Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

Codul proiectului: EC/101083410– WeH/ și POCIDIF/1147/2/1/161799

Titlul proiectului: Wallachia eHUB (WEH)

WP 3. Servicii de dezvoltare a competențelor și de formare profesională (Skills Development and Training Services)

Material de curs pentru programul de instruire pentru introducerea în securitatea cibernetică

Întocmit,

Manea Mihai-Laurențiu

USH_Trainer de coordonare a transformării digitale

Martie 2025

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

Scurt istoric

Odată cu progresul și inovațiile specifice domeniului IT&C, prin implementarea la scară largă a unor tehnologii care să faciliteze interacțiunea cu mediul online, amenințările cibernetice au evoluat, atât din punct de vedere al complexității, formele specifice de manifestare suferind mutații, cât și al frecvenței, numărul atacurilor cibernetice crescând de la an la an.

La începutul anilor ’90, securitatea cibernetică era o preocupare exclusivă a departamentelor IT din cadrul instituțiilor publice și al companiilor private, în prezent, pe fondul creșterii cantitative și calitative a amenințărilor, preocupările specifice domeniului s-au mutat la nivelul strategic al acestor entități.

Primul atac cibernetic notabil a avut loc în 1988, când Robert Morris, tânăr absolvent al universității Cornell din Statele Unite ale Americii, a creat primul worm care a vizat și infectat pe „scară largă” – aproximativ 6000 de sisteme, care la momentul respectiv reprezentau în jur de 10% din totalul de calculatoare conectate la Internet. Morris Worm, așa cum a fost denumit, a fost prima aplicație malware prin care s-a reușit realizarea unui atac de tip Denial-of-Service (DoS). Pentru eliminarea infecției, administratorii rețelelor regionale de Internet au decis deconectarea acestora în vederea neutralizării amenințării, demersul realizându-se într-un orizont de câteva zile. Astfel, pentru câteva zile, toată rețeaua Internet existentă la nivel mondial și-a întrerupt activitatea.

Atacuri care utilizau aplicații malware de tip virus, worm, spyware și chiar ransomware au fost preferate de hackerii anilor ’90. Astfel, mediul de securitate cibernetică existent în acea perioadă poate fi asimilat criminalității cibernetice din zilele noastre, prin prisma motivației și a complexității atacurilor derulate.

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

La nivelul Serviciului Român de Informații, anii ’90 au reprezentat momentul de început în ceea ce privește asigurarea securității cibernetice a propriilor sisteme, existând preocupări pentru securitatea hardware și software.

Începând cu anii 2000, nivelul de complexitate al amenințării cibernetice a început să crească, realizându-se primii pași în direcția anonimizării scopului real al atacatorilor, prin aplicațiile de tip trojan. Acestea au fost și sunt utilizate în prezent, atât de actori din sfera criminalității cibernetice, cât și de entități cu motivație strategică, prima decadă a secolului XXI fiind momentul în care activitățile de spionaj cibernetic au fost inițiate la scară largă. Câteva exemple notabile în acest sens sunt grupările APT1 și APT28, care au vizat atât ținte din spectrul guvernamental (afaceri externe, domeniul militar și administrație publică), cât și entități private (din domeniul financiar, aerospațial, IT&C, transporturi).

La nivelul NATO, Summitul din 2002 de la Praga a fost primul moment în care securitatea cibernetică a Alianței a fost abordată la nivel strategic, în rândul statelor aliate resimțindu-se necesitatea protecției sistemelor informatice ce ar fi trebuit să fie utilizate la Summitul de la Riga din 2006.

Anii 2007-2008 au reprezentat o perioadă-cheie pentru definirea actuală a mediului de securitate cibernetică, fiind prima dată când o entitate cu motivație strategică a atacat cibernetic infrastructura IT&C guvernamentală a altor state. De asemenea, această perioadă poate fi considerată cea în care „armele cibernetice” au început să fie utilizate pe scară largă.

Răspunsul NATO la aceste activități din spațiul cibernetic s-a concretizat prin adoptarea primei strategii a Alianței în acest domeniu, în luna ianuarie 2008 – Policy on Cyber Defence.

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

Anul 2008 a reprezentant momentul în care s-a realizat trecerea de la protecția propriilor sisteme, către o preocupare constantă pentru asigurarea securității cibernetice a infrastructurilor IT&C cu valențe critice existente la nivel național, fiind constituite două departamente cu atribuții în acest sens: unul care a abordat securitatea cibernetică din perspectivă HUMINT și altul care a realizat abordarea din perspectivă tehnică.

Anul 2010 a însemnat o etapă definitorie pentru aceasta. Astfel, a fost cunoscută o nouă formă de manifestare a amenințării, sabotajul cibernetic, aplicația worm Stuxnet vizând producerea unor pagube materiale însemnate. Din punct de vedere tehnologic, Stuxnet a fost concepută să exploateze vulnerabilități zero-day cu scopul compromiterii echipamentelor care controlau centrifugele utilizate pentru producerea și îmbogățirea uraniului.

Un alt moment important pentru mediul de securitate cibernetică din România a fost anul 2013, în care s-a adoptat Hotărârea de Guvern nr. 271/2013 prin care se aproba Strategia de securitate cibernetică a României. Urmare acestui document strategic și a trendurilor tot mai accentuate existente la nivel mondial, prin Hotărârea Consiliului Suprem de Apărare a Țării, SRI a fost desemnat autoritate națională în cyberintelligence. Astfel, la nivelul Serviciului s-a decis „coagularea” domeniului și crearea unei unități specializate în prevenirea și contracararea amenințărilor cibernetice existente la adresa infrastructurilor IT&C cu valențe critice pentru securitatea națională – Centrul Național CYBERINT. În perioada 2014-2016, la nivelul NATO și UE au existat preocupări tot mai intense pentru creșterea nivelului securității cibernetice, atât pentru Alianță și Uniune, cât și pentru membri la nivel național și au fost încheiate numeroase parteneriate public-private pentru a dinamiza cooperarea dintre aceste entități.

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

La Summitul de la Varșovia din 2016, șefii de stat și de guverne din NATO au decis să definească spațiul cibernetic drept domeniu operațional alături de sol, aer, apă. Acest aspect a avut rolul de a îmbunătăți modul în care NATO își îndeplinește obiectivele de apărare a spațiului cibernetic aliat.

Introducere

Securitatea cibernetică este un domeniu al informaticii care se ocupă cu protejarea sistemelor informatice, a rețelelor și a datelor sensibile împotriva accesului neautorizat, a utilizării necorespunzătoare sau a deteriorării. Într-o lume din ce în ce mai conectată digital, securitatea cibernetică este esențială pentru protejarea informațiilor și a infrastructurii împotriva amenințărilor cibernetice.

Securitatea cibernetică reprezintă un ansamblu de măsuri, tehnologii și bune practici implementate pentru a proteja sistemele informatice și datele împotriva atacurilor, accesului neautorizat și altor vulnerabilități. Prin metode precum criptarea datelor, firewall-uri, autentificare multi-factor și software de detecție a amenințărilor, securitatea cibernetică ajută la păstrarea integrității și confidențialității datelor, aspecte critice pentru orice afacere. În lipsa unei strategii de securitate bine gândite, o simplă breșă poate duce la pierderi financiare imense și daune de imagine greu de recuperat.

Într-o lume tot mai interconectată, protejarea datelor devine la fel de importantă ca protejarea activelor fizice ale companiei. Dar ce este securitatea cibernetică și cum îți poate ea salva afacerea de la pierderi financiare și de reputație? În esență, securitatea cibernetică nu mai este doar o măsură preventivă, ci o necesitate strategică pentru orice companie care lucrează cu date, clienți sau sisteme online.

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

În cele ce urmează, vei afla beneficiile securității cibernetice și vei înțelege de ce investițiile în acest domeniu pot însemna diferența între o afacere sigură și una vulnerabilă.

Aceste amenințări pot lua forma unor atacuri cibernetice variate, cum ar fi cele de tip malware care vizează să infecteze computerele și să le controleze, atacurile de tip phishing care încearcă să inducă utilizatorii în eroare și să le fure datele personale sau financiare, sau atacuri de tipul DDoS care încearcă să perturbe sau să blocheze accesul la servicii online.

Securitatea cibernetică utilizează o gamă largă de tehnici și tehnologii pentru a proteja sistemele și datele împotriva acestor amenințări. Acestea includ firewall-uri care controlează traficul de rețea, soluții antivirus care detectează și elimină amenințările de malware, criptarea care protejează datele împotriva accesului neautorizat, autentificarea multi-factor care verifică identitatea utilizatorilor, și multe altele.

În esență, securitatea cibernetică este un efort continuu pentru a asigura confidențialitatea, integritatea și disponibilitatea informațiilor și a sistemelor în mediul online, protejându-le împotriva atacurilor și menținându-le operaționale și funcționale în fața amenințărilor cibernetice în continuă evoluție.

Securitatea cibernetică este modul în care sistemele, rețelele și programele utilizează tehnologii, procese și practici pentru a se proteja împotriva atacurilor digitale. Atacurile cibernetice vizează adesea informații și date sensibile și, obținând acces la aceste date, infractorii cibernetici storc bani de la utilizatori și companii, întrerup procesele normale și distrug site-uri întregi.

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

Securitatea cibernetică eficientă este o componentă esențială a oricărei afaceri și chiar mai mult este în joc pentru organizațiile mici și mijlocii, deoarece adesea le lipsesc resursele necesare pentru a se recupera după astfel de atacuri. În lumea noastră modernă bazată pe date, protecția împotriva atacurilor cibernetice devine din ce în ce mai dificilă din cauza cantității tot mai mari de date și dispozitive disponibile.

Fiecare companie, indiferent de dimensiuni, trebuie să fie conștientă de amenințările cibernetice care pot apărea din multiple direcții. Iată câteva măsuri esențiale pentru o securitate cibernetică eficientă:

- autentificarea în doi pași: adăugând un nivel suplimentar de protecție;
- backup periodic al datelor: pentru a preveni pierderile în caz de atacuri de tip ransomware;
- criptarea informațiilor sensibile: pentru a asigura confidențialitatea în cazul interceptării datelor; monitorizarea constantă a activităților online: pentru a detecta imediat orice activitate neobișnuită.

De ce este importantă securitatea cibernetică

În lumea conectată de astăzi, toată lumea beneficiază de soluții avansate de securitate cibernetică. La nivel individual, un atac de securitate cibernetică poate duce la orice, de la furtul de identitate la tentative de extorcare, până la pierderea de date importante, cum ar fi fotografii de familie. Toată lumea se bazează pe infrastructura critică, cum ar fi centralele electrice, spitalele și companiile de servicii financiare. Securizarea acestora și a altor organizații este esențială pentru menținerea funcționării societății noastre.

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

Securitatea cibernetică este unul dintre cele mai importante aspecte ale oricărei afaceri astăzi. Acest lucru se datorează faptului că guvernele, corporațiile financiare, companiile medicale și, practic, orice altă entitate colectează și stochează cantități masive de date pe computere și dispozitive. O mare parte din aceste date conțin informații sensibile despre aceste companii sau despre public, cum ar fi proprietatea intelectuală, date financiare, detalii personale și multe altele. Aceste date sunt adesea transferate prin rețele și prin dispozitive, ceea ce înseamnă că există multe oportunități ca acestea să fie compromise.

Toată lumea beneficiază, de asemenea, de munca cercetătorilor în domeniul amenințărilor cibernetice, precum echipa de 250 de cercetători în domeniul amenințărilor de la Talos, care investighează amenințările noi și emergente și strategiile de atac cibernetic. Ei dezvăluie noi vulnerabilități, educă publicul cu privire la importanța securității cibernetice și consolidează instrumentele open-source. Munca lor face ca internetul să fie mai sigur pentru toată lumea.

Lumea a fost martoră a multor atacuri cibernetice la scară largă, care au dus la o creștere constantă a neîncrederii publicului în manipularea datelor lor. Aceste tipuri de atacuri dăunează grav și reputației companiilor.

Iată o privire asupra unora dintre cele mai mari atacuri cibernetice din istoria recentă:

- **Chirpici:** În octombrie 2013, hackerii au lovit Adobe, iar raportul inițial spunea că au fost furate aproximativ 3 milioane de înregistrări criptate ale cărților de credit ale clienților și date de conectare pentru alți utilizatori. Cu toate acestea, această estimare a continuat să crească, impactul ajungând la 153 de milioane de înregistrări de utilizatori. Compania a plătit pentru 1.1 milioane de dolari în taxe legale și o sumă nedezvăluită utilizatorilor.

- **Equifax:** În iulie 2017, Equifax a suferit o breșă majoră a datelor care a expus aproximativ 147.9 milioane de consumatori. Informații precum numerele de securitate socială, datele de naștere, adresele și numerele permiselor de conducere au fost compromise și, fiind unul dintre cele mai mari birouri de credit din SUA, compania s-a confruntat cu un control sever pentru probleme de securitate și de răspuns.
- **Sina Weibo:** Într-unul dintre exemplele mai recente, Sina Weibo din China, care este alternativa națională la Twitter, a suferit o breșă în martie 2020. Aproximativ 172 de milioane de nume reale ale utilizatorilor, numele de utilizator ale site-ului, sexul, locația și numerele de telefon au fost afișate pentru vânzare pe piețele dark web.

Tipuri de amenințări de securitate cibernetică

Securitatea cibernetică este esențială pentru protejarea datelor, a infrastructurii și a reputației organizațiilor în fața amenințărilor cibernetice în continuă evoluție. Este un element important al gestionării riscurilor în era digitală și nu poate fi ignorată sau tratată superficial.

O amenințare de securitate cibernetică este o încercare intenționată de a obține acces la sistemul unei persoane sau al unei organizații. Utilizatorii rău intenționați își dezvoltă continuu metodele de atac pentru a evita detectarea și a exploata vulnerabilitățile noi, dar se bazează pe câteva metode comune pentru care vă puteți pregăti.

Există câteva tipuri principale de amenințări la adresa securității cibernetice de care orice persoană și organizație ar trebui să fie conștientă:

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

Malware

Malware-ul este un termen generic pentru orice software rău intenționat, inclusiv viermi, ransomware, spyware și viruși. Este proiectat să dăuneze computerelor sau rețelelor prin modificarea sau ștergerea fișierelor, extragerea datelor confidențiale, cum ar fi parolele și numerele de cont, sau trimiterea de e-mailuri sau trafic rău intenționat. Malware-ul poate fi instalat de un atacator care obține acces la rețea, dar, de multe ori, utilizatorii implementează involuntar malware pe dispozitive sau în rețeaua firmei după ce fac clic pe un link greșit sau descarcă o atașare infectată.

Ransomware

Ransomware-ul este o formă de extorcare care utilizează malware pentru a cripta fișiere, făcându-le inaccesibile. Atacatorii extrag adesea date în timpul unui atac cu ransomware și pot amenința să le publice dacă nu primesc plăți. În schimbul unei chei de decriptare, victima trebuie să plătească o răscumpărare, de obicei în criptomonedă. Nu toate cheile de decriptare funcționează, așadar, plata nu garantează că fișierele vor fi recuperate.

Inginerie socială

În domeniul ingineriei sociale, atacatorii profită de încrederea utilizatorilor pentru a-i păcăli să le ofere informații despre cont sau să descarce malware. În aceste atacuri, utilizatorii rău intenționați își asumă identitatea unui brand cunoscut, unui coleg sau prieten și utilizează tehnici psihologice precum crearea unui sentiment de urgență pentru a-i convinge pe oameni să facă ceea ce ei doresc.

Phishing

Phishingul este un tip de inginerie socială care utilizează e-mailuri, mesaje text sau mesaje de poștă vocală care par să provină de la o sursă de încredere, pentru a convinge alte persoane să divulge informații confidențiale sau să facă clic pe un link necunoscut. Unele campanii de phishing sunt trimise unui număr foarte mare de persoane, în speranța că măcar o singură persoană va face clic. Alte campanii, numite phishing țintit, sunt mai direcționate și se concentrează pe o singură persoană. De exemplu, un adversar poate pretinde că este un căutător de locuri de muncă pentru a păcăli un recrutor să descarce un CV infectat.

Amenințări din interior

Într-o amenințare din interior, persoane care au deja acces la unele sisteme, cum ar fi angajații, furnizorii sau clienții, provoacă o breșă în securitate sau o pierdere financiară. În unele cazuri, acest rău este neintenționat, de exemplu, atunci când un angajat postează accidental informații confidențiale într-un cont personal din cloud. Dar unii utilizatori acționează cu rele intenții.

Amenințare persistentă avansată

Într-o amenințare persistentă avansată, atacatorii obțin acces la sisteme, dar rămân nedetectați pe o perioadă lungă de timp. Adversarii cercetează sistemele firmei țintă și fură date fără a declanșa contramăsuri de apărare.

Tipuri de atacuri prin web:

• Drive-By Downloads - descarcă conținut rău intenționat pe dispozitivul victimei. Utilizatorul final vizitează un site legitim compromis de infractori cibernetici cu scripturi rău intenționate pentru a rula exploit-uri bazate pe browser sau pentru a redirecționa utilizatorul către un alt site web infectat.

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

• Watering Hole - atacuri țintite ca folosesc seturi de exploituri cu caracteristici camuflate. Un actor rău

intenționat este interesat să compromită un anumit grup de utilizatori prin utilizarea de exploit-uri sau conținut rău intenționat injectat pe site-ul web.

• Formjacking - atacatorii injectează cod rău intenționat în formularele de plată legitime ale unui site web.

Acest atac captează în principal informații bancare și alte informații personale de identificare (PII), iar scriptul rău intenționat transmite simultan datele către portal și către infractorii cibernetici.

• URL rău intenționat - linkuri create cu intenția de a distribui malware sau de a facilita o înșelătorie. Procesul implică activități de inginerie socială pentru obținerea informațiilor victimelor și pentru a-i convinge să dea clic pe URL-ul rău intenționat, care execută programe malware și compromite calculatorul victimelor.

Un atac Denial-of-Service (DoS) sau un atac Distributed-Denial-of-Service (DDoS) reprezintă încercări rău intenționate de a perturba traficul normal al unui server, serviciu sau rețea prin suprasolicitarea sistemului țintit sau a infrastructurii cu un volum mare de date.

Tipuri de atacuri DoS sau DDoS:

•Atacuri bazate pe volum - obiectivul atacului este de a satura lățimea de bandă a site-ului atacat (flood UDP, ICMP și alte solicitări cu pachete falsificate).

•Atacuri de protocol - acest tip de atac consumă resurse reale ale serverului sau cele ale echipamentelor de comunicații intermediare, cum ar fi firewall-urile

și echilibratoarele nivelului de încărcare. (flood SYN, atacuri de pachete fragmentate, Ping of Death, Smurf DDoS etc.).

•Atacuri la nivel de aplicație - compuse din cereri aparent legitime, scopul acestor atacuri este de a bloca serverul web. (atacuri reduse și lente, cereri de tip GET / POST, atacuri care vizează vulnerabilitățile Apache, Windows sau OpenBSD etc.).

Securitatea cibernetică este unul dintre cele mai vitale aspecte ale oricărei afaceri în epoca actuală și ar trebui implementată de sus în jos, cu managementul corporativ să conducă. Trebuie să existe o adaptare continuă, deoarece acest domeniu este în continuă schimbare și devine o amenințare din ce în ce mai mare. Poate la fel de importanți ca și tehnologia actuală de securitate cibernetică sunt angajații, care prin educație, conștientizare și o abordare centrată pe securitate sunt cea mai bună apărare împotriva oricărui atac.

Măsuri de securitate cibernetică

În prezent, amenințările provenite din spațiul cibernetic pot fi caracterizate prin complexitate ridicată, dinamism şi automatizare, fapt ce a generat adaptarea instrumentelor pe care experții în securitate cibernetică le utilizează pentru prevenirea şi contracararea atacurilor. În acest sens, se dovedesc de real interes, atât pentru atacatori, cât şi pentru cei care asigură securitatea infrastructurilor IT&C, produsele concepute având la bază inteligența artificială, inclusiv Machine Learning. Din perspectiva atacatorului, prin utilizarea acestor tehnologii pot fi generate automat instrumente necesare desfășurării unui atac cibernetic dificil de detectat prin mijloace tradiționale, iar pentru cei care asigură securitatea infrastructurilor pot fi dezvoltate soluții care detectează automat amenințările cibernetice pe baza analizei anomaliilor de comportament.

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

Directiva NIS este prima lege la nivel european privind securitatea cibernetică. Legea include măsuri concrete pentru creșterea nivelului general de securitate cibernetică în Uniunea Europeană. Directiva este transpusă în România prin Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.

NIS2 este o directivă europeană care actualizează și extinde cerințele pentru securitatea cibernetică stabilite de prima Directivă NIS (Network and Information Security) din 2016. Scopul principal al NIS2 este de a crește reziliența cibernetică a infrastructurilor esențiale și de a asigura o aplicare unitară a măsurilor de securitate cibernetică în toate statele membre ale Uniunii Europene

Managementul entităților importante trebuie să ia o serie de măsuri specifice pentru a se conforma cerințelor Directivei NIS2. Aceste măsuri sunt menite să îmbunătățească securitatea cibernetică și să gestioneze eficient riscurile asociate. Printre măsurile necesare se numără:

Implementarea unui cadru de gestionare a riscurilor cibernetice

Managementul trebuie să adopte un cadru de gestionare a riscurilor cibernetice care include evaluări periodice ale riscurilor și politici de securitate pentru sistemele informatice. Acest cadru trebuie să fie aliniat cu cerințele NIS2 și să se concentreze pe prevenirea, detectarea și răspunsul la incidentele de securitate cibernetică

Entitățile importante trebuie să aibă un plan solid de continuitate a afacerii și un plan de gestionare a crizelor pentru a asigura continuitatea operațională în cazul unor incidente majore de securitate cibernetică. Aceste planuri ar trebui să includă

proceduri de recuperare a datelor, strategii de backup și planuri de comunicare de urgență

Responsabilitatea conducerii pentru măsurile de securitate

Conducerea trebuie să aprobe și să supervizeze măsurile de securitate cibernetică adoptate de companie. Aceasta include monitorizarea implementării politicilor de securitate și asigurarea că măsurile de securitate sunt în concordanță cu cerințele directivei. În caz de neconformitate, conducerea poate fi trasă la răspundere personal și poate primi sancțiuni severe, inclusiv interdicția de a ocupa funcții de management

Raportarea incidentelor cibernetice

Entitățile importante trebuie să stabilească proceduri clare de raportare a incidentelor cibernetice, cu obligația de a notifica autoritățile naționale competente în termen de 24 de ore de la detectarea unui incident major și de a furniza un raport complet în termen de 72 de ore. Aceste cerințe de raportare trebuie integrate în cadrul de gestionare a incidentelor

Gestionarea securității lanțului de aprovizionare

Entitățile trebuie să implementeze măsuri de securitate pentru a gestiona riscurile asociate lanțului de aprovizionare, inclusiv evaluarea furnizorilor și implementarea politicilor de securitate pentru toți partenerii. Este important ca entitățile să stabilească procese pentru a identifica vulnerabilitățile din lanțul de aprovizionare și să asigure conformitatea cu cerințele NIS2 la nivelul întregii rețele de parteneri

Asigurarea instruirii și conștientizării

Managementul trebuie să se asigure că personalul companiei primește instruire periodică privind securitatea cibernetică și că sunt promovate bune practici de securitate în cadrul organizației. Toate persoanele cu roluri în gestionarea riscurilor cibernetice trebuie să fie instruite corespunzător pentru a înțelege impactul măsurilor de securitate asupra activității companiei

Prin implementarea acestor măsuri, managementul entităților importante poate asigura conformitatea cu cerințele directivei NIS2 și poate reduce riscurile asociate securității cibernetice.

Entitățile importante (detalierea lor o gasiti aici: link) trebuie să desfășoare audituri de securitate conform cerințelor NIS2. Directiva prevede că autoritățile naționale pot solicita implementarea auditului de securitate pentru a verifica conformitatea acestor entități cu măsurile de securitate impuse. Auditul poate fi obligatoriu în urma unor suspiciuni de neconformitate sau ca parte a verificărilor periodice pentru a se asigura că sunt respectate standardele de securitate cibernetică.

Entitățile importante sunt supuse unui regim de supraveghere ex-post, ceea ce înseamnă că auditul poate fi impus după ce se constată nereguli sau în baza unor rapoarte de neconformitate. Totuși, pentru a preveni eventualele sancțiuni, este recomandat ca managementul să desfășoare audituri interne regulate pentru a asigura conformitatea și pentru a identifica din timp eventualele deficiențe.

Prin urmare, auditul de securitate reprezintă o măsură preventivă și corectivă importantă pentru a se asigura că entitățile importante îndeplinesc cerințele

directivei NIS2 și sunt pregătite să răspundă eficient la riscurile de securitate cibernetică.

Auditul pentru conformitatea cu NIS2 trebuie realizat de firme specializate în securitate cibernetică și managementul riscurilor, care au experiență în domeniul auditului de securitate și sunt acreditate să ofere astfel de servicii. Aceste firme trebuie să îndeplinească anumite criterii, cum ar fi certificările în securitate cibernetică și conformitate, și să aibă personal cu competențe relevante.

Pentru alegerea unei firme potrivite, companiile ar trebui să verifice dacă auditorul este acreditat de autoritățile naționale competente sau de instituțiile internaționale de reglementare, cum ar fi ENISA (European Union Agency for Cybersecurity) și alte organisme similare.

În România, Directoratul Național de Securitate Cibernetică (DNSC) este autoritatea competentă responsabilă de supravegherea implementării Directivei NIS2. DNSC se ocupă de monitorizarea și asigurarea conformității cu cerințele directivei pentru toate entitățile esențiale și importante care operează pe teritoriul României.

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

Prevenirea atacurilor cibernetice

O abordare proactivă prin concentrarea pe prevenirea atacurilor cibernetice este esențială pentru a vă asigura că rețelele dvs. personale și de firmă sunt sigure. Totuși, majoritatea oamenilor nu știu de unde să înceapă.

Iată câteva modalități care vă pot ajuta să păstrați datele în siguranță:

Investiția într-un sistem fiabil de securitate cibernetică.

Angajarea de administratori IT care vor monitoriza atent toate rețelele dintr-o firmă.

Utilizarea unui sistem de autentificare pe două niveluri sau multifactor. Aceasta vă va asigura că toți membrii cu un cont sau care au acces la sistem sunt angajați verificați sau participanți direct interesați ai firmei.

Instruiți-vă angajații prin cursuri interne continue privind atacurile cibernetice și securitatea cibernetică și ce pași să fie luați dacă apare breșe de date.

Angajați o echipă de securitate terță pentru a vă asista departamentul IT intern cu monitorizarea rețelelor și sistemelor firmei.

Beneficiile pe care le ofera, internetul aduce si riscuri considerabile pentru siguranta noastra personala si a datelor noastre.

Conform unui raport realizat de Centrul pentru Siguranta Cibernetica, atacurile cibernetice au crescut cu peste 30% in ultimii ani, iar milioane de utilizatori devin victime ale furtului de identitate si ale altor infractiuni online in fiecare an. De aceea, este esential sa intelegem cum sa ne protejam in mediul online si sa adoptam masuri de siguranta eficiente.

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

Un expert in securitatea cibernetica, John Smith, a declarat intr-un interviu recent ca: "Cel mai bun mod de a-ti proteja datele online este sa fii constient de riscuri si sa adopti o abordare proactiva in ceea ce priveste siguranta ta. Tehnologia evolueaza rapid, iar atacatorii devin din ce in ce mai sofisticati."

In acest context, este crucial sa ne educam si sa implementam strategii de baza pentru a ne proteja in mod eficient pe internet. S

Sfaturi esentiale pentru a asigura o navigare sigura si protejata pe internet

Utilizarea parolelor complexe si unice

În era digitală, securitatea cibernetică este o preocupare majoră pentru toți utilizatorii de internet. Parolele sunt prima linie de apărare împotriva accesului neautorizat la conturile tale online. Cu toate acestea, crearea și gestionarea parolelor sigure poate fi o provocare.

Unul dintre cele mai simple si eficiente moduri de a-ti proteja conturile online este utilizarea parolelor complexe si unice. O parola puternica trebuie sa fie lunga, sa contina o combinatie de litere mari si mici, cifre si caractere speciale. Evita utilizarea informatiilor personale, cum ar fi numele sau datele de nastere, deoarece acestea pot fi usor deduse sau accesate de catre hackeri.

Parolele sigure sunt esențiale pentru protejarea informațiilor personale, cum ar fi datele bancare, informațiile de conectare și datele de identitate. Un atac cibernetic poate duce la furtul identității, pierderi financiare sau compromiterea conturilor. Prin urmare, este crucial să înțelegi importanța parolelor puternice.

Un studiu realizat de SplashData a aratat ca cele mai comune parole pe care utilizatorii le folosesc sunt "123456" si "password". Acest lucru demonstreaza neglijenta multor persoane fata de securitatea online, facandu-i vulnerabili la

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

atacuri. Este recomandat sa folosesti parole diferite pentru fiecare cont in parte pentru a reduce riscul compromiterii tuturor conturilor tale in cazul in care una dintre parole este furata.

Caracteristicile unei parole sigure

Lungimea: O parolă ar trebui să aibă cel puțin 12 caractere.

Complexitatea: Utilizează o combinație de litere mari și mici, cifre și simboluri.

Imprevizibilitatea: Evită cuvinte comune, date personale sau secvențe ușor de ghicit.

Există diverse tehnici pe care le poți folosi pentru a crea parole sigure.

Manageri de parole

Pentru a-ti usura sarcina de a tine minte parole complexe, poti folosi un manager de parole.

Un manager de parole este un software care stochează și criptează parolele tale. Acesta îți permite să creezi parole complexe și să le accesezi rapid.

Aceste aplicatii stocheaza si genereaza parole unice si complexe pentru fiecare cont, astfel incat sa nu fii nevoit sa te bazezi pe memoria ta pentru a le retine.

Autentificarea cu doi factori (2FA)

Implementarea autentificării cu doi factori adaugă un nivel suplimentar de securitate. Aceasta necesită un al doilea element de verificare, cum ar fi un cod trimis pe telefonul tău, pe lângă parolă.

De asemenea, multi manageri de parole ofera functii de autentificare cu doi factori, adaugand un nivel suplimentar de securitate.

Schimbarea regulată a parolelor

Schimbarea periodică a parolelor este o practică bună de securitate. De exemplu, poți seta o alarmă pentru a-ți reaminti să schimbi parolele la fiecare 3-6 luni.

Folosirea unor parole unice

Fiecare cont ar trebui să aibă o parolă unică. Evită reutilizarea parolelor, deoarece un atac asupra unui cont ar putea compromite și celelalte.

Notează-ți parolele în siguranță

Dacă nu folosești un manager de parole, asigură-te că îți notezi parolele într-un loc sigur, de preferință într-un caiet fizic păstrat într-un loc securizat, nu pe computer sau pe telefon.

Nu împărtăși parolele

Nu împărtăși parolele tale cu nimeni, indiferent de circumstanțe. Dacă este necesar să oferi acces, folosește funcțiile de partajare temporară disponibile în managerii de parole.

Fii atent la phishing

Fii vigilant în fața e-mailurilor sau mesajelor suspecte care solicită informații de conectare. Verifică întotdeauna sursa înainte de a introduce parolele.

In concluzie, asigurându-te ca parolele tale sunt complexe si unice, poți reduce semnificativ riscul de a deveni victima unui atac cibernetic. Este un pas simplu, dar extrem de eficient in protejarea informațiilor tale personale pe internet.

Activarea autentificarii cu doi factori

Autentificarea cu doi factori (2FA) este o metoda simpla si eficienta de a-ti proteja conturile online. Aceasta metoda adauga un strat suplimentar de securitate, cerandu-ti sa oferi o a doua forma de identificare, in plus fata de parola ta, pentru a accesa conturile tale.

Un studiu realizat de Microsoft a aratat ca activarea autentificarii cu doi factori poate preveni 99.9% din atacurile automatizate asupra conturilor online. Acest lucru subliniaza importanta folosirii acestei metode ca o masura de baza pentru securitatea ta cibernetica.

Autentificarea cu doi factori poate include o varietate de metode, cum ar fi:

Coduri trimise prin SMS pe telefonul tau.

Aplicatii de autentificare, precum Google Authenticator sau Authy.

Token-uri hardware care genereaza coduri de autentificare.

Amprente digitale sau recunoastere faciala (daca dispozitivul tau suporta aceste tehnologii).

Intrebari de securitate personalizate.

Este important sa alegi metoda de autentificare cu doi factori care ti se potriveste cel mai bine si sa o activezi pentru toate conturile tale importante, cum

ar fi conturile de email, bancare si sociale. In acest fel, chiar daca cineva reuseste sa obtina parola ta, nu va putea accesa conturile fara codul de autentificare suplimentar.

John Doe, un expert in securitate cibernetica, subliniaza: "In zilele noastre, parolele nu sunt suficiente. Autentificarea cu doi factori ofera o bariera suplimentara care poate face diferenta dintre securitatea contului si compromiterea acestuia."

Prin urmare, activarea autentificarii cu doi factori este o masura esentiala pentru a-ti proteja datele pe internet. Este un pas simplu care poate preveni accesul neautorizat la conturile tale si iti poate oferi linistea necesara in utilizarea internetului.

Foloseste conexiuni de internet sigure

Atunci cand te conectezi la internet, este esential sa folosesti conexiuni sigure pentru a-ti proteja datele personale. Conexiunile nesigure, precum retelele Wi-Fi publice, sunt vulnerabile la atacuri si pot permite hackerilor sa intercepteze traficul tau de date.

Un raport realizat de Norton arata ca 87% din utilizatori au folosit retele Wi-Fi publice fara a lua masuri de protectie. Acest lucru ii expune la riscuri semnificative, inclusiv furt de date si interceptari de informatii personale.

Pentru a te proteja pe internet, evita sa te conectezi la retele Wi-Fi publice fara protectie sau, daca este necesar, utilizeaza un serviciu de retea privata virtuala (VPN). Acesta va cripta traficul tau de date, impiedicand interceptarea acestuia de catre persoane rau intentionate.

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

De asemenea, asigura-te ca site-urile pe care le accesezi folosesc conexiuni sigure HTTPS. Acest lucru poate fi verificat prin prezenta unui simbol de lacat in bara de adrese a browserului tau. HTTPS indica faptul ca datele transmise intre tine si site sunt criptate si protejate de accesul neautorizat.

In plus, actualizeaza-ti constant software-ul si aplicatiile pentru a te asigura ca ai cele mai recente patch-uri de securitate. Acest lucru te va proteja impotriva vulnerabilitatilor cunoscute care pot fi exploatate de hackeri.

In concluzie, folosirea conexiunilor de internet sigure este cruciala pentru protejarea datelor tale personale. Prin evitarea retelelor nesigure si utilizarea de VPN-uri, poti reduce riscul de a deveni victima unui atac cibernetic.

Protejarea informatiilor personale

In mediul online, protejarea informatiilor personale este esentiala pentru a preveni furtul de identitate si alte infractiuni cibernetice. Multi utilizatori impartasesc informatii personale pe retelele sociale si alte platforme fara sa realizeze ca acestea pot fi folosite in scopuri rau intentionate.

Atunci când folosiți internetul și rețelele de socializare, trebuie să fiți atenți la informațiile personale pe care le puneți la dispoziție, cum ar fi:

- Adresa
- Numărul de telefon
- Codul CNP
- Numele de fată al mamei

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

Un studiu realizat de Pew Research Center a aratat ca 64% din utilizatorii de internet au experimentat cel puțin un tip de atac cibernetic, iar 49% dintre aceștia au avut datele personale compromise. Aceste cifre subliniază importanta protejării informațiilor personale in mediul online.

Pentru a te proteja, evita sa partajezi informații sensibile, cum ar fi numărul de telefon, adresa de domiciliu, detaliile financiare si alte date personale pe platforme publice. Fii precaut in privința cererilor de prietenie sau mesajelor de la persoane necunoscute si verifica autenticitatea acestora înainte de a oferi informații suplimentare.

De asemenea, ajustează setările de confidențialitate ale conturilor tale pe retelele sociale pentru a limita accesul la informațiile tale personale. Mulți utilizatori nu sunt conștienți de opțiunile de confidențialitate disponibile si își lasă datele vizibile pentru oricine.

Un alt aspect important este sa fii atent la atacurile de tip phishing, care sunt încercări de a te păcăli sa oferi informații personale prin emailuri sau site-uri web false. Verifica întotdeauna autenticitatea sursei înainte de a face clic pe linkuri sau de a oferi informații personale.

Pentru a vă proteja informațiile personale:

Nu împărtășiți prea multe pe rețelele de socializare. Hoții de identitate pot să vă colecteze postările de pe rețelele de socializare pentru a intra în conturile dvs., pentru a colecta date personale sau pentru a vă fura identitatea. Așadar, trebuie să fiți atenți la informațiile pe care le împărtășiți. Păstrați aceste detalii personale private și în afara internetului.

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

Evitați numele de utilizator reale. Evitați informațiile personale, precum numele de familie sau data nașterii, atunci când vă creați un nume de utilizator.

A fi rațional și a păstra datele personale departe de ochii publicului este o modalitate excelentă de a fi în siguranță și de a vă proteja intimitatea.

Prin luarea acestor masuri de precautie, poti proteja mai eficient informatiile tale personale si te poti bucura de o experienta online mai sigura.

Mesajele primite cu suspiciune

Aplicațiile de mesagerie directă au devenit un element de bază în comunicarea noastră zilnică, dar este important să vă amintiți că acestea presupun și riscuri. Pentru a vă menține în siguranță în timp ce utilizați mesageria directă, protejați-vă prin următoarele:

Feriți-vă de link-uri, fișiere și mesaje de la persoane pe care nu le cunoașteți. Chiar dacă expeditorul pare legitim, verificați-i identitatea înainte de a furniza orice informații personale.

Asigurați-vă că aplicația dvs. este întotdeauna actualizată. Versiunile mai noi includ adesea actualizări de securitate și remedieri de erori care vă pot proteja de atacuri malițioase.

Implementați autentificarea în doi pași. Acest lucru adaugă un nivel suplimentar de securitate conturilor dvs., îngreunând accesul atacatorilor la informațiile dvs. personale.

La prima vedere suntem tentați sa spunem ca nu ni se poate întâmpla noua așa ceva, specialiștii recomanda din ce in ce mai des acordarea unei atenții suplimentare email-urilor si mesajelor primite prin intermediul rețelelor de

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

socializare. Atacurile de tip phishing sunt din ce in ce mai dese in ultimii ani, acestea putând fi evitate extrem de ușor in cazul in care observi anumite suspiciuni in ceea ce privește legitimitatea mesajelor pe care le primești. In plus, amintește-ti întotdeauna ca băncile si alte instituții financiare nu iți vor cere niciodată sa iți dezvălui parolele. Trebuie sa rămâneți vigilenți și fiți în siguranță în timp ce comunicați online.

Securitatea cibernetica reprezintă o metodă esențială de protejare a sistemelor și datelor împotriva amenințărilor cibernetice.

Deși implică investiții semnificative și o gestionare complexă, avantajele oferite în termeni de protecție a datelor și prevenirea atacurilor fac din securitatea cibernetica o prioritate pentru organizațiile moderne.

Implementarea și gestionarea corespunzătoare a securității cibernetice pot preveni multe dintre riscurile asociate cu accesul neautorizat și atacurile cibernetice, asigurând astfel securitatea și integritatea datelor și sistemelor organizaționale.

Normele UE vă garantează că datele dumneavoastră cu caracter personal sunt protejate ori de câte ori este nevoie de colectarea lor – de exemplu, când faceți cumpărături on-line, când vă depuneți candidatura pentru un loc de muncă sau când solicitați un credit. Aceste norme se aplică atât companiilor și organizațiilor (publice și private) din UE, cât și celor din afara UE care oferă bunuri sau servicii în UE, cum ar fi Facebook sau Amazon, ori de câte ori aceste companii solicită sau reutilizează datele cu caracter personal ale cetățenilor din UE.

Str. Italiană nr. 28, sect. 2, București - România
weh@spiruharet.ro weh.spiruharet.ro

Drepturile dumneavoastră în materie de protecție a datelor trebuie să fie respectate, indiferent de modul în care sunt colectate – on-line, într-un sistem computerizat sau pe hârtie, într-un fișier structurat.

Siguranța online este necesară și validată, deoarece multe întreprinderi s-au confruntat cu excese de atacuri pe internet care au dus la pierderea vieții din partea victimelor, sinuciderea sau tulburările psihologice.

Securitatea cibernetica scăzută este rezultatul lipsei de colaborare intre echipa responsabila cu securitatea fizica si echipa tehnica IT. Ambele au priorități si viziuni diferite, putem spune ca securitatea fizica vine de pe Marte, iar departamentul IT de pe Venus. Sunt bariere cauzate de limbaj, de autoritate, fiecare departament dorind sa fie in control. Un astfel de comportament conduce inevitabil la generarea de vulnerabilități grave.

Securitatea cibernetica eficienta presupune evaluarea corecta a riscurilor si a consecințelor si luarea de masuri adecvate. Este vorba de analizarea tuturor produselor, tehnologiilor si a proceselor.

Implementarea și gestionarea corespunzătoare a securității cibernetice poate preveni multe dintre riscurile asociate cu accesul neautorizat și atacurile cibernetice, asigurând astfel securitatea și integritatea datelor și sistemelor organizaționale.