Octombrie 2019

Ghidul securității cibernetice

LUNA EUROPEANĂ A SECURITĂȚII INFORMATICE

DEȚINE. SECURIZEAZĂ. PROTEJEAZĂ.

I.P. "SERVICIUL TEHNOLOGIA INFORMAȚIEI ȘI SECURITATE CIBERNETICĂ"
WWW.STISC.GOV.MD

Introducere

În cadrul inițiativei europene de a promova securitatea cibernetică în rândul cetățenilor și de a asigura informarea și conștientizarea lor cu privire la riscurile și amenințările ce pot surveni - Luna europeană a securității cibernetice (European Cybersecurity Month - ECSM), Serviciul Tehnologia Informației și Securitate Cibernetică Vă propune Ghidul Securității Cibernetice.

În contextul unui mediu informațional dinamic și predispus atacurilor cibernetice de amploare, în care infractorii cibernetici ajung să folosească metode din ce în ce mai avansate pentru a implementa vectori de atac care sunt nedetectabili și dificil de neutralizat, prezentul Ghid este conceput pentru protejarea datelor și securitatea afacerii dumneavoastră dar şi pentru pentru asigurarea confidențialității clienţilor, angajaţilor şi partenerilor dumneavoastră. Fie că vorbim despre companii mai mari sau mai mici, de instituții publice și agenții guvernamentale, Serviciul Tehnologia Informației și Securitate Cibernetică prin intermediul acestui Ghid Vă pune la dispoziție o serie de recomandări privind utilizarea securizată a rețelelor de socializare. Totodată, vor fi examinate cele mai bune practici din mediul on-line, analizate în mod eficient setările de confidențialitate a dispozitivelor mobile și prezentate câteva sfaturi de top pentru utilizarea securizată a rețelelor de socializare.

Vă invităm să consultați ghidul de mai jos și să respectați următorul set minim de măsuri în scopul prevenirii atacurilor cibernetice, dar și pentru diminuarea daunelor produse în eventualitatea atacurilor.

Sfaturi și recomandări privind utilizarea securizată a rețelelor de socializare

Rețele de socializare, precum Snapchat, Facebook, Twitter, Instagram și LinkedIn, sunt resurse uimitoare, care vă permit să vă întâlniți, să interacționați și să împărtășiți lucruri cu oameni din întreaga lume. Cu toate acestea, apar riscuri, nu doar pentru tine, ci și pentru familie, prieteni etc. În acestă publicație informativă, vom acoperi pașii cheie pentru a profita la maxim de siguranța în spațiul social media.

Postările

Fii atent și gândește-te înainte de a posta ceva. Orice postare va deveni publică la un moment dat, ceea ce poate afecta reputația și viitorul tău. Cu cât publicați mai multe informații despre viața personală, cu atât este mai ușor pentru un răufăcător să personalizeze un atac împotriva dvs.

De exemplu dacă postezi informații extinse despre familia ta, despre ocupațiile de care te bucuri sau despre vacanța următoare sau călătoria de serviciu, un atacator ar putea recolta toate acele detalii specifice și ar putea crea un e-mail de tip phishing sau un apel telefonic ce te-ar viza în mod special.

Dacă totuși credeți că este un mesaj real și nu avețiparte de careva suspiciuni, atunci ați să știți că tocmai ați scăpat de oproblemă în plus.

Parolele

Protejați-vă datele dvs. Cel mai bun mod de a vă proteja fiecare cont individual pe rețelele sociale este să folosiți o parolă puternică și unică pentru fiecare cont. Ca parolă poate servi o frază de acces formată dintr-o colecție de cuvinte multiple, ceea ce le face ușor de tastat și de reținut.

De exemplu, în loc să folosiți ca parolă “Password123”, o parolă eficientă ar putea fi “SummerFotballUnicorn!”. Utilizarea unei fraze de acces unic pentru fiecare cont vă asigură că, dacă un cont este compromis, celelalte rămân în siguranță. Dacă nu vă puteți aminti toate parolele, puteți utiliza un manager de parole, care va păstra parolele dvs. în siguranță.

Parolele slabe și ușor de ghicit sunt cele mai vulnerabile la atacuri cibernetice. Răufăcătorii pot sparge cu ușurință și preluatoata informația personală, daca aveți aceleași parole.

Confidențialitatea

Ori de câte ori alegeți să postați informații despre dvs, în mediul online, o practică bună este să presupuneți că orice informație pe care o publicați, ar putea deveni publică. Evitați să comunicați detalii sensibile sau private despre dvs.

De asemenea, este înțelept să evitați să postați imagini despre propria persoană pe care nu ați dori să le vadă cineva cum ar fi familia sau angajatorii dumneavoastră. Când vă înregistrați într-o rețea socială, primul pas trebuie să fie activarea și personalizarea controalelor de confidențialitate. Cu toate că vă poate ajuta, rețineți că acestea pot fi confuze, se pot schimba deseori și este posibil să nu vă protejeze complet informațiile.

Nu presupuneți că, după ce ați stabilit aceste setări de confidențialitate, contul dvs, este complet protejat. Dispunerea de cel mai actualizat software de securitate, browser web, sistem de operare și aplicații este cea mai bună apărare împotriva programelor malițioase și a altor amenințări cibernetice.

Fiți mereu precauți și la alte conturi, s-ar putea să fie compromise și acestea. După spargerea contului, aceștia pot avea acces la contactele dvs., la informațiile personale, fotografii, mesagerie, date importante etc. Aceste măsuri de securitate vă pot ajuta, de asemenea, să vă protejați informațiile în cazul în care dispozitivele dvs. sunt pierdute sau furate.

Pentru a vă proteja în continuare, activați întotdeauna verificarea multifactorială (denumită uneori verificare în doi pași sau autentificare cu doi factori) oride câte ori este disponibilă. Autentificarea cu mai mulți factori se face atunci când vi se oferă acces numai după ce ați furnizat cu succes două sau mai multe dovezi, cum ar fi parola și un cod unic generat de smart phone și care ulterior vor fi transmis prin mesagerie.

Aplicații terțe

Dispozitivele dvs. mobile sunt la fel de vulnerabile, precum calculatorul sau laptopul. Multe dintre rețele sociale sau aplicații ale acestora pentru dispozitivele mobile acceptă și suportă și aplicații terțe. Verificați detaliile când descărcați o aplicație sau vă înregistrați pentru o nouă rețea. Instalați numai aplicații din surse de încredere precum și cele de care credeți că aveți nevoie. Faceți un obicei din a verifica evaluările, recenziile și permisiunile oricărei aplicații înainte de a alege să o instalați. Ar putea fi foarte suspicios dacă o aplicație nouă, are recenzii puține sau negative, sau foarte puține descărcări. În acest caz, ar fi mai înțelept să nu instalați astfel de aplicații.

Se întâmplă adesea să descărcați o aplicație pentru scopuri specifice, pe termen scurt, cum ar fi planificarea unei vacanțe sau renovarea unei case. Efectuați audituri periodice pe aplicațiile dvs. Dacă nu mai aveți nevoie de o aplicație, dezinstalați-o sau dezactivați-i accesul de la profilul personal din rețele de socializare, deoarece aceasta ar putea să colecteze date despre dvs.

În cele din urmă, dvs sunteți cea mai bună apărare. Dacă aveți suspiciuni în privința conexiunii la Wi-Fi evitați să vă conectați. Găsiți o altă rețea Wi-Fi cu care vă simțiți mai siguri sau partajați una de la dispozitivul dvs. mobil. Dacă primiți un e-mail, un mesaj sau un apel telefonic ce pare ciudat sau suspect, în special cele extrem de urgente, atunci cel mai probabil sunteți expuși riscului de a fi victima unui atac cibernetic. un atac. Fiți prudenți și întotdeauna în alertă.

Nu este etic să le spui oamenilor de la locul de muncă să nu folosească niciodată Wi-Fi public. Și eliminarea acestora cu o listă copleșitoare de pași detaliați pentru a rămâne în siguranță nu este doar imposibilă, dar poate avea și un impact negativ asupra productivității și securității datelor la locul de muncă.

Scopul este să vă gestionați riscul uman, permițându-le oamenilor să se asigure în căile pe care le poate urma oricine. Data viitoare când călătorești și trebuie să te conectezi la Wi-Fi, încearcă să ții cont de aceste patru comportamente cheie simple.

Grija de sine

Navigarea în siguranță

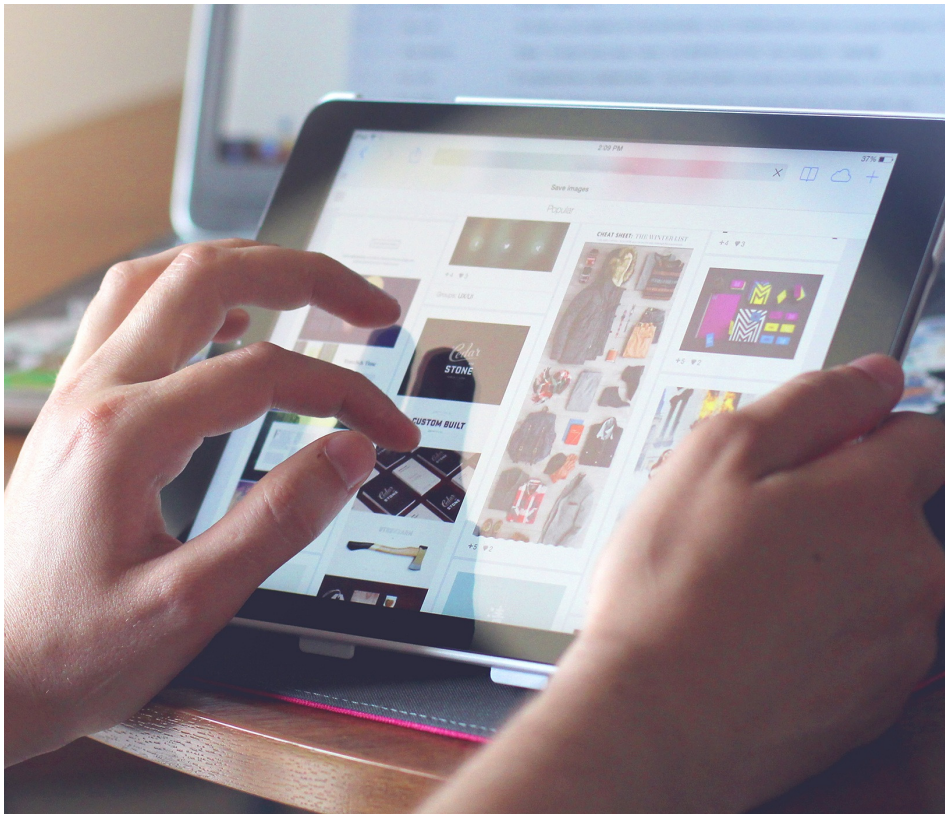
Călătoriile de afaceri sau mai bine zis întâlnirile de afaceri pot fi cu ușurință compromise.
Riscul de securitate la care sunteți expus este foarte sporit. Și asta pentru că sunteți mai tot timpul nevoit să vă conectați la rețelele de WIFI din spațiul public în care vă aflați.

Informațiile transmise prin intermediul rețelelor publice pot fi interceptate cu ușurință, indiferent de dispozitivul folosit – smartphone, laptop sau tabletă. Prin urmare, atunci când vrei să te conectezi la o rețea publică, e bine să limitezi, pe cât posibil, riscurile.

Iată câteva aspecte cheie pentru a reduce riscul de expunere a datelor pentru persoanele care călătoresc și accesează rețele Wi-Fi publice.

Asigurați actualizările

Asigurați-vă că browserele și plugin-urile dvs. au întotdeaunacele mai recente patch-uri și actualizări. Atacatorii cibernetici crează în permanență modalități de a detecta noi vulnerabilități în software-ul pe care îl utilizați, iar furnizorii dvs. le tratează instant.



Sistemele actualizate sunt mult mai dificile pentru atacatorii cibernetici, fapt pentru care este indicat să nu ignorați recomandările de actualizare a sistemului. Astfel încât înmulte cazuri, activarea și setarea actualizărilor automate este una dintre cele mai simple metode de a vă asigura că sistemul dvs. rămâne protejat și sigur. În plus, înainte de a instala orice software, plugin-uri sau extensii, asigurați-vă că verificați politicile și procedurile de securitate a companiei dvs. pentru a vă asigura că programele sunt autorizate. Dăcă aveți neclarități sau incertitudini, vă recomandăm să apelați la secția suport.

Criptarea este o tehnică care vă ajută să vă protejați informațiile atunci când acestea sunt transmise pe internet.

Când vă conectați la punctele Wi-Fi publice, doriți să vă asigurați că toată activitatea dvs. online este criptată, asigurându-vă că alții nu pot monitoriza sau captura ceea ce faceți online. De exemplu, atunci când navigați pe web, doriți să vă asigurați că browserul dvs. este conectat la site-uri web criptate. Nu sunteți sigur dacă conexiunea browserului dvs. este criptată? Atrageți atenția la partea de sus a browser-ului dvs. Dacă vedeți un lacăt sau HTTP lângă adresa site-ului, acesta este un indicator că conexiunea dvs. cu site-ul este criptată.

Unul dintre cele mai simple și eficiente moduri de criptare a întregii activități online este utilizarea unei rețele virtuale private (VPN). Tehnologia din spatele unui VPN creează un tunel privat, criptat pentru activitatea dvs. online, făcând astfel mult mai dificil pentru oricine să vă urmărească sau să vă monitorizeze activitățile online. De asemenea, un VPN vă poate ajuta să vă ascundeți locația, ceea ce face mult mai dificil pentru site-urile web pe care le vizitați să vă determine locația exactă.

Hotspot portabil

Partajarea de date mobile, cunoscută și sub denumirea "hotspot mobil", se referă la acțiunea de conectare a unui dispozitiv, cum ar fi un smartphone sau o tabletă, la altul, cum ar fi un laptop, astfel încât să puteți partaja conexiunea date mobile între dispozitive, atunci când nu este o rețea Wi-Fidisponibilă.

Când aveți îndoieli în privința securității unei rețele Wi-Fi publice, este bine să vă conectați partajarea de date mobile de pe smartphone în loc să utilizați o rețea de Wi-Fi public.

4 Pași simpli pentru a naviga pe

Internet în Siguranță

Fiți atenți la avertismentele browserului.

Primiți un avertisment în legătură cu pagina pe care intenționați să o accesați?
Evitați să-l deschideți și accesați o altă pagină pentru a obține informația de care aveți nevoie.

Verificați criptarea

Găsiți ,,lacătul" sau https alături de adresa paginii web pentru a fi sigur că informația accesată este protejată.

Obține autorizarea.

Înainte a instala programe, plugin-uri, add-onuri sau extensii, verificați politicile și procedurile de securitate pentru a vă asigura daca ele sunt autorizate sau cereți suport de la biroul de asistență.

Odată instalat, păstrează-l actualizat.

Asigurati-vă că browserele și plugin-urile sunt actualizate regulat.

Rețele Virtuale Private (VPNs)

S-ar putea să te simți nevoit să folosești rețeaua de Wi-Fi publică pentru a avea acces la internet atunci când ești departe de casă.
Dar cât de sigure sunt acestea rețelele publice și cine urmărește sau înregistrează activitatea dvs. online? Poate că nici nu aveți încredere în ISP-ul dvs. (Furnizor de servicii Internet) acasă și doresc să fie sigur că nu pot monitoriza ceea ce faci online. Protejați-vă online activitățile și confidențialitate cu o rețea virtuală numită VPN. VPN este o tehnologie carecreează un sistem privat, tunel criptat pentru activitatea dvs. online, făcând
mult mai dificilă urmărirea și mpnitorizarea activității dvs.În plus, un VPN vă ajută să ascundeți locația, ceea ce complică identificarea site-urile web pe care le vizitați.

Cum funcționează?

Un VPN funcționează prin crearea unui tunel criptat privat la un furnizor VPN pe care îl selectați. Toată activitatea dvs. online merge prin acest tunel, apoi lasă rețeaua furnizorului dvs. VPN la destinația dorită. De exemplu, dacă sunteți bazat în Tampa, Florida și vă conectați la un server VPN din Munchen, Germania, orice site web cu care vă conectați va crede că sunteți conectat din Munchen, Germania. Utilizarea unui VPN este foarte simplă.. Primul pas constă în identificarea unui potențial furnizor de VPN și ulterior, stabilirea unui contract cu acesta. Din momentul în care ai dobândit un cont, poți descărca, instala și configura software-ul VPN. Odată instalat și configurat, te poți conecta la Internet. Software-ul VPN vă va crea în mod silențios tunelul criptat și va începe să vă protejeze confidențialitatea dvs.

Selectarea unui furnizor VPN

Activitățile dvs. online sunt la fel de sigure și private ca și furnizorul dvs. VPN. Asigurați-vă că selectați una în care puteți avea încredere.
Vedeți mai jos câteva aspecte-cheie atunci când selectați un furnizor de servicii VPN.

LOGARE

Dacă furnizorul de servicii VPN nu colectează jurnalele, este mult mai greu pentru oricine să se întoarcă și să vadă activitatea dvs. online. În cazul în care se bazează companie: diferiți furnizori VPN au sediul în diferite țări. Asigurați-vă că selectați un furnizor VPN cu sediul într-o țară ce are legi puternice de confidențialitate. Furnizorii VPN aflați în țări cu legi de confidențialitate slabe,pot fi obligați să renunțe la informațiile pe care le colectează asupra ta.

SERVERE

Căutați un serviciu VPN care să aibă serverele localizate în țările sau orașele de care aveți nevoie. Unii furnizori VPN au mii de servere și locații de pe glob. Aveți nevoie să faceți ca conexiunile dvs. să apară așa cum sunt provenind dintr-o anumită țară? Furnizorul VPN poate oferi asta?

COMPATIBILITATE

Căutați servicii care funcționează pe diferite computere și dispozitive mobile.
De exemplu, puteți utiliza un Laptop Windows, o tabletă și un iPhone. Veți dori un serviciu VPN care să funcționeze pe toate aceste dispozitive.

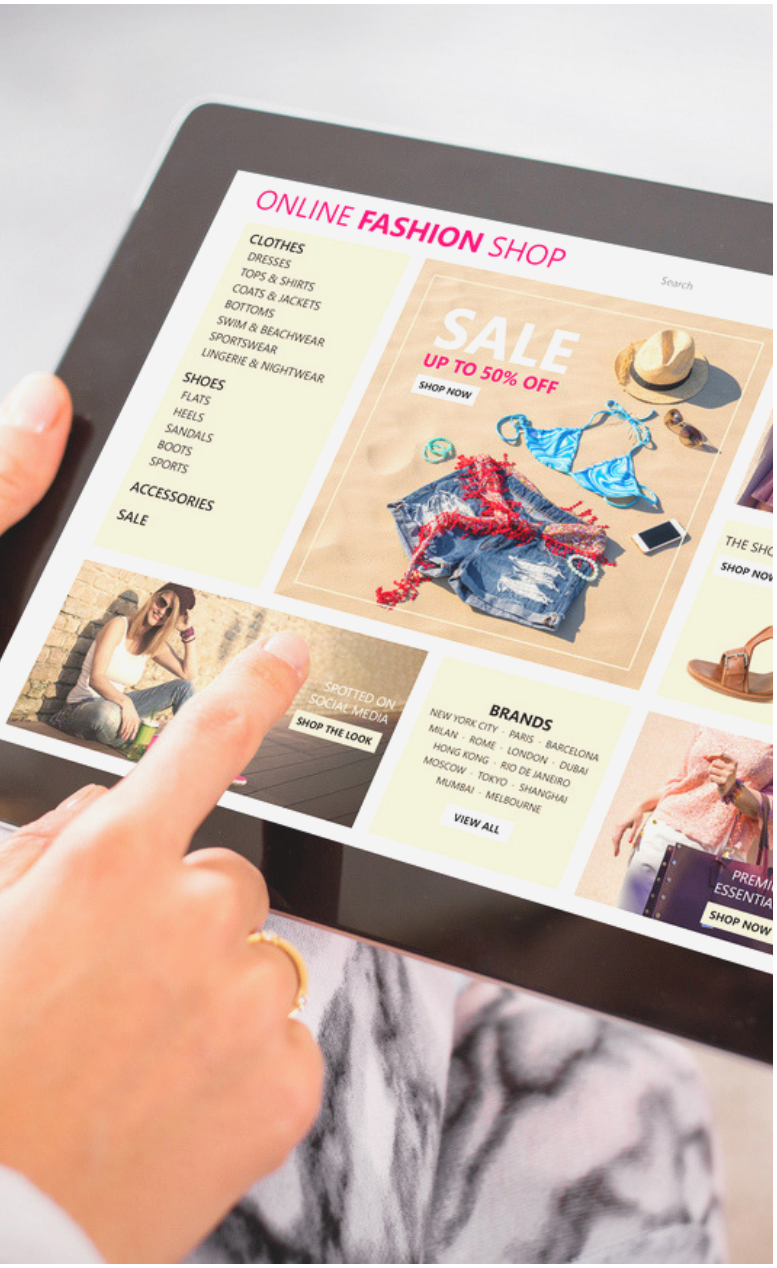
EVITAȚI GRATUIT

Fiți foarte precaut la serviciile VPN „gratuite”; cum fac bani și rămân în afaceri? Serviciile gratuite vă pot colecta și vinde informațiile. Un VPN este o modalitate fantastică de a vă ajuta să vă protejați confidențialitatea online. Cu toate acestea, un VPN nu face nimic pentru a vă asigura computerul, dispozitivele sau conturile online.
Chiar dacă utilizați un VPN, asigurați-vă că respectați întotdeauna pașii de securitate de bază, inclusiv că dispozitivele dvs. sunt actualizate, utilizând o blocare a ecranului și utilizând parole puternice, unice pentru toate conturile.

SHOPPING ON-LINE

Mulți dintre noi vom alege să cumpărăm online în căutarea unor oferte excelente și pentru a evita rândurile lungi și mulțimea nerăbdătoare. Din păcate, aceasta este și perioada anului în care mulți criminali cibernetici creează site-uri de cumpărături false pentru a înșela oamenii. În timp ce multe magazine online sunt legitime, există câteva site-uri false create de infractorii cibernetici. Infractorii creează aceste site-uri false falsificând aspectul unor site-uri reale sau folosind numele unor magazine sau mărci cunoscute. Apoi folosesc aceste site-uri web frauduloase pentru a înșela persoanele care caută cea mai bună ofertă posibilă.

În timp ce multe magazine online sunt legitime, există câteva site-uri false create de infractorii cibernetici. Infractorii creează aceste site-uri false falsificând aspectul unor site-uri reale sau folosind numele unor magazine sau mărci cunoscute. Apoi folosesc aceste site-uri web frauduloase pentru a înșela persoanele care caută cea mai bună ofertă posibilă. Atunci când căutați online cele mai mici prețuri, puteți să accesați unul dintre aceste site-uri false. Când selectați un site web pentru a face o achiziție, aveți grijă de prețurile site-urilor de publicitate cu mult mai ieftine decât oriunde altundeva.



Înainte de a cumpăra orice obiect, asigurați-vă că conexiunea dvs. la site-ul web este criptată.

SHOPPING ON-LINE

- Magazine online false
- Cardul de credit
- Dispozitivul mobil

.Protejați-vă făcând următoarele:

- Cumpărați de pe site-uri web pe care le cunoașteți deja, în care aveți încredere sau ați cumpărat anterior.
- Verificați dacă site-ul web are o adresă poștală legitimă și un număr de telefon pentru întrebări legate de vânzări sau de asistență. Dacă site-ul pare suspect, încercați să telefonați. Dacă nu puteți lua legătura cu nimeni, acesta ar fi primul semn că site-ul este fals.
- Căutați semne de avertizare evidente, cum ar fi oferte care sunt prea bune pentru a fi adevărate sau greșeli gramaticale și ortografice.
- Introduceți numele sau URL-ul magazinului în căutare și vedeți ce au spus alte persoane despre acest site web. Căutați termenii precum „fraudă” „înșelătorie”, „niciodată” sau „fals”. Lipsa de recenzii poate fi de asemenea, un semn care indică faptul că site-ul web este nou și s-ar putea să nu fie de încredere.

I.P. Serviciul Tehnologia Informației și Securitate Cibernetică

Una din direcțiile prioritare de activitate ale STISC, potrivit funcțiilor reglementate prin statutul său este asigurarea și menținerea securității cibernetice a infrastructurii tehnologiei informației și a Sistemului de telecomunicaţii al autorităţilor administraţiei publice conform cerințelor minime obligatorii de securitate cibernetică stabilite de Guvern și a celor mai bune practici internaționale în domeniu.

În conformitate cu prevederile Hotărârii de Guvern nr. 414/2018, prin transmiterea sistemelor informaționale de stat în administrarea STISC, se urmărește nu doar unificarea procedurilor de administrare a sistemelor informaționale, dar și sporirea nivelului de securizare a acestora, întrucât sistemele vor fi migrate în platforma MCloud, asigurându-se în acest mod cerințele necesare de securitate informațională pe care posesorii centrelor de date anterior nu le puteau asigura în mod individual.

incidents@cert.gov.md +373 22 820 921