Laborator 9
Securitatea sistemelor informatice

Ce este securitatea cibernetică?

Toate activitățile necesare pentru protejarea/apararea:

- rețelelor, sistemelor informatice;
- utilizatorilor acestora ;
- persoanelor afectate de amenințările cibernetice,

împotriva accesului neautorizat:

- a atacurilor;
- a prejudiciilor;

cu scopul de a asigura confidențialitatea, integritatea și disponibilitatea datelor (C.I.D).

https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_RO.pdf

Securitatea cibernetică implică:

- prevenirea;
- detectarea incidentelor cibernetice;
- răspunsul;
- redresarea incidentelor de securitate.

Incidentele de securitate pot fi provocate **intenționat sau nu.**

Exemple de incidente de securitate: divulgări accidentale de informații, atacuri asupra firmelor și a infrastructurilor critice, furtul de date cu caracter personal, ingineria sociala etc.

Toate aceste incidente pot avea efecte negative de amploare asupra persoanelor, a organizațiilor și a comunităților.

- **1911 număr scurt dedicat raportării incidentelor de securitate cibernetică la CERT-RO, apelabil din orice rețea, cu tarif normal, disponibil 24/7*.**
- **https://dnsc.ro/contact**

Observatie:

La nivelul factorilor de decizie din UE, conceptul de **securitate cibernetică** acoperă orice activitate ilegală care implică **utilizarea tehnologiilor digitale în spațiul cybernetic ca de exemplu:**

- infracțiuni informatice precum lansarea de atacuri cu viruși informatici;

- fraudele cu mijloace de plată false/clonate;
- campaniile de dezinformare care urmăresc să influențeze dezbaterile pe internet, precum și acțiunile suspectate de ingerință în alegeri.

Securitatea informaţiei

Informaţia este considerată o resursă importantă a organizaţiilor. Informaţia poate fi stocată pe hârtie, electronic, poate fi transmisă prin poştă, transmisă prin mijloace electronice, prezentată pe filme sau comunicată în timpul unei conversaţii etc.

Securitatea informaţiei se obţine prin acţiuni de protecţie faţă de o gamă largă de ameninţări cu scopul de a asigura continuitatea activităţii organizaţiei, minimizarea riscului apariţiei şi manifestării unor evenimente nedorite şi maximizarea investiţiei şi oportunităţilor organizaţiei.

Tipurile de amenințări cibernetice pot fi clasificate în funcție de efectele lor asupra datelor (divulgare, modificare, distrugere sau refuzul accesului) ori în funcție de principiile de bază privind securitatea informațiilor care sunt încălcate - ***figura 1.***

Figura 1 – Tipuri de amenințări și principiile de securitate pe care acestea le pun în pericol

Sursa: Curtea de Conturi Europeană, pe baza unui studiu al Parlamentului European[4]. Lacăt = securitatea nu este afectată; semn de exclamare = securitatea este pusă în pericol.

Securitatea informaţiei este un concept mai larg care se referă la asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei. Dinamica tehnologiei informaţiei induce noi riscuri pentru care organizaţiile trebuie să implementeze noi măsuri de control.

Majoritatea incidentelor de securitate sunt generate de o gestiune şi organizare necorespunzătoare, şi mai puţin din cauza unei deficienţe a mecanismelor de securitate.

Este important ca organizaţiile să conştientizeze riscurile asociate cu utilizarea tehnologiei şi gestionarea informaţiilor şi să abordeze pozitiv acest subiect:

- printr-o conştientizare în rândul angajaţilor a importanţei securităţii informaţiilor;
- prin înţelegerea tipologiei ameninţărilor, riscurilor şi vulnerabilităţilor specifice mediilor informatizate;
- Prin aplicarea politicilor/practicilor de control.

ÎN STRATEGIA NAŢIONALĂ DE APĂRARE A ŢĂRII PENTRU PERIOADA 2020-2024
se specifică următoarele:

Evoluţiile din domeniul tehnologic determină diversificarea şi creşterea complexităţii riscurilor şi ameninţărilor de securitate, precum atacurile cibernetice, activităţile specifice domeniului informaţional (acţiuni ostile/de influenţă derulate în spaţiul public, dezinformare, răspândirea de ştiri false/fabricate etc.) şi posibile efecte nocive şi destabilizatoare ale importului unor tehnologii cu uz civil în cadrul acţiunilor asimetrice şi hibride, generând noi provocări de securitate.

În domeniul social, mediul de securitate este influenţat de evoluţia demografică asimetrică, urbanizarea rapidă, polarizarea societăţilor, accentuarea fenomenului de îmbătrânire a populaţiei, creşterea individualismului şi a izolării în spaţiul virtual, a vulnerabilităţii mediilor de socializare online la acţiunile de război informaţional și de fenomenul migraţiei.

Sursa: https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf

Tendința exponenţială de dezvoltare a tehnologiilor emergente (5G, 6G, inteligenţa artificială, *big data, Internet of Things*, *cloud* şi *smart computing*) generează:

- nevoi de creştere şi îmbunătăţire a comunicaţiilor care vor susţine servicii digitale inovatoare menite să sprijine cetăţenii şi mediul de afaceri,
- necesităţi de colectare şi securizare a datelor şi informaţiilor vehiculate în sistemele respective.

Având în vedere că **rețelele 5G vor susţine multiple aplicații de comunicații și tehnologia informațiilor** implementate inclusiv la nivelul infrastructurilor critice, CONFIDENȚIALITATEA, INTEGRITATEA ȘI DISPONIBILITATEA telecomunicaţiilor, vor constitui probleme importante din perspectiva securităţii naţionale.

Vulnerabilităţi tehnologice ale reţelelor 5G ar putea fi exploatate pentru compromiterea în lanţ a infrastructurilor interdependente, cu riscul provocării unor **daune severe.**

https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf

Utilizarea **noilor tehnologii** de către entităţi ale criminalităţii organizate şi infracţionalităţii cibernetice, grupări şi organizaţii cu profil terorist sau extremist şi actori interesaţi să dezvolte acţiuni ofensive **se situează pe un trend ascendent**.

Dependența serviciilor de comunicații de un **număr restrâns de furnizori de tehnologie** sau existența unor **fluxuri nesecurizate de achiziții de tehnologii** utilizate în furnizarea de servicii esențiale sau critice, reprezintă un fenomen cu impact asupra disponibilității și integrității rețelelor de comunicații.

Nivelul redus de securitate cibernetică a infrastructurilor de comunicații și tehnologia informației din domenii strategice (inclusiv ca efect al vulnerabilităţilor tehnologice şi procedurale ale infrastructurilor deţinute de operatorii de comunicaţii) facilitează derularea de atacuri cibernetice de către actori statali sau non-statali.

https://dnsc.ro/vezi/document/raport-alerte-cert-ro-2016

https://dnsc.ro/citeste/dispozitive-retea-vizate-de-atacatori-cibernetici

Implementarea agendei de cooperare NATO-UE, cu precădere în domeniile apărare cibernetică, combaterea ameninţărilor hibride, contracararea ameninţărilor teroriste, rezilienţă, comunicare strategică şi mobilitate militară, reprezintă o prioritate;

https://www.consilium.europa.eu/ro/policies/defence-security/

https://www.consilium.europa.eu/en/policies/cybersecurity/

Sectoarele critice precum transportul, energia, sănătatea și finanțele au devenit din ce în ce mai dependente de tehnologiile digitale pentru a-și desfășura activitatea de bază.
În timp ce digitalizarea aduce oportunități enorme și oferă soluții pentru multe dintre provocările cu care se confruntă Europa, DAR în ultimul timpul crizei COVID-19, s-a identificat faptul ca, digitizarea EXPUNE economia și societatea la amenințări cibernetice.

Exista numeroase documente publice privind controlul securităţii informaţiei ca de exemplu:

- https://www.sri.ro/assets/files/cyberint/CybersecurityRO2019.pdf
- https://csrc.nist.gov/publications
- https://csrc.nist.gov/csrc/media/Publications/white-paper/2022/02/24/getting-started-with-cybersecurity-risk-management-ransomware/final/documents/quick-start-guide--ransomware.pdf
- https://cert.europa.eu/cert/filteredition/en/CERT-LatestNews.html
- https://dnsc.ro/
- https://ef.ic3.gov/default.aspx
- https://www.consilium.europa.eu/en/policies/cybersecurity/

https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906065

Ghid pentru evaluarea controalelor de securitate si planuri eficiente de evaluare a securității

Archived NIST Technical Series Publication

The attached publication has been archived (withdrawn), and is provided solely for historical purposes. It may have been superseded by another publication (indicated below).

Archived Publication

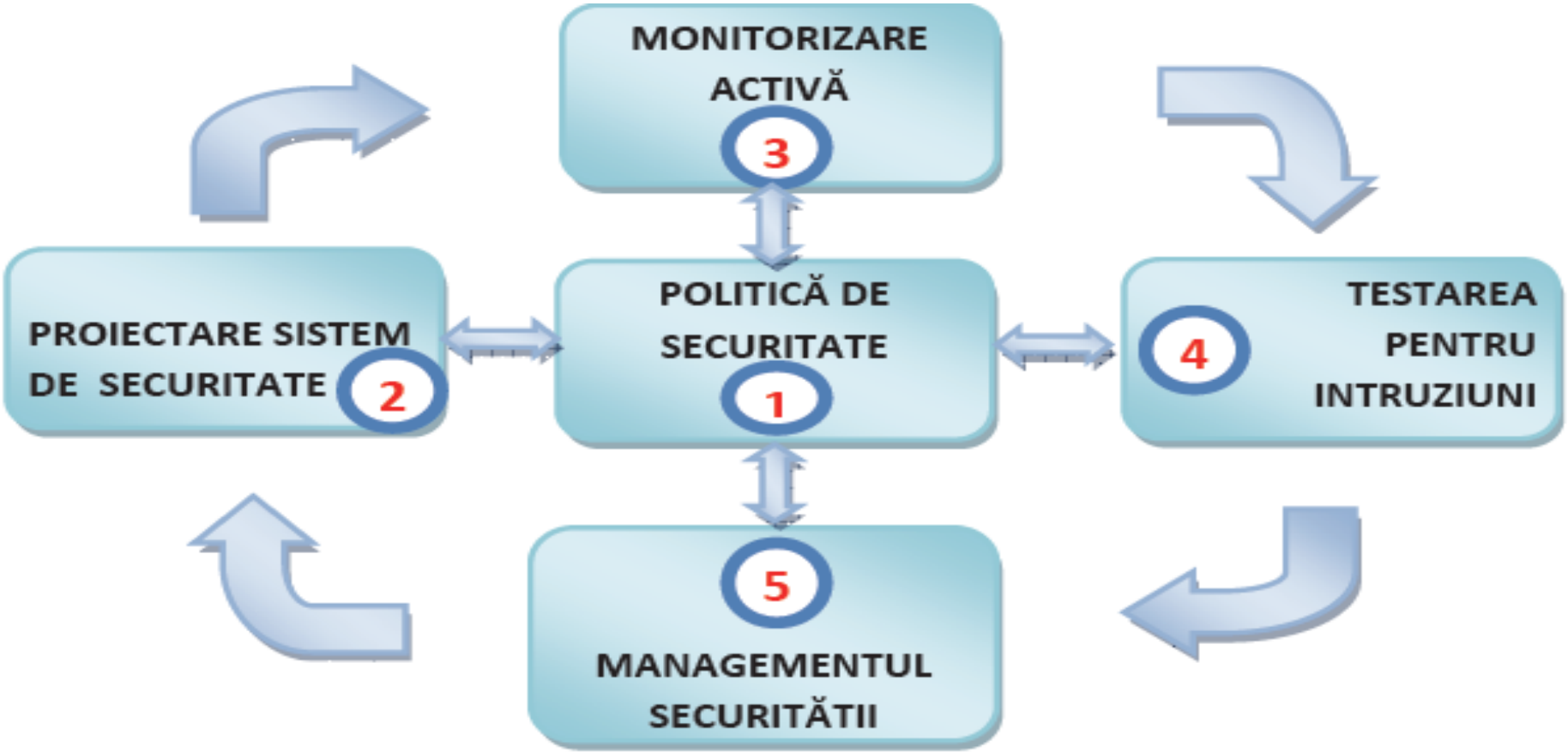
Series/Number:	NIST Special Publication 800-53A Revision 1
Title:	Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans
Publication Date(s):	June 2010
Withdrawal Date:	December 11, 2015
Withdrawal Note:	SP 800-53A Rev. 1 is withdrawn one year after the publication of SP 800-53A Rev. 4 (December 2014), and is superseded in its entirety.

Amenințări și vulnerabilități

Identificarea amenințărilor de securitate impune o analiză amplă asupra impactului și consecințelor acestor evenimente.

Pe termen scurt, impactul unei amenințări a sistemului informatic, poate consta în divulgarea, modificarea, distrugerea ori nefunctionarea acestuia.

Pe termen lung, consecințele pot fi mai grave, ... poate chiar pierderea afacerii unei companii, încălcarea dreptului la viață privată și intimitate, procese civile, amenzi, pierderi de vieți omenești etc.



Model de strategie privind securitatea informaţiilor într-o organizaţie

Sursa: **CMS (Content Management System) Instrument de comunicare online pentru Administraţia Publică**

Solutii pentru evitarea consecintelor negative ale atacurilor cibernetice

Adoptarea unui comportament responsabil la nivel instituțional, care implică:

- evitarea utilizarii de tehnologii si solutii software care nu mai beneficiaza de mentenanță;
- conectarea securizată la infrastructurile IT&C prin utilizarea unui user și a unei parole complexe;
- separarea fizica a rețelei interne (Intranet) de cea externă (Internet);

- utilizarea unei solutii de tip Antivirus si actualizarea constanta a acesteia;
- actualizarea sistemelor de operare dar și a aplicatiilor din cadrul infrastructurilor IT&C;
- realizarea cu regularitate a unor copii de siguranta;
- interzicerea instalarii de software fara licenta;
- utilizarea solutiilor de detectie/preventie (de tip IDS/IPS) a intruziunilor in infrastructurile IT&C;
- gestionarea corecta a dispozitivelor de memorie externa (CD/DVD, stick USB);

- evitarea deschiderii mesajelor care nu prezinta veridicitate;
- evitarea accesarii linkurilor si a deschiderii atasamentelor nesigure din email;
- evitarea introducerii de date personale in cadrul unor pagini web;
- evitarea utilizarii retelelor WI-FI cu acces nerestrictionat;
- pregatire in domeniul securitatii cibernetice;
- instruirea periodica a utilizatorilor infrastructurilor IT&C cu privire la politicile si normele interne de securitate, precum si cu privire la pericolele/riscurile de securitate cibernetica la care se expun in procesul de utilizare a mediului online.

Posibile cauze ale atacurilor informatice--

- Greşelile de configurare, bug-urile software, experienţă, graba…/ etc;
- Lipsa informaţiilor despre securitatea datelor;
- Uneori cărţile de specialitate/programare nu tratează problemele de securitate;
- Existenţa unor limbaje de programare nesigure;
- Utilizatorii nu sunt suficient de atenţi la securitatea datelor;
- Securitatea este consumatoare de timp, costă şi este uneori dificilă;
- O serie de echipamente şi aplicaţii folosesc parole default în momentul instalării, care trebuiesc schimbate cât mai repede posibil.
- Lipsa de specialişti în securitatea informaţiilor/datelor; IoT

- 121118 manager securitatea informaţiei (Chief Information Security Officer -CISO)
- **133008 director departament securitate ??**
- 241239 ofiţer securitatea informaţiei (SecurityOfficer –SO)
- 251402 specialist în proceduri şi instrumente de securitate a sistemelor informatice
- 252201 administrator sistem de securitate bancară
- (Administratorii de sistem dezvoltă, controlează, întreţin şi sprijină performanţa optimă şi securitatea sistemelor de tehnologia informaţiei.)
- 242113 consultant de securitate

http://www.mmuncii.ro/j33/index.php/ro/2014-domenii/munca/c-o-r
http://www.mmuncii.ro/j33/images/Documente/Munca/COR/23062020ISCO_08_lista_alfabetica_ocupatii_cor.pdf

https://static.anaf.ro/static/10/Anaf/Clas_ocup.pdf

Specialistul in proceduri si instrumente de securitate a sistemelor informatice standard ocupational:

- **elaborează şi aplică** elemente din programul de securitate, inclusiv cele referitoare la securitatea fizică a datelor, asigură confidenţialitatea informaţiilor şi disponibilitatea lor pentru persoanele în drept să le obţină şi să le folosească;
- **identifică si evaluează** vulnerabilităţile sistemului informatic, identifică ameninţările potenţiale, evaluează şi prioritizează pierderile;
- **găseşte** răspunsurile la violările de securitate identificate şi **raportate;**
- **proiectează** politici si proceduri de securitate aplicabile sistemului informatic;
- **elaborează** ghiduri de bună practică**?** legate de cerinţele de securitate ale sistemului informatic şi de măsurile necesare pentru protejarea sistemului;

- **aplică** standardele de securitate pentru reţele şi calculatoare şi validează din punctul de vedere al securităţii sistemul informatic (soluţia IT&C aflată in funcţiune);
- **monitorizează / supraveghează** aplicarea măsurilor de securitate proiectate pentru protejarea bunurilor fizice, a aplicaţiilor şi a altor produse software, a datelor şi colecţiilor de date faţă de utilizarea neautorizată;
- **analizează şi revizuieşte** ameninţările, vulnerabilităţile, politicile, procedurile şi instrumentele legate asigurarea securităţii sistemului informatic;
- **elaborează** rapoarte legate de asigurarea securităţii sistemului informatic, de gradul de aplicare a măsurilor de securitate stabilite, de vulnerabilităţile cunoscute şi asumate.

ATENTIE:

- *Nu exista aplicatii 100% lipsite de vulnerabilităţi, dar se pot reduce problemele/vulnerabilitatile odata cu identificarea acestora.*
- *Aplicarea unei masuri de securitate nu trebuie sa consume mult timp.*
- *Nu se fac presupuneri cu privire la securitatea unei aplicatii (exista deja ghiduri de securitate pentru multe tipuri de aplicatii, scanner)*
- *Este recomandata efectuarea de upgrade pentru softul utilizat, folosirea parolelor complexe; schimbarea periodica; blocarea conturilor dupa un numar de încercari nereusite; jurnalizarea încercarilor esuate etc.*

Nu exista aplicatii 100% lipsite de vulnerabilităţi, dar se pot reduce problemele/vulnerabilitatile odata cu identificarea acestora.

https://nvd.nist.gov/vuln/detail/CVE-2021-30642

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/security-advisories/0/SYMSA17969

CVE-2021-30642 este exploatabil în Security Analytics numai atunci când atacatorul de la distanță poate accesa interfața de utilizare web. Administratorii Security Analytics pot configura firewall-ul de pe dispozitiv pentru a restricționa accesul la interfața de utilizare web la adrese IP și subrețele de încredere.

https://owasp.org/www-community/Vulnerability_Scanning_Tools

Securitatea informaţiei se obţine prin implementarea unui set adecvat de politici şi proceduri specifice.

Standard ocupational - Specialist_securitate_IT.pdf

- Informaţiile şi resursele (bunurile) care au legătură cu informaţia pot fi: baze de date, fişiere de date, contracte, acorduri, documentaţii, informaţii rezultate din cercetare, manuale de utilizare, specificaţii de realizare, specificaţii tehnice de orice fel, materiale folosite pentru instruirea personalului, proceduri operaţionale şi ajutătoare, planuri curente şi cele legate de continuarea activităţii (afacerii), arhive şi informaţii arhivate, dovezi de audit, resurse software (programe / aplicaţii, sisteme de operare, programe utilitare, instrumente pentru dezvoltarea şi testarea aplicaţiilor, jurnale de evenimente, jurnale de erori, registrele care consemnează operaţii efectuate şi stări constatate), resurse hardware (echipamente, inclusiv echipamentele mobile, mijloace / medii de comunicaţii).

Securitatea informaţiei înseamnă protecţia în faţa ameninţărilor identificate şi pentru care a fost evaluat riscul materializării, manifestării acestora.

Pentru realizarea unei bune securitati, specialistul în proceduri şi instrumente pentru securitatea sistemelor informatice, trebuie sa detina cunostinte despre:

- **hardware si software: arhitecturi de calculatoare, sisteme de operare, sisteme de fişiere, permisiuni de acces, privilegii, restricţii, baze de date, aplicaţii diverse;**
- **reţele de calculatoare: topologii LAN, WAN, topologii VLAN, principii de securitate a reţelelor, servere, proceduri şi instrumente de autentificare, conectarea în reţea, managementul serviciilor director de resurse, interconectarea reţelelor, echipamente de interconectare, segmentarea reţelelor, firewall, conectivitatea la Internet, protocoale, infrastructură specifică, servicii de reţea, comunicaţii sigure;**
- **managementul riscului, vulnerabilităţi, ameninţări; politici, proceduri, instrumente pentru: detectarea intruşilor şi intruziunilor, protecţia faţă de atacurile asupra sistemului informatic, păstrarea integrităţii şi confidenţialităţii datelor.**

https://dnsc.ro/vezi/document/cod-bune-practici-securitate-it-2015

Securitatea sistemelor informaționale

Securitatea sistemului informațional trebuie să fie o responsabilitate asumată de către structurile de conducere ale oricărei organizații din mediul privat sau public.

Structurile de conducere trebuie să asigure o direcţie clară şi gestionată corespunzator pentru indeplinirea obiectivelor stabilite prin politica de securitate, având în vedere următoarele elemente:

- Revizuirea și aprobarea politicii de Securitate şi stabilirea de responsabilităţi legate de aceasta;
- Monitorizarea schimbărilor semnificative, de expunerea sistemului informațional la ameninţări majore;
- Revizuirea și monitorizarea incidentelor de securitate a sistemului informațional;
- Aprobarea măsurilor de sporire a securității informațiilor.

- În vederea stabilirii și menținerii politicilor de Securitate este esențială implicarea specialiștilor din domeniu în vederea adoptării deciziilor privind securitatea sistemului informațional.

- Accesul la echipamentele de prelucrare a informaţiilor organizației de către terţe părţi trebuie să se facă sub supraveghere.

- Pentru accesul terţilor, o evaluare a riscului ar trebui să fie efectuată pentru a stabili implicaţiile de securitate şi cerinţele de control.

- Toate activele sistemului informațional ar trebui să fie contabilizate şi să aibă un responsabil desemnat.

Activele sunt de obicei persoane, echipamente, sisteme sau infrastructura IT.)

- Responsabilul unui element din sistemul informațional trebuie să aibă responsabilități pentru menţinerea și implementarea de controale adecvate.
- Responsabilitățile pentru control pot fi delegate.

Pentru a reduce riscurile de eroare umană, furt, fraudă sau de abuz de încredere, responsabilităţi cu privire la securitatea informatiei trebuie să fie implementate încă din etapa de recrutare, incluse în contractele de muncă şi monitorizate în timpul activității la locul de muncă.

Toți angajații proprii sau terțele persoane care au acces la sistemul informațional al unei companii ar trebui să semneze un acord de confidențialitate.

Pentru a ne asigura că utilizatorii sunt conştienţi de ameninţările de securitate a informațiilor şi sunt pregătiți pentru a sprijini politica de securitate organizaţională în cursul activităţii lor la locul de muncă, angajații proprii sau terțele persoane ar trebui să fie instruiţi cu privire la procedurile de securitate şi utilizarea corectă a sistemelor de prelucrare a informațiilor.

- Toate incidentele de securitate trebuiesc raportate. Se recomanda implementat un sistem eficient și rapid de raportare a incidentelor de securitate, care să fie cunoscut de către toți angajații.

- Informațiile de business critice sau sensibile trebuie să fie stocate în locuri sigure, protejate într-un perimetru de securitate adecvat, cu bariere de securitate corespunzătoare și controale de acces.

- Acestea ar trebui să fie protejate fizic împotriva accesului neautorizat, deteriorare şi interferenţe. Protecţia oferită trebuie să fie proporţională cu riscurile identificate.

https://cert.ro/vezi/document/ghid-protectie-functionari-publici

Reguli de securitate informatică

- Utilizați echipamentele de calcul de serviciu în scop profesional, de serviciu;
- Instalați pe echipamentele de calcul de serviciu numai aplicații utilizate în scop profesional, de serviciu.
- Utilizați pe echipamentele de calcul de serviciu numai aplicații software validate de către compartimentul IT al instituției dumneavoastră;
- Instalați pe echipamentele de calcul de serviciu numai aplicații cu licență validă (comercială, gratuită sau cu sursă deschisă) și care provin numai din surse sigure, verificabile de către compartimentele IT ale instituției dumneavoastră;

- Utilizați echipamentele de calcul în scop profesional, de serviciu, numai în locații în care riscul de efracție și delapidare este foarte redus;
- Nu lăsați niciodată nesupravegheat și în locații cu risc mai ridicat de efracție sau delapidare un echipament de calcul utilizat în scop profesional, de serviciu;
- Utilizați în rețelele de date de serviciu numai echipamente de calcul pe care este instalat numai software cu licență validă (care nu sunt piratate), care nu au software malware instalat și care nu prezintă risc de securitate cibernetica;

- Păstrați credentialele (nume de utilizator, parole, coduri pin etc.) criptate, utilizând aplicații dedicate acestui scop și validate de către compartimentul IT al instituției dumneavoastră.
- Nu păstrați credențiale scrise pe foi de hârtie în loc vizibil, sau în format electronic în clar (necriptate).

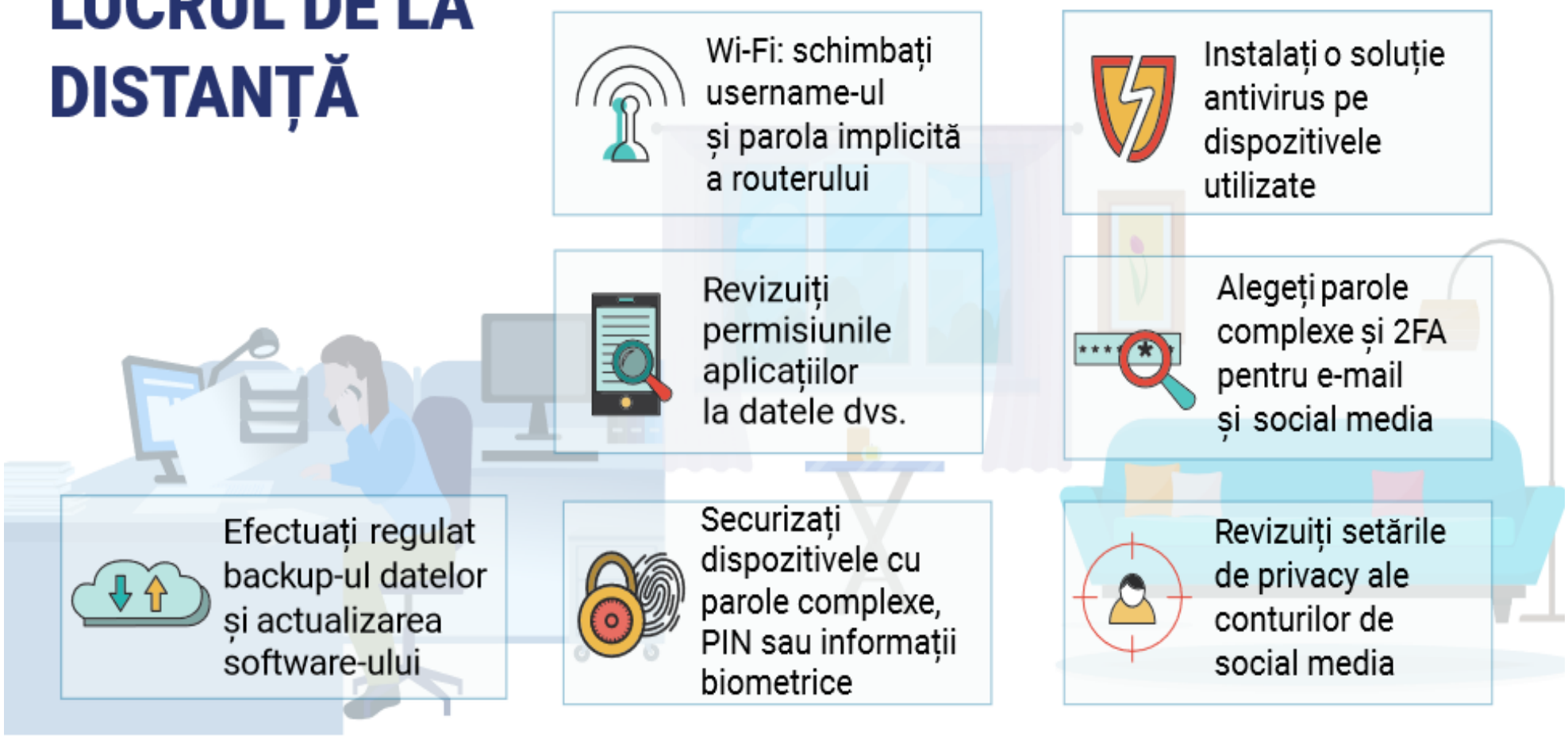
- Solicitați compartimentului IT al instituției dumneavoastră o copie în format hârtie sau electronic a ghidului, sau manualului de utilizare a echipamentelor de calcul în interiorul, sau în interesul unei instituții publice;

…Contabilitate și securitatea cibernetică https://ceccar.ro/ro/?p=8249

- De ce este securitatea cibernetică importantă pentru orice firmă, în special pentru cele care lucrează cu cifre și cu bani? Orice dispozitiv care poate stabili o legătură cu internetul devine o potențială poartă pentru un atac cibernetic prin care se poate ajunge în interiorul rețelei interne și se pot accesa și compromite date. Acest lucru înseamnă nu doar o amenințare serioasă pentru o firmă din punct de vedere al costurilor și al logisticii, dar și o afectare a reputației și a încrederii clienților. Printre soluțiile disponibile pentru orice firmă de contabilitate care dorește să își asigure succesul se numără: apelarea la o firmă de specialitate de IT, alinierea la cele mai recente evoluții tehnologice, o atitudine pro-activă și decizii bine informate.
- Pentru mai multe informații despre securitatea cibernetică, vă invităm să consultați pagina Accountancy Age.

SFATURI PENTRU LUCRUL DE LA DISTANȚĂ

EUROPOL | EC3 European Cybercrime Centre



- Wi-Fi: schimbați username-ul și parola implicită a routerului
- Instalați o soluție antivirus pe dispozitivele utilizate
- Revizuiți permisiunile aplicațiilor la datele dvs.
- Alegeți parole complexe și 2FA pentru e-mail și social media
- Efectuați regulat backup-ul datelor și actualizarea software-ului
- Securizați dispozitivele cu parole complexe, PIN sau informații biometrice
- Revizuiți setările de privacy ale conturilor de social media

Fenomenul de ‘Zoombombing’ a devenit o problemă, iar unii utilizatori pot accesa cu ușurință video-conferinţele altora, dacă nu se respectă câteva măsuri esențiale de securizare a comunicației.

- https://zoom.us/docs/doc/Securing%20Your%20Zoom%20Meetings.pdf
- https://futurumresearch.com/research-notes/what-to-do-about-zoombombing-as-hackers-and-security-issues-plague-zoom/
- Pentru a îmbunătăţi securitatea atunci când folosiţi Zoom şi totodată pentru a evita fenomenul de ‘Zoombombing’:

- Generaţi un ID (cod) unic pentru video-conferinţa dumneavoastră şi evitaţi să faceţi public codul.
- Asiguraţi-vă că aţi creat o parolă pentru video-conferinţă
- Activaţi “Waiting Room (Cameră de Aşteptare)”, care permite doar prezentatorului să deschidă video-conferinţa
- Blocaţi şedinţa în momentul în care toţi invitaţii sunt prezenţi
- Activaţi “Automatic Updates (Actualizarea Automată)” pentru a asigura actualizarea aplicației Zoom
- În opţiunile de securitate, prezentatorul/gazda poate să elimine participanţi, dar și să restricţioneze posibilitatea lor de a prezenta ecranul, de a-şi schimba numele, sau de a aduce modificări materialului prezentat de către gazda video-conferinţei.
- Nu postați poze din Zoom pe rețelele de socializare, deoarece pot dezvălui, din greșeală, ID-urile întâlnirilor.
- Nu partajați ID-ul și parola unei sesiuni Zoom pe rețelele de socializare,deoarece oricine deține aceste detalii poate participa la videoconferința inițiată de dvs.

Infractorii cibernetici

- https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact

- Priorities 2022-2025

Cyber-attacks	To target the criminal offenders orchestrating cyber-attacks, particularly those offering specialised criminal services online.

https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime

Gama imensă de oportunități pe care infractorii cibernetici au căutat să le exploateze este impresionantă. Aceste infracțiuni includ:
utilizarea botnet-urilor – rețele de dispozitive infectate cu malware fără știrea utilizatorilor lor – pentru a transmite viruși care obțin controlul ilicit de la distanță al dispozitivelor, fură parole și dezactivează protecția antivirus;
crearea de „uși din spate” pe dispozitivele compromise pentru a permite furtul de bani și date, sau acces de la distanță la dispozitive pentru a crea botnet-uri;
crearea de forumuri online pentru a tranzacționa expertiză în domeniul hackingului;

- spălarea monedelor tradiționale și virtuale;
- comiterea de fraude online, cum ar fi prin sisteme de plată online, carduri și inginerie socială;
- diverse forme de exploatare sexuală a copiilor online, inclusiv distribuirea online de materiale de abuz sexual asupra copiilor și transmiterea în direct a abuzului sexual asupra copiilor;
- găzduirea online a operațiunilor care implică vânzarea de arme, pașapoarte false, carduri de credit contrafăcute și clonate și medicamente, precum și servicii de hacking.

Crime de înaltă tehnologie

Programele malware, sau software-ul rău intenționat, infiltrează și câștigă controlul asupra unui sistem computerizat sau a unui dispozitiv mobil pentru a fura informații valoroase sau a deteriora datele. Există multe tipuri de malware care se pot completa reciproc atunci când efectuează un atac.

O rețea botnet - este formată din computere care comunică între ele prin internet. Un centru de comandă și control le folosește pentru a trimite spam, pentru a realiza atacuri distribuite de refuzare a serviciului (DDoS) și pentru a comite alte infracțiuni.

Un rootkit este o colecție de programe care permit accesul la nivel de administrator la un computer sau o rețea de computere, permițând astfel atacatorului să obțină acces root sau privilegiat la computer și, eventual, la alte mașini din aceeași rețea.

Worm - un vierme se reproduce într-o rețea de computere și efectuează acțiuni rău intenționate fără îndrumare.

Un troian se prezintă ca un program legitim sau este încorporat într-un program legitim, dar este conceput pentru scopuri rău intenționate, cum ar fi spionajul, furtul de date, ștergerea fișierelor, extinderea unei rețele bot și efectuarea de atacuri DDoS.

A file infector infectează fișierele executabile (cum ar fi .exe) suprascriindu-le sau inserând cod infectat care le dezactivează.

A backdoor/remote-access trojan (RAT)

Un troian backdoor/acces la distanță (RAT) accesează un sistem informatic sau un dispozitiv mobil de la distanță. Poate fi instalat de un alt program malware. Oferă control aproape total atacatorului, care poate efectua o gamă largă de acțiuni, inclusiv: acțiuni de monitorizare, executarea comenzilor, trimiterea de fișiere și documente înapoi către atacator înregistrarea apăsărilor de taste făcând capturi de ecran

- **Ransomware** stops users from accessing their devices and demands that they pay a ransom through certain online payment methods to regain access. A variant, police ransomware, uses law enforcement symbols to lend authority to the ransom message.
- **Scareware** is fake anti-virus software that pretends to scan and find malware/security threats on a user's device so that they will pay to have it removed.
- **Spyware** is installed on a computer without its owner's knowledge to monitor their activity and transmit the information to a third party
- **Adware** displays advertising banners or pop-ups that include code to track the user's behaviour on the internet

https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime

- În 2013, Europol a înființat Centrul european pentru criminalitatea cibernetică (EC3) pentru a consolida răspunsul organelor de aplicare a legii la criminalitatea cibernetică din UE și pentru a ajuta la protejarea cetățenilor, întreprinderilor și guvernelor europene.

- În fiecare an, EC3 emite Evaluarea Amenințării Crimei Organizate pe Internet (IOCTA), menționată mai sus, care stabilește prioritățile pentru Planul Operațional de Acțiune EMPACT în domeniile criminalității cibernetice care sunt vizate pentru anul respectiv.

- EC3 găzduiește, de asemenea, grupul operativ comun de acțiune împotriva criminalității cibernetice (J-CAT). Misiunea sa este de a conduce acțiuni coordonate, conduse de informații împotriva amenințărilor cheie ale criminalității cibernetice prin investigații și operațiuni transfrontaliere ale partenerilor săi.

Aceste cooperari instituționale au condus la succese notabile la nivel operațional, inclusiv:

- coordonarea unei operațiuni comune, inclusiv parteneri din sectorul privat, pentru a viza un botnet, Ramnit, care infectase milioane de computere din întreaga lume;
- coordonarea cu Eurojust într-o operațiune care vizează atacuri malware la scară largă care au avut originea în Ucraina și care erau investigate de o serie de agenții — o operațiune care a dus la zeci de arestări și continuă să furnizeze dovezi care susțin alte investigații privind criminalitatea cibernetică;
- o operațiune care vizează un forum major infracțional cibernetic implicat în tranzacționarea expertizei în hacking, malware și rețele bot, Zero Day Exploits, acces la servere compromise și parteneri de potrivire pentru campanii de spam și atacuri malware.

Art. 249. Frauda informatică

Introducerea, modificarea sau ştergerea de date informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul, dacă s-a cauzat o pagubă unei persoane, se pedepseşte cu închisoarea de la 2 la 7 ani.

Art. 250. Efectuarea de operaţiuni financiare în mod fraudulos

(1) Efectuarea unei operaţiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, prin utilizarea, fără consimţământul titularului, a unui instrument de plată electronică sau a datelor de identificare care permit utilizarea acestuia, se pedepseşte cu închisoarea de la 2 la 7 ani.
(2) Cu aceeaşi pedeapsă se sancţionează efectuarea uneia dintre operaţiunile prevăzute în alin. (1), prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive.
(3) Transmiterea neautorizată către altă persoană a oricăror date de identificare, în vederea efectuării uneia dintre operaţiunile prevăzute în alin. (1), se pedepseşte cu închisoarea de la unu la 5 ani.

Art. 251. Acceptarea operaţiunilor financiare efectuate în mod fraudulos

(1) Acceptarea unei operaţiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, cunoscând că este efectuată prin folosirea unui instrument de plată electronică falsificat sau utilizat fără consimţământul titularului său, se pedepseşte cu închisoarea de la unu la 5 ani.

(2) Cu aceeaşi pedeapsă se sancţionează acceptarea uneia dintre operaţiunile prevăzute în alin. (1), cunoscând că este efectuată prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive.

https://niccs.cisa.gov/about-niccs

Profesioniștii în securitate cibernetică sunt la mare căutare. Experții estimează că până în 2022 va exista o lipsă globală de 1,8 milioane de profesioniști în securitate cibernetică pentru a ocupa acele posturi critice. Cu această lipsă de specialisti în domeniul securității cibernetice, educatorii/tutorii sunt într-o poziție importanta pentru a ajuta studenții să-și dezvolte abilitățile tehnice pentru a urma o carieră în această industrie.

https://fedvte.usalearning.gov/public_fedvte.php

…deocamdată…., în codul ocupaţiilor din România sunt câteva calificări care să reflecte competenţele dobândite in domeniul Securitatii IT.
Administrator de baze de date (213903) ;

- Administrator de retea de calculatoare (252301), Specialist SIG/IT (252901),
- Administrator sistem de securitate bancara (252201),
- Specialist in proceduri si instrumente de securitate a sistemelor informatice (251402), Manager securitatea informatiei (Chief Information Security Officer - CISO) (121118), Ofiter securitatea informatiei (Security Officer – SO)(241239),
- Inginer de sistem in informatica (251203),
- Consultant în informatică (251901);

- Cybercrime To Cost The World $10.5 Trillion Annually By 2025

Dacă ar fi măsurată ca țară, atunci criminalitatea cibernetică – despre care se preconizează că va provoca daune în valoare totală de 6 trilioane USD la nivel global în 2021 – ar fi a treia economie din lume după SUA și China.
Cybersecurity Ventures se așteaptă ca costurile globale ale criminalității cibernetice să crească cu 15% pe an în următorii cinci ani, ajungând la 10,5 trilioane USD anual până în 2025, în creștere de la 3 trilioane USD în 2015.

Acesta reprezintă cel mai mare transfer de bogăție economică din istorie, riscă stimulentele pentru inovație și investiții, este exponențial mai mare decât daunele cauzate de dezastrele naturale într-un an și va fi mai profitabilă decât comerțul global cu toate drogurile ilegale majore combinate.

https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

Estimarea costurilor daunelor se bazează pe cifrele istorice ale criminalității cibernetice, inclusiv pe o creștere recentă de la un an la altul, o creștere dramatică a activităților de hacking a bandelor criminale organizate și sponsorizate de statul național ostil și o suprafață de atac cibernetic care va fi cu un ordin de mărime mai mare în 2025 decât este azi.

Costurile criminalității cibernetice includ deteriorarea și distrugerea datelor, bani furați, pierderea productivității, furtul de proprietate intelectuală, furtul de date personale și financiare, delapidarea, frauda, perturbarea post-atac a activității normale, investigația criminalistică, restaurarea și ștergerea documentelor piratate și daune reputaționale.

Raj Samani, fellow and chief scientist of the combined company formed after the merger of McAfee Enterprise and FireEye, said:

- Over this past year, we have seen cyber criminals get smarter and quicker at retooling their tactics to follow new bad actor schemes – from ransomware to nation states – and we don't anticipate that changing in 2022

- With the evolving threat landscape and continued impact of the global pandemic, it is crucial that enterprises stay aware of the cyber security trends so that they can be proactive and actionable in protecting their information

Top 10 cyber crime trends to watch for in 2022 /

Top 10 tendințe de criminalitate cibernetică de urmărit în 2022

https://www.thenationalnews.com/business/technology/2021/12/29/top-10-cyber-crime-trends-to-watch-out-for-in-2022/

1. Weaponising operational technology environments

Armarea mediilor de tehnologie operațională

Infractorii cibernetici ar putea arma mediile tehnologice operaționale pentru a dăuna sau ucide oameni în următorii patru ani, a spus compania de consultanță și cercetare tehnologică Gartner.

OT este un tip de sistem de calcul și comunicații – inclusiv hardware și software – care controlează operațiunile industriale, concentrându-se în principal pe dispozitivele fizice și procesele pe care le utilizează. Este folosit pentru a colecta și analiza date în timp real, care este folosit în continuare pentru a monitoriza o unitate de producție sau pentru a controla echipamente. Diverse industrii, cum ar fi telecomunicațiile și petrolul și gazele, folosesc OT pentru a se asigura că diferite dispozitive funcționează în coordonare (discutii Claroty din CyberX – UTM).

Atacurile asupra mediilor OT au evoluat de la „întreruperea imediată a procesului”, cum ar fi închiderea unei fabrici – de exemplu în recentul atac ransomware Colonial Pipeline, care a distrus cea mai mare conductă de combustibil din SUA – la compromiterea „integrității mediilor industriale” cu intenția de a provoca vătămări fizice sau reputaționale.

https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack

2. Remote working brings new challenges

Lucrul de la distanță pot in continuare sa stimuleze in pandemia de Covid-19 noi amenințări cibernetice în 2022. Dispozitivele de acasă pe care angajații le folosesc pentru a accesa rețelele de birou nu sunt de obicei supuse acelorași restricții de securitate ca și dispozitivele corporative. Acest lucru complică eforturile de a controla și monitoriza comportamentul digital al angajaților, aplicațiile și datele în afara firewall-urilor tradiționale, au spus semnalat cercetatorii in domeniul securitatii cibernetice.

3. Geopolitical cyber concerns pose growing risks

Unii actori de stat vor lansa atacuri cibernetice pentru că sunt „ieftine, fiabile, portabile, ușor de ascuns și greu de detectat”, a spus Moody’s Investors Service într-un raport de la începutul acestui an.

Atacurile sponsorizate de stat amenință cu deteriorarea reputației, provoacă întreruperea fluxului de lucru și pierderea proprietății intelectuale.

“Entities that find themselves the targets of these attacks could experience substantial credit damage,” the rating agency had said at the time.

4. Utilizarea rețelelor sociale pentru atacuri

Deși utilizarea rețelelor sociale pentru a viza victimele nu este o strategie nouă, este relativ neobișnuită. Necesită un nivel de cercetare pentru a implica ținta vulnerabilă în interacțiuni și pentru a stabili profiluri false. „Țintirea indivizilor s-a dovedit a fi un canal de mare succes și estimam că utilizarea acestui vector ar putea crește nu numai prin intermediul grupurilor de spionaj, ci și al altor actori care doresc să se infiltreze în organizații pentru propriul câștig criminal", au spus McAfee Enterprise și FireEye. în previziunile sale privind amenințările cibernetice pentru 2022.

Discutii despre atacul….

https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident

https://www.techtarget.com/searchsecurity/news/252486398/Twitter-breach-caused-by-social-engineering-attack

5. Schimburile de criptomonede pentru a experimenta o creștere a atacurilor

Bursele de criptomonede au înregistrat o creștere de 10 ori a atacurilor în prima jumătate a anului în comparație cu perioada anului precedent, se arată într-un raport al companiei de informații privind amenințările cibernetice PhishLabs, deși nu a dezvăluit numărul exact de atacuri.
Majoritatea atacurilor cu criptomonede au fost orchestrate prin intermediul rețelelor sociale. „Apreciem că în viitor afacerile cu criptomonede vor continua să fie vizate în mod agresiv de către hackeri, prin intermediul rețelelor sociale… ”, se arată în raport. Hackerii au realizat cel mai mare furt de criptomonede de până acum pe 10 august, furând 613 milioane de dolari în monede digitale de pe platforma de schimb de jetoane Poly Network, doar pentru a returna jetoane în valoare de 260 de milioane de dolari în mai puțin de 24 de ore.

https://www.phishlabs.com/

https://www.thenationalnews.com/business/cryptocurrencies/2021/09/21/how-hackers-pulled-off-the-biggest-cryptocurrency-heist-from-poly-network/

6. Atacurile de phishing

Phishing-ul vine de obicei sub formă de e-mailuri frauduloase sau de mesaje pop-up care au ca scop obținerea de informații personale de la victime, cum ar fi detaliile cardului de credit și date sensibile, inclusiv numerele personale de identificare, nume de utilizator și parole.

E-mailurile de tip phishing pot instala, de asemenea, în secret software rău intenționat sau malware în computerele victimelor. Astfel de instalări nefaste pot fi un virus sau un program spion conceput pentru a colecta mai multe informații, ceea ce ar putea duce la fraude suplimentare.

https://purplesec.us/phishing-whaling-differences/#PhishingAttacks

7. API-ul devenind o țintă profitabilă a IoT și traficul 5G

API-ul a devenind o țintă profitabilă a Internetul lucrurilor și traficul 5G între serviciile API (interfață de programare a aplicațiilor) și aplicații care, devin ținte din ce în ce mai profitabile, provocând expunerea nedorită a informațiilor. Natura conectată a API-urilor introduce, de asemenea, riscuri suplimentare pentru afaceri, deoarece acestea devin un vector de intrare pentru atacuri mai ample ale lanțului de aprovizionare, au spus McAfee Enterprise și FireEye.
„În majoritatea cazurilor, atacurile care vizează API-urile nu sunt detectate, deoarece sunt considerate în general căi de încredere și nu au același nivel de guvernanță și controale de securitate.”

Discutii si exemple practice....

8. Cyber security talent crunch

Anul care vine se va dovedi a fi cel mai provocator de până acum în ceea ce privește criza continuă a talentelor în domeniul securității cibernetice, a declarat firma americană de securitate cibernetică BeyondTrust. „Unii factori care provoacă acest dezechilibru dintre cerere și ofertă includ adoptarea accelerată a inițiativelor de transformare digitală și cloud hibrid, dezvoltarea proiectelor post-pandemie și bugetele care devin disponibile pentru cheltuieli”, a adăugat acesta.

https://www.beyondtrust.com/

9. Rise of ransomware

Utilizarea ransomware-ului a accelerat ritmul și a devenit mai periculoasă în 2021. Acesta își va continua creșterea rapidă și anul viitor, iar variațiile sale vor crește odată cu frecvența atacurilor. „ Organisations must stop trying to prevent adversaries' missions and instead prevent them from being worthwhile", a declarat Marty Edwards, vicepreședinte pentru tehnologie operațională la compania de securitate cibernetică cu sediul central din Columbia, Tenable. „ In other words, organisations must make sure these missions cost too much to conduct. If the reward doesn't cover the cost of the investment, threat actors won't pursue it", a adăugat Marty Edwards.

https://www.tenable.com/press-releases/tenable-appoints-marty-edwards-as-vice-president-of-operational-technology-security

Discutii despre Nessus Tenable - CyberX UTM

RANSOMWARE Ransomware – un malware care infectează computerele (și dispozitivele mobile) și restricționează accesul acestora la fișiere, amenințând adesea cu distrugerea permanentă a datelor, dacă nu se plătește o răscumpărare – a atins proporții epidemice la nivel global și este „metoda de atac de bază” pentru infractorii cibernetici. Un raport din 2017 de la Cybersecurity Ventures a prezis că daunele ransomware vor costa lumea 5 miliarde de dolari în 2017, față de 325 de milioane de dolari în 2015 - o creștere de 15 ori în doar doi ani. Pagubele pentru 2018 au fost estimate la 8 miliarde de dolari, iar pentru 2019 cifra a crescut la 11,5 miliarde de dolari. Cea mai recentă prognoză este ca costurile globale ale daunelor ransomware să ajungă la 20 de miliarde de dolari până în 2021 - ceea ce este de 57 de ori mai mult decât era în 2015.

10. Migrarea în cloud reprezintă o amenințare

Aproape jumătate dintre organizații au mutat în cloud funcții esențiale pentru afaceri, ca rezultat direct al pandemiei, a spus Tenable. Cu toate acestea, migrarea în cloud necesită considerații specifice care probabil vor fi trecute cu vederea în 2022. De exemplu, detectarea și prevenirea activităților rău intenționate în cloud este mult diferită, a spus Bob Huber, director de securitate la Tenable. „Și acest lucru poate fi complicat și mai mult de nuanțele lucrului cu furnizorii de cloud, precum și cu alte părți interesate ale companiei care doresc să adopte rapid noi servicii în cloud.Dacă organizațiile nu își educă întreaga echipă, nu doar echipele de securitate, despre securizarea cloud-ului, ele vor plăti inevitabil prețul pe măsură ce migrarea lor se accelerează”, a spus Bob Huber.

CYBERCRIME HITS HOME

Statele Unite, cea mai mare economie din lume, cu un PIB nominal de aproape 21,5 trilioane de dolari, reprezintă un sfert din economia mondială, potrivit datelor de la Nasdaq. Criminalitatea cibernetică a lovit SUA atât de tare încât, în 2018. Un agent special de supraveghere al FBI care investighează intruziunile cibernetice a declarat pentru The Wall Street Journal că fiecare cetățean american ar trebui să se aștepte ca toate datele lor (informații de identificare personală) să fie furate și să fie în DARK WEB— o parte a rețelei profunde — care este ascunsă în mod intenționat și folosită pentru a ascunde și promova activități odioase. Unele estimări indică dimensiunea deep web-ului (care nu este indexată sau accesibilă de motoarele de căutare) de până la 5.000 de ori mai mare decât suprafața web și crește într-un ritm care sfidează cuantificarea.

- https://money.cnn.com/infographic/technology/what-is-the-deep-web/

- https://money.cnn.com/2014/03/10/technology/deep-web/index.html

DARK WEB este locul în care infractorii cibernetici cumpără și vând programe malware, kituri de exploatare și servicii de atac cibernetic, pe care le folosesc pentru a lovi victimele - inclusiv întreprinderi, guverne, utilități și furnizori de servicii esențiale pe teritoriul SUA.
Un atac cibernetic ar putea dezactiva economia unui oraș, a unui stat.
Ted Koppel dezvăluie că un atac cibernetic major asupra rețelei electrice a Americii este posibil, ci și probabil, si ar fi devastator iar SUA este șocant de nepregătita.

https://www.amazon.com/Lights-Out-Cyberattack-Unprepared-Surviving/dp/0553419986

https://www.amazon.com/Lights-Out-Cyberattack-Unprepared-Surviving/dp/0553419986#customerReviews

Aceasta este o carte grozavă care evidențiază vulnerabilitățile pe care le-am dobândit cu Internetul, lipsa totală de pregătire din partea guvernului și a societății civile, precum și o oarecare lipsă de solidaritate din partea sectorului privat.

Omul de afaceri și filantrop miliardar Warren Buffet numește criminalitatea cibernetică problema principală a omenirii, iar atacurile cibernetice sunt o amenințare mai mare pentru umanitate decât armele nucleare.

Entitățile organizate de criminalitate cibernetică își unesc forțele, iar probabilitatea lor de detectare și urmărire penală este estimată a fi <0,05% în SUA, conform Raportului Global de Risc 2020 al Forumului Economic Mondial (pagina 68).

https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf/

FBI este preocupat în special de ransomware-ul care lovește furnizorii de asistență medicală, spitalele, 911 etc. Aceste tipuri de atacuri cibernetice pot avea un impact asupra siguranței fizice a cetățenilor americani, iar acesta este punctul de vârf pe care se concentrează Herb Stapleton, șeful secției cibernetice FBI și echipa sa.

Luna trecută, ransomware-ul și-a revendicat prima viață... Autoritățile germane au raportat că un atac de tip ransomware care a cauzat defecțiunea sistemelor IT la un spital important din Duesseldorf, iar o femeie care avea nevoie de internare urgentă a murit după ce a trebuit să fie dusă într-un alt oraș pentru tratament.

În 2020, în timp ce publicul american s-a concentrat pe pandemia globală, infractorii cibernetici au profitat de aceasta oportunitate cat si de dependența oamenilor de tehnologie -lucru pe internet. Infractori ciberbetici au folosit **phishing, spoofing, extortion** și diferite tipuri de fraude bazate pe internet care au avut ca obiectiv afectarea celor mai vulnerabili oameni din societatea - lucrătorii medicali care caută echipamente individuale de protecție, familiile care caută informații despre plata online a facturilor și multe altele.

Infracțiunile de acest tip sunt doar o mică parte din ceea ce combate FBI prin activitatea de investigare criminală și cibernetică.

IC3 - Crime Complaint Center a primit un număr record de plângeri din partea publicului american în 2020: 791.790, pierderile raportate depășind 4,1 miliarde de dolari.

Aceasta reprezintă o creștere cu 69 % a numărului total de plângeri față de 2019. Schemele de compromis prin e-mail de afaceri (BEC) au continuat să fie cele mai costisitoare: 19.369 de plângeri, cu o pierdere ajustată de aproximativ 1,8 miliarde de dolari. Înșelătoriile de tip phishing au fost, de asemenea, proeminente: 241.342 de plângeri, cu pierderi ajustate de peste 54 de milioane de dolari. Numărul incidentelor de tip ransomware continuă să crească, fiind raportate 2.474 de incidente în 2020.

https://www.ic3.gov/

Bibliografie suplimentara

- https://www.consilium.europa.eu/ro/policies/cybersecurity/
- https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_RO.pdf
- https://engineering.linkedin.com/blog/2016/10/finding-same-origin-method-execution-vulnerabilities
- https://www.bleepingcomputer.com/news/security/political-themed-actor-using-old-ms-office-flaw-to-drop-multiple-rats/
- https://static.anaf.ro/static/3/Anaf/20211019122833_1487-18.10.2021-cp%20emailuri%20false.pdf
- https://dnsc.ro/threats
- https://us-cert.cisa.gov/ncas/alerts/2021
- https://us-cert.cisa.gov/report-phishing
- https://us-cert.cisa.gov/report-phishing
  https://us-cert.cisa.gov/ncas/alerts/2021
- https://cert.europa.eu/cert/filteredition/en/VulnerabilitiesApplications.html
- https://nvd.nist.gov/
  https://owasp.org/www-community/attacks/
- https://www.bleepingcomputer.com/news/security/political-themed-actor-using-old-ms-office-flaw-to-drop-multiple-rats/