Slide 1:
Cybersecurity

Slide 2:
Ce este Cybersecurity?
Termenul Cybersecurity se referă la tehnologiile și procesele concepute pentru a apăra sistemele informatice, software-ul, rețelele și datele utilizatorilor de acces neautorizat si de asemenea, de amenințările distribuite prin Internet de către infractorii cibernetici, grupurile teroriste și hackerii.
Cybersecurity are drept scop protejarea dispozitivelor și a rețelei împotriva accesului sau modificării neautorizate. Internetul nu este doar sursa principală de informații, ci este și un mijloc prin care oamenii fac afaceri.

Slide 3:
Astăzi, utilizatorii utilizează Internetul pentru a face publicitate și a vinde produse sub diverse forme, pentru a comunica cu clienții și comercianții și pentru a efectua tranzacții financiare. Din această cauză, hackerii și infractorii cibernetici folosesc internetul ca instrument de răspândire a programelor malware și de atacuri cibernetice. Cybersecurity își propune să protejeze computerele, rețelele și programele software de astfel de atacuri cibernetice. Majoritatea acestor atacuri digitale vizează accesarea, modificarea sau ștergerea de informații ; extragerea de bani de la victime; sau întreruperea operațiunilor normale de afaceri.

Slide 4:
Tipuri de Cybersecurity
Cyber Security se clasifică în următoarele tipuri:
Securitatea informațiilor
#Securitatea retelei
Securitatea Aplicației

Slide 5:
Securitatea informațiilor
Siguranța informațiilor vizează protejarea informațiilor personale ale utilizatorilor împotriva accesului neautorizat, a furtului de identitate. Protejează confidențialitatea datelor și a hardware-ului care manipulează, stochează și transmit aceste date. Exemple de securitate a informațiilor includ autentificarea utilizatorilor și criptografia.

Slide 6:
Securitatea rețelei
Siguranța rețelei vizează protejarea utilizării, integrității și siguranței unei rețele, a componentelor asociate și a datelor distribuite în rețea. Atunci când o rețea este asigurată, amenințările potențiale sunt blocate de la intrarea sau răspândirea în acea rețea. Exemple de securitate în rețea include programe Antivirus și Antispyware, Firewall care blochează accesul neautorizat la o rețea și VPN-uri (Virtual Private Networks) folosite pentru acces securizat la distanță.

Slide 7:
Securitatea aplicațiilor
Soluția de securitate a aplicațiilor vizează protejarea aplicațiilor software de vulnerabilitățile care apar datorită defectelor din fazele de proiectare, dezvoltare, instalare, upgrade sau întreținere a aplicațiilor.

Slide 8:
Tipuri de amenintari la adresa securitatii digitale
Există multe tipuri diferite de amenințări la adresa securității informatice, unele dintre cele mai frecvente tipuri de amenințări sunt enumerate mai jos:
Virusii; Furt de identitate; Password attacks; Spyware si keyloggers;Adware; Troienii; Ransomware;

Slide 9:
Virusii
Virușii sunt un tip de programe malware special concepute pentru a provoca daune computerului victimelor. Virușii se pot replica în condiții corecte și pot infecta un sistem informatic fără permisiunea sau cunoștințele utilizatorului.
Au două caracteristici majore, abilitatea de a se replica și capacitatea de a se atașa la alt fișier de computer. Un virus are capacitatea de a corupe fișierele și de a fura informații private cum ar fi detaliile cărții de credit ale utilizatorului și de a le trimite înapoi la hacker.Virușii nu pot exista singuri, adică fără un program gazdă;De asemenea,ei pot provoca ștergerea fișierelor sau încetinirea calculatorului. Ar putea modifica fișierele de date, ar putea afecta sau șterge fișierele și programele de date.

Slide 10:
Furt de identitate
Este un tip de amenințare la adresa securității cibernetice, care implică furtul informațiilor personale ale victimelor de pe site-urile de social media, cum ar fi Facebook, Instagram etc., și folosirea acestei informații pentru a construi o imagine a victimelor. Dacă s-au adunat suficiente informații despre o persoana, aceasta ar putea permite ca infractorul cibernetic să o folosească si sa pretinda ca e persoana data.
În unele cazuri, hackerii pot să fure detaliile bancare ale victimelor și să le folosească pentru câștigul lor personal.

Slide 11:
Atacuri de parola
Este un tip de amenințare împotriva securității cibernetice care implică o încercare de hacking de către hackeri pentru a sparge parolele utilizatorului. Cu ajutorul unui instrument de hacking, hackerii pot introduce mai multe parole pentru a sparge acreditările contului victimei și pentru a obține acces. De asemenea, hackerii pot efectua atacuri cu parolă pe un ecran de conectare la computer pentru a avea acces la computerul victimei și la datele stocate în acesta.

Slide 12:

Spyware si keyloggers

Malware-ul, cum ar fi spyware-ul, poate spiona comportamentul victimelor. Unele programe malware, cum ar fi keyloggerul, pot înregistra înregistrările de taste ale victimelor, inclusiv parolele, numerele PIN și detaliile cărților de credit.

Programele spyware și keylogger-ele colectează informații despre utilizatori, parole, istoricul navigării etc. și apoi le transmit creatorilor (hackerii) care pot vinde sau distribui aceste informații personale. Hackerii pot utiliza, de asemenea, acele informații pentru a fura bani din conturile bancare ale victimei.

Slide 13:

Adware

Adware este un grup de malware despre care se știe că generează aceste ferestre pop-up. Dacă un utilizator observă pe ecranul computerului mesaje ciudate de tip pop-up, este cel mai probabil să fie un atac malware. Principala intenție a adware-ului este să obțină permisiuni care le vor permite să instaleze software rău intenționat suplimentar. Dacă utilizatorul descarca software-ul suplimentar, acesta poate șterge sau fura datele. Unele dintre aceste mesaje pop-up pot fi de asemenea folosite pentru a bombarda ecranul computerului cu informații nedorite, cum ar fi reclamele.

Slide 14:

Troienii

Troienii sunt un tip de programe malware care pretind a fi programe inofensive sau utile. Troieni pot provoca o varietate de activități rău intenționate pe computerul victimelor, inclusiv descărcarea de programe rău intenționate, ștergerea sau furtul de fișiere și furnizarea accesului neautorizat al hackerilor la computerul victimelor.

Slide 15:

Ransomware

Ransomware este un grup de programe malware care blochează sau criptează computerul victimei și solicită plata pentru decriptarea calculatorului. Motivul principal al tuturor atacurilor de răscumpărare este întotdeauna monetar.

Spre deosebire de multe alte tipuri de atacuri cibernetice, atacurile de răscumpărare informează victima despre exploatare și oferă, de asemenea, instrucțiuni cu privire la modul de recuperare a acesteia (de obicei, cere plata pentru recuperare). Pentru a evita reprimarea de către autoritățile de aplicare a legii, hackerii care se află în spatele atacurilor de răscumpărare solicită de obicei plăți în valută virtuală, cum ar fi Bitcoins.

Slide 16:

Documentul de bază ce prevede crearea și implementarea unui sistem de management al securităţii cibernetice a Republicii Moldova este **Programul național de securitate cibernetică a Republicii Moldova** pentru anii 2016-2020, aprobat prin Hotărârea Guvernului nr. 811 din 29.10.2015. Programul are drept scop crearea unui sistem de management al securității cibernetice a Republicii Moldova prin securizarea serviciilor societăţi informaţionale, contribuind astfel la dezvoltarea unei economii bazate pe cunoaştere, ceea ce, la rândul său, va stimula

creşterea gradului de competitivitate economică şi de coeziune socială, precum şi va asigura crearea de noi locuri noi de muncă.
Documentul are la bază prevederile Strategiei Naționale de dezvoltare a societății informaționale "Moldova Digitală 2020" și a Strategiei securităţii naţionale a Republicii Moldova și include 7 domenii de intervenție:

- procesare sigură, stocare și accesare a datelor;
- securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice;
- capacităţi de prevenire şi reacţie de urgenţă (CERT);
- prevenirea şi combaterea criminalităţii cibernetice;
- consolidarea capacităţilor de apărare cibernetică;
- educaţie şi informare;
- cooperare şi interacțiune internațională.

Documentul a fost elaborat în conformitate cu prevederile Acordului de Asociere Republica Moldova - Uniunea Europeană, a Convenției Consiliului Europei privind criminalitatea informatică, a Strategiei securității cibernetice a UE și a Recomandărilor Uniunii Internaționale a Telecomunicaţiilor referitoare la asigurarea securității cibernetice a rețelelor de comunicații electronice.

Slide 17:

De ce e importantă securitatea cibernetică?
Atacurile cibernetice, cum ar fi atacurile ransomware de la GoldenEye și WannaCry, au afectat mai multe organizații și au forțat pe mulți să își închidă operațiunile. În urma acestor atacuri cibernetice și încălcări ale securității, securitatea informatică a luat în prim plan organizațiile de toate dimensiunile.Noi variante. Noi tactici. Cyber-urile continuă să evolueze. Nu numai că am văzut o creștere a atacurilor cibernetice asupra întreprinderilor și persoanelor fizice, dar și nivelul de sofisticare a acestor atacuri cibernetice a crescut de asemenea.
În anii care vor veni, vor exista atacuri cibernetice și mai avansate, folosind noi tehnologii, victime și intenții. Va exista o creștere dramatică a disponibilității serviciilor Ransomware-as-a-Service și Malware-as-a-Service. Va permite oricui, indiferent de cunoștințele tehnice, să inițieze cu ușurință și rapid un atac cibernetic.
Cu toate acestea, datorită amplorii daunelor cauzate de atacurile cibernetice în trecut, există acum o conștientizare mult mai mare cu privire la atacurile cibernetice și necesitatea unor măsuri mai bune de securitate cibernetică în rândul organizațiilor de toate tipurile. Acest lucru va servi ca o motivație pentru criminalii cibernetici de a-și susține jocul, punând în scenă atacuri noi și mai sofisticate în viitor.
The Comodo Cybersecurity este un inovator global al soluțiilor de securitate cibernetică, oferind soluții unice de securitate cibernetică care răspund necesităților organizațiilor de toate dimensiunile.

Slide 18:

https://one.comodo.com/blog/cyber-security/what-is-cyber-security.php