ALEGEREA CU ATENȚIE A UNEI PAROLE

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".

- „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.
- 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 „forța 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 minim 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 ȘI PĂSTREAZĂ-LE ÎN SIGURANȚĂ:

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

CÂTEVA METODE SIMPLE TE POT AJUTA SĂ REALIZEZI PAROLE SOLIDE:

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

De asemenea, pentru a păstra în siguranță parolele tale, poți utiliza suporți externi de memorie criptați. Deși pare o metodă mai complicată, este mai sigură.

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:

- identifică reguli de realizare a parolelor și aplică-le;
- modifică întotdeauna credențialele (utilizator și parolă) inițiale ale echipamentelor (servere, imprimante, routere etc.), cum ar fi: admin/admin;
- nu păstra parolele în fișiere pe stația de lucru sau pe notițe (post-it);
- nu transmite niciodată parolele prin e-mail sau prin atașamente necriptate;
- manifestă atenție la introducerea parolelor în prezența altor persoane, pentru a nu fi observate de acestea.

Sursa: "Ghid de bune practici pentru securitate cibernetica"

https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf