Parlamentul României
Camera Deputaţilor

ROMANIA

CABINET SECRETAR GENERAL

ROMÂNIA
1918-2018 | SĂRBĂTORIM ÎMPREUNĂ

București, 20.06.2018
Nr. 2/6109

S-A LUAT ACT
În ședința Biroului Permanent
al Camerei Deputaților
din data de 20.06.2018
Nr. 890

Parlamentul României
CAMERA DEPUTAȚILOR
BIROUL PERMANENT
Nr. 890 din 20.06.2018

INFORMARE

De la: **Silvia-Claudia MIHALCEA, Secretar general al Camerei Deputaţilor**

Către: **Biroul permanent al Camerei Deputaţilor**

Tema: **Măsuri de securitate vizând sistemul de poștă electronică**

Secretariatul general al Camerei Deputaților acordă o importanță deosebită politicilor de securitate cibernetică. Astfel, există o preocupare permanentă pentru prevenirea unor potențiale vulnerabilități ale sistemului de poștă electronică al Camerei Deputaților.

Spargerea unui cont utilizator din sistemul de poștă electronică, pe lângă efectele negative cauzate de intrarea datelor confidențiale în posesia altor persoane, poate avea efecte negative asupra întregului sistem de poștă electronică. Din aceste motive, pentru **prevenirea vulnerabilităților bazate pe existența unor parole de complexitate redusă**, începând cu **1 iulie 2018** se vor implementa următoarele măsuri de securitate:

- **blocarea timp de 30 de minute** a oricărui cont de poștă electronică din domeniul @cdep.ro în cazul în care **parola este introdusă de 4 ori greșit**;

- **parolele utilizatorilor vor trebui să fie de o complexitate mai mare** - sistemul nu va permite introducerea unor parole de lungime mai mică de 10 caractere, o parolă va trebui în mod obligatoriu să conțină cel puțin o literă majusculă (A, B, C ...), o literă minusculă (a, b, c ...), o cifră (1, 2, 3...) și un caracter special (., ?, !, # ...);

- **în mod obligatoriu parolele vor trebui schimbate la un interval de timp rezonabil** – sistemul va obliga utilizatorii să își schimbe parolele după 90 de zile de la ultima modificare.

Utilizatorii sistemului de poștă electronică sunt rugați să nu folosească adresa de email și parola de acces din sistemul de poștă electronică @cdep.ro pentru a se înregistra și autentifica pe alte site-uri, în special pe site-uri de social media sau de comerț electronic.

Anexăm un ghid de bune practici privind accesul la serviciul de poștă electronică și gestionarea conturilor utilizator.

Secretar general,
Silvia-Claudia MIHALCEA

Secretar general adjunct
George Ionuţ DUMITRICĂ

Direcţia informatică
şi telecomunicaţii,
Director
Marian BOŢOCAN

ANEXĂ

GHID DE BUNE PRACTICI PRIVIND UTILIZAREA SERVICIULUI DE POȘTĂ ELECTRONICĂ[1]

E-mailurile și atașamentele acestora au un rol foarte important în facilitarea atacurilor informatice.

Rețelele de criminalitate informatică distribuie către mai mulți utilizatori mesaje electronice nesolicitate (spam), cu caracter aparent comercial, de publicitate pentru produse și servicii, cu scopul de a infecta utilizatorii.

SECURITATEA E-MAILULUI:

1. evită transmiterea sau recepționarea de informații sensibile prin e-mail;
2. evită încercările de inginerie socială sau phishing (tehnică utilizată de infractorii cibernetici pentru a obține informații sensibile care implică de regulă existența unui link malițios în cadrul mesajului; odată accesat, acesta trimite utilizatorul spre un site web de unde se va descărca automat un malware);
3. nu răspunde la spam și evită e-mailurile în cascadă sau piramidale;
4. nu folosi același nume pentru contul de e-mail personal și pentru cel de serviciu; utilizarea de nume distincte pentru aceste conturi diminuează riscul ca acestea sa fie ținta unui atac informatic;
5. evită stocarea informațiilor critice în conturile personale de e-mail sau în alte rețele din afara instituției/companiei în care îți desfășori activitatea.

În momentul în care primești un e-mail, acordă atenție următoarelor:

6. identitatea expeditorului nu este garantată: verifică relația dintre expeditor și conținutul mesajului;
7. nu deschide atașamente provenind de la persoane necunoscute sau asociate unor conturi legitime, dar având mesaje cu subiect și conținut suspect. Acestea pot conține software malițios (malicious software sau malware, cum ar fi viermi, troieni, spyware, forme de adware etc.);
8. dacă este absolut necesară deschiderea unui atașament, chiar și din e-mailuri legitime, acesta trebuie, în prealabil, descărcat și scanat cu soluția antivirus instalată și, ulterior, deschis cu aplicația asociată;

---

[1] *Extras din Ghidul de bune practici pentru securitate cibernetică emis de către Serviciul Român de Informații*

9. în cazul e-mailurilor care conțin link-uri, nu accesa direct acel link din corpul mesajului; eventual, poate fi copiat acel link și deschis din altă filă (tab) a browser-ului;
10. nu răspunde e-mailurilor conținând solicitări de date personale sau confidențiale (de exemplu codul PIN şi numărul cardului bancar).

DE UNDE ŞTII CĂ E-MAILUL TĂU A FOST „ACCESAT" DE PERSOANE NECUNOSCUTE?

1. contactele tale spun că au primit e-mailuri spam de la tine;
2. primești multe e-mailuri cu erori;
3. apar mesaje în dosarul „trimise" fără ca tu să le trimiți;

ALEGEREA PAROLEI

Parola este un instrument de autentificare folosit pentru a dobândi acces la un echipament și la datele sale. Pentru protecția datelor tale, alege parole dificil de identificat de atacator cu ajutorul instrumentelor automatizate („brute force") sau de ghicit de către acesta.

Atacurile urmăresc identificarea parolei și accesul la informația restricționată prin acea parolă. Cele mai folosite metode de atac de acest tip sunt *„dictionary attacks"* și *„brute force"*.

1. *„Dictionary attack"* urmărește accesarea neautorizată a unor resurse sau sisteme informatice, prin încercarea succesivă a parolelor / cheilor de decriptare aflate într-o listă predefinită de cuvinte sau fraze.

2. Un atac *„brute force"* reprezintă o metodă de acces neautorizat la un sistem informatic sau de decodare a conținutului criptat (cum ar fi parolele) folosind „forţa brută" de calcul – prin programe care aplică metoda încercare – eroare (trial and error). Metoda constă în încercarea succesivă a tuturor combinațiilor posibile de caractere, fără un algoritm elaborat. Este aplicabilă într-un număr limitat de situații, când sistemele nu sunt protejate cu parole sigure (de ex. sunt formate din prea puține caractere) sau nu au implementate mecanisme *anti-brute force* (de ex.: sistemul *captcha*, temporizarea accesului după un număr de accesări eșuate).

În măsura în care acest lucru este posibil, alege parole compuse din minimum 12 caractere de tip diferit (majuscule, minuscule, cifre, caractere speciale de ex. #, &, %, $, @) fără legătură cu tine (nume, data nașterii etc.) sau cu instituția / compania în care îți desfășori activitatea, și care să nu existe în dicționar.

UTILIZEAZĂ PAROLE PUTERNICE ŞI PĂSTREAZĂ-LE ÎN SIGURANȚĂ:

1. utilizează ID-uri şi parole unice şi nu le comunica altor utilizatori;
2. lungimea parolei şi complexitatea acesteia trebuie alese astfel încât să fie dificil de ghicit dar uşor de ţinut minte;
3. schimbarea periodică a parolelor (la un interval de 1-3 luni);
4. utilizarea unor parole diferite, pentru aplicaţii diferite;
5. utilizarea unor metode multiple de autentificare (PIN, amprentă, mesaje alertă, etc);
6. evitarea utilizării unor parole similare acasă şi la locul de muncă

CÂTEVA METODE SIMPLE TE POT AJUTA SĂ REALIZEZI PAROLE SOLIDE:

1. metoda fonetica: „Știu sigur ca am un DVD Blu-Ray!": St1u100%km1DVDBLr!
2. metoda primelor litere: „Știu sigur ca am un DVD Blu-Ray!": „sSka1DVDBr!"
3. metoda substituției (de obicei a vocalelor): „Ador concediile": „@d0rc0nc#d11l#"
4. metoda scrierii inverse și substituție: „Ador concediile": „r0d@3l11d3cn0c"
5. metoda alternării literă mare/mică, cifră/simbol și substituției: „Ador concediile":„@D0rC)nC3d11L3"

Folosește o parolă unică pentru fiecare serviciu sensibil. Parolele care protejează conținut sensibil (internet banking, e-mail profesional etc.) nu trebuie niciodată refolosite pentru alte destinații. Este preferabil să nu folosești instrumentele de reținere a parolelor, cel puțin nu pe aceeași stație de lucru sau nu afișate la vedere.

PE SCURT:

1. identifică reguli de realizare a parolelor și aplică-le;
2. nu păstra parolele în fișiere pe stația de lucru sau pe notițe (post-it);
3. nu transmite niciodată parolele prin e-mail sau prin atașamente necriptate;
4. manifestă atenție la introducerea parolelor în prezenta altor persoane, pentru a nu fi observate de acestea.