între două sisteme informatice folosind rotocolul TCP/IP care, în principiu, se bazează pe trimiterea unei solicitări de conectare cu o adresă de răspuns validă.

Trojan

Calul Troian este o aplicație de backdoor, disimulat într-un program legitim care, odată lansat execuție, instalează pe computerul țintă, o încărcătură dăunătoare (ex. viruși, keylogger etc.). Este un program de calculator care pare a fi benefic sau inofensiv, însă are şi o funcţie ascunsă şi posibil maliţioasă care se sustrage mecanismelor de securitate. Un „Înregistrator de taste," care înregistrează tastările victimelor şi le trimite unui atacator, sau „computerele zombie" controlate de la distanţă, sunt exemple de prejudicii care pot fi aduse de caii troieni. Vezi şi Infecţie electronică.

Troll

Poreclă atribuită unei persoane care, prezentă pe website-uri, forumuri sau liste de discuții online, atrage utilizatorii în dezbateri virtuale fără obiect, sterile, controversate, licențioase ori violente cu scopul de a obține atenția acestora (pe care în alte condiții nu ar fi obținut-o) sau de a decredibiliza pe unii dintre utilizatorii implicați/participanți.

Two-Factor Authentication TFA (trad. autentificare în doi factori)

Proces de autentificare în care, pentru stabilirea veridicității identității utilizatorului unui sistem informatic, sunt folosiți cel puțin doi dintre cei trei factori (definiți prin Directiva nr. 12 de Securitate Națională emisă de Președintele SUA): un element din ceea ce știe utilizatorul (ex. parolă, PIN), un element din ceea ce posedă utilizatorul (ex. smartcard, token) și un element din ceea ce este utilizatorul (ex. amprenta, iris). Exemplu: autentificarea la un bancomat prin folosirea unui card cu chip și a PIN-ului aferent.

TypoSquatting

Metodă de atac informatic (de tip inginerie socială) derivată din practica de a înregistra nume de domeniu similare celor ale unor website-uri cunocute (sau vizate de atacatori) cu scopul de a induce în eroare utilizatorii care, accidental, tastează greșit URL-ul respectivelor website-uri și, astfel, sunt în postura de a "remedia" situația alegând, în realitate, link-uri către pagini web aflate sub controlul atacatorilor. Metoda a fost folosită în trecut pentru derularea de operațiuni de tip Phishing.

URL, Uniform Resource Locator

Localizatorul uniform de resurse este acel identificator standard al locului în care se găsește resursa. Totodată, este un mod de specificare a locului în care se află resursa Internet.

URL Obfuscation (Confuzia URL)

Profitând de avantajul erorii umane, unii escroci utilizează emailuri cu înşelătorii pentru a ghida destinatarii spre site-uri frauduloase cu nume foarte similare cu site-urile stabilite. Aceştia utilizează o uşoară greşeală de ortografie sau altă diferenţă

subtilă în URL, cum ar fi „monneybank.com” în loc de „moneybank.com” pentru a redirecţiona utilizatorii să-şi partajeze informaţiile personale fără să ştie.

USB, Universal Serial Bus

Port al computerului în care pot fi atașate dispozitive periferice diverse (memorii flash, camere video, telefoane celulare etc.).

Virus

Program dăunător care invadează calculatorul fără știrea sau permisiunea utilizatorului acestuia, infectează fișiere, se multiplică și se răspândește în alte sisteme. O secţiune ascunsă, care se autoreproduce, a software-ului de pe calculator, de obicei logică maliţioasă, care se propagă prin infectare—şi anume, inserţia unei copii a acesteia în şi devenirea sa parte din – alt program. Un virus nu poate rula singur; acesta necesită ca programul său gazdă să fie executat pentru a activa virusul. Trimis adesea prin ataşamentele la email.

Vulnerabilitate

Un defect care permite cuiva să opereze un sistem de computere cu nivele de autorizare în exces, pe care deţinătorul sistemului le-a oferit în mod special.

Vishing (Voicemail Phishing)

Atac informatic de tip inginerie socială, similar SMiShing-ului, diferența fiind aceea că victima este abordată sau ademenită să furnizeze informații prin intermediul serviciului de mesagerie vocală.

VPN, Virtual Private Network

Rețea Privată Virtuală – o tipologie aparte de rețea în care legăturile între noduri sunt „virtuale”. Cea mai importantă aplicație asociată acestei rețele este securizarea comunicațiilor prin mediul „nesigur” al Internetului, ceea ce o face preferată pentru conectarea membrilor unei companii, prin intermediul Internetului, în mod sigur, la resursele respectivei organizații.

Wardriving

Definește deplasarea pe jos sau cu un vehicul în scopul descoperirii și marcării (pe o hartă) a rețelelor (punctelor de acces) fără fir (wireless, WiFi) care oferă conectivitate la Internet.

Watering Hole Attack

Noua formă de atac cibernetic direcționat (targetat) care se realizează gradual, astfel: 1. atacatorul studiază și realizează profilul online al victimei, înregistrând website-urile cel mai des vizitate de către aceasta; 2. atacatorul identifică vulnerabilitățile acestor website-uri; 3. în momentul în care website-ul vulnerabil, atacatorul injectează cod HTML sau JavaScript, reușind, astfel, să redirecționeze victima către un alt site, ce conține codul "exploit" pentru vulnerabilitatea identificată/aleasă (de obicei, o vulnerabilitate de tip "zero-day"); 4. în acest moment, website-ul compromis este pregătit să infecteze sistemul victimei.

Web Browser

Aplicație de tip client care permite utilizatorilor afișarea de documente hipertextuale (HTML) și navigarea între acestea în cadrul sistemului World Wide Web (www). Exemple de browsere: Internet Explorer, Mozilla Firefox, Opera, Safari, Chrome (Google) etc.

Web-based Attack

Formă de atac cibernetic care constă în compromiterea unor website-uri și plasarea de coduri "exploit" cu scopul de a infecta sistemele informatice ale vizitatorilor. Încărcătura virală, lansată prin instrumente de atac dedicate (Toolkit), este cel mai adesea de tip "server-side", polimorfic sau generat dinamic și este eficientă în special atunci când victima utilizează produse de securitate care se bazează doar pe analiza "semnăturilor" de viruși. Aceste atacuri reușesc în marea majoritate a cazurilor, întrucât sistemele (servere sau host-uri) nu sunt actualizate cu ultimele "patch-uri" ale modulelor plug-in din browsere (ex. Adobe Flash Player, Acrobat Reader ori Java).

Website-hacking

Ansamblu de activități, de diferite complexități, prin care atacatorii urmăresc inserarea propriului cod în codul-sursă al website-urilor țintă. Tehnic, aceste activități presupun:

- utilizarea de instrumente software special concepute (Toolkit)
- exploatarea unei vulnerabilități (cunoscute și nerezolvate ori necunoscute-de tip 0-day)
- utilizarea atacurilor Phishing sau Pharming, aplicațiilor de tip Spyware sau a ingineriei sociale, prin obținerea, în mod neautorizat, a parolei webmaster-ului
- accesarea neautorizată a infrastructurii "backend" de susținere a website-ului (baza de date, panou de control etc.)
- inserarea, cu plată, pe website-uri legitime de anunțuri publicitare sau reclame online ce conțin în realitate contaminanți informatici.

Whitelisting Software

O formă de filtrare care permite doar conexiunile la o listă pre-aprobată de site-uri care sunt considerate utile şi corespunzătoare pentru copii. Părinţii utilizează uneori astfel de software-uri pentru împiedica copii să viziteze toate site-urile web dar fără câteva anume. Puteţi adăuga şi şterge site-uri pe/de pe lista „permise”. Această metodă este extrem de sigură, însă permite doar utilizarea extrem de limitată a internetului.

Worm

Viermele informatic este o aplicație sau un cod malițios capabil să se autoreproducă prin Internet sau alte sisteme conectate și care poate cauza daune în mai multe moduri. Deoarece au capacitatea de a se reproduce, viermii se pot înmulți foarte repede într-o rețea precum Internet.

Zero-Day Attack

Un atac sau o amenințare de tip "zero-day" este acela/aceea care exploatează vulnerabilități ale aplicațiilor informatice necunoscute sau necomunicate de dezvoltatorul soft-ului. De regulă, "exploit"-urile "zero-day" sunt folosite sau

împărtășite de/între atacatorii informatice mai înainte ca însuși creatorul/dezvoltatorul aplicației să ia la cunoștință despre respectiva vunerabilitate. "Zero" este termenul generic care se referă fix la momentul în care dezvoltatorul identifică/descoperă vulnerabilitatea și începe cursa contra-cronometru de a rezolva problema până la primul atac cunoscut. Ca o particularitate: atacurile de tip "zero-day" au capacitatea de a rămâne nedetectate din momentul lansării.

Surse:

- Institutul naţional de standarde şi tehnologie: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
- http://e-crime.ro/ecrime/site/index.php/home_en/glosar/

XIV. LINKURI UTILE DESPRE SECURITATE CIBERNETICĂ

SECURITATEA CIBERNETICĂ ŞI PROTECŢIA CONFIDENȚIALITĂȚII

- Centrul pentru securitatea pe internet (CIS): www.cisecurity.org
- Verificări de securitate online gratuite: http://www.staysafeonline.org/stay-safe-online/free-security-check-ups
- Alianţa naţională de securitate cibernetică pentru utilizatorii locali din organizațiile: http://www.staysafeonline.org
- OnGuard Online: www.OnGuardOnline.gov
- Institutului SANS (Administrare sistem, Audit, Reţea, Securitate) – Vulnerabilitățile critice ale securităţii pe internet: www.sans.org/top20
- Recomandări de securitate ale Securing our eCity: http://securingourecity.org/
- Soluţii pentru organizații de la StopBadware: http://stopbadware.org/
- Proiectul deschis privind securitatea aplicaţiilor web: www.owasp.org

CENTRELE DE SECURITATE CIBERNETICĂ ÎMPOTRIVA AMENINŢĂRILOR

- Linkuri despre siguranţa cibernetică pentru elevii de liceu: http://blackboard.aacps.org/portal/lor/obj/mods/4students/HSCybrSfty/addlinks.pdf
- Soluţii de securitate McAfee pentru organizații: http://shop.mcafee.com/Default.aspx?site=us&pid=HOME&CID=MFE-MHP001
- Soluţii de securitate Symantec pentru organizații: Http://store.symantec.com/?om_sem_cid=hho_sem_nam_us_Google_SMB_Store_Home&inid=hho_sem_s y:us:ggl:en:e%7Ckw0000006084%7CSMB

INSTRUIRE ŞI EXERCIŢII

- Materiale de instruire, ghiduri de configurare a securităţii gratuite de la Internet Security Alliance: http://www.isalliance.org/
- Instruire utilizatori DOD gratuită: http://iase.disa.mil/eta/Pages/online-catalog.aspx
- Instruire online gratuită utilizatori NIH (versiunea non DOD): http://irtsectraining.nih.gov/publicUser.aspx

RESURSE GUVERNAMENTALE

- Departamentul pentru Securitate Internă (DHS)- Strategia naţională pentru securizarea spaţiului cibernetic: http://www.dhs.gov/national-strategy-secure-cyberspace
- Depoziţia DHS în faţa Comitetului Camerei privind securitatea internă, Subcomitetului despre securitate în spaţiul cibernetic, protecţia infrastructurii şi tehnologiile de securitate: Http://www.dhs.gov/ynews/testimony/testimony_1300283858976.shtm
- Pagină din Enciclopedia FCC despre securitatea cibernetică: http://www.fcc.gov/cyberforsmallbiz
- Biroul FCC pentru Siguranţă publică şi Securitatea internă -Casa de compensare: http://publicsafety.fcc.gov/pshs/Casa de compensare/index.htm
- Biroul FCC pentru Siguranţa publică şi Securitatea internă -Linii directoare pentru planificarea situaţiilor de urgenţă: http://transition.fcc.gov/pshs/emergency-information/guidelines/
- Zece ponturi ale FCC privind securitatea cibernetică pentru organizațiile http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-306595A1.pdf
- Comisia Federală pentru Comerţ Ghid pentru afaceri http://www.ftc.gov/bcp/edu/microsites/infosecurity/
- Comisia Federală pentru Comerţ – Informaţii despre furtul de identitate: http://www.onguardonline.gov/topics/computer-security.aspx
- Comisia Federală pentru Comerţ - Tutorial interactiv: www.ftc.gov/infosecurity
- Institutul naţional de standarde şi tehnologie (NIST)- Centrul de resurse pentru securitatea computerelor: www.csrc.nist.gov
- Instructaj NIST despre Securitate cibernetică pentru organizații: http://csrc.nist.gov/groups/SMA/sbc/documents/smb-presentation.pdf
- Ghid NIST pentru Selectarea produselor de securitate a tehnologiei informaţiei: http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf
- Ghidul NIST de management al riscurilor pentru sistemele de tehnologia informaţiei: www.csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
- Colţul întreprinderilor mici NIST - Un link către paginile de asistenţă NIST-SBA-FBI privind securitatea informaţiilor pentru organizații: http://csrc.nist.gov/groups/SMA/sbc/index.html

- Securitatea informaţiilor NIST pentru organizaţii: http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf
- Parteneriatul SBA, NIST şi FBI despre Securitate cibernetică pentru organizaţii: http://csrc.nist.gov/groups/SMA/sbc/overview.html
- Echipa de pregătire pentru urgenţele informatice din Statele Unite (US-CERT): www.us-cert.gov
- Departamentul pentru Securitate Internă din S.U.A. - Resursele securităţii cibernetice: http://www.dhs.gov/cyber

PUBLICAŢII

- Cloud Security Alliance https://cloudsecurityalliance.org/csaguide.pdf
- Centrul de resurse pentru securitatea computerelor, Institutul Naţional de Standarde şi Tehnologie: http://csrc.nist.gov/groups/SMA/sbc/library.html
- Ghidul Microsoft pentru organizaţii: http://download.microsoft.com/download/3/a/2/3a208c3c-f355-43ce-bab4-890db267899b/ Security_Guide_for_Small_Business.pdf
- Protejarea micii dumneavoastră afaceri, Revista Entrepreneur: http://www.entrepreneur.com/magazine/entrepreneur/2010/june/206656.html
- Securitatea informaţiilor pentru organizaţii: Fundamente, Institutul naţional de standarde şi tehnologie: http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf