Co-funded by the Erasmus+ Programme of the European Union

Module de instruire InCyT

Securitatea informațiilor pentru manageri **Unitatea 3 Săptămâna 5** **Denumirea unității : Managementul securității informațiilor 3**	
Activități de învățare	❑ **Webinar** ❑ **Exerciții** ❑ **Workshop** ❑ **Prezentare** ❑ **Alte**
Responsabil de învățare	• George Matache et al.
Obiectivele activității de învățare	1 Terminologie generală 2. Confidențialitate, Integritate și Disponibilitate (CIA) 3. Reguli și standarde 4. Managementul securității informațiilor 5. Cum funcționează malware-ul? 6. Cele mai importante amenințări cibernetice 7. Tipuri de atacuri 8. Server Web Securizat – SSL 9. Trimiterea și primirea de e-mailuri 10. Managementul activelor
Abilități de dobândit	• TS3 Securitatea retelei • TS4 Testare de penetrare (vulnerabilități exploatabile). • SS3 Analiza cognitivă și comportamentală
Durata activității de învățare	2 săptămâni
Cerințe de învățare	***Ce e necesar?***
	• Acces la internet • Motor de cautare • MS Office365

Informații scurte despre modul

Descriere
Securitatea cibernetică este practica de a apăra computerele, serverele, dispozitivele mobile, sistemele electronice, rețelele și datele de atacuri rău intenționate. Este, de asemenea, cunoscut sub numele de securitatea tehnologiei informației sau securitatea informațiilor electronice. Termenul se aplică într-o varietate de contexte, de la afaceri la computere mobile, și poate fi împărțit în câteva categorii comune. Companiile sunt adesea atât de preocupate de operațiunile lor de zi cu zi încât uită să investească mult în securitatea rețelei. Alții înțeleg necesitatea unei securități cuprinzătoare în rețea, dar au o strategie indulgentă în ceea ce privește IT-ul lor, care poate fi la fel de dăunătoare în cazul unei scurgeri de date. Înțelegerea a ceea ce presupune securitatea rețelei, precum și a celor mai bune practici pe care le puteți respecta, care vă vor asigura că rețeaua companiei dvs. este protejată de numeroasele amenințări externe care doresc să vă infiltreze în rețea, este esențială pentru a vă păstra datele și, în cele din urmă, afacerea dvs. în siguranță. Este extrem de important ca instruirea în domeniul securității cibernetice pentru IMM-uri – manageri și angajați – să fie concretă și interactivă – precum și practică, deoarece IMM-urile mici nu au timp, motivație sau resurse de cheltuit pe această problemă de ce este foarte important. că instruirea este relevantă și gestionabilă pentru managerii care participă. Prin urmare, acest modul este un plan pe baza acestui lucru. Managementul securității informațiilor (ISM) definește și gestionează controalele pe care o organizație trebuie să le implementeze pentru a se asigura că protejează în mod sensibil confidențialitatea, disponibilitatea și integritatea activelor de amenințări și vulnerabilități. Malware sau „software rău intenționat” este un termen umbrelă care descrie orice program sau cod rău intenționat care dăunează sistemelor. Ostil, intruziv și în mod intenționat urât, malware-ul urmărește să invadeze, să deterioreze sau să dezactiveze computerele, sistemele informatice, rețelele, tabletele și dispozitivele mobile, adesea prin preluarea controlului parțial asupra operațiunilor unui dispozitiv. La fel ca gripa umană, interferează cu funcționarea normală. Motivele din spatele programelor malware variază. Programele malware pot fi legate de a face bani din tine, de a-ți sabota capacitatea de a lucra, de a face o declarație politică sau doar de a te lăuda. Deși programele malware nu pot deteriora hardware-ul fizic al sistemelor sau echipamentelor de rețea, ele vă pot fura, cripta sau șterge datele, pot modifica sau deturna funcțiile de bază ale computerului și vă poate spiona activitatea pe computer fără știrea dvs. sau permisiunea dvs. Programele malware sunt descrise și definite, introducând numeroasele sale tipuri diferite și explicând cum funcționează. De asemenea, descriem semnele de avertizare ale unui dispozitiv infectat și explicăm cum să îl prevenim. Cursanții ar putea fi informați despre astfel de aspecte citind

textul corespunzător, urmărind webinarii în flux și rezolvând exerciții în propriul ritm și prin interacțiunea live cu publicul cu feedback continuu și verificarea cunoștințelor de gamification.

Conținutul materialului de învățare

Mai ales dacă aveți o companie care depinde foarte mult de funcționarea și securitatea sistemelor dumneavoastră IT. Amenințările de securitate cibernetică sunt în creștere.

Atacurile cibernetice au continuat să crească în UE în 2020 și 2021 și mai ales în 2022, atât în ceea ce privește sofisticarea și numărul lor, cât și în ceea ce privește impactul lor. UE lucrează pe mai multe fronturi pentru a proteja cetățenii și întreprinderile de criminalitatea cibernetică și pentru a asigura un spațiu cibernetic sigur, deschis și securizat.

În 2022, vom vedea grupuri sponsorizate de stat care vizează industria criptomonedei, în timp ce infractorii cibernetici vor profita de investitori creând portofele digitale cu uși din spate încorporate. Este probabil să vedem o creștere a atacurilor împotriva sistemelor de plată și a amenințărilor mobile mai avansate.

Aproximativ jumătate (47 la sută) din populația (din Danemarca) cu vârste cuprinse între 16 și 89 de ani s-a confruntat cu infracțiuni cibernetice în apropierea vieții, sub formă de e-mailuri false, fraude, hacking sau furt de identitate. Același lucru este valabil și pentru 11%. a companiilor private daneze. 8 la sută dintre companii au experimentat că accesul la serviciile digitale a fost blocat și 3 la sută. au fost șterse sau distruse date. Phishing-ul este cea mai răspândită problemă, dar, din păcate, observăm și o creștere radicală a numărului de site-uri web false, pe măsură ce tot mai mulți oameni cumpără și lucrează de acasă.

Nucleul ISM include managementul riscului informațional, un proces care implică evaluarea riscurilor cu care trebuie să se confrunte o organizație în gestionarea și protecția activelor, precum și diseminarea riscurilor către toate părțile interesate adecvate. Acest lucru necesită identificarea adecvată a activelor și pașii de evaluare, inclusiv evaluarea valorii confidențialității, integrității, disponibilității și înlocuirii activelor. Ca parte a managementului securității informațiilor, o organizație poate implementa un sistem de management al securității informațiilor și alte bune practici găsite în standardele ISO/IEC 27001, ISO/IEC 27002 și ISO/IEC 27035 privind securitatea

informațiilor. Cu toate acestea, acest tip de certificare necesită adesea prea multe resurse pentru IMM-uri, motiv pentru care ne pregătim pentru o practică agilă de securitate cibernetică:

Securitatea Informației și Sistemele de Control Intern

- Terminologie generală
- Triada CIA
- Anatomia unui atac (reducerea suprafeței de atac)
- Cadre de securitate cibernetică

Managementul securității informațiilor
E-mail și birou
Dispozitive
O provocare cheie pentru IMM-uri este malware-ul, care este un termen umbrelă pentru orice tip de „software rău intenționat” care este conceput să se infiltreze în dispozitivul dumneavoastră fără știrea dumneavoastră. Există multe tipuri de malware și fiecare funcționează diferit pentru a-și atinge obiectivele. Cu toate acestea, toate variantele de malware au două trăsături definitorii: sunt ascunse și lucrează activ împotriva interesului tău.

Este malware-ul un virus? Da și nu. În timp ce toți virușii informatici sunt malware, nu toate malware-urile sunt viruși. Virușii sunt doar un tip de malware. Veți auzi că mulți oameni folosesc cei doi termeni în mod interschimbabil, dar din punct de vedere tehnic, virușii și programele malware nu sunt același lucru.
Gândiți-vă la asta astfel: malware este un cod rău intenționat. Virușii informatici sunt coduri rău intenționate care se răspândesc pe computere și rețele.

Cum funcționează malware-ul?

Toate programele malware urmează același model de bază: utilizatorul descarcă sau instalează fără să vrea malware-ul, care infectează dispozitivul.

Cele mai multe infecții cu malware apar atunci când efectuați din neatenție o acțiune care determină descărcarea malware-ului. Această acțiune poate fi să faceți clic pe un link dintr-un e-mail sau să vizitați un site web rău intenționat. În alte cazuri, hackerii răspândesc programe malware prin servicii de partajare de fișiere peer-to-peer și pachete de descărcare gratuită de software. Încorporarea unui pic de malware într-un torrent sau descărcare populară este o modalitate eficientă de a-l răspândi într-o bază largă de utilizatori. Dispozitivele mobile pot fi infectate și prin mesaje text.

O altă tehnică este să încărcați malware în firmware-ul unui stick USB sau al unei unități flash. Deoarece malware-ul este încărcat în hardware-ul intern al dispozitivului (mai degrabă decât în stocarea fișierelor), este puțin probabil ca dispozitivul dvs. să detecteze malware-ul. Acesta este motivul pentru care nu ar trebui să introduceți niciodată o unitate USB necunoscută în computer.

Odată ce malware-ul a fost instalat, acesta vă infectează dispozitivul și începe să lucreze spre obiectivele hackerilor. Ceea ce separă diferitele tipuri de malware unul de celălalt este modul în care fac acest lucru. Deci, cum funcționează malware-ul? Ce este un atac malware?

Cele mai importante amenințări cibernetice

Exploatările de tip drive-by pot exploata automat vulnerabilitățile existente în software-ul instalat pe un computer fără a interacționa cu utilizatorul legitim; și-au extins domeniul de aplicare în 2012 și la terminalele mobile. se concentrează aproape în întregime pe compromiterea site-urilor web legitime. vulnerabilitățile din browser, pluginurile acestuia sau sistemul de operare pot fi exploatate pentru a instala malware pe PC fără știrea utilizatorului, infecția poate fi inițiată prin simpla navigare pe internet.
Viermii sunt programe autoreplicabile; utilizați rețeaua de calculatoare pentru a trimite propriile copii către alte noduri (calculatoare din rețea), reușind să facă acest lucru fără intervenția vreunui utilizator, spre deosebire de un virus informatic, un vierme de computer nu trebuie atașat la un program existent, provoacă daune rețelei, chiar și doar prin ocuparea lățimii de bandă.

Troianul se prezintă sub forma unor programe legitime, care, în realitate, sunt create cu scopul de a sustrage date confidențiale, sau de a permite accesul utilizatorilor sau programelor neautorizate la sistemul infectat; constituie marea majoritate a infecţiilor (80%).

Malware reprezintă orice program a cărui funcție este de a provoca daune software sau hardware unui computer (de exemplu, viruși) – așa cum este descris mai sus.

Track ware sunt programele care folosesc unele vulnerabilități ale browserului web pentru a trimite unui server sau persoanelor informații despre site-urile accesate, informațiile căutate și obiceiurile de navigare ale utilizatorului; Virușii urmăresc să infecteze cât mai multe computere personale, în timp ce programele spion urmăresc să se răspândească pe Internet, virușii au de obicei o sarcină utilă periculoasă, vor să provoace daune computerului infectat, în timp ce programele spion doar încetinesc procesele computerului, adaugă ferestre pop-up și destabiliza browser și are alte efecte „enervante”.

SQL Injection (Code Injection) apare atunci când un atacator poate introduce orice date într-o interogare SQL trimisă la o bază de date; prin injectarea sintaxei se modifică logica enunțului astfel încât să efectueze o acțiune diferită, este cea mai comună vulnerabilitate. Cea mai bună strategie de apărare prin injecție SQL se bazează pe implementarea unor rutine puternice de validare a intrărilor, astfel încât atacatorul să nu poată introduce alte date decât cele necesare aplicației.

Spyware este, în general, definit ca un program care profită de vulnerabilitățile unui sistem în beneficiul unei terțe părți, poate încetini computerul, îl poate face vulnerabil la infecția cu virus și colectează informații confidențiale, cum ar fi numele de utilizator pentru diverse aplicații, parole și informații despre cardul de credit/contul bancar.

Un keylogger este un mic program „inteligent” pe care hackerii îl plasează pe computer fără ca tu să observi. Aici poate sta câteva luni sau ani și să țină cont de fiecare apăsare a tastei pe care o faci pe tastatură. Toate datele sunt trimise hackerilor, care apoi pot folosi diferiți algoritmi și instrumente pentru a obține cele mai bune rezultate din datele dvs. De-a lungul timpului, ei află lucruri diferite despre comportamentul tău și, nu în ultimul rând, acolo unde folosești parole diferite, ai intrat pe tastatură. Apoi poate fi folosit pentru a prelua întreaga identitate digitală în câteva minute.

Adware este o subcategorie de spyware și este un program care face publicitate produselor sau serviciilor. Adesea, aceste reclame apar chiar și după ce programul a fost dezinstalat.
Kiturile de exploatare sunt software automatizat care ajută atacatorii mai puțin experimentați să compromită sistemele prin exploatarea vulnerabilităților la nivelul clientului, în special a celor din browserele web sau aplicațiile care pot fi accesate de site-uri web; se bazează pe atacuri de descărcare drive-by, în care cod rău intenționat este injectat în site-uri web compromise; poate exploata vulnerabilitățile din browser sau din pluginurile acestuia.

Botnet reprezintă un set de computere care se află sub controlul unui atacator; O rețea botnet poate fi folosită în mai multe scopuri: Distributed Denial of Service - atacuri DDoS, spam, furt de identitate, distribuire de malware, infectarea sistemelor informatice; pot rula pe mai multe sisteme de operare; în 2012, rețeaua botnet „Flashback” a reușit să infecteze aproximativ 600.000 de computere Apple.

Refuzarea serviciului este o încercare de a afecta disponibilitatea sistemelor/serviciilor informatice sau a comunicațiilor electronice. Sistemul țintă este atacat prin trimiterea unui număr foarte mare de solicitări nelegitime, care îi consumă resursele hardware sau software, făcându-l indisponibil utilizatorilor legitimi. Principalele motivații pentru atacurile DDoS sunt hacktivismul, vandalismul și frauda. Compromisul informațiilor confidențiale; se referă la încălcări ale securității datelor care au avut loc prin dezvăluirea (intenționată sau neintenționată) de informații confidențiale de către

agenți interni sau externi; Scurgerea de informații se realizează de obicei prin hacking, distribuție de malware, atacuri de inginerie socială, atacuri fizice sau abuz de privilegii

Rogue ware/scareware este un tip de amenințare care ia forma unui software fals; Un caz particular de ware/scareware necinstiți este un software de securitate fals care, odată instalat în sistem, oferă alerte de securitate false și invită utilizatorul să achiziționeze un instrument special de dezinfecție. Acest tip de amenințare se propagă prin diverse metode precum tehnici de inginerie socială, troieni, exploatarea vulnerabilităților (în special java).

Ransomware-ul este una dintre cele mai periculoase și mai agresive forme de criminalitate cibernetică. Hackerii folosesc o bucată de cod extrem de complex pentru a bloca funcționalitatea unui computer sau a unui sistem controlat de computer. Proprietarul sistemului este apoi contactat de hacker cu o cerere de răscumpărare pentru a reactiva sistemul sau a „debloca" informațiile din sistem. In cazurile usoare, este vorba de fotografii de familie sau de conturile companiei, in cazurile grave, poate fi vorba de sisteme vitale, precum; sisteme de control din fabrici sau un stimulator cardiac conectat la internet.

Tipuri de atacuri

Atacurile țintite

- viza o anumită persoană sau organizație
- urmărește fie să colecteze date personale/confidențiale, fie să compromită sistemele informatice țintă
- în general, are o fază în care atacatorul se informează prin diverse tehnici (de exemplu, inginerie socială) despre sistemul IT vizat și apoi declanșează atacul
- deseori acțiunile sale par legitime, deoarece par să provină de la o persoană de încredere

Furt/Pierderi/Distrugere fizică

- datorită mobilității sporite oferite de laptopuri, telefoane inteligente sau tablete, acest tip de amenințare este pe cale să devină una majoră
- copierea consecventă a datelor și criptarea conținutului pot fi o soluție pentru a limita pierderea reală a datelor sau dezvăluirea datelor confidențiale către persoane din afară

Furt de identitate

- reprezintă o amenințare reală într-un mediu din ce în ce mai online
- acreditările de acces sau datele personale sunt ținta atacatorilor astăzi
- odată aflat în posesia lor, atacatorul poate efectua tranzacții frauduloase (în special financiare) sau poate obține date confidențiale

Scurgere de informații

- dezvăluirea intenționată sau neintenționată a informațiilor către o persoană neautorizată
- informații precum localizarea geografică și contactele din agenda telefonică pot cădea cu ușurință în mâinile atacatorilor și pot fi folosite în scopuri frauduloase

Manipularea motorului de căutare (SEP)

- manipulează motoarele de căutare pentru a afișa rezultate de căutare care conțin referințe la site-uri web rău intenționate. Astfel, o pagină web infectată redirecționează utilizatorii către site-uri rău intenționate și dacă victimele accesează site-urile respective își infestează computerele cu malware.
- Certificate digitale false
- sunt folosite de atacatori pentru a semna digital resurse (site-uri web, aplicații, coduri sursă etc.) utilizate în diferite atacuri cibernetice pentru a trece nedetectabile utilizatorului final
- sunt adesea folosite pentru a semna aplicații web rău intenționate, cum ar fi e-banking sau e-commerce, care utilizează protocolul HTTPS
- pot fi create sau furate prin exploatarea vulnerabilităților din sistemele PKI (Public Key Infrastructure) ale autorităților de certificare care emit certificate digitale pentru site-uri web securizate.

Server web securizat – SSL

Protocolul care implementează criptarea cu chei publice se numește SSL (Secure Socket Layer), dezvoltat de Netscape. Acest protocol este folosit de browsere și servere web pentru a transmite date în siguranță, așa că a fost creat pentru a fi utilizat de protocolul HTTP.

Conectarea la un server web securizat se face prin menționarea protocolului https în loc de http în URL - adică accesul la pagina web securizată este indicat de protocol, și nu de numele serverului.

Un server web securizat oferă: Transferul securizat de informații: datele transmise între server și navigator nu pot fi decriptate în cazul interceptării acestora.
Autentificare server: Dacă serverul web a primit un certificat de la o autoritate de certificare (CA).

Lista de verificare a securității

Firewall desktop și mobil
Începeți prin a vă asigura perimetrele exterioare, asigurându-vă că sunteți decît
firewall-urile punctelor (dispozitivelor digitale) funcționează. Sună de bază, dar trebuie să începi și în elementele de bază. De obicei, există trei până la patru tipuri diferite de firewall-uri în rețea:

- Firewall pe sistemul dvs. de operare (Android, iOS, Windows etc.).

- Firewall pe programul dumneavoastră antivirus/securitate.
- Firewall pe routerul dvs. de internet.
- Firewall pe caseta ASA sau comutatorul inteligent (de obicei, doar companiile mai mari).

Backup

Backup-ul ar trebui să fie într-adevăr în fruntea listei, ca și cum nu ar trebui să fie știri. Backup-ul vă poate scuti de a fi nevoit să plătiți o răscumpărare pentru a vă debloca datele. Cu toate acestea, nu vă înșelați cu privire la dimensiunea companiei, majoritatea atacurilor cu acest tip de malware vizează întreprinderile mici și persoanele fizice.

Reguli pentru o navigare mai sigură

- utilizați cea mai recentă versiune de browser
- orientați-vă către alte tipuri de browser (ex. Google Chrome, Opera, Firefox, Safari etc.), mai ales când accesați pagini web potențial nesigure;
- majoritatea programelor malware afectează Microsoft Internet Explorer (utilizat de peste 50% dintre utilizatori)
- verificați destinația reală a legăturilor trecând cursorul mouse-ului peste ea și vizualizând adresa reală în partea din stânga jos a browserului
- aveți grijă ce pluginuri instalați, adesea acestea vin cu software rău intenționat
- nu faceți clic pe linkuri din ferestrele pop-up
- verificați „https://” la începutul adresei web înainte de a introduce informații personale
- in ceea ce priveste efectuarea unei achizitii online trebuie acordata o atentie sporita nivelului de securitate al paginii, daca se opteaza pentru plata online cu card bancar

Trimiterea și primirea de e-mail

- evitați trimiterea sau primirea de informații sensibile prin e-mail;
- evitați încercările de inginerie socială sau de phishing
- căutați un furnizor de e-mail care oferă o filtrare puternică anti-spam
- nu răspunde la spam și evită e-mailurile în cascadă sau piramidă
- nu răspunde la spam și evită e-mailurile în cascadă sau piramidă
- nu utilizați același nume pentru contul dvs. de e-mail personal și de serviciu; utilizarea unor nume distincte pentru aceste conturi reduce riscul ca acestea să fie ținta unui atac informatic
- evitați stocarea informațiilor critice în conturile personale de e-mail sau în alte rețele din afara instituției/companiei în care lucrați

Adevărul este că e-mailul nu a fost niciodată un mediu sigur de comunicare. La urma urmei, doar criminalii trebuie să se preocupe cu adevărat de a-și asigura comunicațiile. Acesta este un mod de

gândire extrem de comun, dar cu totul defectuos, iar Snowden însuși a discreditat acest tip de mentalitate.

A susține că nu îți pasă de intimitate pentru că nu ai nimic de ascuns este ca și cum ai argumenta că nu-ți pasă de libertatea de exprimare pentru că nu ai nimic de spus.

În timp ce mulți oameni încă se pot abona la mentalitatea că nu au de ce să se îngrijoreze dacă nu au nimic de ascuns, realitatea este că există multe motive de îngrijorare și există o mulțime de motive concrete pentru care oamenii să-și cripteze comunicările prin e-mail. și să le protejeze intimitatea. Acest lucru este adevărat indiferent dacă ești jurnalist de investigație, dizident, anunțător sau doar un cetățean obișnuit.

De ce ar trebui cineva să trimită un e-mail securizat?

Pentru a proteja împotriva amenințărilor reprezentate de infractorii cibernetici
V-ați trimis vreodată informații personale sensibile într-un e-mail și v-ați gândit „bine, sper că acel e-mail nu va ajunge cumva în mâinile greșite? Acesta este un gând cu adevărat deconcertant, deoarece dacă altcineva decât destinatarul (destinatarii) preconizat pune mâna pe e-mail - mai ales dacă acel cineva se întâmplă să fie un criminal cibernetic - rezultatele ar putea fi catastrofale.

Trimiterea unui e-mail care conține date personale sensibile, cum ar fi informațiile dvs. medicale, informațiile despre contul financiar, numărul de securitate socială, adresa sau numărul de telefon, poate fi extrem de riscantă, deoarece infractorii cibernetici au nevoie doar de o cantitate minimă de date cu caracter personal pentru a provoca un prejudiciu maxim. Cu acces la astfel de date personale sensibile, infractorii cibernetici vă pot compromite profilurile online, vă pot epuiza conturile bancare și chiar vă pot fura identitatea..

Pentru a împiedica furnizorii de e-mail să monitorizeze e-mailurile și să partajeze date cu agenții de publicitate
Furnizorii de e-mail sunt cunoscuți că monitorizează și scanează mesajele de e-mail ale utilizatorilor pentru a facilita eforturile de publicitate direcționată. Deși în 2017 Gmail se pare că a întrerupt practica scanării e-mailurilor în scopuri publicitare, asta nu înseamnă neapărat că Google a încetat să scaneze e-mailuri în alte scopuri. De exemplu, funcția „Răspuns inteligent” din Gmail oferă sugestii relevante pentru răspunsuri rapide și predefinite la un e-mail pe care l-ați primit pe baza conținutului mesajului său. Deci, dacă nu doriți ca furnizorul dvs. de e-mail să vă scaneze sau să monitorizeze mesajele dvs. de e-mail pentru publicitate sau orice alte scopuri, atunci veți dori să trimiteți e-mailuri securizate care păstrează efectiv conținutul acestor mesaje privat și inaccesibil pentru oricine, altul decât dvs. și partea cu care comunicați prin e-mail.

Supravegherea în masă încalcă libertățile noastre civile și drepturile fundamentale la viață privată. O astfel de supraveghere nejustificată este nejustificat de invazivă și un afront direct la libertățile noastre civile și la drepturile noastre fundamentale la viață privată. Când trimiteți un e-mail securizat, vă puteți cripta comunicarea, astfel încât numai dvs. și cealaltă parte cu care comunicați în siguranță să puteți accesa conținutul mesajului.

Trimiterea unui e-mail criptat vă păstrează confidențialitatea și, în mod eficient, face imposibil ca entitățile guvernamentale să-și caute comunicațiile securizate prin e-mail. Acest lucru este important în special pentru cei ale căror responsabilități de serviciu necesită confidențialitate completă în comunicările lor, dar este, de asemenea, vital pentru oricine, în general, nu dorește ca guvernul să le calce în picioare drepturile la confidențialitate.

Pentru a proteja împotriva eforturilor de supraveghere guvernamentale
După cum am menționat mai devreme, practicile de supraveghere în masă guvernamentale sunt extinse. Și acest lucru este adevărat nu doar în regimurile autoritare precum China sau Iran, ci și în Statele Unite, Marea Britanie, Australia, Canada, Germania și, de asemenea, în alte țări occidentale. Supravegherea în masă nu este o aberație, este o normă și poate fi pernicioasă până la punctul de a fi ilegală.

Acesta este motivul pentru care trimiterea de e-mailuri securizate este esențială, mai ales dacă e-mailul pe care îl trimiteți conține informații personale sensibile.

Cum se trimite un e-mail securizat
Acum că știți motivele pentru care doriți să trimiteți un e-mail securizat, bănuim că probabil veți dori să știți cum să faceți acest lucru. Există câteva modalități de a face acest lucru, fiecare cu anumite avantaje și dezavantaje inerente, dar concluzia este că, dacă veți trimite un e-mail securizat, atunci mesajul dvs. de e-mail va trebui criptat. Când criptați un mesaj de e-mail, în esență amestecați conținutul acelui mesaj și faceți imposibil pentru oricine fără cheia de criptare să decripteze mesajul.

Ce opțiuni vă sunt disponibile dacă doriți să trimiteți un e-mail securizat?

Criptați e-mailurile în clienții de e-mail populari
Mulți dintre cei mai importanți furnizori de e-mail bazați pe web vor permite utilizatorilor să-și cripteze e-mailurile folosind oricare dintre cele două protocoale principale de criptare a e-mailului, S/MIME sau OpenPGP. Dezavantajul este că s-ar putea să nu fie întotdeauna un proces simplu sau direct să faci acest lucru direct din interfața furnizorului tău de e-mail bazat pe web și este posibil să fii nevoit să plătești pentru asta.

De exemplu, dacă doriți să trimiteți un e-mail securizat pe Gmail, mai întâi va trebui să activați criptarea S/MIME conectându-vă la Gmail folosind un cont de administrator GSuite. Conturile GSuite sunt în principal pentru scopuri de afaceri, dar teoretic ați putea configura un cont pentru uz personal. Cealaltă problemă este că destinatarul (destinatarii) pe care îi trimiteți prin e-mail va trebui să aibă și criptarea S/MIME activată pentru ca aceasta să funcționeze.

În mod similar, Outlook acceptă și criptarea S/MIME și va trebui să o activați manual, dar înainte de a face acest lucru, va trebui să obțineți un certificat (sau un ID digital) de la administratorul organizației dvs. Desigur, acesta nu este cel mai eficient proces și nici nu este probabil o soluție foarte practică pentru majoritatea utilizatorilor de e-mail personale. Consultați cum să criptați e-mailurile Outlook pentru mai multe informații despre acest lucru.

Cu toate acestea, puteți ocoli aceste probleme instalând un instrument gratuit de la terți, cum ar fi Mailvelope, pentru a vă cripta e-mailurile cu ușurință. Mailvelope funcționează cu multe dintre cele mai populare servicii de e-mail precum Gmail, Yahoo!, Outlook, Hotmail și GMX. Dar, din nou, destinatarul (destinatarii) mesajului dvs. de e-mail criptat va trebui, de asemenea, să folosească software similar PGP/OpenPGP pentru a decripta e-mailul și a citi conținutul.

Utilizați un furnizor de e-mail securizat dedicat

Dacă nu doriți să treceți prin problema de a activa manual criptarea S/MIME sau OpenPGP pe contul dvs. tradițional de e-mail bazat pe web, o modalitate mult mai ușoară de a trimite un e-mail securizat este să creați un cont la un furnizor de e-mail securizat.

Cu un furnizor de e-mail securizat, cum ar fi ProtonMail, veți putea trimite e-mailuri securizate, criptate altor persoane, indiferent dacă aceștia folosesc același furnizor de e-mail securizat pe care îl utilizați, iar destinatarii dvs. vor putea răspunde în siguranță. Mulți furnizori de e-mail securizat implementează criptarea OpenPGP pentru a securiza e-mailurile utilizatorilor și le vor permite utilizatorilor să trimită și să primească cu ușurință e-mailuri securizate, criptate cu alții care au criptarea OpenPGP activată cu clienții lor de e-mail. Dacă destinatarul dvs. nu are PGP activat, atunci veți putea în continuare să trimiteți un e-mail în siguranță către acel destinatar, care poate fi deschis numai folosind un secret partajat.

Practic, atunci când utilizați un furnizor de e-mail securizat, veți putea proteja cu ușurință mesajele sensibile prin criptarea lor, toate pe o platformă care este de obicei la fel de simplu de utilizat ca și furnizorii de e-mail de renume precum Gmail, Yahoo! sau Outlook. Dar, spre deosebire de acei furnizori de renume, un furnizor de e-mail securizat nu vă va enerva cu reclame și nu vă va monitoriza e-mailurile (din moment ce nici măcar nu le poate accesa datorită criptării end-to-end).

Dezavantajul este că, pentru a accesa gama completă de funcții ale unui furnizor de e-mail securizat, spațiu de stocare extins și mesagerie nerestricționată, va trebui să plătiți. Mulți dintre cei mai buni furnizori de e-mail securizat oferă, totuși, un nivel gratuit (cu anumite limitări) care vă va permite să trimiteți și să primiți e-mailuri securizate gratuit. Dacă veți trimite doar un număr limitat de e-mailuri securizate, atunci o opțiune gratuită ar putea fi cu siguranță o soluție viabilă, dar dacă intenționați să vă desfășurați majoritatea corespondenței prin e-mail într-o manieră sigură, atunci cumpărați o sumă premium. va fi necesar abonamentul.

Când primiți un e-mail, acordați atenție

- identitatea expeditorului nu este garantată: se verifică relația dintre expeditor și conținutul mesajului;
- nu deschide atașamente care provin de la persoane necunoscute sau asociate cu conturi legitime, ci cu mesaje cu subiect și conținut suspect. Acestea pot conține software rău intenționat (software rău intenționat sau malware, cum ar fi viermi, troieni, spyware, forme de adware etc.);
- dacă este absolut necesară deschiderea unui atașament, chiar și din e-mailuri legitime, acesta trebuie mai întâi descărcat și scanat cu soluția antivirus instalată și apoi deschis cu aplicația asociată;
- în cazul e-mail-urilor care conțin linkuri, nu accesați direct acel link din corpul mesajului; eventual, acel link poate fi copiat și deschis dintr-o altă filă de browser;
- nu răspunde la e-mail-uri care conțin solicitări de date personale sau confidențiale (de ex. codul PIN și numărul cardului bancar).

De unde știi că e-mailul tău a fost „accesat” de persoane necunoscute?

- persoanele de contact spun că au primit e-mailuri spam de la tine;
- primești multe email-uri cu erori;
- mesajele apar în folderul „trimis” fără ca tu să le trimiți;
- istoricul locațiilor contului în operațiunea de conectare nu corespunde activității dumneavoastră curente.

Securitate prin parolă. Atacurile au ca scop identificarea parolei și accesarea informațiilor restricționate de acea parolă. Cele mai utilizate metode de atac de acest tip sunt „atacuri de dicționar” și „forța brută”.

„Atacul de dicționar” vizează accesul neautorizat al unor resurse sau sisteme informatice, prin încercarea succesivă a parolelor/cheilor de decriptare aflate într-o listă predefinită de cuvinte sau fraze.

Un atac de „forță brută” este o metodă de acces neautorizat la un sistem informatic sau de decodare a conținutului criptat (cum ar fi parolele) folosind calculul „forță brută” – prin programe care aplică metoda de încercare-eroare. Metoda constă în încercarea succesivă a tuturor combinațiilor posibile de caractere, fără un algoritm elaborat.

Măsuri: sistem captcha, sincronizarea accesului după un număr de accesări eșuate.

- utilizați ID-uri și parole unice și nu le comunicați altor utilizatori;
- lungimea parolei și complexitatea acesteia trebuie alese astfel încât să fie greu de ghicit dar ușor de reținut;
- schimbarea periodică a parolelor (la interval de 1-3 luni);
- folosirea de parole diferite pentru diferite aplicații;
- utilizarea mai multor metode de autentificare (PIN, amprentă, mesaje de alertă etc.);
- evitarea folosirii parolelor similare acasa si la serviciu.

Nu folosi:

- numele tău, al altcuiva din familie sau al animalului tău preferat,
- elemente ale adresei dumneavoastră: numele clădirii, strada, țara,
- numele instituției, al proiectului etc.,
- număr de telefon, număr de înregistrare
- numele vedetei sau personajului preferat (sau al filmului, cărții etc.),
- cuvinte din dicționar;
- numele contului pentru care ai setat parola;

Metode de creare a parolelor puternice

- metoda fonetică: „Știu sigur că am un DVD Blu-Ray!”: St1u100%km1DVDBLr!
- metoda primei litere: „Știu sigur că am un DVD Blu-Ray!”: „sSka1DVDBr!”
- metoda de substituire (de obicei vocale): „Iubesc vacanțele”: „@d0rc0nc#d11l#”
- metoda inversă și de substituție: „Iubesc vacanțele”: „r0d@3l11d3cn0c”
- litere mari/minuscule, număr/simbol și metodă de înlocuire: „Iubesc vacanțele”: „@D0rC)nC3d11L3”
- personalizarea metodelor în funcție de site-uri web în vederea creării unui sistem personal de generare a parolelor: Gmail - „G@D0rC)nC3d!1L3MAIL”, Yahoo - „YA@D0rC)nC3d!1L3HOO”, Wizzair - „WIZZ@D0rC)nC3d! 1L3AIR”.

În general, în acest modul de unitate

Cum să utilizați eficient lanțul Cyber Kill în strategia dvs. de securitate cibernetică

Detectare – Analizați și găsiți încercările de intruziune.

Deny – Opriți atacurile pe măsură ce se întâmplă.

Perturbare – Opriți comunicarea de date

Degradare – Reduceți și limitați eficacitatea atacului.

Înșela – Conduceți atacatorii în direcția greșită.

Conține – Ascunde și restrânge raza de acțiune a atacului, astfel încât să afecteze doar o parte a organizației.

Întrebări:

Forumul de discuții la care se răspunde cu o scurtă explicație. Răspunsurile vor fi discutate cu mentorul în timpul sesiunilor de mentorat

- Ce este Malware
- Care sunt principalele amenințări cibernetice
- Care este rolul Secure Web Server - SSL

- Explicați câteva reguli pentru o navigare mai sigură
- Prezentați câteva măsuri pentru a securiza trimiterea și primirea de e-mail

Întrebări de autoevaluare. După ce răspunde, cursantul poate vedea rezultatele și le poate compara cu cele salvate pe platformă

- Programe malware
- Principalele amenințări cibernetice
- Reguli pentru o navigare mai sigură
- Măsuri pentru a securiza trimiterea și primirea de e-mail

Atasamente (Prezentare PowerPoint, fișe, printuri, link-uri, video…):

Consultați fișierele Powerpoint și Video

Referințe:

- What is Cyber Security?

URL: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

- Malware, or malicious software

URL: https://www.malwarebytes.com/malware

- Cybersecurity for everyone.

https://www.avast.com/c-malware

- Malware Removal Software 2022; Secure your personal data

URL: Malware

- What are Cyber Security Threats?

URL: https://www.imperva.com/learn/application-security/cyber-security-threats/

- 21 Top Cybersecurity Threats and How Threat Intelligence Can Help

URL: https://www.exabeam.com/information-security/cyber-security-threat/

- Sending and receiving e-mail

URL: https://www.ibm.com/docs/en/i/7.1?topic=mail-sending-receiving-e

- Create and send email

URL: https://support.google.com/a/users/answer/9259846?hl=en

The Cyber Kill Chain: The Seven Steps of a Cyberattack

URL: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/