
ROMANIA
SRI
Patria a priori
SERVICIUL ROMAN DE INFORMAȚII
GHID
DE BUNE PRACTICI
PENTRU SECURITATE
CIBERNETICĂ
WWW.SRI.RO

DE CE AR TREBUI LUATE MĂSURI DE SECURITATE?

În fiecare zi, suntem expuși, atât acasă cât și la locul de muncă, la amenințări ce își au originea în spațiul virtual. În majoritatea cazurilor nici măcar nu suntem conștienți de acest lucru, sau dacă-l realizăm, nu reacționăm la aceste amenințări într-o manieră adecvată. În media apar zilnic articole referitoare la incidente de securitate și la impactul pe care acestea îl au asupra noastră, ca indivizi sau organizații deopotrivă.

Aceste incidente relatate sunt de fapt doar vârful iceberg-ului, în realitate fiind cu mult mai expuși decât credem noi că suntem având în vedere că, din nefericire, riscurile asociate mediului virtual sunt în continuă creștere.

Cu toate că mediul virtual, reprezentat de infrastructurile cibernetice, incluzând conținutul informațional procesat, stocat sau transmis, și acțiunile derulate de utilizatori, este deja o parte integrantă a vieții personale și profesionale, securitatea sa este un element luat în calcul mult prea rar și poate insuficient. Acest aspect este potențat de complexitatea noilor tehnologii, care implică noi riscuri ce pot afecta grav individul sau organizația, în condițiile în care există numeroase acțiuni ostile desfășurate în spațiul cibernetic de natură să afecteze funcționarea sistemelor informatice precum și datele vehiculate prin intermediul acestora.

ACȚIUNILE OSTILE VIZEAZĂ, ÎN PRINCIPAL:

- perturbarea, blocarea, distrugerea, degradarea sau controlarea în mod malițios a unui sistem / infrastructură informațională;
- afectarea integrității disponibilității, confidențialității, autenticității și non-repudierii datelor sau sustragerea informațiilor cu acces restricționat.

De exemplu, date sensibile (contracte, proiecte etc.) pot fi exfiltrate de atacatori informatici sau recuperate de aceștia cu ajutorul unor programe specializate în cazul pierderii sau furtului unui dispozitiv portabil (telefon inteligent, tabletă, laptop etc.).

În consecință, securitatea cibernetică trebuie să reprezinte o prioritate pentru buna funcționare a sistemelor guvernamentale sau de control industrial (producția și distribuția de energie electrică, distribuția de apă etc.). Un atac cibernetic asupra unui sistem de control industrial (Superviasory Control and Data Acquisition System - SCADA) poate determina pierderea controlului, oprirea, deteriorarea instalațiilor sau alterarea produsului final. Aceste incidente sunt însoțite adeseori de urmări grave în termeni de securitate, de pierderi economice și financiare și de afectare a imaginii organizației.

Pericolele pot fi totuși reduse semnificativ prin aplicarea unei serii de bune practici puțin costisitoare, chiar gratuite, și ușor de aplicat. Conștientizarea riscurilor de către angajați este foarte eficientă pentru a limita o mare parte din riscuri. Măsurile proactive și reactive pot include politici, concepte, standarde și ghiduri de securitate, managementul riscului, activități de instruire și conștientizare, implementarea de soluții tehnice de protejare a infrastructurilor cibernetice, managementul identității, managementul consecințelor.

Acest ghid își propune să sintetizeze o serie de informații cu privire la riscurile existente și prezintă câteva metode utile pentru a determina reflexe simple pentru folosirea în siguranță a sistemelor informatice, pentru a veni în întâmpinarea nevoilor tale de cunoaștere, atât în calitate de cetățean, utilizator al tehnologiei moderne, cât și în calitate de funcționar (public sau nu) care utilizează infrastructura cibernetică a unei organizații, din moment ce, în ambele ipostaze, suntem toți dependenți de resurse informatice și de comunicații.

ASPECTE CONCEPTUALE

Un element important în configurația de securitate cibernetică este antivirusul. Acesta este un program informatic conceput să detecteze, să prevină și să elimine instalarea oricăror forme de malware (viruși, troieni, adware, spyware etc.) pe sistemele de calcul. Actualizarea acestuia este deosebit de importantă pentru a putea face față celor mai noi (versiuni ale unor) programe malițioase.

Un exemplu de malware este troianul (trojan horse), a cărui denumire provine din mitologia greacă. Acest tip de program pare a avea o funcție utilă, legitimă, dar deține și una ascunsă, potențial malițioasă, care scapă mecanismelor de securitate, uneori exploatând vulnerabilități ale sistemelor vizate. Astfel, odată rulat, programul poate iniția activități malițioase, precum sustragerea de informații, afectarea calculatorului gazdă sau crearea unor căi disimulate de acces de la distanță la sistemul infectat.

ALTE EXEMPLE DE PROGRAME MALIȚIOASE:

- virusul informatic: program care se poate autoreplica în cadrul unui sistem și propaga în alte calculatoare din rețea fără știința utilizatorului. Acesta poate afecta negativ funcționalitatea, integritatea, disponibilitatea sistemului sau a datelor conținute de acesta;
- viermele informatic: un malware ce dispune de capacitatea de a se autoreplica și propaga într-o rețea de calculatoare și dincolo de aceasta (alte sisteme sau rețele), folosind resursele rețelei, fără a se atașa unui alt program sau proces.

În urma infectării sistemului informatic, acesta poate deveni, de exemplu, parte a unui botnet - o rețea de calculatoare infectate prin diverse metode de către o persoană/entitate rău-intenționată în vederea utilizării acesteia în folosul celui care controlează rețeaua (botmaster), pentru sustragerea de date confidențiale sau bancare, pentru inițierea de atacuri de tip DdoS, pentru spargerea parolelor sau pentru căutarea și exfiltrarea de informații.

Componenta software a unui botnet este formată din 2 părți: clientul și serverul de comandă și control (C&C). În general, modulele client au implementate modalități de asigurare a persistenței în sistemul infectat prin autocopierea în zona de start-up a sistemului de operare.

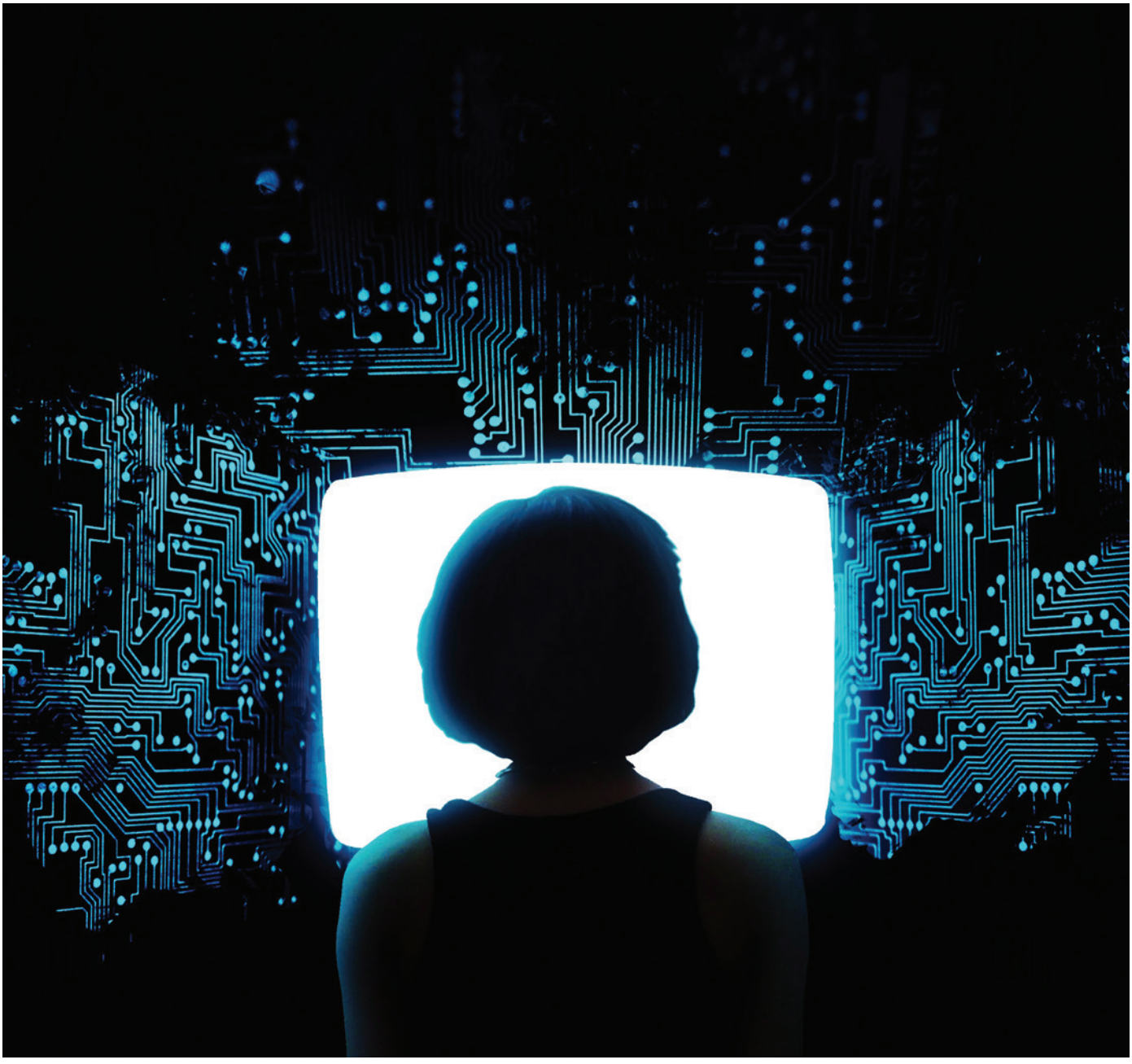
Botmasterul este cel care controlează, prin intermediul serverului C&C, mașinile infectate (boți). El poate, în funcție de tipul botnet-ului, să administreze, monitorizeze și să obțină diverse statistici privind activitatea boților prin intermediul unui panou de comandă și control.

PRUDENȚA
ÎN NAVIGAREA PE INTERNET

Securitatea cibernetică este un subiect discutat frecvent în ultimii ani pentru că mediul virtual este unul dinamic, aflat în permanentă schimbare, pentru că tehnologiile folosite sunt înlocuite, actualizate și modificate constant, apărând astfel noi și noi provocări și pentru că nivelul de conștientizare al utilizatorilor este încă unul foarte scăzut.

Mediul online are din ce în ce mai multe conexiuni cu spațiul fizic. Iar multe dintre lucrurile pe care le facem în primul au implicații în cel de-al doilea: atunci când securitatea este compromisă în spațiul virtual, utilizatorii pot avea parte de consecințe dintre cele mai neplăcute în spațiul fizic.

Acele informații vitale vizate de spionii cibernetici ni se par, de cele mai multe ori, uzuale, banale, inofensive: acestea încep de la datele personale, completarea de diverse formulare online pentru concursuri și ajung la date financiare și contractuale, informații despre angajați și baze de date.



Furtul de identitate în mediul online nu mai este o legendă urbană sau subiectul unui serial TV polițist. Accesul unor terți la date confidențiale creează avantaje strategice, iar blocarea accesului utilizatorilor la un set de date poate aduce prejudicii financiare considerabile, prin simpla lipsă a accesului la documente într-un anumit moment dat. În funcție de specificul instituției, pierderile nu sunt numai de natură financiară în momente de criză.

În general, utilizatorii de Internet care sunt conștienți de riscuri adoptă unele măsuri care, în opinia lor, bazată pe experiențele anterioare, ar trebui să fie suficiente pentru o bună protecție.

Departe de a oferi garanția unei securități impenetrabile, întrebările următoare și comentariile aferente fiecăreia te vor ajuta să înțelegi mai bine multiplele fațete ale securității în spațiul virtual.

REGULI PENTRU O NAVIGARE MAI SIGURĂ:

- utilizează ultima versiune de browser;
- având în vedere că cele mai multe aplicații malițioase afectează Microsoft Internet Explorer (utilizat de peste 50% dintre utilizatori), orientează-te și spre alte tipuri de browser (ex. Google Chrome, Opera, Firefox, Safari etc.), mai ales când accesezi pagini web posibil nesigure (încearcă să folosești opțiunea NotScript sau NoScript);
- verifică secțiunea de contact a site-urilor web (adresă, număr de telefon, e-mail);
- verifică destinația reală a link-urilor prin trecerea cursorului mouse-lui peste acesta și vizualizarea adresei reale în partea stângă-jos a browser-ului;
- atenție la ce plugin-uri instalezi, de multe ori acestea vin însoțite de software malițios;
- nu apăsa pe link-urile din cadrul ferestrelor de tip pop-up;
- verifică existența „https://” în partea de început a adresei web, înainte de a introduce informații personale.

INSTALEZI SOFTURI DIN INIȚIATIVA TA SAU LA PROPUNEREA UNOR TERȚI?

Principiul ar fi următorul: dacă nu l-ai căutat de la început, nu-l instala! Multe amenințări online vin sub forma cererilor de a da click pe un anumit link sau de a deschide atașamentul unui mesaj e-mail. Altele îți deschid ferestre pop-up care îți cer sa rulezi un scanner de securitate sau să instalezi un codec ori un player pentru a putea vizualiza diverse conținuturi.

Evită să dai curs unor asemenea cereri. Dacă dorești totuși să instalezi o astfel de aplicație, fă o verificare înainte pe site-uri web specializate și recunoscute. Iar dacă este necesar să instalezi acel soft, încearcă să îl descarci direct de la sursă (de pe site-ul web al producătorului) și nu de pe site-uri web terțe.

DEZINSTALEZI APLICAȚIILE DE CARE NU MAI AI NEVOIE?

Daca nu mai ai nevoie de un anumit soft, dezinstalează-l! Astfel, vor fi mai ușor de urmărit aplicațiile care necesită a fi actualizate, iar de multe ori acest lucru va permite o executare rapidă a sarcinilor de către calculator (sunt frecvente aplicațiile de mici dimensiuni și add-on-urile care se instalează împreună cu diverse softuri și care pornesc odată cu computerul, ocupând memoria acestuia și afectându-i performanțele).

ÎȚI PROTEJEZI CONEXIUNEA LA INTERNET?

Dacă folosești un router pentru a te conecta la Internet, asigură-te că ai schimbat parolele implicite ale acestuia (de cele mai multe ori, astfel de dispozitive au parole standard de genul „1234", „0000", „admin", „root"). De asemenea, actualizează firmware-ul și instalează patch-urile de securitate.

Asigură-te că router-ul este configurat să ofere conexiuni criptate. Tehnologia de criptare WPA2 este cea mai puternică formulă disponibilă în majoritatea routerelor moderne.

Urmând acești pași, vei reduce considerabil riscul ca agresorii cibernetici să preia sub control conexiunea ta de Internet, folosind-o pentru a-ți compromite computerul, pentru a-ți afla credențialele de acces la diferite conturi sau pentru a o folosi ca paravan („proxy") pentru derularea altor atacuri informatice.

De asemenea, o regulă general valabilă subliniază faptul că nu se utilizează aceleași credențiale de acces pentru router, mesagerie electronică, rețele de socializare etc.

PROTECȚIE ANTI-MALWARE MULTIPLĂ:

Combinarea mecanismelor de filtrare web cu aplicații antivirus, firewall-uri, anti-malware, politici de securitate respectiv o instruire adecvată a utilizatorilor, reduce considerabil riscul unei infectări. Utilizează produse antivirus/antispyware dezvoltate de companii diferite și actualizează frecvent atât sistemul de operare, cât și celelalte aplicații utilizate.

FOLOSEȘTI UN PROGRAM FIREWALL?

Programele firewall sunt destinate protejării calculatorului / serverului / router-ului / telefonului /tabletei împotriva atacurilor informatice, încercării de pătrundere neautorizată, instalării de aplicații software malițioase.

Firewall-ul poate bloca accesul persoanelor neautorizate la informațiile stocate pe echipamentul conectat la Internet.

Un firewall poate fi un dispozitiv hardware sau o aplicație software.

EȘTI ATENT LA DATELE TALE PERSONALE?

Nu completa formulare primite via e-mail, prin care ți se cer date cu caracter personal, parole, coduri secrete sau PIN-uri. Când vine vorba de date sensibile, instituțiile publice, băncile sau marile companii sunt mai... „conservatoare" și nu solicită să le fie transmise prin banalul e-mail. Așa că, cel mai probabil, acel mesaj prin care ți se spune că banca ta dorește să actualizeze datele clienților și are nevoie și de ale tale, inclusiv numărul cardului bancar, codul PIN și parola de conectare la contul de Internet Banking... nu este de la bancă!

În privința realizării unei achiziții online, trebuie acordată o atenție sporită nivelului de securitate al paginii, dacă se optează pentru plata online cu un card bancar.

Dacă pagina care solicită datele bancare nu utilizează protocolul HTTPS (ex: https://www.site-de-cumpărături/finalizarea_tranzacției/...), ci HTTP, care facilitează transmiterea datelor în clar, atunci se recomandă optarea pentru plata ramburs sau orientarea către un alt site web care deține produsul dorit.

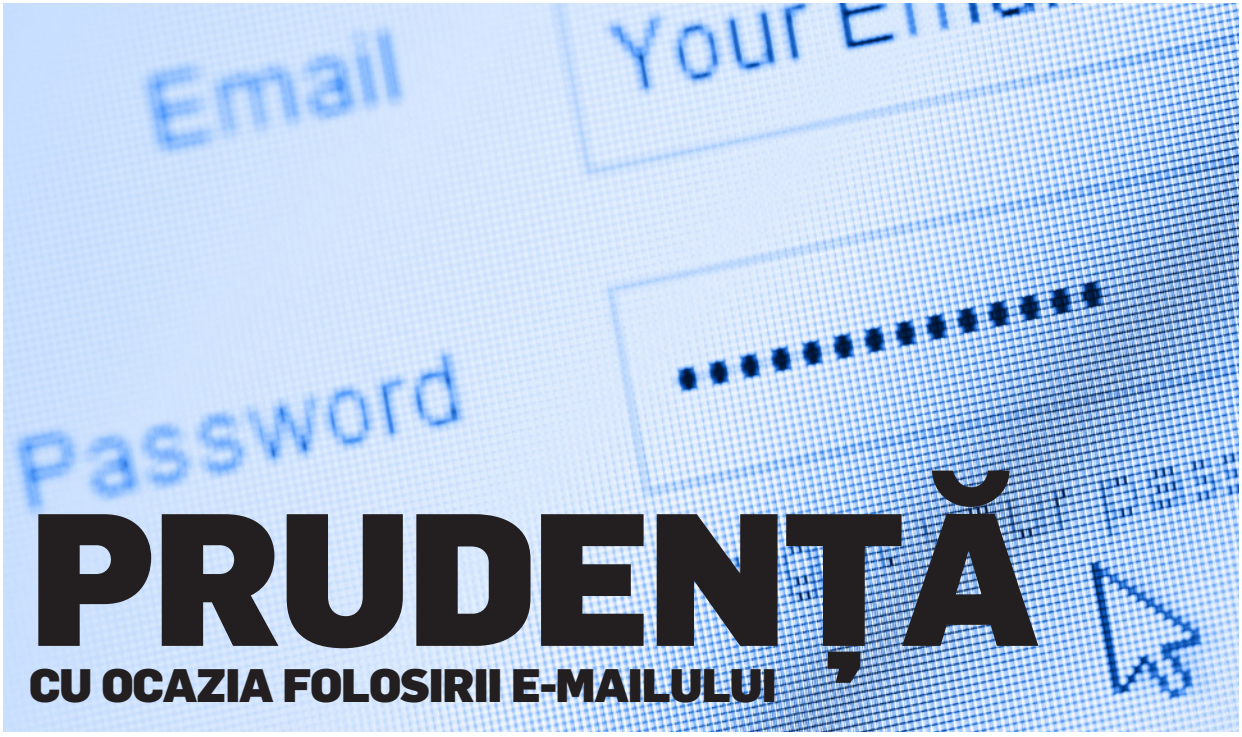
RECOMANDĂM UN SET MINIM DE REGULI:

- cumpărăturile să se realizeze doar de pe site-uri web recunoscute și securizate;
- contravaloarea unui produs achiziționat nu trebuie transmisă înainte de verificarea existenței și funcționalității acestuia, prin folosirea unui serviciu de escrow recunoscut;
- nu se folosesc servicii financiare de transfer rapid WesternUnion sau MoneyGram înainte de recepționarea produsului achiziționat, mai ales când această operațiune este solicitată de vânzător;
- verificarea site-ului web (există magazine online fictive care au ca scop atragerea de clienți și reținerea datelor bancare ale acestora).
- respectarea unei simple metode de verificare, respectiv compararea link-urilor receptate prin mesaje de tip „spam" cu cele legitime ale instituțiilor bancare.

OBSERVI CU UȘURINȚĂ SCHEMELE DE INGINERIE SOCIALĂ?

În ce constă ingineria socială? De exemplu, un banner pe un site web unde scrie că este nevoie doar să dai click pe un link dacă vrei să afli cum s-a produs cel mai recent accident aviatic ori să vezi în ce ipostaze incendiare a fost surprinsă o celebritate. Tot inginerie socială este și atunci când ești anunțat că tocmai ai câștigat o suma de bani, o excursie sau o cină romantică, în urma unei trageri la sorți la care nu îți amintești să te fi înscris, apoi ești rugat să transmiți datele personale ori să depui ceva bani într-un cont pentru a intra în posesia premiului. Indiferent de promisiune, ingineria socială îți va cere ceva: să deschizi un fișier atașat în e-mail sau transmis prin Instant Messaging, să urmezi un link, să instalezi un soft, să completezi cu datele tale un formular. Privește cu suspiciune astfel de cereri și nu te lăsa atras în schemă.

Asigurarea unui nivel ridicat de securitate în mediul online nu este o sarcină ușoară. Dar costurile insecurității se pot dovedi a fi mult mai greu de suportat.



PRUDENȚĂ

CU OCAZIA FOLOSIRII E-MAILULUI

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

Rețelele de criminalitate informatică, prin acțiuni de manipulare a persoanelor (inginerie socială), 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:

- evită transmiterea sau recepționarea de informații sensibile prin e-mail;
- 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);
- orientează-te spre un provider de e-mail ce oferă o filtrare puternică anti-spam;
- nu răspunde la spam și evită e-mailurile în cascadă sau piramidale;
- configurează corect clientul de e-mail;
- 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;

➔ 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:

➔ identitatea expeditorului nu este garantată: verifică relația dintre expeditor și conținutul mesajului;

➔ 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.);

➔ 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;

➔ 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;

➔ nu răspunde e-mailurilor conținând solicitări de date personale sau confidențiale (de exemplu codul PIN și numărul cardului bancar).

PROTEJEAZĂ-ȚI INFORMAȚIILE:

Pe piață sunt accesibile diferite tipuri de criptare a datelor, ce și-au dovedit eficiența în numeroase situații: criptarea mediilor de stocare sau a mesajelor expediate prin poșta electronică (în locul transmiterii prin e-mail a unor date sensibile în format text, conținutul poate fi criptat cu una dintre soluțiile existente pe piață, de exemplu „pgp“).

DE UNDE ȘTII CĂ E-MAILUL TĂU A FOST „ACCESAT“ DE PERSOANE NECUNOSCUTE?

➔ contactele tale spun că au primit e-mailuri spam de la tine;

➔ primești multe e-mailuri cu erori;

➔ apar mesaje în dosarul „trimise” fără ca tu să le trimiți;

➔ istoricul localizării contului în operația de login nu corespunde cu activitatea ta curentă.

CUM SECURIZĂM CONTUL DE E-MAIL CARE A FOST „ACCESAT“ DE PERSOANE NECUNOSCUTE?

➔ recuperarea contului și schimbarea parolei;

➔ schimbarea parolelor de securitate, setarea verificării prin utilizarea telefonului;

➔ verificarea conturilor de acces la bănci sau plăți online și notificarea acestora cu privire la spargerea contului de e-mail;

➔ notificarea contactelor din e-mail că ar putea exista un risc de securitate și că e-mailul (contul) a fost accesat de persoane necunoscute;

➔ efectuarea operației de back-up la fișierele importante.

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!": St1u1OO%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.

NIVELUL DE ACCES AL UTILIZATORILOR

În momentul în care ai acces la calculator, beneficiezi de drepturi de utilizare, care pot fi la nivel „utilizator” sau „administrator”:

- la utilizarea cotidiană a calculatorului (navigare Internet, citirea e-mailului, folosirea soft-urilor profesionale etc.) este indicată folosirea unui cont de utilizator, cu drepturi restrânse;
- contul de administrator nu trebuie utilizat decât pentru a interveni asupra funcționării calculatorului (instalarea de conturi de utilizatori, modificarea politicii de securitate, instalare sau modificare de software etc.).

În măsura în care un agresor va obține acces la contul tău de utilizator, va fi foarte dificil pentru acesta să preia controlul stației sau al rețelei.

PE SCURT, SE RECOMANDĂ:

- folosirea dreptului de administrator revine structurii IT, dacă aceasta există;
- deschiderea conturilor de utilizator, fără a utiliza contul de administrator pentru navigarea pe Internet;
- identificarea precisă a utilizatorilor rețelei informatice și a drepturilor acordate;
- eliminarea conturilor anonime și generice (stagiar, presa, contact etc.) în vederea asocierii activităților din rețea unor utilizatori nominali;
- realizarea unei proceduri pentru intrarea și ieșirea din schema de personal a angajaților pentru a acorda drepturi în funcție de responsabilități și pentru a le revoca la plecarea persoanei din organizație.

ACTUALIZARE SOFTWARE PERIODICĂ

În cadrul fiecărui sistem de operare (Windows, Linux, IOS, MacOS, Android etc.) există vulnerabilități. Acestea pot fi corectate de producător, care, după identificarea acestora, poate emite actualizări de securitate ale softului. Cunoscând faptul că mulți utilizatori nu actualizează software-ul, atacatorii exploatează aceste vulnerabilități, reușind să deruleze activități pe

sistemul țintă mult după descoperirea și corectarea vulnerabilităților de către producător.

Producătorii evaluează în general vulnerabilitățile software-ului și realizează patch-uri - actualizări ale software-ului în vederea înlăturării unor defecțiuni / vulnerabilități anterioare ale acestuia. Din punct de vedere informatic, vulnerabilitatea este un punct slab în proiectarea și implementarea infrastructurilor cibernetice sau a măsurilor de securitate aferente care poate fi exploatată de către un atacator.

Există însă și vulnerabilități de tip „zero day", cele care nu sunt cunoscute de autor astfel încât să poată fi remediate, dar care pot fi descoperite de un individ / entitate rău intenționat/ă și care le poate exploata în scopuri malițioase.

Aceste vulnerabilități sunt utilizate în atacurile de tip Advanced Persistent Threat (APT), agresiuni cibernetice derulate, de regulă, de state, ce vizează ținte din domeniul politic, militar, industrial, al securității naționale, al cercetării și/sau al afacerilor. Prin nivelul tehnologic ridicat, aceste agresiuni pot fi menținute în secret o perioadă lungă de timp. Scopul constă în obținerea neautorizată de informații confidențiale în interesul unei entități statale sau nonstatale (spionaj cibernetic).

Actualizarea sistemului de operare trebuie să se realizeze cât mai des, astfel încât echipamentul (calculator, laptop, server, router, telefon, tabletă etc) să ruleze optim și să fie cât mai puțin vulnerabil la atacuri cibernetice.

ASTFEL, SE IMPUNE APLICAREA UNEI SERII DE REGULI:

- definirea și aplicarea unei politici privind actualizările periodice;
- configurarea softurilor ce au capabilități de actualizare automată;
- utilizarea exclusivă a site-urilor web ale producătorului pentru operarea actualizărilor.

BACK-UP
LA INTERVALE PERIODICE

Pentru a asigura securitatea datelor tale, este recomandat să efectuezi back-up la intervale periodice (zilnic sau săptămânal) astfel încât să poți reveni la date în cazul unei probleme în funcționarea sistemului de operare sau al unui atac. Pentru a salva datele, pot fi folosiți suporți de memorie (hard-disk extern dedicat, stick-uri de memorie sau CD/DVD). Având în vedere creșterea exponențială a atacurilor cu ransomware din ultimii doi ani, se recomandă ca dispozitivul de back-up să nu fie mappat în rețea (mappare - alocarea unei litere în organizarea logică a sistemului pentru partiții/dispozitive de stocare).

Ransomware - specie de malware care blochează / restricționează total accesul utilizatorului la sistemul informatic (prin blocarea ecranului) sau la datele în format electronic (prin criptare), până când acesta plătește o răscumpărare către un terț.

Adițional, dat fiind faptul că suporții de memorie folosiți pentru stocarea copiilor de rezervă a datelor sunt vulnerabili la un acces neautorizat, trebuie să te asiguri că datele sensibile / confidențiale sunt protejate prin criptarea copiilor de rezervă.

O metodă de asigurare a integrității datelor este cloud computing, un model de furnizare a resurselor informaționale care se bazează pe partajarea prin intermediul Internetului a unor resurse (servere, capabilități de stocare, aplicații), ce diferă de modelul tradițional al serverelor și aplicațiilor locale. Astfel pot fi stocate (cloud storage) date pe servere virtuale, utilizatorii având acces la datele stocate din orice locație în condițiile existenței unei conexiuni la rețea. De cele mai multe ori presupune autentificare pe bază de nume de utilizator și parolă unice.

Înainte de a efectua salvări pe platforme online („în cloud"), trebuie sa fii conștient de faptul că acestea pot fi ținta unor atacuri cibernetice și că aceste soluții implică o serie de riscuri specifice:

- la adresa confidențialității, integrității și disponibilității datelor;
- juridice, legate de incertitudinea cu privire la situarea datelor sau ireversibilitatea contractelor.

De asemenea, trebuie să consulți cu atenție termenii contractuali stabiliți cu furnizorii de servicii cloud pentru a te asigura că datele sunt protejate cu același grad de securitate pe care l-ai implementat pe dispozitivele proprii.

SECURIZAREA ACCESULUI LA WI-FI

Utilizarea Wi-Fi, în cazul în care conexiunea nu este securizată sau este securizată incorect, comportă unele riscuri, precum accesul la date al unor persoane neautorizate sau utilizarea acestei conexiuni în scopuri răuvoitoare. Din acest motiv, trebuie evitată folosirea conexiunii wireless în organizații, în favoarea celei cu fir, care rămâne mai sigură și mai performantă.

În cazul în care varianta wireless este singura opțiune, la momentul configurării conexiunii, este indicată activarea criptării tip WPA2 sau, varianta inferioară, WPA-AES. Nu folosi criptarea WEP deoarece aceasta poate fi decriptată în numai câteva minute. De asemenea, este indicat să configurezi o parolă de mai mult de 12 caractere, pe care o vei modifica periodic (vezi capitolul 1. Alegerea cu atenție a unei parole).

De asemenea, în rețelele interne ale organizațiilor este indicată securizarea accesului la conexiunea wireless prin filtrarea după adresa MAC a echipamentului folosit pentru conectare.

Este contraindicată folosirea conexiunilor publice (rețele publice din aeroporturi, restaurante, hoteluri etc.) din punct de vedere al securității și confidențialității. Dacă aceasta este singura posibilitate de conectare, trebuie evitată transferarea oricăror date personale sau confidențiale (cum ar fi tranzacțiile bancare).

Este imperios necesar ca fiecare utilizator de Internet să evite, pe cât posibil, conexiunile publice (din baruri, restaurante, etc.), deoarece acestea nu asigură securitatea și confidențialitatea datelor vehiculate și, în plus, marea majoritatea păstrează datele de conectare ale utilizatorilor.

FOLOSIREA ÎN SIGURANȚĂ A TELEFONULUI INTELIGENT (SMARTPHONE) SAU A TABLETEI

PROTECȚIA SISTEMELOR MOBILE:

Smartphone-urile sunt practic niște minicalculatoare la purtător. Le folosim nu numai pentru a efectua apeluri, ci și pentru operațiuni bancare, cumpărături online, poștă electronică, navigare pe Internet, etc. Cei mai mulți dintre utilizatori păstrează o mare parte dintre datele importante sau personale pe telefonul mobil.

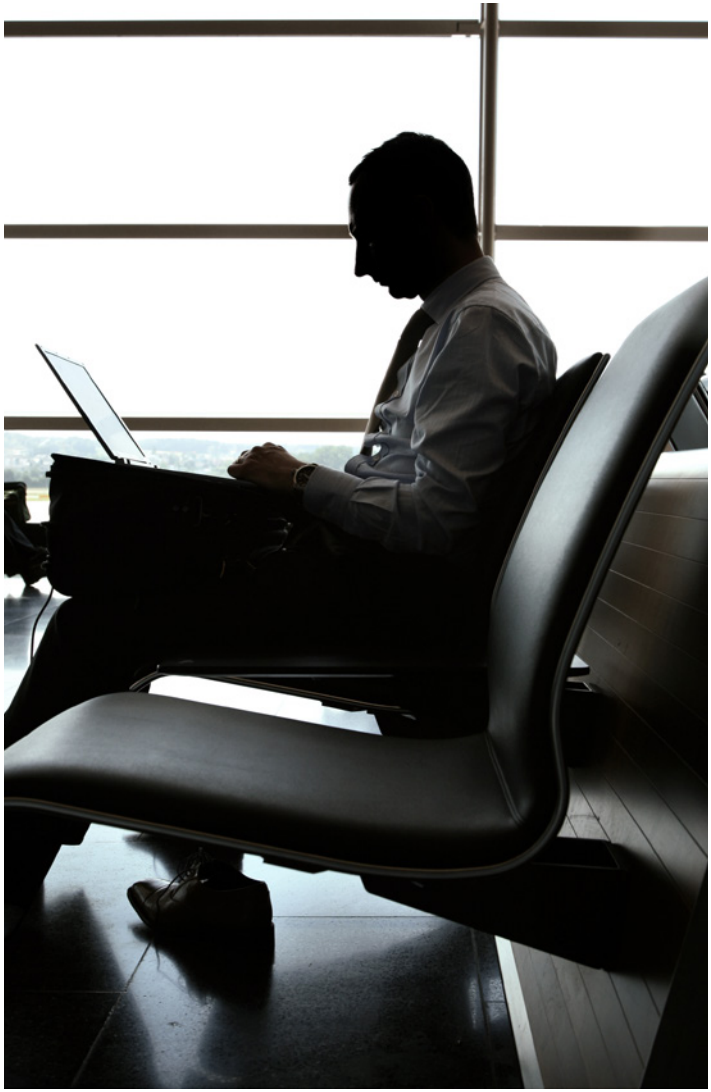
Creșterea exponențială a numărului de aplicații descărcate, partajate sau instalate, face ca aceste telefoane inteligente să devină tot mai vulnerabile la diverse tipuri de malware. Operațiunile bancare derulate de pe dispozitivele mobile au devenit tot mai populare, fără însă de a beneficia de mecanisme de protecție comparabile cu cele de pe PC-uri, încurajând astfel criminalitatea informatică.

Telefoanele inteligente au un nivel de securizare scăzut. Prin urmare trebuie aplicate o serie de reguli elementare de securitate informatică:

- nu instala decât aplicații necesare și verifică la ce date au acces înainte de le descărca (poziționare geografică, contacte, apeluri telefonice etc.). Evită instalarea aplicațiilor care solicită acces la informații care nu le sunt necesare pentru a funcționa;
- în plus față de codul PIN care protejează cartela SIM, folosește o parolă sau un cod pentru a securiza accesul la telefon și configurează-l astfel încât să se blocheze automat după (re)pornire sau la un interval de timp cât mai scurt în cazul inactivității;
- instalează software-uri de securitate special concepute pentru dispozitive mobile; acestea pot detecta și elimina virușii, bloca mesajele spam multimedia sau alte amenințări cibernetice;
- criptează memoria internă a telefonului sau tabletei dacă aceastea conțin informații sensibile; dacă dispozitivul mobil este pierdut, persoana care intră în posesia acestuia nu va putea accesa datele respective;
- realizează salvări periodice ale datelor pe un suport extern pentru a le putea restaura;
- nu permite salvarea parolelor, în special pentru aplicațiile bancare sau cele puse la dispoziție de furnizorii de servicii pentru gestionarea consumului și plata facturilor;
- aplică, periodic, actualizările de securitate furnizate de producătorii software-urilor instalate pe dispozitivele mobile.

PROTECȚIA DATELOR PE DURATA CĂLĂTORIILOR

Utilizarea dispozitivelor mobile (laptop, smartphone, tabletă) este importantă în cazul călătoriilor profesionale, simplificând transportul și schimbul de date. Există totuși o serie de riscuri în condițiile în care datele vehiculate sunt sensibile - date a căror pierdere sau furt pot genera consecințe importante asupra activităților organizației.



ÎNAINTE DE PLECAREA ÎN DELEGAȚIE

- nu folosi decât echipamente dedicate delegației (laptop, telefon, suporți de memorie) și care conțin doar strictul necesar de date;
- realizează un back-up al datelor pentru a le putea restaura în caz de pierdere;
- dacă trebuie să lucrezi în timpul călătoriei, folosește un filtru de protecție pentru ecran și o conexiune securizată pentru accesarea resurselor companiei de la distanță;
- aplică un semn distinctiv dispozitivelor tale pentru a fi sigur/ă că nu a avut loc o substituire;
- nu permite salvarea parolelor;
- șterge istoricul conexiunilor de pe tabletă / telefon; acestea ajută un potențial agresor să identifice o serie de date despre tine (locații, obiceiuri, cerc relațional etc.)

PE DURATA DELEGAȚIEI

- păstrează dispozitivele (echipamentele și suporții de memorie) permanent asupra ta;
- dezactivează funcțiile Wi-Fi și Bluetooth;
- îndepărtează cartela SIM și bateria dacă trebuie să lași telefonul nesupravegheat;
- informează reprezentanții organizației de care aparții în caz de inspecție a bagajelor sau de confiscare a dispozitivelor de către autorități străine;
- nu folosi echipamente primite cadou dacă nu le poți verifica înainte;
- evită conectarea echipamentelor tale la cele ale altor entități. Dacă trebuie să scoți fișiere (prezentări etc.) din laptop, folosește un stick USB dedicat, pe care îl vei formata ulterior cu un software specializat;
- nu permite conectarea altor echipamente (smartphone, stick USB, MP3 player, cameră foto etc.) la cele cu care călătorești;
- este recomandat să utilizezi modemuri mobile, provenite de la operatori de telefonie mobilă;
- implementează mecanismele software de dezactivare de la distanță a dispozitivului mobil și de protejare a informațiilor stocate împotriva intruziunii, în cazul unei pierderi sau al unui furt.

LA ÎNTOARCEREA DIN DELEGAȚIE

- șterge istoricul apelurilor și al navigației GPS;
- schimbă parolele folosite pe durata delegației;
- predă echipamentele la verificare, dacă este posibil;
- nu folosi/scana/verifica stick-uri de memorie/telefoane/laptop-uri/tablete/cd-uri cu prezentări/servicii VPN/VPS care ți-au fost oferite pe durata delegației deoarece ar putea conține software malițios.
- dacă se impune, pentru o mai mare siguranță, folosește funcția de resetare a dispozitivului mobil, care permite ca toate datele existente / aplicații software instalate ulterior, să fie șterse și distruse, cu revenire la setările inițiale ale producătorului.

UTILIZAREA SIGURĂ A UNITĂȚILOR EXTERNE DE MEMORIE

- Asigură-te că sunt introduși în echipamentul informatic doar suporți de memorie externă (USB stick, card memory, CD/DVD) verificați în prealabil cu aplicații antivirus actualizate.
- Ține apăsată tasta „Shift“ în momentul în care introduci suportul de memorie externă, pentru a bloca rularea automată („autorun“) a software-urilor malițioase.

PLATFORMELE SOCIALE ȘI COPIII

Cu toții utilizăm platformele sociale, în special Facebook, un mediu preferat de infractori pentru a culege date despre țintele lor. Dacă adulții sunt, în general, mai prudenți în activitatea online, copiii nu conștientizează anumite necesități de autoprotecție.

SE RECOMANDĂ:

- evitarea publicării informațiilor personale, precum ziua de naștere, adresa de e-mail sau adresa fizică;
- atunci când postezi fotografii, asigură-te că o faci doar cu persoanele cunoscute, iar acestea nu surprind locații exacte (ex.: adrese de domiciliu);
- nu dezvălui niciodată informații referitoare la perioadele în care părăsiți locuința;
- în cazul în care ai copii care au voie să folosească calculatorul familiei, nu le oferi privilegii de administrator asupra respectivului computer;
- instalează o soluție antivirus cu control parental, filtru de conținut și filtru pentru rețelele sociale. Dată fiind ponderea conținutului pornografic și a violenței online, este de datoria părinților să își păstreze copilul în siguranță;
- informează-te despre cyber-bullying și poartă discuții cu copilul tău.

CONSIDERAȚII FINALE

Acest document nu se dorește a fi un ghid absolut împotriva amenințărilor cibernetice, are un caracter general și nu oferă garanții pentru o protecție sigură (nu poate înlocui expertiza în domeniu și nu este neapărat complet sau actualizat), dar poate contribui la dezvoltarea unei culturi și crearea unor reflexe în ceea ce privește securitatea informației, într-un mediu digital caracterizat printr-o continuă transformare și dezvoltare.

PENTRU CREȘTEREA NIVELULUI DE SECURITATE CIBERNETICĂ A UNEI ORGANIZAȚII SUNT IMPORTANTE:

- crearea unei viziuni și a unor principii ce ar trebui translatate într-o politică a securității informației;
- implementarea acestei politici în cadrul organizației și definirea clară a rolurilor și responsabilităților;
- dezvoltarea unei culturi și a unei stări de spirit adecvate, prin implementarea corectă a principiilor ce privesc securitatea informației.

Utilizatorul reprezintă primul zid de apărare împotriva amenințărilor din spatele monitorului, primul și uneori ultimul senzor în identificarea pericolelor și, în funcție de caz, semnalarea acestora responsabilului IT al instituției. Utilizatorul este, totodată, cel care poate preveni crearea unor prejudicii substanțiale atât pentru sine, cât și pentru instituția în care activează.

CULTURA ÎN SECURITATEA INFORMAȚIEI PRESUPUNE:

- comunicare sigură și responsabilă;
- utilizarea înțeleaptă a rețelelor de socializare;
- transferul conținutului digital într-o manieră sigură;
- utilizarea adecvată a parolelor;
- evitarea pierderii informațiilor importante;
- asigurarea că doar anumite persoane au acces la informații;
- protecția împotriva virușilor sau a altor aplicații malware.

GLOSAR

add-on	Aplicații care modifică și îmbunătățesc funcționarea navigatorului web Internet Explorer. Aceste mici programe ajută la personalizarea browserului cu unele caracteristici care pot ușura și îmbunătăți experiența online.
amenințare cibernetică	Circumstanță sau eveniment care constituie un pericol potențial la adresa securității cibernetice.
antivirus	Program conceput să detecteze, elimine și să prevină instalarea oricăror forme de malware (viruși, troieni, adware, spyware etc.) pe sistemele de calcul.
atac cibernetic	Acțiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică.
autentificare	Procesul de verificare a identității sau a altor atribute presupuse a aparține unei entități (utilizator, proces, dispozitiv).
codec	Un program sau o bibliotecă de software, eventual chiar și un echipament hardware corespunzător, care asigură codarea și decodarea unei informații. Cuvântul este un acronim care provine de la codificare/decodificare.
cookie	Reprezintă un text special, deseori codificat, trimis de un server către browserul web, care este reutilizat de acesta de fiecare dată când navigatorul accesează acel server pe durata unei sesiuni de lucru a unui utilizator. Cookie-urile pot conține și anumite informații despre utilizatori, motiv pentru care folosirea lor este supusă unor restricții legale în SUA și statele UE.
cyber-bullying	Reprezintă hărțuirea cibernetică, respectiv folosirea tehnologiilor informației și comunicațiilor, cum ar fi e-mailul, telefoanele mobile, pager-ele, site-urile web defaimatoare, blog-urile etc. cu scopul de a ataca, în mod deliberat, repetat și ostil un individ sau un grup de indivizi.
escrow	Contul escrow este un instrument utilizat frecvent în tranzacțiile dintre părți, mai ales când este vorba de sume mari de bani, însă beneficiile acestuia sunt la fel de importante pentru orice schimb comercial și în cazul oricărei tranzacții, indiferent de valoare.
exploit	Un software sau o secvență de cod care folosește o vulnerabilitate a unei aplicații sau a unui sistem informatic cu scopul de a obține controlul asupra acestuia sau de a derula atacuri de tip denial-of-service (DOS).
firewall	Sistem (hardware sau software) proiectat cu scopul de a proteja un calculator sau o rețea internă (privată) de accesul neautorizat din exterior, prin implementarea unor politici de securitate, prin care sunt filtrate cererile și sunt respinse cele care nu respectă criteriile specificate.
hacker	Specialist IT care caută și exploatează vulnerabilități ale sistemelor informatice.
network mapping (maparea rețelei)	Efectuarea de operațiuni electronice de inventariere a sistemelor și serviciilor dintr-o rețea.

parolă	O înșiruire de litere, cifre și/sau caractere speciale, cu rol de protecție, folosită (de regulă împreună cu un nume de utilizator) la autentificare sau pentru obținerea accesului autorizat la anumite sisteme/servicii/date.
player	Reprezintă un program de calculator/software care redă înregistrări (fișiere) audio-vizuale.
world wide web („the web", www sau w3)	Sistem de documente de tip hipertext interconectate care pot fi accesate prin rețeaua de Internet. Aceste documente pot fi vizualizate sau accesate cu ajutorului unui browser și pot conține text, imagini, videoclipuri și alte formate multimedia. Cu ajutorul browser-ului se poate naviga de la o pagină la alta prin intermediul hiperlink-urilor.
wi-fi	Numele comercial al tehnologiilor construite pe baza standardelor de comunicație din familia IEEE 802.11 utilizate pentru realizarea de rețele locale de comunicație (LAN), fără fir (wireless) la viteze echivalente cu cele ale rețelelor cu fir electric de tip Ethernet.
cache	Memorie specială utilizată pentru stocarea temporară a datelor care asigură accesul rapid la anumite date utilizate frecvent de procese sau componente ale sistemului. Termenul este folosit în două accepțiuni: memorie cash și disk cash.
credențiale	Elemente utilizate în cadrul sistemelor informaționale pentru accesul la informații sau alte resurse. În general, termenul se referă la perechi de tip nume de utilizator – parolă. Drept credențiale pot fi utilizate și: datele biometrice (amprentele, recunoașterea vocală, scanarea retinei), certificatele digitale etc.
malware	Software realizat în scopuri nelegitime sau malițioase (prescurtare a sintagmei malicious software; exemple: viermi, troieni, spyware, forme de adware etc). Alte exemple: HAVIJ – aplicație software folosită în atacuri tip SQLi; SLOWLORIS – aplicație software ce permite unui computer să compromită un server web, folosind în acest scop resurse minime; PYLORIS – aplicație folosită la testarea nivelului de vulnerabilitate a unui serviciu, în vederea lansării unui atac DdoS; folosește metoda Slowloris.
patch	Actualizarea unui software în vederea înlăturării unor defecțiuni/vulnerabilități anterioare ale acestuia.
patching	Procesul de actualizare a unei aplicații software cu o versiune îmbunătățită.
spyware	Software creat pentru sustragerea de date (în special confidențiale, de acces sau bancare) de pe sistemele țintă aparținând unor persoane sau organizații
(cal) troian	Program informatic care pare a avea o funcție utilă, legitimă, dar deține și una ascunsă și potențial malițioasă, care scapă mecanismelor de securitate, uneori exploatând vulnerabilități ale sistemelor vizate. Astfel, odată rulat, programul poate derula activități malițioase, precum sustragerea de informații, afectarea calculatorului gazdă sau crearea unor căi disimulate de acces de la distanță la sistemul infectat.
virus informatic	Program care se poate autoreplica în cadrul unui sistem și propaga în alte calculatoare din rețea fără știința utilizatorului. Acesta poate afecta negativ funcționalitatea, integritatea, disponibilitatea sistemului sau datelor conținute de acesta.

WWW.SRI.RO