Serviciul Tehnologia Informației și Securitate Cibernetică
Centrul de Răspuns la Incidente Cibernetice CERT-GOV-MD

RFC 2350 DESCRIERE PENTRU CLIENTI AL CERT-GOV-MD

1. DESPRE ACEST DOCUMENT

Clienții CSIRT dețin dreptul legal de a intra în esența politicilor și procedurile Echipei de Răspuns la Incidente de Securitate Cibernetică sale.

O modalitate de a susține această conștientizare este de a furniza informații detaliate, compuse în conformitatea cu RFC-2350, pe care utilizatorii le pot lua în considerare.

Acest document reflectă și descrie setul de subiecte-cheie, care prezintă interes pentru clienții CERT-GOV-MD.

1.1 Data ultimei actualizări

Aceasta este versiunea 2.2, publicată pe 12.08.2018

1.2 Lista distribuirii pentru notificări

Nu este disponibilă

1.3 Locații unde acest document poate fi găsit

Cea mai recentă versiune a acestui document de descriere a CSIRT este disponibilă pe site-ul web CERT-GOV-MD - CERT-STISC.GOV.MD

Asigurați-vă că utilizați cea mai recentă versiune.

2. INFORMAȚII DE CONTACT

2.1 Numele echipei

Centrul de Răspuns la Incidente Cibernetice CERT-GOV-MD

2.2 Adresa

Instituția publică "Serviciul tehnologia informației și securitate cibernetică"
Centrul de Răspuns la Incidente Cibernetice CERT-GOV-MD
Piața Marii Adunări Naționale, 1
Chișinău, MD-2012
Republica Moldova

2.3 Fusul orar

GMT + 0200 și GMT + 0300 din aprilie până în octombrie

2.4 Număr de telefon

(+373 22) 820-900 (solicitați CERT-GOV-MD)

2.5 Numărul faxului

(+373 22) 250 522

2.6 Alte surse de telecomunicații

Nu sunt disponibile

2.7 Adresa poștei electronice

Pentru incidente: incidents@cert.gov.md
Pentru alte întrebări: info@cert.gov.md

2.8 Cheile publice și alte informații despre criptare

Cheie PGP pentru info@cert.gov.md:
User ID: Cyber Security Center CERT-GOV-MD <info@cert.gov.md>
KeyID: 0x8FB768E238D9FF60
Fingerprint: 7113 B2B6 ECD1 E297 FFD1 0D43 8FB7 68E2 38D9 FF60

Cheie PGP pentru incidents@cert.gov.md
User ID: Center for Response on Cybersecurity Incidents (Incident Reporting PoC) <incidents@cert.gov.md>
KeyID: 0xB392CF67D9FF9E9C
Fingerprint: ED0A 3330 6139 B3F1 E204 32BF B392 CF67 D9FF 9E9C

2.9 Alte informații

Informația generală despre CERT-GOV-MD, precum și linkurile către diferite resurse de securitate recomandate pot fi găsite la adresa CERT-STISC.GOV.MD

2.10 Modalități de contact pentru clienți

Secretariat
Telefon: (+373 22) 820-900
Fax: (+373 22) 250-522
E-mail: stisc@stisc.gov.md

Info CERT-GOV-MD
Telefon: (+373 22) 820 – 921
E-mail: info@cert.gov.md
PGP Key**:** 0x8FB768E238D9FF60

Raportare incidentelor de securitate cibernetică
Incidente: incidents@cert.gov.md
PGP Key: 0xB392CF67D9FF9E9C

Relatii cu presa
E-mail: (+373 22) 820-900
Telefon: (+373 22) 250-522
Persoană desemnată:

Program de lucru
08: 00-17:00 de luni până vineri, cu excepția sărbătorilor oficiale

3. STATUT

3.1 Misiunea

Centrul de Răspuns la Incidente Cibernetice CERT-GOV-MD este o echipă de experţi în securitate cibernetică, a cărei principală sarcină este să răspundă la incidente ce ţin de securitatea sistemelor informaționale. Centrul asistă beneficiarii sistemelor informaţionale şi de telecomunicaţii al autorităţilor administraţiei publice în implementarea măsurilor proactive şi reactive în vederea reducerii riscurilor de incidente ale securităţii TI şi acordarea asistenţei în reacţionarea la incidente.

Obiective CERT-GOV-MD:

- Îmbunătățirea nivelului de securitate cibernetică în cadrul guvernului și sporirea încrederii în noile tehnologii;
- Reducerea daunelor cauzate de incidentele de securitate;
- Creșterea gradului de conștientizare a autorităților publice și instituțiilor guvernamentale prin informare, sensibilizare și formare continuă;
- Construirea unor relații strategice pentru a îmbunătăți securitatea cibernetică.
- Împărtășirea informațiilor dar și a lecțiilor învățate.

3.2 Clienți

Beneficiari ai serviciilor CERT-GOV-MD sunt autorităţile publice centrale și regionale, organele specializate de securitate și telecomunicații de stat, academiile și universitățile din Republica Moldova cum este stipulat în Hotărârea Guvernului nr. 840 din 26.07.2004 și anexa nr. Nr.1

Domeniul Internet și / sau adresa IP care descriu clienți: AS25319 și AS39279

3.3 Sponsorizare și / sau afiliere

Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) este o instituție publică subordonată Guvernului Republicii Moldova (Hotărârea Guvernului nr. 414 din 08.05.2018),

responsabilă de administrarea și întreținerea sistemelor informaționale de stat și a infrastructurii sistemului de telecomunicații a autorităților administrației publice, asigurarea securității cibernetice, gestionarea infrastructurii publice unificate a cheilor publice, precum și implementarea tehnologiilor informaționale în sectorul public. Centrul de Răspuns la Incidentele Cibernetice CERT-GOV-MD este parte componentă a organizației ca departament intern în structura sa organizațională. stisc.gov.md

3.4 Autoritate

Autoritatea CERT-GOV-MD acoperă sisteme informaționale și de telecomunicații ale autorităților administrației publice (AS25319 și AS39279) și este limitată de rolul al instituției publice "Serviciul Tehnologia Informației și Securitate Cibernetică".

4. POLITICI

4.1 Tipuri de incidente și gradul de implicare

CERT-GOV-MD este autorizat să abordeze toate tipurile de incidente ce țin de securitatea cibernetică apărute în sistemele informaționale și de telecomunicații ale autorităților administrației publice și "Serviciul Tehnologia Informației și Securitate Cibernetică".

Sprijinul acordat de CERT-GOV-MD include:

- coordonarea acțiunilor în caz de incident cibernetic;
- consilierea privind găsirea unei soluții de răspuns;
- consilierea privind implementarea masurilor proactive cu scopul de a preveni apariția acestor incidente in viitor.

4.2 Cooperarea, interacțiunea și divulgarea informații

CERT-GOV-MD face schimb de informații cu alte CSIRT-uri dacă sunt parteneri CERT-GOV-MD în scopul investigării unui incident de securitate, doar in cazul dacă s-au luat toate măsurile necesare pentru a preveni orice formă de divulgare a identității și, dacă acest lucru nu este posibil, numai dacă CERT-GOV-MD este autorizat explicit de către partea afectată.

Toate datele și informațiile sensibile sunt transmise în formă criptată.

4.3 Comunicare și autentificare

Luând în calcul informația cu care se confruntă CERT-GOV-MD, telefoanele vor fi considerate suficient de sigure pentru a fi utilizate chiar și în mod necriptat. E-mail-urile necriptate vor fi considerate mai puțin sigure, însă vor putea fi folosite pentru transmiterea datelor sensibile. Dacă este necesar să trimiteți date extrem de sensibile prin e-mail, PGP va fi utilizat.

5. SERVICII

Serviciul Tehnologia Informației și Securitate Cibernetică
Centrul de Răspuns la Incidente Cibernetice CERT-GOV-MD

Centrul de Raspuns la Incidente Cibernetice CERT-GOV-MD asista beneficiarii sistemelor informationale si de telecomunicatii al autoritatilor administratiei publice în implementarea masurilor proactive si reactive în vederea reducerii riscurilor de incidente ale securitatii TI si acordarea asistentei în reactionarea la incidente prin oferirea o ampla gama de servicii.

Serviciile de bază ale CERT-GOV-MD sunt:

- **Pregătirea și prevenirea**
  - **Alerte şi avertizări**. Acest serviciu implică propagarea informaţiilor care descriu ameninţările curente, vulnerabilități noi, alerte de intruziuni, tipuri de viruși, cât și acţiuni recomandate pe termen scurt pentru gestionarea problemelor existente.
  - **Anunţuri.** Aici sunt incluse, dar fără a se limita la număr, alertele de intruziune, avertismente de vulnerabilitate şi consultanţă de securitate. Aceste anunţuri informează beneficiarii în legătură cu noi dezvoltări cu impact pe termen mediu şi lung, de exemplu vulnerabilităţile nou-găsite sau instrumentele intruşilor. Anunţurile permit beneficiarilor să-şi protejeze sistemele şi reţelele împotriva oricăror probleme nou găsite, înainte ca acestea să poată fi exploatate.
- **Depistarea și reacția**
  - **Urmărirea originilor unui intrus sau identificarea sistemelor la care intrusul are acces**. Această activitate implica depistarea sau urmărirea modului în care intrusul a intrat în sistemele afectate şi reţelele asociate, care sisteme au fost folosite pentru obținerea accesului, unde a început atacul şi ce alte sisteme şi reţele au fost folosite ca parte a atacului. Ar putea fi vorba şi de determinarea identităţii intrusului. Această activitate ar putea fi efectuată pe cont propriu, dar de obicei implică lucrul cu personalul de aplicare a legii, furnizorii de servicii de internet sau alte organizaţii implicate.
  - **Activităţile de răspuns** la incidente particulare care a avut loc în cadrul sistemelor informaţionale ale beneficiarilor sunt desfăşurate nemijlocit de către beneficiarul, care pot să includă: luarea unor măsuri pentru protejarea sistemelor şi reţelelor afectate sau ameninţate de activitatea intruşilor, furnizarea de soluţii şi strategii de diminuare de la documente consultative relevante sau alerte, căutarea activităţii intruşilor în alte părţi ale reţelei, filtrarea traficului de reţea, refacerea sistemelor, instalarea patch-urilor sau repararea sistemelor.
- **Reducerea riscurilor**.
  - **Auditurile şi evaluările de securitate**. Acest serviciu furnizează o imagine şi analiză detaliate ale infrastructurii de securitate ale unei organizaţii pe baza cerinţelor definite de aceasta sau conform altor standarde din industrie care se aplică. Poate să implice şi o analiză a practicilor de securitate ale organizaţiei. Există multe tipuri de audituri şi evaluări care pot fi furnizate.
  - **Analiza celor mai bune practici**. Intervievarea angajaţilor şi a administratorilor de sistem şi reţea pentru a stabili dacă practicile lor de securitate se potrivesc cu politica de securitate definită în organizaţie sau cu unele standarde specifice industriei.
  - **Scanarea vulnerabilitatilor.** Folosirea scanerelor de vulnerabilitate pentru a stabili care sisteme şi reţele sunt vulnerabile.

6. FORMULARE DE RAPORTARE A INCIDENTELOR

Versiunea actuală a formularului de raport de incident este disponibilă pe site-ul CERT-STISC.GOV.MD.

7. EXONERARE DE RĂSPUNDERE

Deși toate precauțiile vor fi luate la pregătirea informațiilor, notificărilor și alertelor, CERT-GOV-MD nu își asumă nici o responsabilitate pentru erori, omisiuni sau pentru daune rezultate din utilizarea informațiilor prezente pe site-ul web al CERT-GOV-MD.