UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

Programul Operaţional Capital Uman 2014 – 2020
Axa Prioritară 3: Locuri de muncă pentru toţi
POCU/82 „România Start Up Plus”
OS 3.7 „Creșterea ocupării prin susținerea întreprinderilor cu profil non-agricol din zona urbană”
Titlu proiect: Start-UP Hub: Laboratorul antreprenorilor
Cod SMIS proiect: 105648
Proiect co-finanțat din Programul Operațional Capital Uman 2014-2020

Introducere în Securitate Cibernetică

Nicolai Sandu - Exeprt RED, instructor certificat Cisco Networking Academy

Bibliografie:

- Curs Intro To CyberSecurity by Cisco Networking Academy

- e-Ghid pentru securitate cibernetică. Un proiect din cadrul programului european "E-skills for jobs" (Competente digitale pentru locuri de munca) coordonat de Asociația Producătorilor și Distribuitorilor de Echipamente de Tehnologia Informației și Comunicații, în colaborare cu Poliția Română – Ins tutul de Cercetare și Prevenire a Criminalității și Cisco România

Oricine utilizează resurse internet ar trebui sa urmeze un curs introductiv de securitate cibernetica. Cu atat mai mult cei care planuesc sa dezvolte o afacere.

Participanții pot opta pentru lectura textului "Introducere in securitate cibernetica" sau înscrierea la cursul online coordonat de Nicolai Sandu, expert RED instructor certificat.

Link-ul pentru înscriere la curs va fi disponibil pe situl ULBS si KONFIDA.

Capitolul 1: Nevoia de securitate cibernetica

Acest capitol explică ce este securitatea cibernetică și motivul pentru care cererea pentru profesioniștii din domeniul securității cibernetice este în creștere. Aceasta explică ce sunt identitatea voastră online și datele, de provin, și de ce infractorii cibernetici sunt interesați de aceste date.

De asemenea, acest capitol discută despre ce sunt datele organizaționale, și de ce trebuie să fie protejate. Se discută despre cine sunt atacatorii cibernetici și ceea ce doresc. Profesioniștii cybersecurity trebuie să aibă aceleași abilități ca atacatorii cibernetici, dar profesioniștii securității cibernetice trebuie să lucreze în limitele legii locale, naționale și internaționale. Profesioniștii cybersecurity trebuie să utilizeze, de asemenea, abilitățile lor intr-un mod etic.
De asemenea, în acest capitol este inclus conținut care explică pe scurt ce este războiul

cibernetic și de ce națiunile și guvernele au nevoie de profesioniști și securitate informatică pentru a ajuta la protejarea cetățenilor și a infrastructurii lor.

Ce este securitatea cibernetica?

Rețeaua de informații electronice conectată a devenit o parte integrantă a vieții noastre de zi cu zi. Toate tipurile de organizații, cum ar fi instituțiile de învățământ medicale, financiare, și educaționale utilizează această rețea pentru a putea să funcționeze în mod eficient. Ele folosesc rețeaua pentru colectarea, prelucrarea, stocarea și schimbul de mari cantități de informații digitale.

Deoarece cantitatea de informații digitale colectate și partajate este tot mai mare, protecția acestor informații devine tot mai importantă pentru securitatea noastră națională și stabilitatea economică.
Cybersecurity este efortul continuu de a proteja aceste sisteme de rețea și toate datele de utilizări sau vătămări neautorizate. La nivel personal, aveți să vă protejați identitatea, datele și dispozitivele de calcul. La nivel corporativ, este responsabilitatea fiecăruia de a proteja reputația, datele și clienții organizației. La nivel de stat sunt în joc securitatea națională, precum și siguranța și bunăstarea cetățenilor.

Identitatea online și offline

Deoarece petrecem din ce în ce mai mult timp on-line, identitatea, atât online cât și offline, ne poate afecta viata. Identitatea ta off-line este persoana cu care prietenii și familia interacționează în fiecare zi acasă, la școală sau locul de muncă. Ei știu informațiile personale, cum ar fi numele, vârsta, sau unde locuiți. Identitatea online este cine sunteți în spațiul virtual. Identitatea online este modul în care vă prezentați on-line. Această identitate on-line ar trebui să dezvăluie doar o cantitate limitată de informații despre voi.

Ar trebui să aveți grijă la alegerea unui nume de utilizator pentru identitatea online. Numele de utilizator ar trebui să nu includă nicio informație cu caracter personal. Ar trebui să fie ceva adecvat și respectuos. Acest nume de utilizator nu ar trebui să le sugereze străinilor că sunteți o țintă ușoară pentru cybercrimes sau o atenție nedorită.

Datele tale

Orice informație despre voi poate fi considerată a face parte din datele voastre. Această informație cu caracter personal, vă poate identifica în mod unic ca individ. Aceste date

includ imaginile și mesajele pe care le schimbați cu familia și prietenii online. Alte informații, cum ar fi numele, numărul de securitate socială, data și locul nașterii, sau numele de fată al mamei, este cunoscută de voi și folosit pentru a vă identifica. Informații cum ar fi informații medicale, educaționale, financiare, ocuparea forței de muncă și, de asemenea, pot fi folosite pentru a vă identifica on-line.

Dosarele medicale

De fiecare dată când mergeți la cabinetul medicului, se adaugă mai multe informații pentru înregistrările medicale electronice (EHRs). Prescrierea de la medicul dumneavoastră de familie devine parte din DES (Dosarul electronic de sănătate) al dumneavoastră. DES include informații despre sănătatea voastră fizică, sănătatea psihică, precum și alte informații cu caracter personal, care nu pot fi medical legate. De exemplu, dacă ați avut consiliere când erați copii atunci când au existat schimbări majore în familie, acest lucru va fi undeva în înregistrările medicale. În afară de istoricul medical și informațiile personale, DES poate include, de asemenea, informații despre familia voastră.

Dispozitive medicale, cum ar fi benzile de fitness, folosesc platforma de cloud pentru a permite transferul fără fir, stocarea și afișarea datelor clinice cum ar fi pulsul, tensiunea arterială sau zaharurile din sânge. Aceste dispozitive pot genera o cantitate enormă de date clinice, care ar putea deveni o parte din înregistrările medicale.

Înregistrările privind educația

Pe măsură progresați prin educație, informațiile despre notele și rezultatele testelor, participarile la diferite activități, cursuri luate, premii și diplome recompensate, precum și orice rapoarte disciplinare pot fi stocate în dosarele voastre de educație. Acest înregistrări pot include, de asemenea, informații de contact, fișele medicale și de imunizare, precum și înregistrările educaționale speciale, inclusiv programe de educație individualizate (IEP-uri).

Înregistrările financiare si de munca

Înregistrarile dvs. financiare pot include informații despre veniturile și cheltuielile dumneavoastră. înregistrările fiscale ar putea include detalii referitoare la salariu, extrasele de card de credit, de rating de credit și alte informații bancare. Informațiile dvs. de muncă pot include locuri de muncă anterioare și performanța.

Unde sunt datele dvs.?

Toate aceste informații sunt despre voi. Există legi diferite care protejează confidențialitatea și datele din țara dvs. Dar știți unde sunt datele voastre?

Când vă aflați la cabinetul medicului, conversația pe care o aveți cu medicul este înregistrată în istoricul medical. În scopul facturării, aceste informații pot fi distribuite societăților de asigurări pentru a asigura facturarea și calitatea corespunzătoare. Acum, o parte a înregistrării medicale pentru vizită se află și la compania de asigurări.

Cardurile de loialitate ale magazinului pot fi o modalitate convenabilă de a economisi bani pentru achizițiile dvs. Cu toate acestea, magazinul compilează un profil al achizițiilor dvs. și utilizează aceste informații pentru uz propriu. Profilul arată cum cumpărătorul achiziționează în mod regulat o anumită marcă și aromă de pastă de dinți. Magazinul utilizează aceste informații pentru a viza cumpărătorul cu oferte speciale de la partenerul de marketing. Prin utilizarea cardului de fidelitate, magazinul și partenerul de marketing au un profil pentru comportamentul de cumpărare al unui client.

Atunci când partajați fotografiile online cu prietenii, știi cine ar putea avea o copie a imaginilor? Copii ale pozele sunt pe propriile dispozitive. Prietenii tăi pot avea copii ale acestor imagini descărcate pe dispozitivele lor. În cazul în care imaginile sunt partajate în mod public, străini pot avea copii ale acestora, de asemenea. Ei pot descarca acele imagini sau lua capturi de ecran ale acestor imagini. Pentru că imaginile au fost postate online, acestea sunt, de asemenea, salvate pe servere situate în diferite părți ale lumii. Acum, imaginile nu mai sunt gasite doar pe dispozitivele de calcul.

Dispozitivele dvs. de calcul

Dispozitivele de calcul nu doar stochează datele dvs. Acum aceste dispozitive au devenit portalul datelor voastre și generează informații despre voi.
Cu excepția cazului în care ați ales să primiți declarații de hârtie pentru toate conturile dvs., utilizați dispozitivele de calcul pentru a accesa datele. Dacă doriți o copie digitală a celui mai recent extras de cont, utilizați dispozitivele dvs. de calcul pentru a accesa site-ul web al emitentului cărții de credit. Dacă doriți să plătiți factura de pe cardul dvs. de credit online, accesați site-ul web al băncii dvs. pentru a transfera fondurile utilizând dispozitivele dumneavoastră. Pe lângă faptul că vă permite să accesați informațiile, dispozitivele de calcul pot genera și informații despre dvs.

Cu toate aceste informații despre dvs. disponibile online, datele dvs. personale au devenit profitabile pentru hackeri.

Își doresc banii tai

Credențialele dumneavoastră online sunt valoroase. Aceste credențiale oferă accesul hoților la conturile dvs. S-ar putea să credeți că milele frecvente ale flyerului pe care le-ați câștigat nu sunt valoroase pentru infractorii cibernetici. Mai gandiți-vă. După ce aproximativ 10.000 de conturi americane și americane au fost atacate, infractorii cibernetici au rezervat zboruri gratuite și upgrade-uri folosind aceste credențiale furate. Chiar dacă milele furate au fost returnate clienților de către companiile aeriene, acest lucru demonstrează valoarea credențialelor de conectare. Un infractor ar putea de asemenea să profite de relațiile voastre. Ei pot accesa conturile dvs. online și reputația dvs. pentru a vă înșela să vă conectați la bani prietenilor sau familiei. Infractorul poate trimite mesaje care să ateste că familia sau prietenii dvs. au nevoie de bani pentru a putea ajunge acasă din străinătate după ce și-au pierdut portofelul.

Criminalii cibernetici sunt foarte imaginativi atunci când încearcă să va păcălească în a le oferi bani. Ei nu fură doar banii; Ei ar putea, de asemenea, să vă fure identitatea și să vă distrugă viața.

Își doresc identitatea ta

Pe lângă faptul că fura banii pentru un câștig pe termen scurt, infractorii doresc profituri pe termen lung prin furtul identității.

Pe măsură ce costurile medicale cresc, furtul de identitate medicală este, de asemenea, în creștere. Hoții de identitate vă pot fura asigurarea medicală și pot folosi beneficiile medicale pentru ei înșiși, iar aceste proceduri medicale se află acum în evidențele medicale.

Procedurile anuale de depunere a taxelor pot varia de la o țară la alta, cu toate acestea, infractorii cibernetici văd acest moment ca o oportunitate. De exemplu, oamenii din Statele Unite trebuie să își depună impozitele până la data de 15 aprilie a fiecărui an. Serviciul de venituri interne (IRS) nu verifică declarația fiscală împotriva informațiilor furnizate de angajator până în iulie. Un hoț de identitate poate depune o declarație fiscală falsă și poate colecta rambursarea. Dosarele legitime vor observa când declarațiile lor vor fi respinse de IRS. Cu identitatea furată, ei pot deschide și conturi de carduri de credit și pot executa datorii

în numele dvs. Acest lucru va afecta ratingul dvs. de credit și va face mai dificilă obținerea de împrumuturi.
De asemenea, acreditările personale pot duce la accesul datelor corporative și la datele guvernamentale.

Tipuri de date organizaționale

Datele tradiționale

Datele companiei includ informații despre personal, proprietăți intelectuale și date financiare. Informațiile despre personal includ materialele de înscriere, salarizare, scrisori de ofertă, contractele angajaților și orice informație utilizată în luarea deciziilor privind ocuparea forței de muncă. Proprietatea intelectuală, cum ar fi brevetele, mărcile comerciale și noile planuri de produse, permit unei întreprinderi să obțină un avantaj economic față de concurenții săi. Această proprietate intelectuală poate fi considerată un secret comercial; Pierderea acestor informații poate fi dezastruoasă pentru viitorul companiei. Datele financiare, cum ar fi declarațiile de venit, bilanțurile și situațiile fluxurilor de trezorerie ale unei companii, oferă o imagine asupra sănătății companiei.

Internetul lucrurilor (IoT) și "Big Data"

Odată cu apariția internetului lucrurilor(IoT), există foerte multe date de gestionat și securizat. IoT este o rețea vastă de obiecte fizice, cum ar fi senzori și echipamente care se extind dincolo de rețeaua de calculatoare tradițională. Toate aceste conexiuni, plus faptul că am extins capacitățile de stocare și serviciile de stocare prin Cloud și virtualizare, au dus la creșterea exponențială a datelor. Aceste date au creat un nou domeniu de interes în domeniul tehnologiei și al afacerilor numit "Big Data". Având în vedere viteza, volumul și varietatea datelor generate de IoT și operațiunile zilnice ale afacerilor, confidențialitatea, integritatea și disponibilitatea acestor date este Vitală pentru supraviețuirea organizației.

Confidențialitate, integritate și disponibilitate

Confidențialitatea, integritatea și disponibilitatea, cunoscută sub numele de triada CIA (Figura 1), este un ghid pentru securitatea informațiilor unei organizații. Confidențialitatea asigură confidențialitatea datelor prin restricționarea accesului prin criptarea autentificării. **criptarea** este procesul de ascundere a informației pentru a o face ilizibilă fără cunoștințe

speciale. Criptarea a fost folosită pentru protejarea comunicațiilor de secole[*necesită citare*], dar doar organizații sau indivizi cu necesități de intimitate extraordinare s-au preocupat de a o implementa. În prezent, este utilizată în protejarea unei mari varietăți de sisteme, precum e-comerț, rețele de telefonie mobilă și ATM-urile băncilor.Integritatea asigură faptul că informațiile sunt corecte și demne de încredere. Disponibilitatea asigură că informațiile sunt accesibile persoanelor autorizate.

Confidențialitatea

Un alt termen pentru confidențialitate ar fi intimitatea (privat). Politicile companiei ar trebui să restricționeze accesul la informații pentru personalul autorizat și să se asigure că doar acele persoane autorizate văd aceste date. Datele pot fi compartimentate în funcție de nivelul de securitate sau de sensibilitate al informațiilor. De exemplu, un dezvoltator de programe Java nu ar trebui să aibă acces la informațiile personale ale tuturor angajaților. În plus, angajații ar trebui să beneficieze de instruire pentru a înțelege cele mai bune practici în protejarea informațiilor sensibile pentru a se proteja pe ei înșiși și compania de atacuri. Metodele de asigurare a confidențialității includ criptarea datelor, ID-ul de utilizator și parola, autentificarea cu doi factori și minimizarea expunerii informațiilor sensibile.

Integritatea

Integritatea este acuratețea, consecvența și fiabilitatea datelor pe parcursul întregului lor ciclu de viață. Datele trebuie să fie neschimbate în timpul tranzitului și nu sunt modificate de entități neautorizate. Permisiunile fișierelor și controlul accesului utilizatorilor pot împiedica accesul neautorizat. Controlul versiunilor poate fi folosit pentru a preveni modificările accidentale de către utilizatorii autorizați. Trebuie să fie disponibile copii de rezervă pentru a restabili datele corupte, iar hașura de control poate fi utilizată pentru a verifica integritatea datelor în timpul transferului.

O sumă de control este utilizată pentru a verifica integritatea fișierelor sau a șirurilor de caractere, după ce au fost transferate de pe un dispozitiv pe altul în rețeaua locală sau pe Internet. Sumele de control se calculează cu ajutorul funcțiilor hash. Unele dintre sumele de control comune sunt MD5, SHA-1, SHA-256 și SHA-512. O funcție hash utilizează un algoritm matematic pentru a transforma datele în valoare de lungime fixă care reprezintă datele, așa cum este reprezentat în figura 2. Valoarea hashed este pur și simplu acolo pentru comparație. Din valoarea hashed, datele originale nu pot fi preluate direct.

De exemplu, dacă ați uitat parola, parola dvs. nu poate fi recuperată din valoarea hashed. Parola trebuie resetată.

După descărcarea unui fișier, puteți verifica integritatea acestuia verificând valorile hash din sursă cu cea pe care ați generat-o utilizând orice calculator de tip hash. Comparând valorile hash, puteți asigura că fișierul nu a fost modificat sau deteriorat în timpul transferului.

Disponibilitatea

Întreținerea echipamentelor, efectuarea reparațiilor hardware, actualizarea sistemelor de operare și a software-ului și crearea de copii de siguranță asigură disponibilitatea rețelei și a datelor de către utilizatorii autorizați. Trebuie să fie planificate planuri de recuperare rapidă a dezastrelor naturale sau provocate de om. Echipamente de securitate sau software, cum ar fi firewall-uri, protejează împotriva perioadelor de nefuncționare din cauza atacurilor, cum ar fi negarea serviciului (DoS). Refuzul de serviciu apare atunci când un atac încearcă să copleșească resursele, astfel încât serviciile să nu fie disponibile utilizatorilor.

Consecințele unei breșe de securitate cibernetică

Nu este posibil ca o organizație să fie protejată de orice posibil atac cibernetic, din câteva motive. Expertiza necesară pentru înființarea și întreținerea unei rețelei sigure poate fi costisitoare. Atacatorii vor continua să găsească noi modalități de a viza și ataca rețelele. În cele din urmă, se va reuși un ciber-atac avansat și orientat. Prioritatea va fi atunci cât de repede echipa de securitate poate răspunde la atac pentru a minimiza pierderea de date și venituri și timpii de întrerupere.

De acum știți că orice postat online poate trăi online pentru totdeauna, chiar dacă ați reușit să ștergeți toate copiile aflate în posesia dvs. Dacă serverele dvs. au fost atacate, informațiile personale confidențiale ar putea fi făcute publice. Un hacker (sau un grup de hackeri) poate vandaliza site-ul companiei prin postarea de informatii incorecte si distrugerea reputatiei unei companiei care a luctat pentru reputatia sa ani întregi. De asemenea, hackerii pot opri site-ul companiei, cauzând pierderi de venituri companiei. În cazul în care site-ul este nefuncțional pentru perioade mai lungi de timp, compania poate părea nesigură și poate pierde credibilitatea. În cazul în care site-ul sau rețeaua companiei au fost atacate, acest lucru ar putea duce la scurgeri de documente confidențiale, dezvăluirea secretelor comerciale și furtul de proprietate intelectuală. Pierderea tuturor acestor informații poate împiedica creșterea și extinderea companiei.

Costul financiar al unui atac este mult mai mare decât înlocuirea dispozitivelor pierdute sau furate, investirea în securitatea existentă și consolidarea securității fizice a clădirii. Compania poate fi responsabilă pentru contactarea tuturor clienților afectați de încălcare și poate fi necesară pregătirea pentru soluționarea litigiilor. Cu toate aceste probleme, angajații pot alege să părăsească compania. Compania poate avea nevoie să se concentreze mai puțin pe creșterea și mai mult pe refacerea reputației sale.

Exemplu #1 de breșă de securitate cibernetică

Managerul de parole online, LastPass, a detectat o activitate neobișnuită în rețeaua sa în iulie 2015. S-a dovedit că hackerii au furat adrese de e-mail de utilizator, mementouri de parole și hashes de autentificare. Din fericire pentru utilizatori, hackerii nu au reușit să obțină seifuri de parole criptate de nimeni.

Chiar dacă a existat o încălcare a securității, LastPass ar putea să protejeze în continuare informațiile contului utilizatorilor. LastPass necesită o verificare prin e-mail sau autentificare multi-factor atunci când există o nouă autentificare de la un dispozitiv necunoscut sau o adresă IP. De asemenea, hackerii ar avea nevoie de parola de bază pentru a accesa contul.

Utilizatorii LastPass au, de asemenea, o anumită responsabilitate în protejarea propriilor conturi. Utilizatorii ar trebui să utilizeze întotdeauna parole principale complexe și să modifice periodic parolele principale. Utilizatorii ar trebui să fie mereu atenți la atacurile de tip phishing. Un exemplu de atac de tip phishing ar fi dacă un atacator a trimis e-mailuri false care susțin că sunt de la LastPass. E-mailurile solicită utilizatorilor să facă clic pe un link încorporat și să schimbe parola. Linkul din e-mail se referă la o versiune frauduloasă a site-ului folosit pentru a fura parola principală. Utilizatorii nu ar trebui să facă clic pe link-urile încorporate într-un e-mail. Utilizatorii ar trebui, de asemenea, să fie atent cu memento-ul de parolă. Reamintirea parolei nu ar trebui să vă dea parolele. Cel mai important, utilizatorii ar trebui să acorde autentificare multi-factor atunci când sunt disponibile pentru orice site web care o oferă.

Dacă utilizatorii și furnizorii de servicii folosesc instrumente și proceduri adecvate pentru a proteja informațiile utilizatorilor, datele utilizatorilor ar putea fi totuși protejate, chiar și în cazul încălcării securității.

Exemplu #2 de breșă de securitate cibernetică

Producătorul de jucării de înaltă tehnologie pentru copii, Vtech, a suferit o încălcare a securității în baza sa de date în noiembrie 2015. Această încălcare ar putea afecta milioane de clienți din întreaga lume, inclusiv copiii. Încălcarea datelor a expus informații sensibile, inclusiv numele clienților, adresele de e-mail, parolele, fotografiile și jurnalele de chat.

O tabletă de jucărie a devenit o țintă nouă pentru hackeri. Clienții au împărtășit fotografiile și au folosit funcțiile de chat prin tabletele de jucărie. Informațiile nu au fost asigurate corespunzător, iar site-ul web al companiei nu a susținut comunicarea securizată SSL. Chiar dacă încălcarea nu a expus informații despre cartea de credit și date personale de identificare, compania a fost suspendată la bursă, deoarece îngrijorarea cu privire la atacul cibernetic a fost foarte mare.

Vtech nu a asigurat corect informațiile clienților și a fost expus în timpul încălcării. Chiar dacă compania și-a informat clienții că parolele lor au fost șterse, era încă posibil ca hackerii să le descifreze. Parolele din baza de date s-au codificat utilizând funcția hash MD5, dar întrebările și răspunsurile de securitate au fost stocate în text simplu. Din păcate, funcția hash-urilor MD5 are vulnerabilități cunoscute. Hackerii pot determina parolele originale prin compararea a milioane de valori de hash pre-calculate.

Cu informațiile expuse în această încălcare a datelor, infractorii cibernetici ar putea să-l folosească pentru a crea conturi de e-mail, pentru a aplica credite și a comite crime înainte ca copiii să fie suficient de bătrâni pentru a merge la școală. Pentru părinții acestor copii, infractorii cibernetici puteau prelua conturile online, deoarece mulți oameni reutilizează parolele lor pe diferite site-uri și conturi.

Încălcarea securității nu a afectat numai confidențialitatea clienților, ci a distrus reputația companiei, așa cum a indicat compania atunci când a fost suspendată prezența sa pe bursă.

Pentru părinți, este un apel de trezire pentru a fi mai vigilenți privind viața privată online a copiilor lor și pentru a solicita o mai bună securitate pentru produsele copiilor. Pentru producătorii de produse conectate la rețea, aceștia trebuie să fie mai agresivi în protejarea datelor și a vieții private acum și în viitor, pe măsură ce peisajul cyberattack evoluează.

Tipuri de atacatori

Atacatorii sunt persoane sau grupuri care încearcă să exploateze vulnerabilitatea pentru câștiguri personale sau financiare. Atacatorii sunt interesați de tot felul de informații, de la cardurile de credit la design-urile de produse și orice altceva cu valoare.

Amatori - Acești oameni sunt uneori numiți Script Kiddies. Aceștia sunt de obicei atacatori cu puține sau fără abilități, folosindu-se adesea instrumente sau instrucțiuni existente pe Internet pentru a lansa atacuri. Unii dintre ei sunt doar curioși, în timp ce alții încearcă să-și demonstreze abilitățile și să aducă daune. Ei pot folosi instrumente de bază, dar rezultatele pot fi totuși devastatoare.

Hackerii - Acest grup de atacatori intră în computere sau rețele pentru a avea acces. În funcție de intenția intervenției, acești atacatori sunt clasificați ca pălării albe, gri sau negre. Atacatorii pălării albe fac teste de penetrare în rețele sau sisteme informatice pentru a descoperi punctele slabe, astfel încât securitatea acestor sisteme să poată fi îmbunătățită. Aceste spargeri se fac cu permisiunea prealabilă a proprietarilor și orice rezultate sunt raportate acestuia. Pe de altă parte, atacatorii cu pălării negre profită de orice vulnerabilitate pentru a realiza câștiguri personale, financiare sau politice ilegale. Atacatorii cu pălării gri se află undeva între atacatorii de pălărie albe și negri. Atacatorii de pălărie gri pot găsi o vulnerabilitate într-un sistem. Greble hackerii de hat pot raporta vulnerabilitatea proprietarilor sistemului dacă acea acțiune coincide cu agenda lor. Unii hackeri de pălărie gri publică faptele despre vulnerabilitate pe Internet, astfel încât alți atacatori să-l poată exploata. Figura oferă detalii despre termenii hacker de pălărie albă, hacker de pălărie negru și hacker de pălărie gri.

Hackeri organizați - Acești hackeri includ organizații de infractori cibernetici, hacktiviști, teroriști și hackeri sponsorizați de stat. Infractorii criminali sunt de obicei grupuri de infractori profesioniști care se concentrează pe control, putere și bogăție. Criminalii sunt foarte sofisticați și organizați și pot chiar să ofere criminalității informatice ca un serviciu pentru alți infractori. Hacktivistii fac declaratii politice pentru a crea constientizarea unor probleme importante pentru ei. Atacatorii sponsorizați de stat adună informații sau fac sabotaj în numele guvernului lor. Acești atacatori sunt, de obicei, foarte instruiți și bine finanțați, iar atacurile lor se concentrează asupra obiectivelor specifice care sunt benefice pentru guvernul lor.

Amenințări interne și externe

Amenințări interne ale securității

Atacurile pot proveni din cadrul unei organizații sau din afara organizației, după cum se arată în figură. Un utilizator intern, cum ar fi un angajat sau un partener contractual, poate accidental sau intenționat:

- Administra greșit confidențialitatea datelor
- Amenința operațiile serverelor interne sau ale dispozitivelor de infrastructură de rețea

- Facilitata atacurile externe conectând mediile USB infectate la sistemul informatic corporativ
- Introduce în mod accidental malware în rețea prin e-mail-uri rău intenționate sau pe site-uri web

Amenințările interne au, de asemenea, potențialul de a provoca daune mai mari decât amenințările externe, deoarece utilizatorii interni au acces direct la clădire și la dispozitivele sale de infrastructură. Angajații au, de asemenea, cunoștințe despre rețeaua companiei, resursele și datele sale confidențiale, precum și diferitele niveluri de privilegii utilizator sau administrative.

Amenințările externe ale amatorilor sau ale atacatorilor calificați pot exploata vulnerabilități în dispozitivele de rețea sau de calcul sau pot folosi ingineria socială pentru a avea acces la acestea.

Aspecte juridice privind securitatea cibernetică

Profesioniștii în domeniul securității ciberneticii trebuie să aibă aceleași competențe ca și hackerii, în special hackerii black hat, pentru a oferi protecție împotriva atacurilor. O diferență între un hacker și un profesionist în domeniul securității informatice este că profesionistul în domeniul securității informatice trebuie să lucreze în limitele legalității.

Probleme juridice personale

Nici măcar nu trebuie să fii angajat pentru a fi supus legilor privind securitatea cibernetică. În viața dvs. privată, puteți avea oportunitatea și abilitățile de a ataca computerul sau rețeaua unei alte persoane. Există o veche zicală: "Doar pentru că puteți face, nu înseamnă că și trebuie să faceții". Majoritatea hackerilor lasă urme, indiferent dacă știu sau nu, iar aceste piste pot duce înapoi la hacker.

Profesioniștii în domeniul cybersecurity dezvoltă multe abilități care pot fi folosite pentru a face bine sau rău. Cei care își folosesc abilitățile în cadrul sistemului juridic, pentru a proteja infrastructura, rețelele și viața privată sunt mereu foarte căutați.

Probleme juridice corporative

Majoritatea țărilor au anumite legi privind securitatea cibernetică. Acestea pot avea legătură cu infrastructura critică, cu rețelele și cu confidențialitatea corporativă și individuală. Companiile trebuie să respecte aceste legi.

În unele cazuri, dacă încălcați legile privind securitatea cibernetică în timp ce vă faceți datoria, compania poate fi pedepsită și vă puteți pierde locul de muncă. În alte cazuri, ați putea fi urmărit penal, amendat și eventual condamnat.

În general, dacă atunci când nu sunteți sigur dacă o acțiune sau comportament ar putea fi ilegală, presupuneți că este ilegală și nu o faceți. Compania dvs. poate avea un departament juridic sau o persoană din departamentul de resurse umane care vă poate răspunde la întrebări înainte de a face ceva ilegal.

Dreptul internațional și securitatea cibernetică

Domeniul legilor privind securitatea cibernetică este mult mai nou decât securitatea cibernetică. După cum sa menționat mai sus, majoritatea țărilor au anumite legi în vigoare și vor exista mai multe legi care vor veni.

Legea privind securitatea cibernetică este încă nouă. Parteneriatul multilateral internațional împotriva amenințărilor informatice (IMPACT) este primul parteneriat public-privat internațional axat pe amenințările cibernetice. IMPACT este un parteneriat global al guvernelor, industriilor și mediului academic, dedicat îmbunătățirii capacităților globale în ceea ce privește amenințările cibernetice. Figura arată site-ul pentru IMPACT.

Probleme etice în securitatea cibernetică

Pe lângă faptul că lucrează în limitele legii, profesioniștii din domeniul securității informatice trebuie să demonstreze și comportamentul etic.

Probleme etice personale

O persoană poate acționa neetic și să nu poată face obiectul urmăririi penale, a amenzilor sau a închisorii. Acest lucru se datorează faptului că este posibil ca acțiunea să nu fi fost tehnic ilegală. Dar asta nu înseamnă că comportamentul este acceptabil. Comportamentul etic este destul de ușor de constatat. Este imposibil să enumerați toate diferitele comportamente neetice care pot fi expuse de cineva cu abilități de securitate cibernetică. Mai jos sunt doar două.

Intreaba-te pe tine insuti:
• Vreau să descopăr că cineva a intrat în calculatorul meu și a modificat imaginile în site-urile rețelei mele sociale?

• Vreau să descopăr dacă tehnician IT în care am avut încredere să-mi repare rețeaua le-a spus colegilor informații personale despre mine care au fost obținute în timp ce lucra în rețeaua mea?
Dacă răspunsul dvs. la oricare dintre aceste întrebări a fost "nu", atunci nu faceți astfel de lucruri altora.

Probleme etice corporative

Etica este un cod de comportament care uneori este impus de legi. Există multe zone în domeniul securității informatice care nu sunt reglementate de legi. Aceasta înseamnă există posibilitatea de a face ceva care este legal din punct de vedere tehnic dar nu și etic. Deoarece atât de multe domenii de securitate cibernetică nu sunt (sau încă nu sunt) acoperite de legi, multe organizații profesionale IT au creat coduri de etică pentru persoanele din industrie. Mai jos este o listă a trei organizații cu coduri de etică:

- Institutul CyberSecurity Institute (CSI) a publicat un cod de etică pe care îl puteți citi aici.
- Asociația pentru Securitatea Sistemelor Informaționale (ISSA) are un cod de etică care poate fi găsit aici.
- Asociația Profesioniștilor în Tehnologia Informației (AITP) are atât un cod de etică, cât și un standard de comportament găsit aici.

Căutați online pentru a găsi alte organizații legate de IT cu coduri de etică. Încearcă să găsești ceea ce au toți în comun.

Ce este războiul cibernetic

Cyberspace-ul a devenit o altă dimensiune importantă a războiului, în care națiunile pot efectua conflicte fără ciocniri de trupe și mașini tradiționale. Acest lucru permite țărilor cu o prezență militară minimă să fie la fel de puternice ca și alte națiuni din spațiul cibernetic. Cyberwarfare este un conflict pe internet care implică pătrunderea sistemelor informatice și rețelelor altor națiuni. Acești atacatori au resursele și expertiza pentru a lansa atacuri masive pe internet împotriva altor națiuni pentru a provoca daune sau pentru a întrerupe servicii importante, cum ar fi închiderea unei rețele electrice.

Un exemplu al unui atac sponsorizat de stat a implicat malware-ul Stuxnet care a fost conceput pentru a distruge instalația de îmbogățire nucleară a Iranului. Malware-ul Stuxnet nu a deturnat computerele vizate pentru a fura informații. A fost proiectat pentru a distruge echipamentele fizice controlate de computere. Acesta a folosit codificarea modulară programată pentru a efectua o anumită sarcină în cadrul programului malware. A folosit certificate digitale furate, astfel încât atacul a părut legitim sistemului. Faceți clic pe Redare pentru a vizualiza un videoclip despre Stuxnet.

Mergi AICI să vezi un video despre Stuxnet.

Scopul războiului cibernetic

Scopul principal al războiului cibernetic este de a câștiga avantajul față de adversari, fie că sunt națiuni sau competitori.
O națiune poate continua să invadeze infrastructura altor națiuni, să fure secretele de apărare și să adune informații despre tehnologie pentru a reduce decalajele din industriile și armata sa. Pe lângă spionajul industrial și militarist, războiul cibernetic poate să saboteze infrastructura altor națiuni și să coste vieți în țările vizate. De exemplu, un atac poate perturba grila electrică a unui oraș important. Traficul ar fi întrerupt. Schimbul de bunuri și servicii este oprit. Pacienții nu pot beneficia de îngrijirea necesară în situații de urgență. Accesul la Internet poate fi, de asemenea, perturbat. Prin afectarea rețelei electrice, atacul poate afecta viața de zi cu zi a cetățenilor obișnuiți.

Mai mult, datele sensibile compromise pot da atacatorilor posibilitatea de a șantaja personalul din cadrul guvernului. Informațiile pot permite unui atacator să pretindă că este un utilizator autorizat pentru a accesa informații sau echipamente sensibile.

Dacă guvernul nu poate apăra împotriva atacurilor cibernetice, cetățenii pot pierde încrederea în capacitatea guvernului de a ii proteja. Cyberwarfare poate destabiliza o națiune, poate perturba comerțul și poate afecta credința cetățenilor în guvernul lor fără să invadeze fizic națiunea țintă.

Capitolul 2: Concepte și tehnici ale atacurilor

Acest capitol se referă la modalitățile în care profesioniștii din domeniul securității informatice analizează ce sa întâmplat după un atac cibernetic. Aceasta explică vulnerabilitățile software și hardware de securitate și diferitele categorii de vulnerabilități de

securitate.
Diferitele tipuri de software rău intenționat (cunoscut sub numele de malware) și simptomele malware-ului sunt discutate. Diferitele moduri prin care atacatorii pot infiltra un sistem sunt acoperite, precum și atacuri de negare a serviciilor.
Majoritatea atacurilor cibernetice moderne sunt considerate atacuri mixte. Atacurile combinate utilizează mai multe tehnici pentru a se infiltra și a ataca un sistem. Atunci când un atac nu poate fi prevenit, este de datoria unui profesionist în domeniul cibernetic să reducă impactul acestui atac.

Identificarea vulnerabilităților de securitate

Vulnerabilitățile de securitate sunt orice defect de software sau hardware. După ce au obținut cunoștințe despre o vulnerabilitate, utilizatorii rău-intenționați încearcă să o exploateze. Exploit este termenul folosit pentru a descrie un program scris pentru a profita de o vulnerabilitate cunoscută. Actul de folosire a unui exploit împotriva unei vulnerabilități este considerat un atac. Scopul atacului este de a avea acces la un sistem, la datele pe care le găzduiește sau la o anumită resursă.

Vulnerabilități software

Vulnerabilitățile software sunt, de obicei, introduse de erori în sistemul de operare sau în codul de aplicație, în ciuda tuturor eforturilor făcute de companii pentru găsirea și corectarea vulnerabilităților software, este comun noilor vulnerabilități la suprafață. Microsoft, Apple și alți producători de sisteme de operare eliberează patch-uri și actualizări aproape în fiecare zi. Actualizările aplicațiilor sunt de asemenea des întâlnite. Aplicațiile precum browserele web, aplicațiile mobile și serverele web sunt adesea actualizate de companiile sau organizațiile responsabile de acestea.

În 2015, o vulnerabilitate majoră, numită SYNful Knock, a fost descoperită în Cisco IOS. Această vulnerabilitate a permis atacatorilor să obțină controlul asupra routerelor pentru întreprinderi, cum ar fi cele ruterele mai vechi Cisco 1841, 2811 și 3825. Atacatorii ar putea apoi să monitorizeze toate comunicațiile de rețea și să aibă capacitatea de a infecta alte dispozitive de rețea. Această vulnerabilitate a fost introdusă în sistem când a fost instalată o versiune IOS modificată în routere. Pentru a evita acest lucru, verificați întotdeauna integritatea imaginii IOS descărcate și limitați accesul fizic al echipamentului numai la personalul autorizat.

Scopul actualizărilor de software este să rămână actual și să evite exploatarea vulnerabilităților. În timp ce unele companii au echipe de testare a penetrării dedicate

căutării, găsirii și patch-urilor vulnerabilităților software înainte ca acestea să poată fi exploatate, cercetătorii de securitate terți se specializează și în găsirea vulnerabilităților în software.

Proiectul Google Zero este un exemplu excelent al unei astfel de practici. După ce a descoperit o serie de vulnerabilități în diverse aplicații software utilizate de utilizatorii finali, Google a format o echipă permanentă dedicată găsirii vulnerabilităților software. Cercetarea în domeniul securității Google poate fi găsită aici.

Vulnerabilități hardware

Vulnerabilitățile hardware sunt adesea introduse de defectele de proiectare hardware. Memoria RAM, de exemplu, este formată în esență din condensatoare instalate foarte aproape una de cealaltă. S-a descoperit că, datorită proximității, modificările constante aplicate la unul dintre aceste condensatoare ar putea influența condensatorii vecini. Pe baza defectului de proiectare, a fost creat un exploit numit Rowhammer. Prin rescrierea în mod repetat a memoriei în aceleași adrese, exploatarea Rowhammer permite ca datele să fie preluate din celulele de memorie adresate din apropiere, chiar dacă celulele sunt protejate. Vulnerabilitățile hardware sunt specifice modelelor de dispozitive și nu sunt, în general, exploatate prin încercări aleatorii de compromitere. În timp ce exploatările hardware sunt mai frecvente în atacurile foarte bine direcționate, protecția tradițională împotriva malware-ului și securitatea fizică reprezintă o protecție suficientă pentru utilizatorul de zi cu zi.

Categoriile vulnerabilităților de securitate

Majoritatea vulnerabilităților de securitate ale software-ului se încadrează într-una din următoarele categorii:

Buffer overflow - Această vulnerabilitate apare atunci când datele sunt scrise dincolo de limitele unui buffer. Tampoanele sunt zone de memorie alocate unei aplicații. Prin schimbarea datelor dincolo de limitele unui buffer, aplicația accesează memoria alocată altor procese. Acest lucru poate duce la un accident de sistem, la compromiterea datelor sau la creșterea gradului de privilegii.

Intrare nevalidată - Programele funcționează adesea cu introducerea de date. Aceste date care intră în program ar putea avea conținut rău intenționat, conceput pentru a forța

programul să se comporte neintenționat. Luați în considerare un program care primește o imagine pentru procesare. Un utilizator rău intenționat ar putea să realizeze un fișier imagine cu dimensiuni de imagine nevalide. Dimensiunile dăunătoare ar putea forța programul să aloce tampoane de dimensiuni incorecte și neașteptate.

Condițiile cursei - această vulnerabilitate este atunci când ieșirea unui eveniment depinde de ieșirile comandate sau temporizate. O condiție de cursă devine o sursă de vulnerabilitate atunci când evenimentele comandate sau temporizate nu se produc în ordinea corectă sau în timpul corespunzător.

Deficiențe în practicile de securitate - Sistemele și datele sensibile pot fi protejate prin tehnici precum autentificarea, autorizarea și criptarea. Dezvoltatorii nu ar trebui să încerce să creeze algoritmi de securitate proprii, deoarece probabil vor introduce vulnerabilități. Este recomandat ca dezvoltatorii să folosească biblioteci de securitate care au fost deja create, testate și verificate.

Probleme de control al accesului - Controlul accesului este procesul de a controla cine face ceea ce variază de la gestionarea accesului fizic la echipament pentru a dicta cine are acces la o resursă, cum ar fi un fișier, și ce pot face cu acesta, cum ar fi citirea sau schimbarea fișierul. Multe vulnerabilități de securitate sunt create de utilizarea necorespunzătoare a controalelor de acces.

Aproape toate controalele de acces și practicile de securitate pot fi depășite dacă atacatorul are acces fizic la echipamentele țintă. De exemplu, indiferent de ce ați stabilit permisiunile unui fișier, sistemul de operare nu poate împiedica pe cineva să ocolească sistemul de operare și să citească datele direct de pe disc. Pentru a proteja mașina și datele pe care le conține, accesul fizic trebuie restrâns, iar tehnicile de criptare trebuie folosite pentru a proteja datele de furt sau de corupție.

Tipuri de malware

Pe scurt pentru software-ul rău intenționat, malware-ul este orice cod care poate fi folosit pentru a fura date, a ocoli controlul accesului sau a provoca daune sau compromite unui sistem. Mai jos sunt câteva tipuri obișnuite de malware:

Spyware - Acest program malware este proiectat pentru a urmări și spiona utilizatorul. Spyware include deseori urmărirea activității, colectarea a ceea ce s-a tastat și captura de

date. În încercarea de a depăși măsurile de securitate, aplicațiile spyware modifică adesea setările de securitate. Spyware se îmbină adesea cu software-ul legitim sau cu cai troieni.

Adware - Software-ul publicitar acceptat este conceput pentru a difuza anunțuri în mod automat. Adware-ul este adesea instalat cu unele versiuni de software. Unele adware sunt concepute să difuzeze numai anunțuri, dar este, de asemenea, obișnuit ca adware să vină cu spyware.

Bot - Din **robot** cuvânt, un bot este un program malware conceput pentru a efectua automat acțiuni, de obicei online. În timp ce majoritatea bot-ilor sunt inofensivi, o utilizare tot mai mare a bot-ilor rău intenționați sunt botneturile. Mai multe computere sunt infectate cu bot-uri care sunt programați să aștepte în liniște comenzile furnizate de atacator.

Ransomware - Acest program malware este conceput pentru a ține captiv un sistem informatic sau datele pe care le conține până la efectuarea unei plăți. Ransomware funcționează de obicei prin criptarea datelor în computer cu o cheie necunoscută utilizatorului. Unele alte versiuni ale programului ransomware pot beneficia de vulnerabilități specifice sistemului pentru blocarea sistemului. Ransomware este răspândit de un fișier descărcat sau de o vulnerabilitate software.

Scareware - Acesta este un tip de malware conceput pentru a convinge utilizatorul să întreprindă o acțiune specifică bazată pe frică. Scareware deschide ferestre pop-up care seamănă cu ferestrele de dialog de sistem de operare. Aceste ferestre transmit mesaje false care indică faptul că sistemul este în pericol sau are nevoie de executarea unui program specific pentru a reveni la funcționarea normală. În realitate, nu au fost evaluate sau detectate probleme și dacă utilizatorul este de acord și șterge programul menționat pentru a fi executat, sistemul său va fi infectat cu programe malware.

Rootkit - Acest malware este proiectat pentru a modifica sistemul de operare pentru a crea un backdoor. Atacatorii folosesc apoi backdoor-ul pentru a accesa computerul de la distanță. Majoritatea rootkiturilor profită de vulnerabilitățile software pentru a realiza escaladarea privilegiilor și a modifica fișierele de sistem. Este, de asemenea, obișnuit ca rootkiturile să modifice instrumentele de monitorizare a sistemului, ceea ce le face foarte greu de detectat. Adesea, un calculator infectat de un rootkit trebuie să fie șters și reinstalat.

Virus - Un virus este un cod executabil malware care este atașat la alte fișiere executabile, adesea programe legitime. Majoritatea virușilor necesită activarea utilizatorilor finali și se pot activa la un anumit moment sau dată. Virușii pot fi inofensivi și pot afișa o imagine sau pot fi distrugătoari, cum ar fi cei care modifică sau șterg datele. Virușii pot fi, de asemenea,

programați să se modifice pentru a evita detectarea. Majoritatea virușilor sunt acum răspânditi de unități USB, discuri optice, acțiuni de rețea sau e-mail.

Troian horse - Un cal troian este un program malware care efectuează operațiuni rău intenționate sub masca unei operații dorite. Acest cod rău intenționat exploatează privilegiile utilizatorului care îl execută. Adesea, troienii se găsesc în fișiere imagine, fișiere audio sau jocuri. Un cal troian diferă de un virus deoarece se leagă de fișiere ne-executabile.

Worms - viermii sunt cod rău intenționat care se replică prin exploatarea independentă a vulnerabilităților din rețele. Viermii încetinesc, de obicei, rețelele. În timp ce un virus necesită un program gazdă pentru a rula, viermii pot rula singuri. În afară de infectarea inițială, ei nu mai necesită participarea utilizatorilor. După ce o gazdă este infectată, viermele se poate răspândi foarte repede în rețea. Viermii împărtășesc modele similare. Toți au o vulnerabilitate care le permite, o modalitate de a se propaga și toate conțin o sarcină utilă.

Viermii sunt responsabili pentru unele dintre cele mai devastatoare atacuri pe Internet. Așa cum se arată în figura 1, în 2001, viermii de cod roșu au infectat 658 de servere. În 19 ore, viermele a infectat peste 300.000 de servere.

Man-In-The-Middle (MitM) - MitM permite atacatorului să preia controlul asupra unui dispozitiv fără cunoștința utilizatorului. Cu acel nivel de acces, atacatorul poate intercepta și capta informații despre utilizatori înainte de a le trimite la destinația dorită. Atacurile MitM sunt folosite pe scară largă pentru a fura informații financiare. Există multe programe malware și tehnici care să ofere atacatorilor posibilitatea de a folosi funcțiile MitM.

Man-In-The-Mobile (MitMo) - O variantă de om-în-mijloc, MitMo este un tip de atac folosit pentru a prelua controlul asupra unui dispozitiv mobil. Când este infectat, dispozitivul mobil poate fi instruit să exfiltreze informații sensibile la utilizatori și să le trimită atacatorilor. ZeuS, un exemplu de exploatare cu capabilități MitMo, permite atacatorilor să efectueze în liniște SMS-uri de verificare în două trepte trimise utilizatorilor.

Simptomele de malware

Indiferent de tipul de malware cu care a fost infectat un sistem, acestea sunt simptome comune ale malware-ului:

- Există o creștere a utilizării CPU.
- Există o scădere a vitezei calculatorului.
- Computerul se blochează sau se blochează frecvent.
- Există o scădere a vitezei de navigare pe Web.
- Există probleme inexplicabile cu conexiunile la rețea.
- Fișierele sunt modificate.
- Fișierele sunt șterse.
- Există prezența unor fișiere, programe sau pictograme necunoscute.
- Există procese necunoscute care rulează.
- Programele se opresc sau se reconfigurează.
- Email-ul este trimis fără cunoștințele sau acordul utilizatorului.

Inginerie socială

Ingineria socială este un atac de acces care încearcă să manipuleze indivizii în efectuarea de acțiuni sau în divulgarea informațiilor confidențiale. Inginerii sociali se bazează adesea pe dorința oamenilor de a fi de ajutor, dar și pe slăbiciunilor oamenilor. De exemplu, un atacator ar putea apela un angajat autorizat cu o problemă urgentă care necesită acces imediat la rețea. Atacatorul ar putea apela la vanitatea angajatului, poate invoca autoritate folosind tehnici de renunțare la nume sau poate apela la lăcomia angajatului.

Acestea sunt câteva tipuri de atacuri de inginerie socială:

- Pretexting - Acesta este momentul în care un atacator apelează la un individ și îl minte în încercarea de a avea acces la date privilegiate. Un exemplu îl reprezintă un atacator care pretinde că are nevoie de date personale sau financiare pentru a confirma identitatea destinatarului.
- Tailgating - Acesta este cazul în care un atacator urmează repede o persoană autorizată într-o locație sigură.
- Ceva pentru ceva (Quid pro quo) - Atunci când un atacator cere informații personale de la o petrecere în schimbul unui ceva, ca un cadou gratuit.

Spargerea parolei Wi-Fi

Spargerea parolei Wi-Fi este procesul de descoperire a parolei care protejează o rețea fără fir. Acestea sunt câteva tehnici utilizate pentru cracarea parolelor:

Ingineria socială - Atacantul manipulează o persoană care cunoaște parola pentru furnizarea acesteia.
Atacurile brute - atacatorul încearcă mai multe parole posibile în încercarea de a ghici parola. Dacă parola este un număr de 4 cifre, de exemplu, atacatorul ar trebui să încerce fiecare din cele 10000 de combinații. Forțele de atac brute implică de obicei un fișier de liste de cuvinte. Acesta este un fișier text care conține o listă de cuvinte preluate dintr-un dicționar. Un program încearcă fiecare cuvânt și combinații comune. Deoarece atacurile brute-force necesită timp, parole complexe durează mult mai mult pentru a ghici. Câteva instrumente de forțare a parolei brute includ Ophcrack, L0phtCrack, THC Hydra, RainbowCrack și Medusa.
Sniffing în rețea - prin ascultarea și captarea pachetelor trimise în rețea, un atacator poate descoperi parola dacă parola este trimisă necriptată (în text simplu). Dacă parola este criptată, atacatorul ar putea să-l dezvăluie folosind un instrument de spargere a parolei.

Phishing

Phishing este atunci când cineva rău intenționat trimite un e-mail fraudulos, deghizat ca fiind dintr-o sursă legitimă și de încredere. Scopul mesajului este de a păcăli destinatarul pentru a instala programe malware pe dispozitivul lui sau pentru a permite accesul la informații personale sau financiare. Un exemplu de phishing este un email falsificat pentru a arăta că a fost trimis de un magazin de vânzare cu amănuntul, solicitând utilizatorului să facă clic pe un link pentru a revendica un premiu. Linkul poate merge la un site fals care solicită informații personale sau poate instala un virus.

Spear phishing - săgeată este un atac de phishing foarte bine direcționat. În timp ce phishingul și phishingul cu sulițe folosesc atât e-mail-uri pentru a ajunge la victime, e-mailurile cu phishing-uri de tip phishing sunt personalizate pentru o anumită persoană. Atacatorul investighează ținta înainte de a trimite e-mailul. De exemplu, un atacator învață că țintă este interesat de mașini și căuta să cumpere un model specific de mașină. Atacantul se alătură aceluiași forum de discuții în cazul în care țintă este un membru, forteaza o ofertă

de vânzare de mașini și trimite e-mail către țintă. E-mailul conține un link pentru imagini ale mașinii. Când țintă face clic pe link, malware-ul este instalat pe computerul țintă.

Exploatarea vulnerabilităților

Exploatarea vulnerabilităților este o altă metodă comună de infiltrare. Atacatorii vor scana computerele pentru a obține informații despre ele. Mai jos este o metodă comună de exploatare a vulnerabilităților:

Pasul 1. Obțineți informații despre sistemul țintă. Acest lucru se poate face în mai multe moduri diferite, cum ar fi un scaner port sau inginerie socială. Scopul este de a învăța cât mai mult posibil despre computerul țintă.
Pasul 2. O parte din informațiile relevante învățate în pasul 1 ar putea fi sistemul de operare, versiunea sa și o listă de servicii care rulează pe acesta.
Pasul 3. Când sistemul de operare și versiunea țintă sunt cunoscute, atacatorul caută orice vulnerabilități cunoscute specifice acelei versiuni a sistemului de operare sau a altor servicii OS.
Pasul 4. Când se găsește o vulnerabilitate, atacatorul caută o exploatare scrisă în prealabil pentru utilizare. Dacă nu au fost scrise atacatorul poate lua în considerare scrierea unui exploit.

Amenințări persistente avansate (APT)

Un mod în care se realizează infiltrarea este prin amenințări persistente avansate (APT). Acestea constau într-o operațiune multifazică, pe termen lung, furt și operații avansate împotriva unei ținte specifice. Datorită complexității și nivelului de calificare necesar, un APT este de obicei bine finanțat. Un APT vizează organizații sau națiuni din motive comerciale sau politice.

De obicei, legat de spionajul bazat pe rețea, scopul APT este de a implementa malware personalizat pe unul sau mai multe dintre sistemele țintă și rămâne nedetectat. Cu mai multe faze de operare și mai multe tipuri personalizate de malware care afectează diferite dispozitive și îndeplinesc anumite funcții, un atacator individual nu are adesea setul de calificări, resursele sau persistența pentru a efectua APT.

Denial-of-Service (DoS)

Atacurile Denial-of-Service (DoS) sunt tipuri de atac de rețea. Un atac DoS duce la un fel de întrerupere a serviciului de rețea pentru utilizatori, dispozitive sau aplicații. Există două tipuri majore de atacuri DoS:

Cantitatea copleșitoare de trafic - atunci când o rețea, o gazdă sau o aplicație primește o cantitate enormă de date la o rată pe care nu o poate gestiona. Acest lucru determină o încetinire a transmisiei sau a unui răspuns sau o cadere a unui dispozitiv sau a unui serviciu.

Pachete cu format MALIȚIOS - Atunci când un pachet formatat în mod necorespunzător este trimis unui gazdă sau unei aplicații și receptorul nu poate să il gestioneze. De exemplu, un atacator transmite pachete care conțin erori care nu pot fi identificate de către aplicație sau care înaintează pachete formatate incorect. Acest lucru determină ca dispozitivul de recepție să funcționeze foarte lent sau să se prăbușească.
Atacurile DoS sunt considerate un risc major, deoarece pot întrerupe cu ușurință comunicarea și pot cauza pierderi semnificative de timp și bani. Aceste atacuri sunt relativ simple de efectuat, chiar și de către un atacator necalificat.

Atac DoS distribuit (DDoS)

Un atac de DoS distribuit (DDoS) este similar cu un atac DoS, dar provine din mai multe surse coordonate. De exemplu, un atac DDoS ar putea continua după cum urmează:
Un atacator construiește o rețea de gazde infectate, numită botnet. Gazdele infectate sunt numite zombi. Zombiile sunt controlate de sistemele de manipulare.
Computerele zombie scanează constant și infectează mai multe gazde, creând mai multe zombi. Când este gata, hacker-ul instruiește sistemele de handler să facă botnet-ul zombiilor să efectueze un atac DDoS.

OTRĂVIRE DE TIP SEO

Motoarele de căutare, cum ar fi Google, lucrează prin clasificarea paginilor și prezintă rezultate relevante pe baza interogărilor pe care le fac utilizatorii. În funcție de relevanța conținutului site-ului web, acesta poate apărea mai mult sau mai puțin în lista rezultatelor căutării. SEO, scurt pentru optimizarea motorului de căutare, este un set de tehnici utilizate pentru îmbunătățirea clasamentului unui site de către un motor de căutare. În timp ce multe companii legitime se specializează în optimizarea site-urilor pentru a le poziționa mai bine, un utilizator rău intenționat ar putea utiliza SEO pentru a face ca un site rău intenționat să apară mai sus în rezultatele căutării. Această tehnică se numește otrăvire SEO.

Obiectivul cel mai comun al otrăvirii SEO este creșterea traficului către site-uri rău intenționate, care pot găzdui programe malware sau pot efectua ingineria socială. Pentru a forța un site rău intenționat să se situeze mai bine în rezultatele căutării, atacatorii profită de termenii populare de căutare.

Ce este un atac combinat

Atacurile combinate sunt atacuri care folosesc mai multe tehnici pentru a compromite o țintă. Prin utilizarea mai multor tehnici de atac simultan, atacatorii au malware care sunt un hibrid de viermi, cai troieni, spyware, keyloggers, spam-uri și scheme de phishing. Această tendință de atacuri combinate dezvăluie malware mai complex și introducerea datelor de utilizator la un risc mare.

Cel mai obișnuit tip de atac combinat utilizează mesaje de e-mail spam, mesaje instantanee sau site-uri legitime pentru a distribui linkuri unde malware sau spyware sunt descărcate în secret în computer. Un alt atac comun combinat utilizează DDoS combinat cu e-mailuri de phishing. În primul rând, DDoS este folosit pentru opri un site popular al băncii și a trimite e-mailuri clienților băncii, scuzându-se pentru neplăcerile. De asemenea, e-mailurile direcționează utilizatorii către un site de urgență fals, unde informațiile lor de autentificare pot fi furate.

Mulți dintre cei mai dăunători viermi ai computerului, precum Nimda, Code Red, BugBear, Klez și Slammer, sunt mai bine clasificați ca atacuri combinate, după cum se arată mai jos:

- Unele variante Nimbda au folosit atașamente de e-mail; Descărcări de fișiere de pe un server web compromis; Și partajarea de fișiere Microsoft (de exemplu, acțiuni anonime) ca metode de propagare.
- Alte variante Nimbda au fost capabile să modifice conturile clienților sistemului pentru a furniza atacatorului sau codului malware cu privilegii administrative.

Ultimii viermi Conficker și ZeuS / LICAT au fost de asemenea atacuri amestecate. Conficker a folosit toate metodele tradiționale de distribuție.

Ce este Reducerea Impactului?

Deși majoritatea companiilor de succes de astăzi sunt conștiente de problemele de securitate comune și depun eforturi considerabile pentru prevenirea acestora, niciun set de practici de securitate nu este eficient de 100%. Deoarece se poate realiza o încălcare în cazul în care miza este mare, companiile și organizațiile trebuie, de asemenea, să fie pregătite să contracareze daunele.
Este important să înțelegem că impactul unui atac nu se referă numai la aspectul tehnic al acestuia, la datele furate, la bazele de date deteriorate sau la deteriorarea proprietății intelectuale, prejudiciul se extinde și la reputația companiei. Răspunsul la o încălcare a datelor este un proces foarte dinamic.
Mai jos sunt câteva măsuri importante pe care o companie ar trebui să le ia atunci când se constată o încălcare a securității, conform mai multor experți în securitate:

- Comunicați problema. Angajații interni ar trebui să fie informați despre această problemă și să fie chemați la acțiune. Pe plan extern, clienții trebuie să fie informați prin comunicări directe și anunțuri oficiale. Comunicarea creează transparență, care este crucială în acest tip de situație.
- Fiți sincer și responsabil în cazul în care compania este vinovată.
- Furnizați detalii. Explicați de ce a avut loc situația și ce a fost compromis. Este, de asemenea, de așteptat ca societatea să aibă grijă de costurile serviciilor de protecție împotriva furtului de identitate pentru clienții afectați.
- Înțelegeți ce a provocat și a facilitat încălcarea. Dacă este necesar, angajați experți în medicina legală pentru a studia și a afla detaliile.
- Aplicați ceea ce a fost învățat din investigația criminalistică pentru a vă asigura că viitoarele încălcări similare nu se vor întâmpla.
- Asigurați-vă că toate sistemele sunt curate, nu au fost instalate spații de depozitare și nimic altceva nu a fost compromis. Atacatorii vor încerca adesea să părăsească o backdoor pentru a facilita viitoare încălcări. Asigurați-vă că acest lucru nu se întâmplă.
- Educarea angajaților, partenerilor și clienților cu privire la modul de prevenire a încălcărilor viitoare.

Capitolul 3: Protejarea datelor și confidențialitatea datelor

Acest capitol se concentrează asupra dispozitivelor dvs. personale și a datelor dvs. personale. Acesta include sfaturi pentru protejarea dispozitivelor, crearea de parole puternice și utilizarea în siguranță a rețelelor wireless. De asemenea, discută despre menținerea în siguranță a datelor.

Datele dvs. online sunt valoroase pentru infractorii cibernetici. Acest capitol acoperă pe scurt

tehnicile de autentificare care vă ajută să vă mențineți în siguranță datele. Acesta acoperă, de asemenea, modalități de îmbunătățire a securității datelor dvs. online, cu sfaturi despre ce să faceți și ce să nu faceți online.

Protejați-vă dispozitivele de calcul

Dispozitivele dvs. de calcul stochează datele dvs. și sunt portalul pentru viața dvs. online. Mai jos este o scurtă listă de pași pe care îi puteți lua pentru a vă proteja dispozitivele de calcul împotriva intruziunii:

- **Păstrați firewall-ul activat** - Dacă este un paravan de protecție software sau un paravan de protecție hardware pe un router, paravanul de protecție ar trebui să fie pornit și actualizat pentru a împiedica hackerii să acceseze datele dvs. personale sau de companie. Faceți clic pe Windows 7, Windows 8 sau Windows 10 pentru a activa paravanul de protecție în versiunea respectivă a Windows. Faceți clic aici pentru a activa firewall-ul pentru dispozitivele Mac OS X.

- **Utilizați antivirus și antispyware** - Software rău intenționat, cum ar fi virusi, cai troieni, viermi, rromi și spyware, sunt instalate pe dispozitivele dvs. de calcul fără permisiunea dvs., pentru a avea acces la computer și date. Virușii vă pot distruge datele, încetini computerul sau prelua computerul. Virușii pot prelua computerul dvs. permitând spammerilor să difuzeze e-mailuri utilizând contul dvs. Spyware-ul vă poate monitoriza activitățile online, vă poate colecta informațiile personale sau puteți crea anunțuri pop-up nedorite pe browserul dvs. web în timp ce sunteți conectat. O regulă bună este să descărcați doar software-ul de pe site-urile web de încredere pentru a evita să obțineți spyware în primul rând. Software-ul antivirus este proiectat pentru a scana computerul și e-mailurile primite pentru viruși și pentru a le șterge. Uneori software-ul antivirus include și programe antispyware. Păstrați actualizarea software-ului pentru a vă proteja calculatorul de cel mai nou software rău intenționat.

- **Gestionați sistemul de operare și browserul dvs.** - Hackerii încearcă întotdeauna să profite de vulnerabilitățile din sistemele de operare și din browserele dvs. web. Pentru a vă proteja computerul și datele, setați setările de securitate pe computer și pe browser la nivel mediu sau superior. Actualizați sistemul de operare al calculatorului,

inclusiv browserele dvs. web, și descărcați și instalați în mod regulat cele mai recente patch-uri software și actualizări de securitate de la furnizori.

- **Protejați toate dispozitivele dvs.** - Dispozitivele dvs. de calcul, fie că sunt computere, laptopuri, tablete sau smartphone-uri, trebuie să fie protejate prin parolă pentru a preveni accesul neautorizat. Informațiile stocate trebuie să fie criptate, în special pentru date sensibile sau confidențiale. Pentru dispozitivele mobile, stocați numai informațiile necesare, în cazul în care aceste dispozitive sunt furate sau pierdute atunci când vă aflați departe de casa dvs. Dacă vreunul dintre dispozitivele dvs. este compromis, infractorii pot avea acces la toate datele dvs. prin intermediul furnizorului dvs. de servicii de stocare în cloud, cum ar fi iCloud sau unitatea Google.

Dispozitivele IoT prezintă un risc și mai mare decât celelalte dispozitive de calcul. În timp ce platformele desktop, laptop și mobile primesc actualizări frecvente de software, majoritatea dispozitivelor IoT au în continuare firmware-ul original. Dacă se constată vulnerabilități în firmware, este posibil ca dispozitivul IoT să rămână vulnerabil. Pentru a face problema mai rău, dispozitivele IoT sunt adesea concepute să sune la domiciliu și să necesite acces la Internet. Pentru a ajunge la Internet, majoritatea producătorilor de dispozitive IoT se bazează pe rețeaua locală a clientului. Rezultatul este că dispozitivele IoT sunt foarte probabil incluse și când sunt, permit accesul la rețeaua și datele locale ale clientului. Cea mai bună modalitate de a vă proteja de acest scenariu este să aveți dispozitive IoT care utilizează o rețea izolată, partajând-o numai cu alte dispozitive IoT.

Vizitati pagina web scaner IoT

Utilizați rețelele fără fir în siguranță

Rețelele fără fir permit dispozitivelor cu funcții Wi-Fi, cum ar fi laptopurile și tabletele, să se conecteze la rețea prin intermediul identificatorului de rețea, cunoscut sub numele de SSID (Service Set Identifier). Pentru a împiedica intruții să intre în rețeaua fără fir acasă, SSID-ul prestabilit și parola implicită pentru interfața administrativă bazată pe browser trebuie modificate. Hackerii vor fi conștienți de acest tip de informații de acces implicite. Mai mult, ar trebui să criptați comunicațiile fără fir, permițând securitatea wireless și caracteristica de criptare WPA2 pe routerul fără fir. Opțional, routerul wireless poate fi configurat să nu

difuzeze SSID, ceea ce adaugă o barieră suplimentară pentru descoperirea rețelei, însă aceasta nu ar trebui considerată o securitate adecvată pentru o rețea fără fir.

Click AICI pentru a afla mai multe despre protejarea dvs. atunci când utilizați rețele fără fir.

Când sunteți departe de casă, un punct public hotspot Wi-Fi vă permite să accesați informațiile dvs. online și să navigați pe Internet. Cu toate acestea, cel mai bine este să nu accesați sau să trimiteți informații personale sensibile prin intermediul unei rețele publice fără fir. Verificați dacă computerul este configurat cu partajarea de fișiere și medii și că necesită autentificarea utilizatorului cu criptare. Pentru a împiedica interceptarea de către cineva a informațiilor dvs. (cunoscută sub numele de "interceptări") în timpul utilizării unei rețele publice fără fir, utilizați tuneluri și servicii VPN criptate. Serviciul VPN vă oferă acces securizat la Internet, cu o conexiune criptată între computerul dvs. și serverul VPN al furnizorului de servicii VPN. Cu un tunel VPN criptat, chiar dacă este interceptată o transmisie de date, aceasta nu este descifrată.

Multe dispozitive mobile, cum ar fi smartphone-uri și tablete, vin cu protocolul wireless Bluetooth. Această capabilitate permite dispozitivelor compatibile Bluetooth să se conecteze și să împărtășească informații. Din nefericire, Bluetooth poate fi exploatat de hackeri pentru a asculta pe anumite dispozitive, să instaleze controale de acces la distanță, să distribuie programe malware și să descarce bateriile. Pentru a evita aceste probleme, țineți Bluetooth dezactivat atunci când nu îl utilizați.

Utilizați parole unice pentru fiecare cont online

Probabil aveți mai multe conturi online și fiecare cont trebuie să aibă o parolă unică. Aceasta este o mulțime de parole de reținut. Cu toate acestea, consecința nefolositoarei parole puternice și unice vă lasă pe dvs. și pe datele dvs. vulnerabile la criminali. Folosind aceeași parolă pentru toate conturile dvs. online este ca și cum ați folosi aceeași cheie pentru toate ușile blocate, dacă un atacator ar trebui să vă descopere parola, el ar avea capacitatea de a accesa tot ceea ce dețineți. Dacă infractorii vă obțin parola prin phishing, de exemplu, ei vor încerca să intre în celelalte conturi online. Dacă utilizați o singură parolă pentru toate conturile, acestea pot intra în toate conturile dvs., pot fura sau șterge toate datele sau pot decide să vă impersoneze.

Folosim atât de multe conturi online, care au nevoie de parole; Este prea mult să-ți amintești. O soluție pentru a evita reutilizarea parolelor sau utilizarea parolelor slabe este utilizarea unui manager de parole. Un manager de parole stochează și criptează toate

parolele dvs. diferite și complexe. Managerul vă poate ajuta apoi să vă conectați automat la conturile dvs. online. Trebuie doar să vă amintiți parola principală pentru a accesa managerul de parole și pentru a gestiona toate conturile și parolele.

Sfaturi pentru alegerea unei parole bune:

- Nu utilizați dicționarul sau numele în nici o limbă
- Nu utilizați scrierea greșită a cuvintelor din dicționar
- Nu utilizați nume de computer sau nume de cont
- Dacă este posibil, folosiți caractere speciale, cum ar fi! @ # $% ^ & * ()
- Utilizați o parolă de zece sau mai multe caractere

Utilizați fraze de acces mai degrabă decât o parolă

Pentru a împiedica accesul fizic neautorizat la dispozitivele dvs. de calcul, utilizați fraze de acces, mai degrabă decât parole. Este mai ușor să creați o fraza de acces lungă decât o parolă, deoarece este în general sub forma unei propoziții, mai degrabă decât a unui cuvânt. Lungimea mai lungă face frazele de acces mai puțin vulnerabile la atacurile cu dicționarul sau forțele brute. Mai mult, o frază de acces poate fi mai ușor de reținut, mai ales dacă vi se cere să schimbați frecvent parola. Iată câteva sfaturi în alegerea parolelor sau a parolelor de acces:

Sfaturi pentru alegerea unei expresii de acces bune:

- Alegeți o declarație semnificativă pentru dvs.
- Adăugați caractere speciale, cum ar fi! @ # $% ^ & * ()
- Cu cât mai mult cu atât mai bine
- Evitați declarații comune sau celebre, de exemplu, versuri dintr-un cântec popular

Chiar și cu accesul la calculatoarele și dispozitivele de rețea protejate, este de asemenea important să vă protejați și să păstrați datele.

Criptați datele

Datele dvs. ar trebui să fie întotdeauna criptate. S-ar putea să credeți că nu aveți secrete și nimic de ascuns, de ce să folosiți criptarea? Poate crezi că nimeni nu vrea datele tale. Cel mai probabil, probabil că nu este adevărat.
Ești gata să-ți arăți toate fotografiile și documentele străinilor? Sunteți gata să împărțiți prietenilor dvs. informațiile financiare stocate pe computer? Doriți să distribuiți publicului larg e-mailurile și parolele de cont?

Acest lucru poate fi și mai dificil dacă o aplicație rău intenționează să vă infecteze computerul sau dispozitivul mobil și să fure informații potențial valoroase, cum ar fi numerele de cont și parolele, precum și alte documente oficiale. Acest tip de informații pot duce la furtul de identitate, la fraudă sau la răscumpărare. Criminalii pot decide să vă cripteze datele și să le facă inutilizabile până când plătiți răscumpărarea.

Ce este criptarea? Criptarea este procesul de conversie a informațiilor într-o formă în care o parte neautorizată nu o poate citi. Numai o persoană de încredere, autorizată cu cheia secretă sau parola poate decripta datele și accesa-o în forma sa originală. Criptarea însăși nu împiedică pe cineva să intercepteze datele. Criptarea poate împiedica o persoană neautorizată să vizualizeze sau să acceseze conținutul.

Programele software sunt utilizate pentru criptarea fișierelor, folderelor și chiar a unităților întregi.
Sistemul de criptare a fișierelor (EFS) este o caracteristică Windows care poate cripta datele. EFS este conectat direct la un anumit cont de utilizator. Numai utilizatorul care a criptat datele va putea accesa după ce a fost criptat utilizând EFS. Pentru a cripta datele utilizând EFS în toate versiunile de Windows, urmați acești pași:

Pasul 1. Selectați unul sau mai multe fișiere sau dosare.
Pasul 2. Faceți clic dreapta pe datele selectate> Proprietăți.
Pasul 3. Faceți clic pe Advanced ...
Pasul 4. Selectați caseta de selectare Criptare conținuturi pentru securizarea datelor.
Pasul 5. Fișierele și folderele care au fost criptate cu EFS sunt afișate în verde, după cum se arată în figură.

Faceți o copie de rezervă a datelor dvs

Unitatea hard disk se poate strica. Laptopul tău ar putea fi pierdut. Telefonul tău inteligent furat. Poate ați șters versiunea originală a unui document important. O rezervă poate

împiedica pierderea unor date de neînlocuit, cum ar fi fotografii de familie. Pentru a face copii de siguranță ale datelor, veți avea nevoie de o locație suplimentară de stocare pentru date și trebuie să copiați datele în locația respectivă în mod regulat și automat.

Locația suplimentară pentru fișierele cu copii de rezervă poate fi în rețeaua dvs. de domiciliu, în locația secundară sau în cloud. Prin stocarea backup-ului datelor local, aveți control total asupra datelor. Puteți decide să copiați toate datele pe un dispozitiv de stocare atașat la rețea (NAS), pe o unitate hard disk externă externă sau poate selectați doar câteva foldere importante pentru copierea de rezervă pe unități de memorie, pe CD-uri / DVD-uri sau chiar pe casete. În acest scenariu, sunteți proprietarul și sunteți total responsabil pentru costul și întreținerea echipamentului dispozitivului de stocare. Dacă vă abonați la un serviciu de stocare în cloud, costul depinde de cantitatea de spațiu de stocare necesară. Cu un serviciu de stocare în cloud ca Amazon Web Services (AWS), aveți acces la datele de rezervă, atâta timp cât aveți acces la contul dvs. Când vă abonați la serviciile de stocare online, este posibil să fie nevoie să fiți mai selectivi în privința datelor care sunt salvate în urma costurilor de stocare și a transferurilor constante de date online. Unul dintre avantajele stocării unei copii de siguranță într-o locație alternativă este că este sigur în caz de incendiu, furt sau alte catastrofe, altele decât eșecul dispozitivului de stocare.

Ștergerea permanentă a datelor dvs.

Pentru a șterge datele astfel încât acestea să nu mai poată fi recuperate, datele trebuie să fie suprascrise cu altele și zerouri de mai multe ori. Pentru a preveni recuperarea fișierelor șterse, este posibil să aveți nevoie să utilizați instrumente special create pentru a face acest lucru. Programul SDelete de la Microsoft (pentru Vista și versiuni ulterioare) pretinde că are capacitatea de a elimina complet fișierele sensibile. Shred pentru Linux și coșul de gunoi securizat pentru Mac OSX sunt câteva instrumente care pretind că furnizează un serviciu similar.

Singura modalitate de a fi siguri că datele sau fișierele nu sunt recuperabile este de a distruge fizic hard disk-ul sau dispozitivul de stocare. A fost nebunia multor infractori în a gândi că dosarele lor erau impenetrabile sau irecuperabile.

Pe lângă stocarea datelor pe hard discurile locale, datele dvs. pot fi de asemenea stocate online în cloud. Aceste copii vor trebui, de asemenea, să fie șterse. Ia-ți un moment să te

întrebi: "Unde îmi salvez datele? Este susținută undeva? Este criptat? Când trebuie să ștergeți datele sau să scăpați de un hard disk sau un computer, întrebați-vă: "Am păstrat datele pentru a nu lăsa să cadă în mâinile greșite?"

Autentificare cu doi factori

Serviciile online populare, cum ar fi Google, Facebook, Twitter, LinkedIn, Apple și Microsoft, utilizează autentificarea cu doi factori pentru a adăuga un nivel suplimentar de securitate pentru logarea contului. Pe lângă numele de utilizator și parola sau numărul personal de identificare (PIN) sau model, autentificarea cu doi factori necesită un al doilea simbol, cum ar fi:

• Obiect fizic - card de credit, card bancar, telefon sau fob
• Scanare biometrică - amprentă digitală, imprimare palmă, precum și recunoaștere facială sau vocală

Chiar și cu autentificarea cu două factori, hackerii pot obține acces la conturile dvs. online prin atacuri precum atacurile de tip phishing, programele malware și ingineria socială.

Du-te aici pentru a afla dacă site-urile pe care le vizitați utilizează autentificarea cu doi factori.

Autorizația deschisă (OAuth)

Autorizația deschisă (OAuth) este un protocol standard deschis, care permite unui utilizator final să acceseze aplicații terțe, fără a expune parola utilizatorului. OAuth acționează ca omul din mijloc pentru a decide dacă permite accesul utilizatorilor finali la aplicații terțe. De exemplu, spuneți că doriți să accesați aplicația web XYZ și nu aveți un cont de utilizator pentru a accesa această aplicație web. Cu toate acestea, XYZ are opțiunea de a vă permite să vă conectați utilizând acreditările de pe un site web social media ABC. Deci, accesați site-ul web utilizând login-ul social media.

Pentru ca acest lucru să funcționeze, aplicația "XYZ" este înregistrată cu "ABC" și este o aplicație aprobată. Când accesați XYZ, utilizați acreditările utilizatorului pentru ABC. Apoi, XYZ solicită un semn de acces de la ABC în numele dvs. Acum aveți acces la XYZ. XYZ nu știe nimic despre dvs. și acreditările dvs. de utilizator, iar această interacțiune este absolut fără probleme pentru utilizator. Utilizarea jetoanelor secrete împiedică o aplicație rău intenționată să obțină informațiile și datele dvs.

Nu distribui prea multe informații pe mediile de socializare

Dacă doriți să vă păstrați intimitatea pe social media, împărtășiți cât mai puține informații. Nu ar trebui să distribuiți informații despre data de naștere, adresa de e-mail sau numărul dvs. de telefon în profilul dvs. Persoanele care au nevoie să știe informațiile tale personale probabil știu deja. Nu completați complet profilul dvs. de mass-media socială, oferiți doar informațiile minime necesare. Mai mult, verificați setările media sociale pentru a permite numai persoanelor pe care le cunoașteți să vă vadă activitățile sau să se angajeze în conversațiile dvs.

Cu cât distribuiți mai multe informații personale online, cu atât este mai ușor ca cineva să creeze un profil despre dvs. și să profite de dvs. offline.

Ați uitat vreodată numele de utilizator și parola pentru un cont online? Chestiunile de securitate cum ar fi "Care este numele fetei mamei tale?" Sau "În ce oraș te-ai născut?" Ar trebui să te ajute să ții contul în siguranță de la intruși. Cu toate acestea, oricine dorește să vă acceseze conturile poate căuta răspunsurile de pe Internet. Puteți răspunde la aceste întrebări cu informații false, atâta timp cât vă puteți aminti răspunsurile false. Dacă aveți o problemă de reținere a acestora, puteți utiliza managerul de parole pentru a le gestiona pentru dvs.

Confidențialitatea pe Email și browser

În fiecare zi, milioane de mesaje de e-mail sunt folosite pentru a comunica cu prietenii și a desfășura afaceri. E-mailul este o modalitate convenabilă de a comunica rapid între ele. Când trimiteți un e-mail, este similar cu trimiterea unui mesaj utilizând o carte poștală. Mesajul cu cartea poștală este transmis prin vedere directă oricărei persoane care are acces la aspect, iar mesajul e-mail este transmis în text simplu și poate fi citit de oricine are acces. Aceste comunicații sunt, de asemenea, transmise între diferite servere în timpul deplasării către destinație. Chiar și atunci când ștergeți mesajele de e-mail, mesajele pot fi arhivate pe serverele de e-mail de ceva timp.

Oricine are acces fizic la computerul dvs. sau la ruterul dvs., poate vizualiza site-urile web pe care le-ați vizitat utilizând istoricul browser-ului web, memoria cache și eventual fișierele de jurnal. Această problemă poate fi redusă la minimum prin activarea modului de navigare

privat din browserul web. Cele mai multe dintre browserele web populare au propriul nume pentru modul browser privat:

- **Microsoft Internet Explorer**: InPrivate
- **Google Chrome**: Incognito
- **Mozilla Firefox**: Private tab / private window
- **Safari**: Private: Private browsing

Cu modul privat activat, cookie-urile sunt dezactivate, iar fișierele Internet temporare și istoricul navigării sunt eliminate după închiderea ferestrei sau a programului.

Păstrarea istoricului dvs. privat de navigare pe Internet poate împiedica pe alții să adune informații despre activitățile dvs. online și vă atrage să cumpărați ceva cu anunțuri direcționate. Chiar și în cazul în care navigarea privată este activată, iar cookie-urile sunt dezactivate, companiile dezvoltă diferite modalități de amprentare a utilizatorilor pentru a culege informații și a urmări comportamentul utilizatorilor. De exemplu, dispozitivele intermediare, cum ar fi routerele, pot avea informații despre istoricul navigării pe web a unui utilizator.

În cele din urmă, este responsabilitatea dvs. să vă protejați datele, identitatea și dispozitivele dvs. de calcul. Când trimiteți un e-mail, trebuie să includeți fișele medicale? Data viitoare când navigați pe Internet, este transmisia dvs. sigură? Doar câteva precauții simple vă pot salva problemele mai târziu.

Capitolul 4: Protecția organizației

În acest capitol se discută despre o parte din tehnologiile și procesele folosite de profesioniști în domeniul securității informatice atunci când securizează rețeaua, echipamentele și datele organizației. În primul rând, acesta acoperă pe scurt multe tipuri de firewall-uri, dispozitive de securitate și software-uri care sunt utilizate în prezent, inclusiv cele mai bune practici.

Apoi, acest capitol explică botneturile, lanțul kill, securitatea bazată pe comportament și utilizarea NetFlow pentru a monitoriza o rețea.

Cea de-a treia secțiune discută abordarea Cisco privind securitatea informatică, inclusiv echipa CSIRT și agenda de securitate. Acesta acoperă pe scurt instrumentele pe care profesioniștii din domeniul securității informatice le utilizează pentru a detecta și a preveni atacurile de rețea.

Tipuri de Firewall

Un firewall este un perete sau o partiție care este proiectată pentru a preveni răspândirea focului dintr-o parte a unei clădiri în alta. În rețelele de calculatoare, un firewall este proiectat să controleze sau să filtreze ce comunicații sunt permise să inre sau să iasă dintr-un dispozitiv sau rețea, așa cum se arată în figură. Un paravan de protecție poate fi instalat pe un singur computer în scopul de a proteja acel computer (firewall bazat pe gazdă) sau poate fi un dispozitiv de rețea autonom care protejează o întreagă rețea de computere și toate dispozitivele gazdă din acea rețea (Firewall bazat pe rețea).
De-a lungul anilor, deoarece atacurile de calculator și de rețea au devenit mai sofisticate, s-au dezvoltat noi tipuri de firewall-uri care servesc unor scopuri diferite în protejarea unei rețele. Iată o listă de tipuri comune de firewall:

- Firewall Layer Firewall - filtrarea pe baza adreselor IP sursă și de destinație
- Firewall Layer Transport - filtrarea bazată pe porturile de date sursă și de destinație și filtrarea pe baza stărilor de conexiune
- Firewall Layer Application -filtering bazat pe aplicație, program sau serviciu
- Context Aware Application Firewall - filtrarea bazată pe utilizator, dispozitiv, rol, tipul aplicației și profilul de amenințare
- Proxy Server - filtrarea cererilor de conținut web precum URL, domeniu, media etc.
- Reverse Proxy Server - plasat în fața serverelor web, serverele proxy reverse protejează, ascund, elimină și distribuie accesul la serverele web
- Paravanul de traducere a adreselor de rețea (NAT) - ascunde sau maschează adresele private ale gazdelor de rețea

- Firewall bazat pe gazdă - filtrarea porturilor și a apelurilor pentru servicii de sistem pe un singur sistem de operare

Scanarea porturilor

Scanarea porturilor este un proces de scanare a unui computer, a unui server sau a altei gazde de rețea pentru porturile deschise. În rețea, fiecărei aplicații care rulează pe un dispozitiv i se atribuie un identificator denumit un număr de port. Acest număr de port este utilizat la ambele capete ale transmisiei, astfel încât datele corecte să fie transmise aplicației corecte. Scanarea prin port poate fi folosită premeditat, cu rea intenție, ca instrument de recunoaștere pentru a identifica sistemul de operare și serviciile care rulează pe un computer sau o gazdă sau poate fi utilizat inofensiv de către un administrator de rețea pentru a verifica politicile de securitate ale rețele.

În scopul evaluării firewall-ului rețelei proprii și a securității portului, puteți utiliza un instrument de scanare a portului ca Nmap pentru a găsi toate porturile deschise din rețea. Scanarea prin port poate fi văzută ca un precursor al unui atac de rețea și, prin urmare, nu ar trebui făcută pe servere publice pe Internet sau într-o rețea a companiei fără permisiune.

Pentru a executa o scanare port Nmap a unui computer în rețeaua locală locală, descărcați și lansați un program precum Zenmap, furnizați adresa IP țintă a computerului pe care doriți să îl scanați, alegeți un profil de scanare implicit și apăsați scanarea. Scanarea Nmap va raporta orice servicii care rulează (de exemplu, servicii web, servicii de poștă electronică etc.) și numere de porturi. Scanarea unui port are ca rezultat, în general, una din cele trei răspunsuri:

- Deschis sau Acceptat - Gazda a răspuns că un serviciu ascultă pe port.
- închise, respinse sau nedorite - Host-ul a răspuns că indică faptul că conexiunile vor fi interzise portului.
- Filtrare, Dropped sau Blocat - Nu a existat nici un răspuns de la gazdă.

Pentru a executa o scanare de port a rețelei din afara rețelei, va trebui să inițiați scanarea din afara rețelei. Aceasta va implica rularea unui port de scanare Nmap impotriva firewall-ului sau a adresei IP publice a routerului. Pentru a descoperi adresa IP publică, utilizați un motor de căutare, cum ar fi Google, cu interogarea "care este adresa mea IP". Motorul de căutare va returna adresa dvs. publică IP.

Pentru a rula o scanare port pentru șase porturi comune împotriva ruterului dvs. de acasă sau a paravanului de protecție, accesați Nmap Online Scanner Port la adresa https://hackertarget.com/nmap-online-port-scanner/ și introduceți adresa IP publică în intrare Caseta: adresa IP pentru scanare ... și apăsați Scanare rapidă Nmap. Dacă răspunsul este deschis pentru oricare dintre porturi: 21, 22, 25, 80, 443 sau 3389, cel mai probabil, a fost activată redirecționarea portului pe router sau firewall și executați servere în rețeaua dvs. privată, după cum se arată În figură.

Echipamente de securitate

Astăzi nu există un singur dispozitiv de securitate sau o tehnologie care să rezolve toate cerințele de securitate a rețelei. Deoarece există o varietate de aparate și instrumente de securitate care trebuie implementate, este important ca toate să lucreze împreună. Aparatele de securitate sunt cele mai eficiente atunci când fac parte dintr-un sistem.

Aparatele de securitate pot fi dispozitive independente, cum ar fi un router sau un firewall, un card care poate fi instalat într-un dispozitiv de rețea sau un modul cu procesor propriu și memorie memorată în cache. Aparatele de securitate pot fi, de asemenea, unelte software-uri care se execută pe un dispozitiv de rețea. Aparatele de securitate intră în aceste categorii generale:

Routere - Routerele ISR (Cisco Integrated Services Router) au multe capabilități de firewall în afară de funcțiile de rutare, inclusiv filtrarea traficului, capacitatea de a rula un sistem de prevenire a intruziunilor (IPS), criptare și capabilități VPN pentru tuneluri criptate securizate .

Firewall-urile - firewall-urile Cisco Next Generation au toate capabilitățile unui router ISR, precum și gestionarea și analiza avansată a rețelelor.

IPS - dispozitivele Cisco Next Generation Cisco sunt destinate prevenirii intruziunilor.

VPN - dispozitivele de securitate Cisco sunt echipate cu un server de rețele private virtuale (VPN) și cu tehnologii client. Este proiectat pentru tuneluri criptate securizate.

Malware / Antivirus - protecția avansată împotriva programelor malware Cisco (AMP) vine în următoarea generație de rutere Cisco, firewall-uri, dispozitive IPS, dispozitive de securitate pentru Web și e-mail și pot fi de asemenea instalate ca software în computerele gazdă.

Alte dispozitive de securitate - Această categorie include dispozitive de securitate pentru web și e-mail, dispozitive de decriptare, servere de control al accesului clienților și sisteme de gestionare a securității.

Detectarea atacurilor în timp real

Software-ul nu este perfect. Atunci când un hacker exploatează un defect într-o bucată de software înainte ca creatorul să o rezolve, este cunoscută ca un atac de ziua zero. Datorită modului complicat și vast al atacurilor de zi zero întâlnite astăzi, devine comun faptul că atacurile de rețea vor reuși și că o apărare reușită este acum măsurată în cât de repede o rețea poate răspunde la un atac. Abilitatea de a detecta atacurile în timp real, precum și oprirea atacurilor imediat sau în câteva minute de la apariția lor este obiectivul ideal. Din nefericire, multe companii și organizații de astăzi nu reușesc să detecteze atacurile câteva zile sau chiar luni după ce au avut loc.

- **Scanarea în timp real** de la Edge la Endpoint - Detectarea atacurilor în timp real necesită scanare activă a atacurilor utilizând firewall-uri și dispozitive de rețea IDS / IPS. Următoarea generație de detecție malware client / server cu conexiuni la centrele globale de amenințare online trebuie de asemenea să fie utilizată. Astăzi, dispozitivele și soft-urile de scanare active trebuie să detecteze anomaliile de rețea utilizând analiza bazată pe context și detectarea comportamentului.

- **Atacurile DDoS și răspunsul în timp real -** DDoS este una dintre cele mai mari amenințări de atac care necesită răspuns în timp real și detectare. Este extrem de greu să te aperi împotriva unui atac DDoS, deoarece atacurile provin de la sute sau mii de gazde zombie, iar atacurile par a fi trafic legitim, așa cum se arată în figură. Pentru multe companii și organizații, atacurile DDoS care au loc în mod regulat împiedică serverele și rețelele să fie disponibilitatea. Capacitatea de a detecta și de a răspunde atacurilor DDoS în timp real este crucială.

Protejarea împotriva programelor malware

Cum vă asigurați apărarea împotriva prezenței constante a atacurilor de zero zile, precum și a amenințărilor persistente avansate (APT) care fură date pe perioade lungi de timp? O soluție este folosirea unei soluții avansate de detectare a malware-urilor la nivel de întreprindere, care oferă detectarea malware în timp real.
Administratorii de rețea trebuie să monitorizeze constant rețeaua pentru a observa semne de malware sau comportamente care dezvăluie prezența unui APT. Cisco are o grila de protectie avansată împotriva amenințărilor malware (AMP), care analizează milioane de fișiere și le corelează cu sute de milioane de alte artefacte malware analizate. Aceasta oferă o imagine globală asupra atacurilor, campaniilor și distribuției malware. AMP este un software client / server implementat pe obiectivele gazdă, ca server independent sau pe alte dispozitive de securitate a rețelei. Figura prezintă avantajele rețelei AMP Threat Grid.

Cele mai bune practici de securitate

Multe organizații naționale și profesionale au publicat liste cu cele mai bune practici de securitate. Următoarea este o listă a celor mai bune practici de securitate:

Efectuați evaluarea riscurilor - cunoașterea valorii datelor celor pe care le protejezi va ajuta la justificarea cheltuielilor de securitate.

- **Creați o politică de securitate** - Creați o politică care să descrie în mod clar regulile companiei, sarcinile de muncă și așteptările.

- **Măsuri de securitate fizică -** restricționați accesul la dulapurile de rețea, la locațiile serverului, precum și la suprimarea incendiilor.

- **Măsuri de securitate a resurselor umane** - Angajații trebuie să fie evaluați în mod corespunzător.

- Efectuați și testați copii de rezervă - efectuați copii de siguranță periodice și testați recuperarea datelor din copiile de rezervă.
- Păstrați patch-uri și actualizări de securitate - Actualizați în mod regulat sisteme și programe de operare pentru servere, clienți și dispozitive de rețea.
- Utilizați Controalele de acces - Configurați rolurile utilizatorilor și nivelurile de privilegii, precum și autentificarea puternică a utilizatorilor.
- Testați periodic răspunsul la incidente - Utilizați o echipă de răspuns la incidente și testați scenariile de răspuns la situații de urgență.

-

- Implementați un instrument de monitorizare a rețelei, analiză și gestionare - alegeți o soluție de monitorizare a securității care se integrează cu alte tehnologii.
- Implementarea dispozitivelor de securitate a rețelei - Utilizați routere de generație nouă, firewall-uri și alte dispozitive de securitate.
- Implementarea unei soluții complete de securitate pentru endpoint - Utilizați antimalware la nivel de întreprindere și software antivirus.
- Educarea utilizatorilor - educarea utilizatorilor și a angajaților prin proceduri sigure.
- Criptarea datelor - Criptați toate datele delicate ale companiei, inclusiv e-mailurile.

mergi aici pentru a afla mai multe despre SANS și tipurile de instruire și certificări pe care le oferă.

Unele dintre cele mai utile ghiduri se găsesc în arhivele organizaționale, cum ar fi National Institute of Standards and Technology (NIST) Computer Security Resource Center.

Una dintre cele mai cunoscute și respectate organizații de formare în domeniul securității informatice este Institutul SANS.

Botnet

Un botnet este un grup de but-uri, conectate prin Internet, cu capacitatea de a fi controlate de un individ sau de un grup rău intenționat. Un computer infectat bot este de obicei infectat vizitând un site web, deschizând un atașament de e-mail sau deschizând un fișier media infectat.

Un botnet poate avea zeci de mii sau chiar sute de mii de bot-i. Aceștia pot fi activați pentru a distribui programe malware, pentru a lansa atacuri DDoS, pentru a distribui e-mailuri spam sau pentru a executa atacuri de forță bruta. Botnet-urile sunt controlate de obicei prin intermediul unui server de comandă și de control.

Criminalii cibernetici vor închiria adesea Botnets, contra unei taxe, unor terțe părți în scopuri nefaste.

Kill Chain in apărrea cibernetică

În securitatea cibernetică, Kill Chain reprezintă etapele unui atac al sistemelor informatice. Dezvoltat de Lockheed Martin ca un cadru de securitate pentru detectarea și răspunsul la incidente, Cyber Kill Chain este alcătuit din următoarele etape:

Etapa 1. Recunoaștere - atacatorul culege informații despre țintă.
Etapa 2. Weaponization - Atacatorul creează un exploit și o încărcătură rău intenționată pentru a o trimite către țintă.
Etapa 3. Livrare - atacatorul trimite exploatarea și încărcătura utilă rău intenționat prin e-mail sau altă metodă.
Etapa 4. Exploatare - Exploatarea este executată.
Etapa 5 Instalare - Malware-ul și backdoor-ul sunt instalate la țintă.
Etapa 6. Comandă și control - Controlul la distanță al țintei este obținut printr-un canal de comandă și de control sau un server.
Etapa 7. Acțiune - atacatorul efectuează acțiuni rău intenționate precum furtul de informații sau execută atacuri suplimentare asupra altor dispozitive din cadrul rețelei, trecând din nou prin etapele Kill Chain.

Pentru a apăra împotriva Kill Chain, sistemele de securitate ale rețelei sunt proiectate în jurul etapelor Kill Chain. Acestea sunt câteva întrebări legate de securitatea unei companii, bazate pe Cyber Kill Chain:
• Care sunt indicatorii de atac în fiecare etapă a "Kill Chain"?
• Care instrumente de securitate sunt necesare pentru a detecta indicatorii de atac în fiecare etapă?
• Există lacune în capacitatea companiei de a detecta un atac?

Potrivit lui Lockheed Martin, înțelegerea etapelor lui Kill Chain le-a permis să pună obstacole în defensivă, să încetinească atacul și, în cele din urmă, să prevină pierderea datelor..

Securitatea bazată pe comportament

Securitatea bazată pe comportament este o formă de detectare a amenințărilor care nu se bazează pe semnături rău intenționate, ci folosește contextul informațional pentru detectarea anomaliilor din rețea. Depanarea bazată pe comportament implică captarea și analizarea fluxului de comunicare între un utilizator din rețeaua locală și o destinație locală sau la distanță. Aceste comunicări, atunci când sunt capturate și analizate, dezvăluie contextul și modelele de comportament care pot fi folosite pentru detectarea anomaliilor.

Depanarea bazată pe comportament poate descoperi prezența unui atac printr-o schimbare față de comportamentul normal.

- Honeypots - Un Honeypot este un instrument de detectare bazat pe comportament care atrage atacantul în primul rând apelând la modelul prezis de atacator al comportamentului rău intenționat, iar apoi, în interiorul honeypot-ului, administratorul de rețea poate captura, loga și analiza comportamentul atacatorului . Acest lucru permite unui administrator să câștige mai multe cunoștințe și să construiască o apărare mai bună.

- Arhitectura soluției de apărare a amenințărilor Cyber împotriva amenințărilor Cyber - Aceasta este o arhitectură de securitate care utilizează detectarea și indicatorii bazați pe comportament, pentru a asigura o vizibilitate mai mare, un context și un control mai bun. Scopul este să știe cine, ce, unde, când, și cum are loc un atac. Această arhitectură de securitate utilizează multe tehnologii de securitate pentru a atinge acest obiectiv.

NetFlow

Tehnologia NetFlow Cisco este utilizată pentru a culege informații despre datele care circulă printr-o rețea. Informațiile NetFlow pot fi comparate cu o factură telefonică pentru traficul de rețea. Vă arată ce dispozitive sunt în rețeaua dvs., precum și când și cum au accesat utilizatorii dispozitivele dvs. în rețea. NetFlow este o componentă importantă în detectarea și analiza comportamentală. Switch-urile Cisco, routerele și firewall-urile echipate cu NetFlow pot raporta informații despre datele care intră, părăsesc și călătoresc prin rețea. Informațiile sunt trimise colectorilor NetFlow care colectează, stochează și analizează înregistrările NetFlow.

NetFlow este capabil să colecteze informații privind utilizarea prin multe caracteristici diferite ale modului în care sunt mutate datele prin rețea, după cum se arată în figură. Prin colectarea informațiilor despre fluxurile de date din rețea, NetFlow este capabil să stabilească comportamente de bază pe mai mult de 90 de atribute diferite.

CERT.RO

https://www.cert.ro/

Multe organizații mari au o echipă de răspuns la incidentele de securitate a calculatoarelor pentru a primi, a examina și a răspunde rapoartelor privind incidentele de securitate a computerului. Misiunea principală a CSIRT este de a contribui la asigurarea securității companiei, sistemului și conservarea datelor realizând investigații cuprinzătoare privind incidentele de securitate informatică. Pentru a preveni incidentele de securitate, Cisco CSIRT oferă o evaluare proactivă a amenințărilor, planificarea atenuării, analiza tendințelor incidentelor și revizuirea arhitecturii de securitate.

CSIRT colaborează cu Forumul de răspunsuri și echipele de securitate (FIRST), National Exchange of Information Exchange (NSIE), Exchange Security Information Exchange (DSIE) și Centrul de analiză și cercetare a DNS (DNS-OARC).
Există organizații CSIRT naționale și publice, cum ar fi divizia CERT a Institutului de Inginerie Software de la Universitatea Carnegie Mellon, care sunt disponibile pentru a ajuta organizațiile și CSIRT-urile naționale să dezvolte, să opereze și să-și îmbunătățească capabilitățile de gestionare a incidentelor.

In Romania: **CERT.RO: https://www.cert.ro/**

ț

Manual (Playbook) securitate cibernetică

Tehnologia se schimbă în mod constant. Asta inseamna ca si atacurile cibernetice evolueaza. Noi vulnerabilități și metode de atac sunt descoperite continuu. Securitatea devine o preocupare importantă din cauza reputației și a impactului financiar rezultat din încălcarea securității. Atacurile vizează rețelele critice și datele sensibile. Organizațiile ar trebui să aibă planuri de a se pregăti pentru, de a face față și de a le recupera de la o încălcare.

Una dintre cele mai bune modalități de a se pregăti pentru o încălcare a securității este de a preveni una. Ar trebui să existe metode de identificare a riscurilor de securitate cibernetică pentru sisteme, active, date și capabilități, protejarea sistemului prin implementarea măsurilor de protecție și pregătirea personalului și detectarea cât mai curând a evenimentului de securitate cibernetică. Atunci când se constată o încălcare a securității, ar trebui luate măsuri adecvate pentru a minimiza impactul și daunele. Planul de răspuns trebuie să fie flexibil, cu multiple opțiuni de acțiune în timpul încălcării. După ce încălcarea este limitată și sistemele și serviciile compromise sunt restaurate, măsurile de securitate și procesele ar trebui să fie actualizate pentru a include lecțiile învățate în timpul încălcării.

Toate aceste informații trebuie compilate într-un manual de securitate. Un manual de securitate este o colecție de interogări repetate (rapoarte) împotriva surselor de date de evenimente de securitate care duc la detectarea și răspunsul la incidente. În mod ideal, agenda de securitate trebuie să realizeze următoarele acțiuni:

- Detectarea mașinilor infectate cu programe malware.
- Detectarea activității de rețea suspecte.
- Detectarea încercărilor de autentificare neregulată.
- Descrierea și înțelegerea traficul de intrare și de ieșire.

- Oferă informații sumare, inclusiv tendințe, statistici.
- Oferă acces rapid și ușor la statistici și la valori.
- Corelează evenimentele în toate sursele de date relevante.

Instrumente pentru prevenirea și detectarea incidentelor

Acestea sunt câteva dintre instrumentele utilizate pentru detectarea și prevenirea incidentelor de securitate:

- Sistemul SIEM (SIEM) este un software care colectează și analizează alerte de securitate, jurnale și alte date în timp real și istorice de la dispozitivele de securitate din rețea.

- DLP - Software de prevenire a pierderilor de date (DLP) este un sistem software sau hardware conceput pentru a împiedica furtul de date drintro rețea. Un sistem DLP se poate concentra pe autorizarea accesului la fișiere, schimbul de date, copierea datelor, monitorizarea activității utilizatorilor și multe altele. Sistemele DLP sunt concepute pentru a monitoriza și proteja datele în trei stări diferite: date în utilizare, date în mișcare și date în repaus. Datele în uz sunt focalizate pe client, datele în mișcare se referă la date în timp ce călătoresc prin rețea, iar datele în repaus se referă la stocarea datelor.

- Cisco ISE și TrustSec - Cisco Identity Services Engine (Cisco ISE) și Cisco TrustSec impun accesul la resursele de rețea prin crearea unor politici de control al accesului pe bază de roluri, care să asigure accesul la rețea (oaspeți, utilizatori mobili, angajați) fără complexitate sporită. Clasificarea traficului se bazează pe identitatea utilizatorului sau a dispozitivului. Faceți clic pe redare în figură pentru a afla mai multe despre ISE.

IDS and IPS

Un sistem de detecție a intruziunilor (IDS), prezentat în figură, este fie un dispozitiv dedicat de rețea, fie unul din mai multe instrumente dintr-un server sau un firewall care scanează date împotriva unei baze de date de reguli sau semnături de atac, căutând trafic rău intenționat. Dacă se detectează o potrivire, IDS va înregistra detectarea și va crea o alertă pentru un administrator de rețea. Sistemul de detecție a intruziunilor nu ia măsuri atunci când se detectează o potrivire, astfel încât nu împiedică apariția atacurilor. Funcția IDS este doar de a detecta, înregistra și raporta.

Scanarea efectuată de IDS încetinește rețeaua (cunoscută sub numele de latență). Pentru a preveni întârzierea în rețea, un IDS este, de obicei, plasat offline, separat de traficul obișnuit în rețea. Datele sunt copiate sau oglindite de un switch și apoi redirecționate către IDS pentru detectarea offline. Există, de asemenea, instrumente IDS care pot fi instalate în partea superioară a sistemului de operare al unui computer gazdă, cum ar fi Linux sau Windows.

Un sistem de prevenire a intruziunilor (IPS) are capacitatea de a bloca sau de a refuza traficul bazat pe o potrivire pozitivă a regulii sau semnăturii. Unul dintre cele mai cunoscute sisteme IPS / IDS este Snort. Versiunea comercială a lui Snort este Sourcefire de la Cisco. Sourcefire are capacitatea de a efectua analize în timp real privind traficul și porturile, logarea, căutarea și potrivirea conținutului și poate detecta sonde, atacuri și scanări port. Se integrează, de asemenea, cu alte instrumente de terță parte pentru raportare, performanță și analiză a jurnalului.

Capitolul 5: Certificări în domeniul securității cibernetice

Acest capitol acoperă căile de urmat dacaţă doriți sa obțineți certificări recunoscute la nivel globsal în domeniul securității cibernetice.

Pagina NetAcad Advantage din netacad.com oferă informații bune pentru a vă ajuta să scrieți un cv minunat și să vă pregătiți pentru un interviu de angajare. De asemenea, conține liste pentru locurile de muncă Cisco și Cisco Partner. Trei motoare externe de căutare de locuri de muncă pe Internet sunt prezentate pentru a vă explora.

Academia Cisco Networking Academy oferă multe cursuri pentru a vă pregăti să faceți examene de certificare Cisco, precum și alte examene de certificare.
Conectați-vă la Cisco Networking Academy și mergeți aici pentru a vedea o listă de cursuri disponibile. Multe dintre aceste cursuri sunt legate de o industrie sau certificare Cisco. Aceasta înseamnă că, după ce finalizați cu succes cursul, veți fi pregătit să susțineți examenul de certificare. Faceți clic aici pentru a vedea videoclipul "Devino un Cyberhero".

Mergi aici pentru a vedea o listă de certificări care sunt susținute de cursurile Cisco Networking Academy. Certificarea în anumite domenii ale Tehnologiei Internet (IT) este adesea o cerință pentru locurile de muncă pentru securitatea informatică.
Mergi aici pentru a citi povestiri despre studenții și instructorii Cisco care au un impact pe tot globul.
Compania pentru Tehnologia Industriei de Calcul (CompTIA) este un alt furnizor care oferă certificări de securitate. Certificarea CompTIA Security + acoperă principiile necesare pentru securitatea rețelei și gestionarea riscurilor. Această certificare poate fi o piatră de temelie importantă a unei cariere în materie de securitate IT. Accesați aici pentru a citi mai multe informații despre certificarea Security +.

Advanced Certification Opportunities

Desemnarea specialiștilor certifică faptul că profesioniștii din domeniul tehnic au expertiză în domenii precum rețele industriale, computere unificate, programabilitate în rețea și multe altele. Există certificări de carieră Cisco la nivel asociat, profesional sau expert. Prin câștigarea certificărilor specializate, profesioniștii din rețea își pot îmbunătăți cunoștințele legate de rețele de bază în tehnologii, cum ar fi securitatea, centrul de date sau video. Accesați aici pentru a afla mai multe despre structura de certificare și pentru a obține acces la detalii despre toate certificările oferite de Cisco.

Multe certificări de specializare se aliniază cerințelor programului Cisco Partner Specialization.
Certificările de securitate avansate de la alte organizații, precum (ISCP) ^ 2 și SANS, oferă instruiri, oportunități de certificare și alte resurse ale profesioniștilor din domeniul securității informatice.

Cariere în Cybersecurity

Descoperiți modalități de avansare a carierei prin accesarea unei varietăți de resurse pe site-ul nconceput special pentru studenții Cisco Networking Academy. Site-ul oferă resurse valoroase pentru a vă ajuta să vă pregătiți pentru a fi o parte a forței de muncă și a căuta cu succes locuri de muncă, inclusiv:

- Sfaturi privind solicitarea unui loc de muncă, crearea unui CV impresionant și cum să vă pregătiți pentru interviuri
- Accesul la o căutare de locuri de muncă exclusivă, care oferă mii de oportunități de locuri de muncă pe plan mondial în întreaga lume cu partenerii Cisco și Cisco
- Webinarii care îți dezvoltă abilitățile de carieră
- Sfaturi pentru îmbunătățirea abilităților de carieră non-tehnice
- Sfaturi privind studierea examenelor dvs. de certificare
- Idei privind modul de obținere a experienței înainte de a intra în forța de muncă

Alte locuri de muncă in domeniul securității cibernetice

Multe alte întreprinderi și industrii recrutează profesioniști în domeniul securității informatice. Există mai multe motoare de căutare online care vă ajută să găsiți locul potrivit în domeniul securității informatice:

- ITJobMatch –. Motorul de căutare ITJobMatch este specializat în locuri de muncă IT de toate felurile, pe tot globul.

- Monster – Monster este un motor de căutare pentru toate tipurile de locuri de muncă. Linkul furnizat se îndreaptă direct către locurile de muncă în domeniul securității informatice.
  CareerBuilder – CareerBuilder este, de asemenea, un motor de căutare pentru toate tipurile de locuri de muncă. Linkul furnizat se îndreaptă direct către locurile de muncă în domeniul securității informatice.

Acestea sunt doar trei dintre numeroasele site-uri de căutare online a locurilor de muncă. Chiar dacă începeți să vă învățați în domeniul tehnologiei informației și a securității

informatice, uita-te la motoarele de căutare a locurilor de muncă este o modalitate bună de a vedea ce fel de locuri de muncă sunt disponibile în întreaga lume.

În funcție de interesul dvs. pentru securitatea informatică, pot fi disponibile diferite tipuri de locuri de muncă și pot necesita certificări de competențe specializate. De exemplu, un tester de penetrare, cunoscut și ca un hacker etic, caută și exploatează vulnerabilitățile de securitate în aplicații, rețele și sisteme. Pentru a deveni un tester de penetrare, va trebui să câștigați experiență în alte locuri de muncă IT, cum ar fi:

administrator de securitate,

administrator de rețea

administratorul de sistem.

Fiecare dintre aceste locuri de muncă necesită un set propriu de competențe care vă vor ajuta să deveniți un bun valoros pentru o organizație.

Speranța noastră este că acest curs v-a stârnit interesul pentru securitatea informatică și poate veți alege să urmați o cariera în acest domeniu.
Doar pentru distracție, faceți clic AICI pentru a citi un roman grafic despre un super-erou de securitate digitală!

Elaborat de: Luna

Nicolai Sandu

Expert Elaborare RED si utilizare TIC in dezvoltarea afacerii

TEST FINAL

1. Care declarație descrie securitatea informatică?

- Este un cadru pentru dezvoltarea politicii de securitate.
- Acesta este un model bazat pe standarde pentru dezvoltarea de tehnologii firewall pentru a lupta împotriva infractorilor cibernetici.
- Este numele unei aplicații complexe de securitate pentru utilizatorii finali pentru a proteja stațiile de lucru împotriva atacurilor.
- Este un efort continuu de a proteja sistemele conectate la Internet și datele asociate cu aceste sisteme împotriva utilizării neautorizate sau a pagubelor.

2. Care sunt două obiective ale integrității datelor? (Alege doua.)

- ☐ Datele sunt disponibile tot timpul.
- ☐ Datele sunt neschimbate în timpul tranzitului.
- ☐ Accesul la date este autentificat.
- ☐ Datele nu sunt modificate de entități neautorizate.
- ☐ Datele sunt criptate în timp ce sunt în tranzit și când sunt stocate pe discuri.

3. Un administrator de server web configurează setările de acces pentru a solicita utilizatorilor să se autentifice mai întâi înainte de a accesa anumite pagini Web. Care cerință de securitate a informațiilor este abordată prin configurație?

- integritate
- scalabilitate
- disponibilitate
- confidențialitate

4. O companie se confruntă cu vizite copleșitoare la un server web principal. Departamentul IT dezvoltă un plan de adăugare a mai multor servere web pentru echilibrarea încărcăturii și redundanță. Care cerință a securității informațiilor este abordată prin implementarea planului?

- integritate
- scalabilitate
- disponibilitate
- confidențialitate

5. Adevărat sau fals?

Un angajat face ceva ca reprezentant al companiei cu cunoștințele acelei companii și această acțiune este considerată ilegală. Compania ar fi legal responsabilă pentru această acțiune.

- Adevărat
- Fals

6. Care este principalul scop al traficului cibernetic?

- pentru a proteja centrele de date bazate pe cloud
- pentru a obține avantaj față de adversari
- să dezvolte dispozitive de rețea avansate
- pentru a simula posibile scenarii de război între națiuni

7. În descrierea malware-ului, care este diferența dintre un virus și un vierme?

- Un virus se concentrează pe obținerea accesului privilegiat la un dispozitiv, în timp ce un vierme nu are.
- Un virus poate fi utilizat pentru a difuza anunțuri fără consimțământul utilizatorului, în timp ce un vierme nu poate.
- Un virus se replică prin atașarea la un alt fișier, în timp ce un vierme se poate replica independent.
- Un virus poate fi folosit pentru a lansa un atac DoS (dar nu un DDoS), dar un vierme poate fi utilizat pentru lansarea atacurilor DoS și DDoS.

8. Pentru a răspunde la întrebare, nu este nevoie să luați în considerare expoziția. Expoziția prezintă gheare care se întind de la obiecte colorate crăpate. În ghearele sunt smartphone-uri.

- Ce tip de atac folosește zombi?
- Cal troian
- DDoS
- SEO otrăvire
- pescuit cu sulita

9. Departamentul IT declară că un server web de companie primește simultan un număr anormal de solicitări de pagini web din diferite locații. Ce tip de atac de securitate apare?

- adware
- DDoS
- phishing
- Inginerie sociala
- spyware

10. Care este cea mai bună abordare pentru a împiedica un dispozitiv IoT compromis să acceseze în mod malefic datele și dispozitivele dintr-o rețea locală?

- Instalați un firewall pentru software pe fiecare dispozitiv de rețea.
- Plasați toate dispozitivele IoT care au acces la Internet într-o rețea izolată.
- Deconectați toate dispozitivele IoT de pe Internet.
- Setați setările de securitate ale browserelor web de la o stație de lucru la o înălțime mai mare

11 Care este cea mai bună metodă pentru a evita obtinerea de programe spyware pe o mașină?

- Instalați cele mai noi actualizări ale sistemului de operare.
- Instalați cele mai recente actualizări ale browserului web.
- Instalați cele mai recente actualizări antivirus.
- Instalați software-ul numai de pe site-uri de încredere.

12. Care sunt două implementări de securitate care utilizează biometrice? (Alege doua.)

- ☐ recunoaștere vocală
- ☐ buzunar
- ☐ telefon
- ☐ amprentă digitală
- ☐ card de credit
- ☐

13. Ce tehnologie creează un jeton de securitate care permite unui utilizator să se conecteze la o aplicație web dorită folosind acreditările de pe un site de social media?

- manager de parole
- Deschideți autorizația
- în modul privat de navigare
- Serviciul VPN

14. Un angajat al unei instituții medicale trimite e-mailuri către pacienți cu privire la vizitele recente ale pacienților la unitate. Ce informații ar pune confidențialitatea pacienților în pericol dacă ar fi inclusă în e-mail?

- dosarele pacientului
- numele și prenumele
- informatii de contact
- urmatoarea numire

15. Care două instrumente utilizate pentru detectarea incidentelor pot fi folosite pentru a detecta comportamentul anormal, pentru a detecta traficul de comandă și de control și pentru a detecta gazdele infectate? (Alege doua.)

- ☐ Sistem de detectare a intruziunilor
- ☐ Borcan cu miere
- ☐ NetFlow
- ☐ Nmap
- ☐ Un server proxy invers

16. În ce scop ar folosi un administrator de rețea instrumentul Nmap?

- detectarea și identificarea porturilor deschise
- protecția adreselor IP private ale gazdei interne
- identificarea anomaliilor de rețea specifice
- colectarea și analizarea alertelor și a buștenilor de securitate

17. Care etapă a lanțului de ucideri folosit de atacatori se axează pe identificarea și selectarea țintelor?

- livrare
- exploatare
- înarmare
- recunoaştere

18 Ce este un exemplu de Cyber Kill Lane?

- un grup de botneturi
- un proces planificat de cyberattack
- serie de viermi bazați pe același cod de bază
- combinație de virus, vierme și cal troian

19. Ce instrument folosiți pentru a atrage un atacator, astfel încât un administrator să poată captura, înregistra și analiza comportamentul atacului?

- NetFlow
- IDS
- Nmap
- borcan cu miere

20. Care este o funcție principală a echipei Cisco Security Response?

- pentru a proiecta programe malware polimorfe
- pentru a proiecta rutere și switch-uri de generație următoare care sunt mai puțin predispuse la atacurile cibernetice
- pentru a furniza standarde pentru noile tehnici de criptare
- pentru a asigura conservarea companiei, a sistemului și a datelor

21 Ce acțiuni va avea un IDS asupra detectării traficului rău intenționat?

- blocați sau respingeți tot traficul
- aruncați numai pachetele identificate ca fiind rău intenționate
- creați o alertă de rețea și înregistrați detectarea
- redirecționa traficul rău intenționat către un honeypot