ROMÂNIA
JUDEŢUL SATU MARE
CONSILIUL LOCAL AL COMUNEI CĂPLENI

Hotărâre Nr.13/2021.-
privind aprobarea documentelor de organizare a activităţii de protecţia datelor în cadrul Primăriei comunei Căpleni

Consiliul local al comunei Căpleni, întrunit în şedinţa ordinară din data de 20 aprilie 2021.-

Având în vedere:
- referatul de aprobare nr.13/09.04.2021 al primarului comunei Căpleni,
- raportul secretarului general nr.36/09.04.2021,
- avizul comisiei speciale pentru buget-finanţe, patrimoniu, activităţi economico-financiare; amenajarea teritoriului şi urbanism; agricultură; protecţie mediu şi turism,
- contractul de prestări servicii încheiat cu S.C. BONEA S WORLD S.R.L.
- prevederile Regulamentului (UE) 679/2016 al Parlamentului European si al Consiliului privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (GDPR),
- prevederile Legii nr.190/2018 privind masuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European si al Consiliului din 27 aprilie 2016 privind protectia persoanelor fizice în ceea ce priveste prelucrarea datelor cu caracter personal si privind libera circulatie a acestor date si de abrogare a Directivei 95/46/CE (Regulamentul general privind protectia datelor)

În temeiul prevederilor art.129 alin.(2) lit.a), art.139 alin.(1), art. 196 alin.(1) lit.a) din Ordonanţa de urgenţă nr. 57/2019 privind Codul administrativ, cu modificările şi completările ulterioare,

HOTĂRĂŞTE:

Art.-1.- Se aprobă Analiza de risc în domeniul securităţii şi protecţiei datelor cu caracter personal al primăriei comunei Căpleni, judeţul Satu Mare, conform Anexei nr.1, care face parte integrantă din prezenta hotărâre.

Art.-2.- Se aprobă Politica de Securitate IT în domeniul GDPR, conform Anexei nr.2, care face parte integrantă din prezenta hotărâre.

Art.-3.- Se aprobă Regulamentul de Securitate privind Sistemul Resurselor Informatice şi de Comunicaţii privind GDPR din cadrul Primăriei comunei Căpleni, judeţul Satu Mare, conform Anexei nr.3, care face parte integrantă din prezenta hotărâre.

Art.-4.- Se aprobă Regulamentul de conformitate al Primăriei comunei Căpleni, judeţul Satu Mare, privind protecţia datelor cu caracter personal, conform Anexei nr.4, care face parte integrantă din prezenta hotărâre.

Art.-5.- Cu ducerea la îndeplinire şi punerea în aplicare a acestei hotărâri se încredinţează Megyeri Tamás-Róbert, primarul comunei Căpleni.

Art.-6.- Prezenta va fi comunicată prin intermediul secretarului comunei Căpleni, în termenul prevăzut de lege, cu:
-Primarul comunei Căpleni,
-Instituţia Prefectului – Judeţul Satu Mare,
-Se aduce la cunoştinţă publică prin afişare la sediul Primăriei şi publicare pe site-ul propriu.

Căpleni, 20 aprilie 2021.-

Președinte de ședință
Csizmár Antal-Tamás

Contrasemnează
Csizmar Erika
Secretar general

Prezenta hotărâre a fost adoptată cu respectarea prevederilor art.139 din Ordonanța de Urgență **Nr. 57/2019, privind Codul administrativ, cu modificările și completările ulterioare.** Nr. total al consilierilor în funcție:13, Nr. total al consilierilor prezenți: 13, Nr. total al consilierilor absenți:0, Voturi pentru:13, Voturi împotrivă:0, Abțineri:0.

Anexa nr.1 la hotărârea nr.13/2021

ANALIZA DE RISC
ÎN DOMENIUL SECURITĂȚII ȘI PROTECȚIEI
DATELOR CU CARACTER PERSONAL A
PRIMĂRIEI COMUNEI CAPLENI,
JUDEȚUL SATU MARE

RAPORT DE ANALIZĂ A RISCURILOR ȘI VULNERABILITĂȚILOR PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
EVALUAREA ORGANIZĂRII ȘI MANAGEMENTULUI SECURITĂȚII INTERNE				
1.	Lipsa unor documente specifice de planificare şi organizare a activităţii de securitate a informaţiei, subliniind aici lipsa unei politici de securitate formalizate printr-un document programatic, avizat de conducerea Primăriei şi în fapt, lipsa unor prevederi clare privind calitatea serviciilor pe zona securităţii informatice, dar și responsabilităților pe linia administrării serviciilor tehnice informatice, coroborate cu lipsa unor clauze sancţionatorii cuantificabile.	La nivelul Primăriei nu sunt elaborate documente specifice de planificare şi organizare a activităţii de securitate a informaţiei, politicii de securitate formalizate printr-un document programatic, avizat de conducerea Primăriei. Lipsa unor prevederi clare privind calitatea serviciilor pe zona securităţii informatice, dar și a responsabilităților pe linia administrării serviciilor tehnice informatice, coroborate cu lipsa unor clauze sancţionatorii cuantificabile.	Risc mediu privind posibilitatea apariției unor incidente de securitate și incapacitatea stabilirii unui responsabil pentru realizarea incidentului.	Impact mediu. Securitatea redusă a sistemului, posibilitatea exfiltrării/compromiterii de date fără determinarea responsabilităților de securitate. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
2.	Lipsa unei persoane încadrate în funcția de DPO (Data Protection Officer) în Primărie sau externalizarea serviciului..	Funcția nu există la momentul actual deoarece legislația abrogată, tradusă prin Legea nr. 677/2001 nu impunea această funcție în organigrama Primăriei.	Risc Major, Imposibilitatea conformării cu politica GDPR 2018, inexistența unui responsabil pe domeniu generează protecția deficitară a datelor cu caracter personal, lipsa punctului unic de contact și a coordonării unitare a domeniului în Primărie.	Impact major, Neconformare încălcare art.37 alin.1 secțiunea 4. din Politica GDPR
3.	Lipsa procedurilor pe domeniul securității informatice interne: procedură de urgentă privind apariția unui incident de securitate ce a generat compromiterea datelor cu caracter personal, procedură de sistem privind colectarea, prelucrarea, ștergerea, transferul, datelor cu caracter personal, procedură de sistem la apariția unui eveniment de securitate, procedură privind accesul la sisteme informatice și aplicații, procedura de back-up /	Nu sunt definite: - procedură de urgență privind acțiunea la apariția unui incident de securitate ce a generat compromiterea datelor cu caracter personal (GDPR); - procedură de back-up date cu caracter personal; - procedură/politica de update a produselor software utilizate; - procedură de acces și utilizare sistem informatic al Primăriei; - procedura de obținere, prelucrare,	Risc Major privind acțiunea ineficientă în situația compromiterii datelor cu caracter personal, în situația aplicării dreptului de a fi uitat sau în situația solicitării transferului de date. Risc mediu privind posibilitatea compromiterii datelor și informațiilor specifice Primăriei.	Impact major, NECONFORMARE Imposibilitatea acțiunii coordonate pentru punerea în practică a prevederilor art. 33, art. 34 și art. 35 din capitolul IV.

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
	disaster recovery.	stocare, utilizare, transmitere și ștergere a datelor cu caracter personal (GDPR).		
4.	Nu sunt nominalizate persoanele care îndeplinesc funcțiile de administrator de securitate și administrator de sistem.	Aceste activități sunt parțial realizate de un consilier local în a cărui fisă a postului sunt trecute unele dintre responsabilitățile administratorului de sistem și unele din responsabilitățile administratorului de rețea	Risc mediu privind apariția unui incident de securitate ca urmare a implementării partiale a politicilor de securitate a infrastructurii Primăriei.	Impact mediu Securizarea neadecvată a datelor cu caracter personal. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
5.	Inexistența în cadrul Primăriei a unei persoane responsabile pe domeniul securității care să coordoneze modul de asigurare a securității datelor și informațiilor cât și organizarea și administrarea internă a securității pentru protecția datelor fapt care poate genera lipsa unui management pe acest domeniu si apariția unor breșe de securitate.	Aceste responsabilități nu sunt îndeplinite efectiv de nicio persoană din cadrul Primăriei. Nu sunt prevăzute responsabilități și sarcini privind asigurarea securității infrastructurii informatice a Primăriei și responsabilități GDPR, nici standarde de performanță privind serviciile funcționale informatice.	Risc mediu privind apariția unui incident de securitate ca urmare a implementării partiale a politicilor de securitate a infrastructurii Primăriei.	Impact mediu Securizarea neadecvată a datelor cu caracter personal, lipsa unui control al configurației sistemelor informatice. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
6.	Nu sunt implementate şi nu sunt însuşite de personalul propriu, strategiile de securitate cu privire la protecţia datelor cu caracter personal;	Primăria nu are stabilite proceduri interne pentru protecția datelor cu caracter personal.	Risc mediu privind apariția unui incident de securitate ca urmare a lipsei unor proceduri interne care să stabileasca modul corect de a acționa.	Impact mediu Securizarea neadecvată a datelor cu caracter personal. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
7.	Nu sunt precizate clar în contractele cu Companiile de prestări servicii informatice responsabilitatile în domeniul managementului securității interne privind dezvoltarea, mentenanța și hosting-ul pentru site-ul web, precum și pentru dezvoltarea aplicațiilor de management al bazelor de date sau în procedurile interne, prin care Primăria își rezervă drepturile de exercitare a controlului privind implementarea măsurilor de	Contractele pe care Primăria le are cu furnizorii de servicii IT și cu furnizorii aplicațiilor folosite de Primărie nu conțin clauze clare pentru stabilirea responsabilităților în ceea ce privește sercuritatea aplicațiilor și în ceea ce privește compatibilitatea plicațiilor folosite cu regulile GDPR.	Risc mediu privind procesarea datelor cu caracter personal într-o manieră neconformă cu reglementările GDPR.	Impact mediu Securizarea neadecvată a datelor cu caracter personal. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
	securitate informatică prin controale inopinate, inspecții și evaluări tehnice, pe baza unui raport QoS			
8.	Lipsa clauzelor contractuale clare prin care sa se reglementeze: modul de asigurare a serviciilor informatice, persoanele din cadrul Companiilor de prestări servicii informatice care au acces la infrastructura de rețea a Primăriei, precum și responsabilitățile privind asigurarea securității cibernetice pentru aplicațile utilizate de Primărie	Contractele pe care Primăria le are cu furnizorii de servicii IT și cu furnizorii aplicațiilor folosite de Primărie nu conțin clauze clare prin care să se stabilească persoanele din cadrul companiilor care au acces la datele cu caracter personal prelucrate de Primărie.	Risc mediu privind procesarea datelor cu caracter personal într-o manieră neconformă cu reglementările GDPR.	Impact mediu Securizarea neadecvată a datelor cu caracter personal. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
9.	Existența unei imagini incomplete a infrastructurii informatice deținute de Primărie și lipsa documentelor de lucru pe domeniul securității cibernetice interne (documentație sistem informatic, liste utilizatori și drepturi de acces în sistemul informatic, inventar echipamente tehnice, proceduri de back-up/disaster recovery etc.).	Primăria nu are elaborată și aprobată o documentație scrisă clară din care să rezulte arhitectura rețelei, liste utilizatori și drepturi de acces în sistemul informatic, inventar echipamente tehnice, proceduri de back-up/disaster recovery etc.	Risc mediu datorat lipsei imaginii de ansamblu a arhitecturii de rețea, bine documentate.	Impact mediu Securizarea neadecvată a datelor cu caracter personal. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
10.	Jurnalele stațiilor de lucru și ale unor elemente componente ale sistemului informatic se rescriu periodic automat, fără a se face salvare și copii de siguranță ale acestora	La nivelul Primăriei nu există un management clar al jurnalelor stațiilor de lucru (logurilor de sistem).	Risc scăzut datorat incapacității administratorului de sistem de a determina când au avut loc incidente de sistem. Doar că nu toate incidentele de sistem sunt datorate unor tentative de a accesa neautorizat date cu caracter personal.	Impact mediu, poate duce la incapacitatea Primăriei de a determina cauza incidentului de securitate care a dus la scurgerea de informații confidențiale. Imposibilitatea acțiunii coordonate pentru punerea în practică a prevederilor art. 33, art. 34 și art. 35 din capitolul IV.
11.	Managementul securității se rezumată la managementul utilizatorilor și drepturilor de acces, simpla funcționare a sistemelor	La nivelul Primăriei nu sunt luate în calcul scenarii de penetrare a rețelei și documentate posibilele vulnerabilități și masurile necesare remedierii acestora.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei.

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
	informatice și având un grad ridicat de formalism.			Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
12.	Neaplicarea unitară a unor politici de securitate pe stațiile de lucru.	La nivelul Primăriei fiecare stație de lucru are propriile setări de siguranță și propria politică pentru Update-uri influențată de abilitățile utilizatorului.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
13.	Accesarea de către personalul Primăriei a sistemelor informatice, printr-un cont de utilizator cu drepturi de administrator local.	Conturile de utilizator pe care angajații Primăriei le folosesc pentru folosirea stațiilor de lucru ale Primăriei sunt conturi cu drepturi de administrator local.	Risc ridicat datorat posibilității compromiterii securității cibernetice a rețelei Primăriei și accesarea neautorizată la datele cu caracter personal procesate în cadrul Primăriei.	Impact ridicat, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
14.	Primăria nu deține procedură de procesare specifică pe linia securității datelor și nici proceduri standard de acces și utilizare a sistemelor informatice de către utilizatori, funcționând în acest sens pe baza cunoștințelor fiecărui utilizator și pe baza unei pregătiri minimale inițiale, la angajare.	Primăria nu deține procedură de procesare specifică pe linia securității datelor și nici proceduri standard de acces și utilizare a sistemelor informatice de către utilizatori, funcționând în acest sens pe baza cunoștințelor fiecărui utilizator și pe baza unei pregătiri minimale inițiale, la angajare.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
15.	Activitățile de control de securitate și de audit intern ar trebui să aibă o periodicitate cel puțin anuală, dar nu au fost executate până în prezent.	La nivelul sistemului informatic al Primăriei nu au fost realizate până în prezent audituri de control al securității.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
16.	Prevenţia evenimentelor nedorinte nu este o preocupare principală în cadrul politicii de securitate, iar măsurile de securitate sunt în marea	La nivelul sistemului informatic al Primăriei nu au fost realizate până în prezent audituri de control al securității.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei.

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
	lor majoritate de tip reactiv la situațiile apărute.			Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
17.	Nerespectarea regimului de management a parolelor conturilor de utilizatori din cadrul sistemului informatic al Primăriei.	La nivelul sistemului informatic al Primăriei nu existe configurate parole pentru conturile de utilizatori ale angajaților Primăriei	Risc ridicat datorat posibilității compromiterii securității cibernetice a rețelei Primăriei și accesarea neautorizată la datele cu caracter personal procesate în cadrul Primăriei.	Impact ridicat, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
18.	Obligativitatea angajaților Primăriei de a salva date cu caracter personal pe suport fizic – CD și de transmitere a acestor informații autorităților statului.	Date cu caracter personal procesate de Primărie sunt transferate, pe suport fizic – CD, către autoritătile statului.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
	SECURITATEA INFRASTRUCTURII ȘI SISTEMELOR DE TEHNOLOGIE A INFORMAȚIEI (IT)			
1.	Lipsa unui sistem de detecție și protecție împotriva intruziunilor (IDS/IPS) implementat la nivelul întregii rețele ca protecție de perimetru și ca soluție complementară de securitate, care să protejeze mediul de rețea, și să poată fi utilizată pentru eficientizarea managementului de securitate.	Lipsa unui sistem de detecție și protecție împotriva intruziunilor (IDS/IPS) implementat la nivelul întregii rețele ca protecție de perimetru și ca soluție complementară de securitate, care să protejeze mediul de rețea, și să poată fi utilizată pentru eficientizarea managementului de securitate.	Risc ridicat datorat posibilității compromiterii securității cibernetice a rețelei Primăriei și accesarea neautorizată la datele cu caracter personal procesate în cadrul Primăriei.	Impact ridicat, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
2.	Lipsa unei soluții de tip SIEM (securitatea informațiilor și managementul evenimentelor) dimensionate corespunzător numărului de stații pentru colectarea	Log-urile de securitate (fișierele jurnal) la nivel de utilizator nu sunt salvate/stocate într-o zonă de memorie separată, cu acces limitat și nu sunt analizate de către responsabilul cu	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la incapacitatea Primăriei de a determina cauza incidentului de securitate care a dus la scurgerea de informații

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
	și monitorizarea automată și activă a logurilor de securitate și accesului la date cu caracter personal, ca soluție integratoare de securitate. La momentul evaluarii, log-urile de securitate (fișierele jurnal) la nivel de utilizator nu sunt salvate/stocate într-o zonă de memorie separată, cu acces limitat și nu sunt analizate de către responsabilul cu securitatea, deoarece în sistem nu există o politică de management a log-urilor de securitate aplicată tehnic. De asemenea, procesele de modificare/ștergere/corectare a datelor cu caracter personal nu pot fi documentate cu exactitate în timp.	securitatea, deoarece în sistem nu există o politică de management a log-urilor de securitate aplicată tehnic. De asemenea, procesele de modificare/ștergere/corectare a datelor cu caracter personal nu pot fi documentate cu exactitate în timp.		confidențiale. Imposibilitatea acțiunii coordonate pentru punerea în practică a prevederilor art. 33, art. 34 și art. 35 din capitolul IV.
3.	Neimplementarea unitară a unei soluții profesionale anti-spam, anti-malware, anti-ransomware.	Stațiile de lucru din rețeaua interna a Primăriei au instalate ca soluție anti-malware Malwarebites home și instalarea update-urilor nu este unitară	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
4.	Stocarea datelor cu caracter personal în toate bazele de date interne în clar, fără instrumente de criptare și pseudoninimizare și fără posibilitatea de a păstra o evidență electronică completă a activităților de prelucrare/modificare/ștergere prin monitorizare activă și salvare de log-uri ale utilizatorilor.	Datele cu caracter perssonal sunt salvate în clar în baza de date și baza de date este stocata într-o zona de memorie nesecurizată – necriptată.	Risc scăzut datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact scăzut, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
5.	Neexecutarea periodică a testelor pentru securitatea infrastructurii informatice a Primăriei și nerealizarea sistematică a update-	Nu există stabilite politici pentru update-uri automate sau stabilite reguli de instalare a update-urilor. Nu există politici pentru scanarea periodică pentru	Risc scăzut pentru scanarea vurnerabilităților sistemului informatic al Primăriei. Risc ridicat pentru lipsa update-urilor	Impact scăzut, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei.

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
	urile software și patch-urile de securitate.	vurnrabilități.	regulate a sistemului informatic al Primăriei.	Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
6.	Lipsa controlului porturilor de tip USB și a mediilor de stocare externe, prin politici de securitate manuale instalate pe stațiile client sau printr-un sistem automat.	Stațiile de lucru din rețeaua interna a Primăriei permit conectarea prin porturile USB a memoriilor stick si HDD-urilor externe.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
7.	Lipsa controlului sistemelor de tipărire prin produse software de jurnalizare.	Nu există nici o posibilitate la nivelul sistemului informatic al Primărie de a stabili cine, ce și unde a scos la imprimantă.	Risc scăzut, nu afectează securitatea sistemului informatic dar poate afecta securitatea accesului la datele cu caracter personal procesate în cadrul sistemului informatic al Primăriei.	Impact mediu, poate duce la incapacitatea Primăriei de a determina cauza incidentului de securitate care a dus la scurgerea de informații confidențiale. Imposibilitatea acțiunii coordonate pentru punerea în practică a prevederilor art. 33, art. 34 și art. 35 din capitolul IV.
8.	Utilizarea de către angajații primăriei a conturilor de acces cu drepturi de administrator local și fără parolă.	Angajații Primăriei pot accesa stațiile de lucru din sistemul informatic al Primăriei fără a specifica o parola și conturile folosite au drepturi de administrator local.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
9.	Lipsa unei politici privind managementul parolelor de acces la sistemele informatice și la aplicațiile specializate în care se procesează date cu caracter personal.	Nu exista parole de acces configurate pe stațiile din sistemul informati al Primăriei.	Risc ridicat datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact ridicat, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
10.	Accesul la rețeaua LAN a Primăriei se face automat în momentul în care calculatorul este conectat la rețea.	Accesul la rețeaua LAN a Primăriei se face automat în momentul în care calculatorul este conectat la rețea.	Risc scăzut, datorită separării rețelei LAN în zona protejată unde sunt procesate datele cu caracter personal	Impact scăzut, poate duce la accesarea neautoriaztă a datelor cu caracter personal

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
			și zona neprotejată care permite doar accesul la INTERNET.	procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
11.	Accesul la rețeaua WLAN a Primăriei se face folosind parola specifică.	Accesul la rețeaua WLAN a Primăriei se face folosind parola specifică.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
12.	Existența unei singure rețele de WIFI la care se pot conecta atât angajații primăriei în interes de sericiu cât și vizitatorii.	Există o singură rețea de WIFI la care se pot conecta atât angajații primăriei în interes de sericiu cât și vizitatorii.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
13.	Inexistența unui firewall hardware dedicat pentru sistemul informatic al Primăriei, care să protejeze sistemul informatic al Primăriei împotriva accesului neautorizat la date din exterior.	Nu există nici un firewall hardware configurat pentru protejarea rețelei informatice a Primăriei.	Risc ridicat datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact ridicat, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
14.	Inexistența unui controler de domeniu și a unui server de Active Directory (AD) care să gestioneze unitar conturile de utilizatori ale angajaţilor Primăriei, să permită aplicarea unei politici uniforme de securitate și să ofere facilități centralizate de management al accesului angajaților la resursele informatice ale Primăriei.	Nu există nici un server de AD configurat pentru getiunea unitară a conturilor de utilizator ale rețelei Primăriei.	Risc ridicat datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact ridicat, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
15.	Folosirea sericiilor externe de FTP (WeTransfer).	Angajații Primăriei folosesc serviciile de FTP oferite de https://wetransfer.com/ sau altor furnizori din această categorie.	Risc ridicat datorat posibilității accesării de către persoane neautorizate a datelor cu caracter	Impact ridicat, poate duce la accesarea neautoriaztă a datelor cu caracter personal

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
			personal procesate de Primărie.	procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR dar și art. 33, art. 34 și art. 35 din capitolul IV
16.	Lipsa unor politici de tip white list sau black list pe ruterul central pentru a împiedica accesul la resursele de internet care compromit securitatea datelor și a rețelei de calculatoare a Primăriei.	La nivelul sistemului informatic al Primăriei nu exista stabilite reguli de filtrare al accesului la resursele Internet, angajații Primăriei pot accesa orice site doresc.	Risc ridicat datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie și de compromitere a securității sistemului informatic al Primăriei.	Impact ridicat, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR dar și art. 33, art. 34 și art. 35 din capitolul IV.
17.	Inexistența unei soluții profesionale de back-up.	Nu există o soluție de back-up pentru datele personale procesate de Primărie.	Risc mediu datorat de imposibilitatea angajaților Primăriei de a recupera datele cu caracter personal sterse accidental sau cu bună voință.	Impact mic, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
18.	Folosirea pe stațiile de lucru ale Primăriei, de către angajați, atât a conturilor de email personale cât și a celor de serviciu.	Folosirea pe stațiile de lucru ale Primăriei, de către angajați, atât a conturilor de email personale cât și a celor de serviciu.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
19.	Lipsa criptării unităților de memorie pentru stațiile de lucru pe care sunt procesate date cu caracter personal.	Datele cu caracter personal procesate de Primărie sunt salvate într-un format necriptat pe stațiile de lucru.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact ridicat, nerespectarea principiului de „privacy by default and privacy by design".
20.	Folosire de către angajații Primăriei a telefoanelor cu tehnologia de dual sim pentru a avea și numărul personal și numărul de serviciu în același telefon.	Angajații Primăriei folosesc telefoane dual sim pentru a avea în acelasi echipament atât cartela SIM personală cât și cartela SIM primită de la Primărie.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei.

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
				Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
21.	Stocarea locală, în memoria telefonului a datelor cu caracter personal procesate.	Angajații Primăriei salvează datele cu caracter personal procesate de în memoria internă a primăriei.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
22.	Lipsa unor modalități de sercurizare a accesului la datele din telefoanele angajaților Primăriei.	Lipsa unor modalități de sercurizare a accesului la datele din telefoanele angajaților Primăriei.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
23.	Lipsa unei politici centralizate pentru activarea ștergerii de la distanță a telefoanelor pierdute / furate.	La nivelul Primăriei nu există stabilită o procedură aprobată de Primărie pentru stergerea conținutului unui telefon în cazul în care acesta este pierdut sau furat.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
24.	Lipsa unei politici interne pentru gestionarea unităților optice	Stațiile de lucru din cadrul rețele informatice a Primăriei dispun de unități optice pe care angajații le pot folosi pentru a salva informațiile din stațiile de lucru pe CD/DVD.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
25.	Lipsa unei politici interne privind modul cum sunt stocate datele cu caracter personal de către angajați pe telefoanele de serviciu sau cele personale care conțin și cartela SIM de serviciu.	Fiecare angajat al Primărie folosește telefonul mobil pe care procesează date cu caracter personal după cum consideră de cuviință.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR
				capitolul II, politica GDPR.
26.	Lipsa unei politici interne pentru securizarea leptopurilor pentru a preveni accesul neautorizat la datele salvate pe unitatea de stocare internă.	Primăria nu are stabilite politici și proceduri pentru securizarea datelor cu caracter personal salvate pe unitățile de stocare internă	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
27.	Conturile de email pe care Primăria le utilizează nu folosesc versiunile securizate ale protocoalelor de comunicare.	Serverul de email al Primăriei nu folosește protocoalele securizate de comunicare.	Risc mediu datorat posibilității accesării de către persoane neautorizate a datelor cu caracter personal procesate de Primărie.	Impact mediu, poate duce la accesarea neautoriaztă a datelor cu caracter personal procesate în cadrul Primăriei. Nerespectarea în consecință a prevederilor art.5 lit. f alin 1 și 2 din capitolul II, politica GDPR.
EVALUARE ȘI PREGĂTIRE PERSONAL				
MANAGEMENT JURIDIC AL CONTRACTELOR, IN VEDEREA CONFORMARII CU POLITICA GDPR				

Nr. crt.	Vulnerabilitatea identificată	Stare de fapt	Riscul asociat identificat și estimat	Impact GDPR

ANALIZA ELEMENTELOR DE NECONFORMITATE ÎN RAPORT CU REGULAMENTUL UE NR.679/2016 PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL ȘI SOLUȚII DE OPTIMIZARE

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
ORGANIZAREA ȘI MANAGEMENTUL SECURITĂȚII INTERNE			
1.	Lipsa unor documente specifice de planificare şi organizare a activităţii de securitate a informaţiei, subliniind aici lipsa unei politici de securitate formalizate printr-un document programatic, avizat de conducerea Primăriei şi în fapt, lipsa unor prevederi clare privind calitatea serviciilor pe zona securității informatice, dar și responsabilităților pe linia administrării serviciilor tehnice informatice, coroborate cu lipsa unor clauze sancţionatorii cuantificabile.	- Crearea documentației specifice pentru politicile de securitate implementate. - Stabilirea responsabilului cu securitatea infrastructurii IT a Primăriei și stabilirea unor responsabilități clare pentru persoana numită. - Stabilirea modalităților clare de sancționare a persoanei numite resonsabil cu securitatea infrastructurii IT pentru neîndeplinirea sarcinilor.	
2.	Lipsa unei persoane încadrate în funcția de DPO (Data Protection Officer) în Primărie sau externalizarea serviciului..	- Numirea unui DPO din cadrul Primăriei; - Stabilirea clară a responsabilităților și obiectivelor de performanță; - Instruirea și pregătirea continuă a acestuia.	
3.	Lipsa responsabilităților în domeniul managementului și administrării securității sistemului informatic intern și a infrastructurii informatice ale Primăriei precizate clar în procedurile interne și stabilite prin fișa postului pentru o persoană din cadrul Primăriei.	Numirea și responsabilizarea clară a unei persoane privind administrarea de securitate a Primăriei prin: - Precizarea clară a administrării de sistem, a administrării de securitate și a protecției resurselor informaționale; - Precizarea clară a calității serviciilor oferite și a responsabilităților. Persoana numită administrator de sistem nu poate îndeplini în același timp și funcția de administrator de securitate și mai ales pe cea de DPO, datorită incompatibilității descrise în Regulamentul European al protecției datelor cu caracter personal.	
4.	Nu sunt nominalizate persoanele care îndeplinesc funcțiile de administrator de securitate și administrator de sistem.	- Numirea unei persoane cu competențe specifice pe poziția de administrator de securitate; - Instruirea și pregătirea continuă a acestuia; - Numirea unei persoane cu cumpetențe specifice pe poziția de administrator de sistem;	

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
		- Instruirea și pregătirea continuă a acestuia;	
5.	Inexistența în cadrul Primăriei a unei persoane responsabile pe domeniul securității care să coordoneze modul de asigurare a securității datelor și informațiilor cât și organizarea și administrarea internă a securității pentru protecția datelor fapt care poate genera lipsa unui management pe acest domeniu si apariția unor breșe de securitate.	- Numirea unei persoane cu competențe specifice pe poziția de coordonator al implementării și gestionării sercurității informatice; - Instruirea și pregătirea continuă a acestuia;	
6.	Nu sunt implementate şi nu sunt însuşite de personalul propriu, strategiile de securitate cu privire la protecţia datelor cu caracter personal;	- Elaborarea strategiilor de securitate specifice primăriei, conform raportului de evaluare; - Instruirea personalului intern al Primăriei cu privire la mudul în care aceste strategii de securitate se aplică pentru fiecare departament în parte; - Adaptarea continuă a strategiilor de securitate conform ultimelor descoperii în domeniul;	
7.	Nu sunt precizate clar în contractele cu Companiile de prestări servicii informatice responsabilitățile în domeniul managementului securității interne privind dezvoltarea, mentenanța și hosting-ul pentru site-ul web, precum și pentru dezvoltarea aplicațiilor de management al bazelor de date sau în procedurile interne, prin care Primăria își rezervă drepturile de exercitare a controlului privind implementarea măsurilor de securitate informatică prin controale inopinate, inspecții și evaluări tehnice, pe baza unui raport QoS.	- Includerea unor clauze contractuale clare privind managementu securității interne prin anexe pentru contractele pe care Primăria le are sau urmează să le încheie cu Companiile de prestări servicii informatice.	
8.	Lipsa clauzelor contractuale clare prin care sa se reglementeze: modul de asigurare a serviciilor informatice, persoanele din cadrul Companiilor de prestări servicii informatice care au acces la infrastructura de reţea a Primăriei, precum şi responsabilităţile privind asigurarea securităţii cibernetice pentru aplicaţile utilizate de Primărie	- Includerea unor clauze contractuale clare privind reglementarea modului de asigurare a serviciilor informatice, prin anexe, pentru contractele pe care Primăria le are sau urmează să le încheie cu Companiile de prestări servicii informatice; - Includerea unor clauze contractuale clare ce fac referire explicită la persoanele din cadrul Companiilor de prestări servicii informatice care au acces la infrastructura de rețea a Primăriei, prin anexe, pentru contractele pe care Primăria le are sau urmează să le încheie cu Companiile de prestări servicii informatice;	

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
		- Stabilirea unor clauze contractuale clare, prin anexe la contract, ce stabilesc responsabilitățile privind asigurarea securității cibernetice pentru aplicațile utilizate de Primărie.	
9.	Existența unei imagini incomplete a infrastructurii informatice deținute de Primărie și lipsa documentelor de lucru pe domeniul securității cibernetice interne (documentație sistem informatic, liste utilizatori și drepturi de acces în sistemul informatic, inventar echipamente tehnice, proceduri de back-up/disaster recovery etc.).	- Realizarea unui audit intern sau extern din care să rezulte imaginea completă a infrastructurii informatice a Primăriei și a vulnerabilităților existente; - Realizarea unui audit intern sau extern care să descrie în mod clar, concret și explicit lista utilizatorilor existenți în sistemul informatic și enumurarea drepturilor de acces pe care fiecare dintre acestia le au; - Inventarierea detaliată a echipamentelor tehnice existente în Primărie; - Stabilirea procedurilor de back-up pentru sistemul informatic al Primăriei; - Stabilirea procedurilor disaster recovery pentru sistemul informatic al Primăriei;	
10.	Jurnalele stațiilor de lucru și ale unor elemente componente ale sistemului informatic se rescriu periodic automat, fără a se face salvare și copii de siguranță ale acestora.	- Realizarea unei proceduri interne privind managementul logurilor de sistem pentru sistemul informatic al primăriei.	
11.	Managementul securității se rezumată la managementul utilizatorilor și drepturilor de acces, simpla funcționare a sistemelor informatice și având un grad ridicat de formalism.	- Realizarea periodica a unor teste de penetrare a sistemului informatic al Primăriei și a unui plan de măsuri pentru îmbunătățirea securității sistemului informatic;	
12.	Neaplicarea unitară a unor politici de securitate pe stațiile de lucru.	- Implementarea la nivelul serverului de AD a politiciilor de update automat al sistemului de operare de pe stațiile de de lucru ale Primăriei; - Implementarea unei soluții de antivirus centralizată la nivel de server	
13.	Accesarea de către personalul Primăriei a sistemelor informatice, printr-un cont de utilizator cu drepturi de administrator local.	- Eliminarea dreptului de administrator local pentru conturile de utilizator folosite de angajații Primăriei.	
14.	Primăria nu deține procedură de procesare specifică pe linia securității datelor și nici proceduri standard de acces și utilizare a sistemelor informatice de către utilizatori, funcționând în acest sens pe baza cunoștințelor fiecărui utilizator și pe baza unei pregătiri minimale inițiale, la	- Dezvoltarea unei proceduri interne specifice securității datelor în cadrul sistemului informatic propriu; - Adaptarea continuă a procedurilor interne specifice securitații conform ultimelor descoperii în domeniul; - Instruirea periodică a angajaților Primăriei referitor la modul de	

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
	angajare.	aplicare al acestor proceduri în cadrul departamentului din care angajatul face parte.	
15.	Activitățile de control de securitate și de audit intern ar trebui să aibă o periodicitate cel puțin anuală, dar nu au fost executate până în prezent.	- Realizarea a cel putin un audit intern de sercuritate pe an;	
16.	Prevenția evenimentelor nedorinte nu este o preocupare principală în cadrul politicii de securitate, iar măsurile de securitate sunt în marea lor majoritate de tip reactiv la situațiile apărute.	- Auditarea periodică a securității sistemului informatic propriu.	
17.	Nerespectarea regimului de management a parolelor conturilor de utilizatori din cadrul sistemului informatic al Primăriei.	- Configurarea conturilor de utilizator ale angajaților Primăriei să solicite parolă pentru autentificarea în sistemul informatic; - Parola să fie exprire, cel mult, odată la 3 luni; - Puterea parolei să fie cel puțin mediu și un minim de 9 caractere.	
18.	Obligativitatea angajaților Primăriei de a salva date cu caracter personal pe suport fizic – CD și de transmitere a acestor informații autorităților statului.	- Realizarea unei proceduri interne prin care să se stabilească nominal persoanele responsabile cu salvarea datelor cu caracter personal pe suport fizic – CD, modul de lucru și responsabilitățile pe care aceștia le au;	
	SECURITATEA INFRASTRUCTURII ȘI SISTEMELOR DE TEHNOLOGIE A INFORMAȚIEI		
1.	Lipsa unui sistem de detecție și protecție împotriva intruziunilor (IDS/IPS) implementat la nivelul întregii rețele ca protecție de perimetru și ca soluție complementară de securitate, care să protejeze mediul de rețea, și să poată fi utilizată pentru eficientizarea managementului de securitate.	- Implementarea la nivelul întregii rețele a unui sistem împotriva intruziunilor (IDS/IPS)	
2.	Lipsa unei soluții de tip SIEM (securitatea informațiilor și managementul evenimentelor) dimensionate corespunzător numărului de stații pentru colectarea și monitorizarea automată și activă a logurilor de securitate și accesului la date cu caracter personal, ca soluție integratoare de securitate. La momentul evaluarii, log-urile de securitate (fișierele jurnal) la nivel de utilizator nu sunt salvate/stocate într-o zonă de memorie separată, cu	- Implementarea unei soluții SIEM pentru monitorizarea activității din rețea. - Crearea pe server a unei zone de memorie dedicată păstrării logurilor echipementelor din infrastructura IT a Primăriei; - Analiza regulată a logurilor stocate. - Securizarea accesului la zona de memorie de pe server unde sunt stocate logurile de sistem și	

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
	acces limitat și nu sunt analizate de către responsabilul cu securitatea, deoarece în sistem nu există o politică de management a log-urilor de securitate aplicată tehnic. De asemenea, procesele de modificare/ștergere/corectare a datelor cu caracter personal nu pot fi documentate cu exactitate în timp.	permiterea accesului pentru administratorul de sistem și DPO;	
3.	Neimplementarea unitară a unei soluții profesionale anti-spam, anti-malware, anti-ransomware.	- Implementarea la nivel de server a unei soluții profesionale antivirus, antispam, antimalware, antiransomware care să monitorizeze activitatea întregii rețele.	
4.	Stocarea datelor cu caracter personal în toate bazele de date interne în clar, fără instrumente de criptare și pseudoninimizare și fără posibilitatea de a păstra o evidență electronică completă a activităților de prelucrare/modificare/ștergere prin monitorizare activă și salvare de log-uri ale utilizatorilor.	- Acolo unde este cazul implementarea unor modalități de criptare, pseudonimizare a datelor stocare în baza de date; - Criptarea zone de memorie de pe server unde bazele de date sunt stocate, pentru cazul în care nu se pot salva într-o manieră criptată datele în baza de date.	
5.	Neexecutarea periodică a testelor pentru securitatea infrastructurii informatice a Primăriei și nerealizarea sistematică a update-urile software și patch-urile de securitate.	- Realizarea testelor de sercuritate a infrastructurii informatice a Primăriei, cel puțin o dată pe an; - Configurarea politicilor de update automat la nivel de server.	
6.	Lipsa controlului porturilor de tip USB și a mediilor de stocare externe, prin politici de securitate manuale instalate pe stațiile client sau printr-un sistem automat.	- Configurarea sistemului informatic al Primăriei pentru a permite doar citirea de pe porturile USB și doar acolo unde este necesar pentru buna desfășurare a activității departamentului permiterea scrierii pe porturile USB; - Realizarea unor proceduri interne prin care se stabileste cine are dreptul de a scrie pe porturile USB ale statiei de lucru și cadrul organizațional în care să își desfășoare activitatea.	
7.	Lipsa controlului sistemelor de tipărire prin produse software de jurnalizare.	- Instalarea unei soluții software pentru monitorizarea activității de tipărire.	
8.	Utilizarea de către angajații primăriei a conturilor de acces cu drepturi de administrator local și fără parolă.	- Conturile de acces ale angajatilor la infrastructura informatica a Primăriei să se realizeze prin conturi de utilizator normal, fără drepturi de administrator local și care să necesite autentificare prin parolă. Puterea parolei să fie cel puțin mediu și lungimea de 8 caractere.	

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
9.	Lipsa unei politici privind managementul parolelor de acces la sistemele informatice și la aplicațiile specializate în care se procesează date cu caracter personal.	- Configurarea conturilor de utilizator conform cu punctul 8; - Configurarea valabilității parolei nu mai lungă de 90 zile (3 luni).	
10.	Accesul la rețeaua LAN a Primăriei se face automat în momentul în care calculatorul este conectat la rețea.	- Filtrarea accesului la rețeaua LAN a Primăriei pe baza adresei MAC a echipamentului conectat.	
11.	Accesul la rețeaua WLAN a Primăriei se face folosind parola specifică.	- Separarea rețelei WLAN a Primăriei în două rețele separate, una pentru vizitatori care oferă doar accesul la resursele Internet, la care se poate conecta pe baza de parolă și o a doua rețea pentru angajații Primăriei care să permită accesul la infrastructura informatică a Primăriei. SSID-ul acestei a doua rețea să nu fie vizibil și accesul la aceasta să se facă pe bază adresei MAC a echipamentului conectat.	
12.	Existența unei singure rețele de WIFI la care se pot conecta atât angajații primăriei în interes de sericiu cât și vizitatorii.	- Conform punctului 11 din prezentul raport.	
13.	Inexistența unui firewall hardware dedicat pentru sistemul informatic al Primăriei, care să protejeze sistemul informatic al Primăriei împotriva accesului neautorizat la date din exterior	- Achizitionarea şi configurarea unui firewall hardware dedicat pentru protejarea reţelei interne a Primăriei de atacurile din exterior.	
14	Inexistența unui controler de domeniu și a unui server de Active Directory (AD) care să gestioneze unitar conturile de utilizatori ale angajaților Primăriei, să permită aplicarea unei politici uniforme de securitate și să ofere facilități centralizate de management al accesului angajaților la resursele informatice ale Primăriei.	- Configurarea unui calculator cu functie de AD şi gestionarea utilizatorilor şi drepturilor de acces la reţeaua informatică a Primăriei centralizat din serverul de AD. Dacă este necesar achizitionarea unui calculator nou care să deservească acestui scop.	
15.	Folosirea sericiilor externe de FTP (WeTransfer).	- Configurarea unui server intern de FTP, folosind protocoalele secure pe care Primăria să îl folosească pentru a transmite fișiere de dimensiuni mari către Terți sau pe care angajații Primăriei să îl folosească pentru a transmite intern fișiere;	
16.	Lipsa unor politici de tip white list sau black list pe ruterul central pentru a împiedica accesul la resursele de internet care compromit securitatea datelor și a rețelei de calculatoare a Primăriei.	- Restricționarea accesului la resursele de Internet, pe principiul nevoii de a cunoaște, pentru angajații Primăriei folosind fie politicile de tip White List fie politicile de Black List.	
17.	Inexistența unei soluții profesionale de back-up.	- Configurarea unei soluții profesionale de back-up.	

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
18.	Folosirea pe stațiile de lucru ale Primăriei, de către angajați, atât a conturilor de email personale cât și a celor de serviciu.	- Introducerea în cadrul politicilor de limitare a accesului la resursele de Internet a adreselor pentru serverele de email altele decât cel al Primăriei dar și la Rețelele de socializare și Web WhatsUp.	
19.	Lipsa criptării unităților de memorie pentru stațiile de lucru pe care sunt procesate date cu caracter personal.	- Criptarea unităților de memorie a stațiilor de lucru pe care sunt procesate date cu caracter personal.	
20.	Folosire de către angajații Primăriei a telefoanelor cu tehnologia de dual sim pentru a avea și numărul personal și numărul de serviciu în același telefon.	- Securizarea accesului la telefon prin activarea unui mecanism de autentificare: recunoaștere facială, amprentă, parola sau simbol în funcție de modelul telefonului; - Activarea pe telefon a serviciilor de formatare la distanță și găsire telefon; - Configurarea unui client pentru o soluție software centralizată care să permită stergerea datelor de pe telefon de la distanță; - Realizarea unor proceduri înterne de lucru cu telefoanele mobile și de comunicare a deposedării.	
21.	Stocarea locală, în memoria telefonului a datelor cu caracter personal procesate.	- Salvarea datelor în soluția de cloud oferită de producătorul telefonului; - Folosirea telefonului doar ca terminal de acces la datele stocate în cloud;	
22.	Lipsa unor modalități de sercurizare a accesului la datele din telefoanele angajaților Primăriei.	- Securizarea telefoanelor modile conform punctelor 17 și 18 din prezentul raport.	
23.	Lipsa unei politici centralizate pentru activarea ștergerii de la distanță a telefoanelor pierdute / furate.	- Securizarea telefoanelor modile conform punctului 17 din prezentul raport; - Dezvoltarea unor proceduri interne prin care să se detalieze modul de prin care sunt sterse telefoanele mobile de la distanță.	
24.	Lipsa unei politici interne pentru gestionarea unităților optice.	- Configurarea sistemului informatic al Primăriei pentru a permite doar citirea datelor de pe unitățile optice și doar acolo unde este necesar pentru buna desfășurare a activității departamentului permiterea scrierii datelor folosind unitățile optice; - Realizarea unor proceduri interne prin care se stabileste cine are dreptul de a scrie date folosind unitățile optice și cadrul organizațional în care să	

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
		își desfășoare activitatea.	
25.	Lipsa unei politici interne privind modul cum sunt stocate datele cu caracter personal de către angajați pe telefoanele de serviciu sau cele personale care conțin și cartela SIM de serviciu.	- Realizarea unor politici interne privind modul de stocare al datelor pe telefoanele mobile ale angajaților astfel încât aceștia să le poată folosi într-un mod sigur și securizat.	
26.	Lipsa unei politici interne pentru securizarea leptopurilor pentru a preveni accesul neautorizat la datele salvate pe unitatea de stocare internă.	- Realizarea unor politici interne privind modalitățile de securizare a leptopurilor.	
27.	Conturile de email pe care Primăria le utilizează nu folosesc versiunile securizate ale protocoalelor de comunicare.	- Cofigurarea serverului de email al Primăriei să folosească versiunile securizate ale protocoalelor de comunicare; - Configurarea clienților de email pentru a se conecta la serverul de email folosint protocoalele securizate;	
	EVALUARE ȘI PREGĂTIRE PERSONAL		
28.	Posibilitatea conectării la bazele de date cu caracter personal și la sistemele informatice ale Primăriei utilizând credențialele altui utilizator sau parole implicite salvate in cache-ul sistemelor/ aplicațiilor.	Interzicerea conectării cu credențialele altor utilizatorilor interni, prin intermediul unei proceduri interne.	30.04.2020
29.	Stocarea datelor cu caracter personal în format nestructurat, pe stațiile de lucru, deși Primăria deține bazele de date structurate în cadrul aplicațiilor de sistem de dezvoltate de companiile informatice.	Interzicerea prin procedură internă a salvării de date cu caracter personal în alte locuri decât bazele de date structurate operaționale la nivelul serverelor Primăriei concomitent cu respectarea principiului minimalității.	30.04.2020
30.	Utilizarea resurselor informatice aparținând Primăriei pentru interese personale, în timpul serviciului (acces la rețele de socializare, activități de chat electronic, vizualizare/descărcare, acces video-contet, conturi de torent, copiere date personale de pe medii USB).	Reglementarea acestei practici prin procedură internă, concomitent cu implementarea soluțiilor de tip ACCES cu TOKEN și a implementării unor profile de securitate organizaționale diferite.	Martie 2020/ Ianuarie 2021
31.	Angajații pot conecta telefoane mobile, device-uri externe și medii de stocare personale la sistemele informatice de la birou.	Interzicerea/limitarea acestei practici. Managementul porturilor USB.	30.04.2020
32.	Necunoașterea prevederilor noii politici GDPR, referitoare la definirea, colectarea, procesarea, stocarea și ștergerea datelor cu caracter personal.	Realizarea unui curs de instruire specializat cu toți operatorii fie în format WEB BINAR fie pe categorii de personal pentru cunoașterea noilor prevederi GDPR.	30.06.2020

Nr. crt.	Limitarea curentă/Elementul de neconformitate	Soluții posibile	Evaluare termen de implementare
33.	Nu există și nu pot fi aplicate proceduri standard de colectare, procesare, stocare, ștergere și transmitere a datelor cu caracter personal prelucrate de Primărie.	Conștientizarea persoanelor autorizate de către operator prin prevederea responsabilităților respectării noilor proceduri, la nivelul fișelor postului.	
34.	Lipsa instruirii personalului pentru cunoașterea prevederilor politicii GDPR referitoare la colectarea, stocarea și procesarea datelor cu caracter personal.	Aplicarea prevederilor de la punctele 31 și 32, precizate mai sus.	30.06.2020
35.	Utilizarea resurselor informatice aparținând Primăriei pentru interese personale, în timpul serviciului (acces la rețele de socializare, activități de chat electronic, vizualizare/descărcare, acces video-contet, conturi de torent, copiere date personale de pe medii USB).	Reglementarea acestei practici prin procedură internă, concomitent cu implementarea soluțiilor de tip ACCES cu TOKEN și a implementării unor profile de securitate organizaționale diferite.	Martie 2020/ Ianuarie 2021
MANAGEMENT JURIDIC AL CONTRACTELOR, IN VEDEREA CONFORMARII CU POLITICA GDPR			
36.	Lipsa clauzelor contractuale ce stabilesc obligația de protecție a datelor cu caracter personal și răspunderea pentru incidentele de securitate apărute.	Completarea contractelor cu clauze specifice GDPR, în vederea conformării cu politica GDPR și evitarea angajării răspunderii pentru faptele terților.	Odată cu prelungirea, prin act adițional a contractelor ajunse la termen sau prin completarea celor în vigoare și care se prelungesc automat, dar nu mai târziu de luna Aprilie 2020.
37.	Nu există clauze care să stabilească obligația de protecție a datelor cu caracter personal și nici consimțământul potențialului angajat pentru prelucrarea acestora.	Includerea în contracte a unui paragraf specific prin care acesta să-și exprime consimțământul privind prelucrarea datelor cu caracter personal și posibilitatea retragerii acestui acord.	Aprilie 2020 și apoi permanent.

Constantin Bonea
Specialist protecția datelor cu caracter personal
Manager Securitatea Informației

Marian Duminică
Specialist protecția datelor cu caracter personal
Specialist informatician

Președinte de ședință
Csizmár Antal-Tamás

ROMÂNIA JUDEȚUL SATU MARE COM. CĂPLENI CONSILIUL LOCAL

Contrasemnează
Csizmar Erika
Secretar general

Anexa nr.2 la hotărârea nr.13/2021

APROBAT : Primar
MEGYERI TAMAS ROBERT

S.S. _____

Avizat,
Responsabil Protecția
Datelor cu Caracter Personal
_____

Politica de Securitate IT în domeniul Protecției Datelor cu Caracter Personal

COLECTIV DE ELABORARE :

1. Marian DUMINICĂ – MANAGER SECURITATEA INFORMATIEI IT/ SPECIALIST PROTECȚIA DATELOR CU CARACTER PERSONAL
2. Ramona Mariana POP – SPECIALIST PROTECȚIA DATELOR CU CARACTER PERSONAL / CONSILIER EVALUATOR JURIDIC

Cuprins

Introducere

Context

Calculatorul a devenit o componentă normală a activităţii noastre zilnice, iar tehnologia comunicaţiilor şi posibilităţile oferite de Internet au produs transformări în întreaga societate, pătrunzând în toate aspectele vieţii economice, sociale şi culturale.

Informaţia este o resursă care are o importanţă deosebită pentru desfăşurarea activităţilor Primăriei comunei Capleni, judeţul Satu Mare numită în continuare Operator şi necesită o protecţie adecvată. Informaţiile pot exista sub diferite forme: tipărite sau scrise pe hârtie, stocate electronic, transmise prin poştă sau prin mijloace electronice, prezentate în filme, sau rostite în cadrul unor conversaţii. Orice formă ar avea informaţiile şi indiferent de mijloacele utilizate pentru a fi distribuite sau stocate, trebuie întotdeauna să fie protejate corespunzător.

Securitatea informaţiilor înseamnă protejarea informaţiilor faţă de o gamă largă de ameninţări şi vulnerabilităţi pentru a asigura continuitatea activităţii şi reducerea riscului organizaţional. Securitatea informaţiilor este obţinută prin implementarea unui set adecvat de măsuri de securitate, incluzând proceduri, structuri organizaţionale, funcţionalităţi software şi hardware. Este necesar ca aceste măsuri de securitate să fie stabilite, implementate, monitorizate, revizuite şi îmbunătăţite, după caz, pentru a se asigura atingerea obiectivelor specifice şi de securitate. Angajaţii sunt responsabili să se asigure că gestionarea datelor şi informaţiilor sensibile este făcută conform legilor şi regulilor aflate în vigoare.

Datorită utilizării extensive în prezent a dispozitivelor mobile, atât pentru uz personal cât şi pentru desfăşurarea activităţilor specifice locului de muncă, angajaţii şi colaboratorii trebuie să se asigure de faptul că acest proces se desfăşoară în concordanţă cu politicile şi liniile directoare ale Operatorului. Majoritatea datelor prelucrate şi stocate de către Operator sunt protejate printr-o procedură de securitate.

Scop

Prezenta politică cuprinde o serie de recomandări cu caracter general menite să îmbunătăţească cultura de securitate informatică a personalului şi să-i familiarizeze pe aceştia cu modul în care ar trebui implementate şi folosite tehnicile, instrumentele şi mecanismele de securitate astfel încât să fie asigurată securitatea informaţiilor Operatorului.

Politica nu trebuie considerată ca fiind exhaustivă, măsurile cuprinse de acesta putând fi considerate ca necesare însă nu neapărat şi suficiente.

Obiective

Procedura Operaţională de securitate informatică pentru Operator îşi propune următoarele obiective:

- creşterea confidenţialităţii, integrităţii şi disponibilităţii datelor şi informaţiilor vehiculate în cadrul sistemelor informatice şi de comunicaţii utilizate în cadrul activităţilor desfăşurate de Operator;
- oferirea mijloacelor de ghidare şi susţinere a activităţii referitoare la securitatea informaţiei în cadrul activităţilor desfăşurate de Operator, prin definirea de controale şi măsuri ce vizează identificarea şi reducerea riscurilor şi vulnerabilităţilor de securitate manifestate în cadrul acesteia;

- creșterea nivelului general de cunoștințe în domeniul securității cibernetice, în scopul îmbunătățirii climatului general de securitate cibernetică în activitățile desfășurate în cadrul Operatorului.

Reguli de securitate informatică

În rândurile următoare se regăsesc câteva reguli generale de utilizare a dispozitivelor de calcul:

- Utilizați echipamentele de calcul de serviciu în scop profesional, de serviciu;
- Instalați pe echipamentele de calcul de serviciu numai aplicații utilizate în scop profesional, de serviciu. Preferabil, utilizați pe echipamentele de calcul de serviciu numai aplicații software cu licență și pentru care producătorul oferă suport;
- Utilizați echipamentele de calcul în scop profesional, de serviciu, numai în locații în care riscul de efracție și delapidare este foarte redus;
- Nu lăsați niciodată nesupravegheat și în locații cu risc mai ridicat de efracție sau delapidare un echipament de calcul utilizat în scop profesional, de serviciu;
- Utilizați în rețelele de date de serviciu numai echipamente de calcul pe care este instalat numai software cu licență validă (care nu sunt piratate), care nu sunt afectate de o formă sau alta de virus, malware, troian, vierme sau orice alt tip de aplicație dăunătoare și care nu prezintă risc de securitate cibernetică;
- Păstrați credentialele (nume de utilizator, parole, coduri pin etc.) criptate, utilizând aplicații dedicate. Nu păstrați credențiale scrise pe foi de hârtie în loc vizibil, sau în format electronic în clar (necriptate).
- Instalați și utilizați numai programe și fișiere (inclusiv documente și fișiere multimedia) publicate sub licență validă (comercială, gratuită, sau deschisă) și care provin din surse sigure, legitime și verificabile.
- Pentru orice problemă de securitate identificată sau suspectată, deconectați echipamentul de calcul suspectat de la rețeaua de date și contactați de urgență compartimentul IT.
- Dacă utilizați echipamente de calcul personale în scop profesional, aplicați toate regulile de mai sus și în ceea ce privește utilizarea și administrarea acestora.

Reguli privind utilizarea stațiilor de lucru

Pentru a asigura integritatea calculatorului și a datelor personale, vă recomandăm respectarea următoarelor reguli:

- Atunci când este posibil, încercați să utilizați sisteme de operare și platforme hardware moderne. Multe dintre caracteristicile de securitate ale acestor sisteme sunt acum activate implicit și pot preveni o multitudine de atacuri des întâlnite. Mai mult, versiunile acestor sisteme de operare pe 64 de biți solicită eforturi mai mari din partea unui atacator care încearcă să capete controlul unui computer;
- Setare obligatorie, indiferent de sistemul de operare pe care îl folosiți, este de a activa mecanismele automate de actualizare (update) ale sistemului de operare;

- Instalaţi o soluţie de securitate ce oferă cel puţin protecţie de tip antivirus, antimalware, antispam şi antiphishing. O soluţie completă de securitate trebuie să ofere şi capabilităţi de tip firewall şi IPS (Intrusion Prevention System), de prevenire a atacurilor şi de navigare securizată. Aceste servicii, utilizate împreună, pot oferi o apărare stratificată împotriva celor mai des întâlnite ameninţări. Multe dintre aceste soluţii oferă şi un serviciu care verifică siteurile pe care le accesaţi, având un istoric al reputaţiei domeniilor web care au avut vreodată un rol în răspândirea de malware;

- Nu uitaţi să activaţi orice serviciu de actualizare automată a acestor softuri de securitate pentru a vă asigura că folosiţi ultimele versiuni de semnături ale programelor antimalware;

- Evitaţi pe cât posibil folosirea contului de administrator al sistemului de operare. Este necesară crearea unui cont de utilizator care să nu aibă toate privilegiile specifice contului de administrator. Acest cont va fi folosit pentru activităţile uzuale, cum ar fi web-browsing, creare sau editare de documente, acces la e-mail etc. Contul de administrator ar trebui folosit numai atunci când se fac actualizări de software sau când este necesară reconfigurarea sistemului. Navigarea pe web sau accesul la e-mail folosind contul de administrator este riscantă, dând ocazia atacatorilor să preia controlul asupra sistemului;

- Folosiţi versiuni ale aplicaţiilor de tip Office cât mai recente. În versiunile mai recente, formatul de stocare al documentelor este XML, un format care nu permite executarea de cod la deschiderea unor documente, astfel protejând utilizatorii de malware-ul ce foloseşte ca mod de propagare astfel de documente. Unele din versiunile cele mai recente oferă o facilitate de tip "protected view", deschizând documentele în modul "read-only", astfel eliminând o serie de riscuri generate de un fişier infectat;

- Actualizaţi-vă software-ul! Majoritatea utilizatorilor nu au timpul sau răbdarea de a verifica dacă aplicaţiile instalate pe computer sunt actualizate. De vreme ce există multe aplicaţii ce nu au capabilităţi de auto-actualizare, atacatorii vizează astfel de aplicaţii ca mijloace de a prelua controlul asupra sistemului;

- Utilizaţi parole complexe. Ca o regulă generală, toate parolele asociate cu orice cont de utilizator ar trebui să aibă cel puţin 10 caractere şi să fie complexe, în sensul de a include caractere speciale, cifre, litere mici şi litere mari;

- Conturile de e-mail, atât cele web-based, cât şi cele locale, sunt ţinte foarte vizate de atacatori. Următoarele recomandări se pot dovedi utile pentru a reduce riscurile legate de acest serviciu:

- În ideea de a nu vă compromite atât contul de e-mail de la birou, cât şi cel personal, este recomandat să folosiţi nume diferite pentru aceste conturi. Numele de utilizator unice pentru aceste conturi diminuează riscul de a fi vizate ambele conturi într-un atac;

- Setarea unor mesaje de genul "out-of-office" pentru contul personal de e-mail nu este recomandată, fiind o sursă preţioasă de informaţii pentru spammeri şi confirmând faptul că este o adresă de e-mail validă;

- Folosiţi întotdeauna protocoale securizate atunci când accesaţi e-mailul (IMAPS, POP3S, HTTPS), mai ales atunci când folosiţi o reţea wireless. Majoritatea clienţilor de email suportă aceste protocoale, prevenind astfel o interceptare a e-mailului atunci când este în tranzit între computerul dumneavoastră şi serverul de e-mail;

- E-mailurile nesolicitate, care conţin ataşamente sau link-uri, trebuie tratate ca suspecte. Dacă identitatea celui care a trimis respectivul e-mail nu poate fi verificată, sfatul este de a şterge acel e-mail fără a-l deschide pentru a-i vedea conţinutul. Nu răspundeţi la e-mailuri care vă

solicită date cu caracter personal. Orice entitate cu care relaţionaţi prin intermediul unor aplicaţii web ar trebui deja să aibă aceste informaţii. În cazul e-mailurilor care conţin link-uri, nu navigaţi direct către acel link. Puteţi copia acel link şi să îl căutaţi de exemplu pe Google. Dacă este absolut necesară deschiderea unui ataşament, se recomandă ca acesta să fie descărcat şi scanat cu soluția antivirus instalată pe calculator;

- Nu vă lăsați amăgiți de probleme privind cardul de credit, sau invitații diverse care provin din partea unor surse necunoscute. Atunci când găsiți astfel de mesaje în Inbox, luați legătura cu banca (sau mergeți personal la bancă) pentru a vă asigura ca totul este în regulă referitor la contul dumneavoastră. Nu trimiteți niciodată parolele dumneavoastră de cont prin e-mail sau prin ataşamente. Nici un furnizor de servicii nu ar trebui să solicite astfel de informații. Este greu de imaginat că o agenție guvernamentală v-ar contacta prin Internet pentru a colecta o amendă, aşadar, tratați astfel de mesaje cu suspiciune, și sub nici o formă nu accesați link-urile sau ataşamentele conținute de mesajul respectiv. În această situație, chiar și existența unei soluții de securitate eficiente, factorul uman joacă un rol decisiv. Ingineria socială poate ajuta un hacker sau un program să stabilească o conexiune cu utilizatorul, și convingerea acestuia în a oferi date critice sau bani. De asemenea, încercați să contactați un reprezentant al instituției, care să vă ofere cât mai multe informații posibil;

Browserele sunt programele folosite pentru navigarea pe internet. Ele permit accesarea şi vizualizarea site-urilor, navigarea prin link-uri, descărcarea de fişiere de pe internet etc. Pentru a reduce riscurile legate de navigarea pe internet, ar trebui respectate următoarele recomandări:

- Utilizaţi browsere web cu capabilităţi de tip Sandbox. În momentul de faţă, există câteva astfel de browsere, care, atunci când se execută un cod malware, izolează acest cod de sistemul de operare, făcând astfel imposibilă exploatarea unei eventuale vulnerabilităţi a sistemului de operare. Majoritatea acestui gen de browsere au şi capabilitatea de auto-actualizare sau de notificare a utilizatorului atunci când apar versiuni noi;

- Evitaţi să accesaţi link-uri care sunt marcate drept periculoase de către soluția de securitate instalată pe sistem, sau de către browser-ul de internet. Dacă primiți orice mesaj de atenționare în timpul navigării pe o pagină, ieşiţi imediat de pe respectiva pagină de internet;

- Atunci când este posibil, este recomandat să folosiţi versiunile criptate ale protocoalelor utilizate de aplicaţiile web. Criptarea la nivel de aplicaţie (numită SSL - Secure Soket Layer) asigură confidenţialitatea informaţiilor atunci când sunt în tranzit prin alte reţele. Marea majoritate a browsere-lor web indică faptul că o aplicaţie foloseşte SSL, folosind simbolul unui lacăt plasat lângă URL-ul respectivului site. Acest gen de criptare previne furtul de identitate de către eventuali atacatori care interceptează traficul din reţele wireless şi care ar putea să vadă credenţialele atunci când vă autentificaţi la aplicaţii web.;

- Atunci când doriți să efectuați cumpărați online, asigurați-vă că este un website pe care îl cunoașteți dinainte și, alternativ, verificați cât mai multe comentarii ale utilizatorilor despre serviciile respectivului website;

- Dezactivaţi executarea scripturilor în browsere. Dacă folosiţi anumite browsere, puteţi folosi opțiunea NoScript / NotScript sau plugin-uri pentru a nu permite execuția de scripturi ce provin de pe site-uri necunoscute. Dezactivarea execuției de scripturi poate cauza probleme de folosire facilă a browserului, dar este o tehnică foarte eficientă pentru a elimina o serie de riscuri legate de execuția acestor scripturi;

- Nu instalați software-ul dorit din locații despre care nu sunteți sigur, mai ales software care pare să fie de tip codec (program sau o bibliotecă de software, eventual chiar și un aparat hardware corespunzător, care asigură codarea și decodarea unei informații).

Reguli privind utilizarea echipamentelor portabile de tip laptop

Regulile de utilizare a echipamentelor portabile de tip laptop sunt similare cu cele privind utilizarea stațiilor de lucru. Suplimentar, având în vedere caracterul mobil al acestor dispozitive, ar trebui respectate următoarele recomandări:

- Este recomandat să aveţi tot timpul controlul asupra laptop-urilor deoarece acestea pot fi ţinta unui atac dacă un atacator ar avea acces la ele. Dacă sunteţi nevoit să lăsaţi, de exemplu, un laptop în camera de hotel, se recomandă ca acesta să fie oprit şi să aibă unitatea de stocare criptată. Sistemele de operare recente oferă nativ capabilitatea de criptare a discurilor prin mecanisme proprii. Pentru versiuni mai vechi, dar şi pentru celelalte există produse care implementează acest serviciu. Astfel, puteţi evita accesul neautorizat la informaţii confidenţiale, în caz că laptop-ul este pierdut sau furat;

- Dispozitivele mobile ar trebui să fie conectate la internet folosind reţelele 3G/4G, această modalitate fiind de preferat în locul hotspot-urilor WiFi publice;

- Dacă se foloseşte un hotspot Wi-Fi public (nesigur) pentru accesul la internet, se va folosi o soluție de VPN pentru a proteja traficul de date efectuat și a preveni accesul neautorizat la datele transmise;

- Dezactivați funcția "Network Share" înainte de a vă conecta la un hotspot public;

- Utilizați o aplicație firewall care să filtreze accesul din exterior;

- Dacă utilizarea unui hotspot Wi-Fi este singura modalitate de a accesa internetul și nu folosiți o soluție de VPN este recomandat să vă rezumați doar la navigarea pe web și să evitați să accesați servicii unde trebuie să vă furnizați numele de utilizator și parola pentru a le accesa;

- Evitați să faceți cumpărături online atunci când sunteți conectați la un hotspot Wi-Fi public, precum cele din aeroporturi, cafenele sau mall-uri. De obicei, informațiile schimbate între dumneavoastră și magazinul online, nu sunt criptate, și pot fi interceptate ușor de către un atacator. În orice caz, dispozitivele utilizate pentru serviciu nu ar trebui utilizate pentru activități personale;

- Nu folosiți niciodată calculatoare publice pentru a efectua tranzacții bancare, sau pentru alte tipuri de achiziții online. Aceste calculatoare ar putea conține programe care înregistrează datele personale, precum troienii bancari.

Reguli privind utilizarea echipamentelor portabile de tip tabletă și smartphone

În afara casei, telefoanele mobile și tabletele devin cele mai utilizate dispozitive electronice, iar provocările și amenințările asociate acestora sunt diferite și necesită o abordare specială. Principalele probleme care pot apărea, sunt furtul sau pierderea dispozitivelor, descărcarea de aplicații ce conțin viruși, fură informații sensibile și direcționează utilizatorii către site-uri și documente compromise.

Următoarele reguli vor contribui la reducerea riscurilor:

- Actualizaţi-vă sistemele de operare pentru dispozitivele mobile. Este recomandat să faceţi acest lucru atunci când apar versiuni noi şi să verificaţi acest lucru periodic. Sunteţi mult mai vulnerabili atunci când utilizaţi dispozitivele mobile (telefon, tabletă etc.) în timpul unor călătorii, deoarece ameninţările, sunt probabil mai prezente în reţelele publice din aeroporturi, gări, obiective turistice etc.

- Protejaţi-vă terminalul cu parole şi opţiuni de criptare. În cazul în care cineva vă fură sau vă găseşte telefonul/tableta, îngreunaţi-i accesul la informaţiile stocate. De asemenea, criptaţi datele cu ajutorul unui software dedicat sau – dacă dispozitivul o permite – cu ajutorul opţiunii de criptare disponibilă în terminal;

- Folosiţi o soluţie de securitate care să aibă un modul antifurt. În cazul în care pierdeţi echipamentul sau vă este furat, modulul antifurt vă poate ajuta să identificaţi şi să îl recuperaţi. De asemenea acesta poate fi utilizat pentru a bloca echipamentul sau pentru a şterge informaţiile de pe el de la distanţă. În cazul telefonului aceste operaţii pot fi efectuate chiar dacă acesta nu are acces la internet, un simplu SMS putând fi utilizat pentru blocarea acestuia sau pentru ştergerea informaţiilor personale;

- Sincronizaţi-vă telefonul/tableta cu un calculator personal. În cazul în care pierdeţi aceste echipamente sau vă sunt furate, veţi avea o copie de siguranţă a contactelor, mesajelor, imaginilor şi documentelor stocate pe acestea;

- Accesaţi doar hotspot-uri sigure. Asiguraţi-vă că opţiunile de conexiune prin infraroşu, Wi-Fi şi Bluetooth-ul sunt oprite atunci când nu le utilizaţi. Acestea vor consuma bateria şi pot facilita accesul neautorizat la datele de pe dispozitivul mobil;

- Fiţi atenţi ce aplicaţii descărcaţi şi de unde. Să fie descărcate numai din magazinele oficiale ale operatorilor şi producătorilor precum Google Play, Apple App Store sau Microsoft Store. Softurile provenite de la distribuitorii neoficiali vă pot infecta telefonul sau tableta şi pot trimite mai departe, unor terţe părţi informaţii private. În zone necunoscute, aţi putea fi tentaţi să descărcaţi aplicaţii care să vă ajute să găsiţi diferite locaţii precum restaurante, hoteluri sau muzee. Aveţi însă încredere doar în cele care provin din surse autorizate. Pentru a evita descărcarea din greşeală a aplicaţiilor nesigure, verificaţi configuraţia terminalului accesând SETĂRI, SECURITATE şi asigurându-vă că opţiunea SURSE NECUNOSCUTE este nebifată.

- Fiţi atenţi la ofertele prea bune pentru a fi reale. Dacă primiţi dintr-o dată oferte incredibil de avantajoase cu hoteluri de lux la preţuri foarte mici, rezervări de apartamente sau oferte de reîncărcare a telefonului mobil, ignoraţi-le. Un click pe link-urile incluse în emailuri pot infecta telefonul sau tableta sau vă pot atrage să completaţi formulare cu informaţii personale. Nu uitaţi de asemenea că telefonul/tableta dumneavoastră este de fapt un mini-calculator personal, care poate fi infectat prin simpla vizitare a unui website;

- Când folosiţi reţelele sociale, asiguraţi-vă că fotografiile făcute cu smartphone-ul şi pe care doriţi să le încărcaţi pentru a le partaja cu prietenii, nu conţin informaţii legate de poziţia dumneavoastră actuală. Partajarea locaţiei e ideală pentru întâlnirile cu amicii în locuri publice, dar în acelaşi timp, permit persoanelor rău-intenţionate să vă monitorizeze obiceiurile şi rutina zilnică facilitând tentativele de hărţuire;

- Aveţi mare grijă la ce fotografiaţi. Puteţi fi tentat să fotografiaţi şi să procesaţi coduri QR (coduri de bare care stochează informaţii despre diverse produse sau linkuri către website-uri). Dacă fotografierea şi procesarea codurilor QR de pe ambalajele produselor nu sunt, de obicei,

periculoase, puteți găsi coduri QR lipite în locuri publice sau chiar desenate pe elemente de mobilier stradal, ziduri etc. Aceste coduri pot conține URL-uri către website-uri care să exploateze vulnerabilități din telefonul dumneavoastră care să se finalizeze cu o infecție.

Reguli de folosire a propriilor dispozitive la locul de muncă:

- Majoritatea instituțiilor permit angajaților introducerea propriilor dispozitive mobile în sediu și folosirea acestora în desfășurarea activității. Pentru securitatea dumneavoastră și a rețelei instituției în care lucrați, vă sfătuim să urmați aceste reguli:

- Anunțați de urgență pierderea unui dispozitiv mobil pe care aveți date care aparțin instituției. Acest lucru este esențial pentru limitarea accesului unor persoane neautorizate la aceste informații. În cazul pierderii, echipa IT vă va arăta cum să vă ștergeți de la distanță conținutul telefonului;

- Nu uitați că un smartphone e și un dispozitiv de stocare portabil. Scanați conținutul memoriei interne și externe a telefonului la fiecare introducere în calculatorul de serviciu cât și în cel de acasă. In acest fel, nu veți transfera viruși de la serviciu, acasă și viceversa;

- Din același motiv, nu introduceți nici un dispozitiv de stocare găsit (de exemplu, USB stick, CD/DVD-ROM, card SD etc.) în calculatoarele instituției. Majoritatea atacurilor asupra rețelei instituțiilor încep cu un astfel de dispozitiv "uitat" de atacator în lift, în parcare sau în locuri din instituție în care e permis accesul personalului de întreținere sau a publicului (recepții, spații de aprovizionare etc.).

Reguli de prevenire a accesului neautorizat la informații confidențiale

Multe dintre atacurile cibernetice ce vizează furtul de date confidențiale din cadrul organizațiilor sunt realizate cu complicitatea unor persoane din interior, fie că vorbim de angajați sau persoane din exterior care au acces în spațiile unde sunt amplasate sistemele informatice (spre exemplu reprezentanții companiilor cu care organizația derulează diferite activități contractuale).

O altă tehnică din ce în ce mai utilizată de atacatori este ingineria socială, cunoscută ca „social engineering" în limba engleză, care presupune exploatarea vulnerabilităților psihologice ale oamenilor pentru a-i determina să întreprindă anumite acțiuni sau să divulge informații confidențiale fără să conștientizeze acest lucru. Un exemplu clasic este acela în care atacatorii sună un angajat al organizației țintă și încearcă obținerea de informații confidențiale (numele altor persoane din organizație, credențiale de acces la anumite sisteme informatice etc.) dându-se drept cineva din interiorul organizației (o persoană cu atribuții de conducere, un angajat de la alt departament sau reprezentantul unor furnizori etc.).

Pentru a evita accesul unor persoane neautorizate la informații confidențiale vă recomandăm următoarele:

- Evitați divulgarea de informații confidențiale la telefon sau prin email, daca nu puteți verifica identitatea celui cu care comunicați. Încercați să verificați identitatea persoanei care va cere aceste informații, o metodă eficientă fiind contactarea persoanei printr-un mijloc cunoscut (sunați pe nr. de telefon mobil al acestuia, contactați o persoană din apropierea acestuia etc.);

- Manifestați precauție la accesarea emailurilor. Nu deschideți mesajele email venite de la surse nesigure (expeditor necunoscut, subiect și conținut suspect) și a link-urilor sau atașamentelor conținute de acestea;

- Păstrați credențialele (nume utilizator, parolă, token etc.) de acces la sistemele informatice în siguranță. Evitați păstrarea acestora la vedere (pe monitor, tastatură, birou etc.);
- Închideți sesiunea de lucru (logoff) când părăsiți biroul unde se află computerul. Se recomandă setarea unui screensaver care să se activeze automat după un interval de maxim 2 minute de pauză în interacțiunea cu computerul;
- Manifestați precauție la introducerea credențialelor de acces la computer în prezența altor persoane pentru a nu fi observate de aceştia.

Procedură de îmbunătățire a securității unui computer

Pentru a asigura securitatea calculatorului trebuie urmate câteva principii, cum ar fi folosirea de firewall-uri, programe antivirus, filtre pentru e-mail şi parole. Principalele sfaturi pentru a asigura securitatea calculatorului sunt:

- Actualizaţi în permanență sistemul de operare;
- Instalaţi un program antivirus eficient;
- Folosiţi un Firewall;
- Securizaţi browser-ul dumneavoastră;
- Descărcaţi programe numai din surse sigure/legitime;
- Nu deschideţi ataşamentele suspecte ale e-mail-urilor;
- Parolaţi conturile, schimbaţi parolele şi nu folosiţi aceeaşi parolă pentru toate conturile;
- Realizaţi copii de siguranță (backup) pentru datele importante;
- Raportaţi către structura IT, sau responsabililor cu securitatea informatică a sistemelor informatice, orice comportament suspect al staţiilor de lucru, cum ar fi, apariţia excesivă a ferestrelor de tip pop-up, performanța extrem de slabă a computer-ului sau un browser de Internet extrem de lent.

În cazul în care nu puteţi apela la un administrator de sistem, este indicat să urmaţi sfaturile detaliate mai jos, pentru a vă proteja calculatorul:

- Actualizaţi în permanență sistemul de operare

Actualizarea sistemului de operare reprezintă alegerea şi instalarea celor mai recente componente, perfecţionări, îmbunătăţiri, actualizări de securitate şi drivere pentru computer. Această actualizare trebuie să se realizeze cât mai des, astfel încât calculatorul să ruleze optim şi să fie cât mai puţin vulnerabil la atacuri sau viruşi.

Majoritatea programelor şi a sistemelor de operare pot fi actualizate vizitând pagina de web a acestora şi instalând cele mai noi componente, module etc. Sistemele de operare moderne oferă un program integrat în sistem, care atenţionează automat utilizatorul despre apariţia acestor componente noi şi facilitează instalarea lor (Actualizări Automate – Automatic Updates).

- Instalaţi pe calculatorul dumneavoastră un program antivirus eficient

Programele antivirus identifică viruşii cu ajutorul unei baze de date, şi dacă pe parcursul scanării întâlneşte un fişier modificat de un virus, atenţionează utilizatorul, oferind posibilitatea de ştergere sau "corectare" a fişierelor afectate. Întrucât corectarea nu este întotdeauna posibilă (caz în care se pot pierde date importante), cel mai eficient mijloc de a vă feri calculatorul de acţiunea viruşilor este împiedicarea instalării acestora. Pentru aceasta, ţineţi seama de următoarele recomandări:

- Scanaţi cu un program antivirus actualizat orice suport (dischetă, stick USB, CD, DVD) pe care îl introduceţi în calculator şi abia pe urmă folosiţi datele stocate pe acestea;
- Scanaţi toate fişierele descărcate de pe Internet şi cele primite ca ataşament prin e-mail înainte de a le deschide sau salva în calculator;
- Păstraţi programul antivirus în funcţiune pe toată perioada sesiunii de lucru la calculator, pentru ca acesta să monitorizeze automat fişierele în uz;
- Actualizaţi în mod regulat programului antivirus astfel încât acesta să cuprindă definiţiile viruşilor nou apăruţi şi mijloacele de combatere a acestora. În prezent majoritatea programelor antivirus se actualizează on-line în mod automat.
- Folosiţi un program Firewall
- Programele firewall sunt folosite pentru a proteja calculatorul de pătrunderi neautorizate şi de viruşi. Firewall-ul filtrează toate informaţiile care vin şi pleacă spre/dinspre calculator, în funcţie de anumite criterii prestabilite (destinatar/expeditor, tipul informaţiei etc.).
- Firewall-ul poate împiedica persoanele străine (de ex. hackerii, dar şi programele create de aceştia, cum ar fi viermii şi anumite tipuri de viruşi) să intre pe computerul dumneavoastră prin Internet. Utilizarea unui firewall este importantă în special dacă sunteţi conectat în permanenţă la Internet.
- Un firewall poate lua două forme, software sau hardware. Cele hardware sunt mai rar întâlnite şi sunt în general instalate şi întreţinute de administratorul de reţea. Pentru a instala un firewall software, se pot folosi programe gratuite (disponibile pe Internet) sau achiziţionate, unele fiind chiar incluse în sisteme de operare mai recente.

➢ Controlaţi ceea ce rulează în browser-ul dumneavoastră

Când browser-ul descarcă un program pe calculatorul dumneavoastră, va căuta informaţii despre programul respectiv şi despre firma care l-a creat. În cazul în care aceste informaţii sunt găsite, veţi fi întrebat dacă doriţi să instalaţi programul în cauză. Dacă informaţiile despre program nu sunt disponibile, instalarea obiectului este riscantă şi browser-ul vă va avertiza în acest sens.

Securitatea navigării în Internet poate fi crescută prin stabilirea nivelului de securitate a browserului, acesta putând bloca anumite programe sau putând cere confirmări pentru a permite rularea lor.

➢ Descărcaţi programe numai din surse sigure

Este bine să limitaţi descărcarea şi instalarea de programe de pe Internet la strictul necesar şi acest lucru să se facă din site-uri sigure. Evitaţi să descărcaţi fişiere din grupurile de discuţii publice, deoarece accesul la acestea este nelimitat şi riscul este pe măsură!

➢ Nu deschideţi ataşamentele suspecte ale e-mail-urilor

Obişnuiţi-vă să verificaţi cu un program antivirus absolut tot ce intră în calculator – de la dischete, stick-uri USB şi CD-uri, până la e-mail-uri şi ataşamentele acestora. Este întotdeauna mai indicat să previi decât să remediezi.

Aşa cum s-a arătat mai sus, cea mai frecventă metodă de răspândire a aplicaţiilor maliţioase este prin e-mail. Deseori utilizatorul este păcălit să deschidă fişierul ataşat printr-un text sau printr-un titlu interesant al ataşamentului, însă ataşamentul lansează în fapt un virus sau o altă aplicaţie maliţioasă.

Ca atare, este indicat să nu deschideţi ataşamentele despre care nu sunteţi convinşi că sunt documente utile.

➢ Parolaţi conturile, schimbaţi parolele şi nu folosiţi aceeaşi parolă pentru toate conturile

Pentru a evita accesul unor persoane străine la calculatorul dumneavoastră, la diversele aplicaţii cu informaţii confidenţiale sau la conturile de e-mail, este indicat să folosiţi parole de acces pe care să le cunoaşteţi numai dumneavoastră. Este indicat să folosiţi parole diferite pentru diferitele conturi, astfel ca, în eventualitatea că o persoană străină descoperă parola pentru un anumit cont, aceasta să nu obţină automat acces la toate conturile dumneavoastră. Câteva reguli de urmat la stabilirea de parole:

- nu folosiţi numele dumneavoastră, al altcuiva din familie sau al animalului preferat,
- nu folosiţi elemente ale adresei dumneavoastră: numele clădirii, străzii, ţării,
- nu folosiţi denumirea instituţiei, a proiectului etc.,
- nu folosiţi numărul de telefon, numărul de înmatriculare
- nu folosiţi numele starului sau personajului preferat (sau al filmului, cărţii etc.),
- nu folosiţi cuvinte din dicţionar;
- nu folosiţi numele contului pentru care stabiliţi parola;
- utilizaţi combinaţii de caractere mici şi majuscule, cifre şi alte caractere (de ex. #, &, %, $, @);
- utilizaţi parole mai lungi de 6 caractere;
- schimbaţi parola de cel puţin trei- patru ori pe an.
- Exemple de parole: parola bună - %C26p03A1979$; parole de evitat – orice cuvânt din dicţionar

➢ Faceţi Back-up pentru datele importante

Întrucât există numeroşi factori de risc şi datele stocate pe calculator sunt adesea mai valoroase decât însuşi calculatorul, aceste date trebuie arhivate periodic – operaţie numită „back-up". Această operaţiune trebuie realizată frecvent (în funcţie de importanţa informaţiilor, arhivarea se poate face

lunar, săptămânal sau zilnic – în unele cazuri chiar mai des), deoarece datele pierdute sunt adesea imposibil de recuperat.

Indicii de infectare a computerului

Utilizatorii sunt adesea sfătuiți să verifice periodic sistemul împotriva infectărilor, însă în condițiile scenariilor actuale ale atacurilor informatice, acest lucru nu mai este de ajuns. Frecvent, este nevoie de mai mult decât de informații de bază despre securitate IT, pentru a remedia un calculator infectat, iar mulți utilizatori începători nu au cunoștințe despre acest lucru. În condițiile în care multe amenințări din prezent sunt create special pentru a nu fi detectate, există totuși câteva indicii prin care putem identifica un calculator compromis.

Cele mai răspândite 10 semne de infectare sunt:

- "Computerul vorbește cu mine". Apar pe ecran tot felul de ferestre "pop-up" și mesaje publicitare, precizând că PC-ul este infectat și că are nevoie de protecție. Acesta este un exemplu tipic de infectare. Este vorba fie de un program spion ("spyware") în computer sau de o infectare cu un antivirus fals (numit și "rogueware");

- "Computerul meu funcționează extrem de încet". Acesta poate fi un simptom pentru multe cauze, inclusiv infectarea cu un virus. În cazul în care s-a produs infectarea cu un virus, vierme sau troian, acestea pot consuma resursele calculatorului, făcându-l să funcționeze mai greu decât de obicei;

- "Aplicații care nu pornesc". De câte ori ați încercat să porniți o aplicație din meniul start sau de pe desktop și nimic nu se întâmplă? Uneori se poate deschide chiar un alt program. Ca și în cazul anterior, poate fi vorba de orice altă problemă, însă este cel puțin un simptom care vă spune că ceva nu este în regulă;

- "Nu mă pot conecta la Internet sau acesta rulează extrem de încet". Pierderea accesului la Internet este un alt semn al infectării, deși poate fi cauzat și de probleme legate de furnizorul de Internet sau router. Pe de altă parte, este posibil să aveți o conexiune la Internet care funcționează mult mai greu decât de obicei. Dacă ați fost infectat, malware-ul se poate conecta la o anumită adresă de Internet sau poate deschide anumite conexiuni separate, limitând astfel viteza de accesare a Internetului sau chiar făcând imposibilă folosirea acestuia;

- "Când mă conectez la Internet, mi se deschid pe ecran tot felul de ferestre sau pagini web nesolicitate". Acesta este cu siguranță un alt semn al infectării cu malware. Multe fișiere virale sunt concepute special pentru redirectarea traficului de Internet către anumite website-uri, fără consimțământul utilizatorului, sau chiar să imite anumite website-uri, creând impresia unui site legitim;

- "Unde au dispărut fișierele mele?" . Să sperăm că nimeni nu va pune această întrebare, deși anumite atacuri sunt concepute special pentru criptarea sau ștergerea anumitor fișiere și chiar mutarea documentelor dintr-un loc în altul. Dacă vă găsiți în această situație, este cazul să începeți să vă faceți griji;

- "Antivirusul meu a dispărut, firewall-ul este dezactivat". O altă acțiune tipică a amenințărilor de pe Internet este dezactivarea sistemelor de securitate (antivirus, firewall etc.) instalate pe calculator. Dacă un singur program s-ar opri, poate că ar fi vorba de o eroare de software, dar dacă toate componentele de securitate s-ar dezactiva, aveți cu siguranță computerul infectat;

- "Computerul meu vorbește în altă limbă". Dacă limba anumitor aplicații se schimbă, ecranul apare inversat, "insecte" ciudate încep să "mănânce" ecranul, este posibil să aveți de asemenea, un sistem infectat;
- "Îmi lipsesc fișiere necesare pentru a rula jocuri, programe etc.". Din nou, acest lucru ar putea fi un semn de infectare, deși este posibil să fie vorba de o instalare incompletă sau incorectă a acelor programe;
- "Computerul meu practic nu mai poate fi controlat". În cazul în care computerul dumneavoastră începe să acționeze singur sau să trimită email-uri fără să știți, dacă aplicații sau ferestre de Internet se deschid singure, în mod sporadic, sistemul ar putea fi compromis de malware.

Amenințări cibernetice – breviar

Ransomware

Ransomware este un software malițios ce împiedică accesul la fișiere, sau chiar la întregul sistem infectat, până la plata unei „recompense". Acest tip de malware nu reprezintă o noutate, însă pentru a îngreuna procesul de recuperare a fișierelor, ransomware-urile actuale blochează accesul la documente, fotografii, muzică, filme etc., prin criptarea asimetrică a acestora.

În continuare sunt prezentate câteva variante cunoscute de ransomware împreună cu indicații referitoare la prevenirea infecției cu acest tip de malware, dar și măsuri ce pot fi aplicate pentru limitarea impactului în cazul în care s-a produc infecția.

Recomandarea noastră este să evitați plătirea recompensei solicitate, pentru că astfel contribuiți în mod direct la încurajarea acestui tip de activități frauduloase și riscați să nu re-dobândiți accesul la fișierele criptate nici după efectuarea plății.

CTB Locker

CTB Locker (Curve-Tor-Bitcoin Locker), cunoscut și sub numele de Critroni, reprezintă un software malițios de tipul ransomware al cărui scop este de a cripta fișierele stocate pe sistemul afectat. Acesta a fost lansat la mijlocul lunii iulie a anului 2014 și vizează toate versiunile de Windows, inclusiv Windows XP, Windows Vista, Windows 7, Windows 8 și Windows 10.

Odată infectat cu acest malware, sistemul afectat va fi scanat, iar fișierele regăsite pe acesta vor fi criptate. Este important de știut că, dacă în trecut fișierele criptate își schimbau extensia în CTB sau CTB2, ultimele versiuni de CTB Locker identificate adaugă fișierelor criptate o extensie aleatoare (spre exemplu .ftelhdd, .ztswgmc, etc.). După criptarea fișierelor, este deschisă o fereastră de răscumpărarea datelor .

CryptoWall

Ca și în cazul CTB Locker, și acest ransomware criptează fișierele stocate pe sistemul infectat și apoi solicită o sumă de bani (500$, 500 EUR, 0.5 Bitcoin etc.) în schimbul decriptării acestora. CryptoWall 3.0/4.0 utilizează rețeaua TOR pentru direcționarea utilizatorului victimă către pagina web unde acesta va regăsi instrucțiunile pentru modul de plată a „recompensei" și decriptarea datelor. De asemenea atacatori au extins perioada de răscumpărare de la 5 zile la o săptămână, după care prețul pentru decriptarea fișierelor se va dubla.

Odată instalat pe sistemul infectat, CryptoWall începe procesul de criptare a fişierelor în fundal, fapt pentru care majoritatea utilizatorilor nu observă că sistemul lor a fost infectat până în momentul în care programul maliţios afişează fereastra de răscumpărare a fişierelor deja criptate.

CryptoWall 3.0 utilizează algoritmul de criptare RSA-2048 pentru criptarea fişierelor. Odată finalizat procesul de criptare a fişierelor, malware-ul le şterge pe cele originale, iar în cazul în care nu există backup pentru acestea, şansele de a le recupera scad dramatic.

Scopul programului maliţios este de a cripta fişierele valoroase pentru utilizator. Acesta criptează pe lângă documentele MS Office, imagini, fişiere audio, video etc. Astfel de malware este de obicei greu de detectat de utilizatori deoarece se ascunde în spatele unui software legitim răspândit via email, site-uri web, drive-in downloads etc., iar mesajul de răscumpărare este un fişier HTML .

Spyware

Programele de tip spyware sunt scrise cu scopuri maliţioase. Ele se pot afişa extrem de simplu, ca nişte ferestre de tip pop-up extrem de enervante, care au menirea să îţi distragă atenţia sau să te atragă către site-uri maliţioase. Totodată, pot fi software-uri care înregistrează obiceiurile din browser-ul pe care îl foloseşti pentru navigarea pe Internet sau chiar intrările de la tastatură (keylogger), cu intenţia de a capta credenţiale de acces sau parole.

Utilizatorii sunt sfătuiţi să raporteze cazurile de activitate suspicioasă pe staţiile de lucru, cum ar fi, apariţia excesivă a ferestrelor de tip pop-up, performanţa extrem de slabă a computer-ului sau un browser de Internet extrem de lent, care ar putea fi redirectat către site-uri nelegitime sau nedorite, precum cele pornografice sau cele de pariuri online. În astfel de cazuri trebuie să vă adresaţi pentru asistenţă Departamentului IT, şi să raportaţi suspiciunea că staţia dvs. a fost infectată cu spyware.

Cum vă protejaţi de spyware

Încercaţi să evitaţi accesarea site-urilor necunoscute şi să le frecventaţi pe cele de încredere. Siteurile de încredere sunt de regulă foarte atent monitorizate de către administratorii acestora şi foarte rar veţi găsi software de tip spyware încorporat în astfel de pagini.

Recomandăm activarea caracteristicilor de securitate ale browser-ului folosit la navigarea pe Internet. Browsere precum Internet Explorer, Mozilla, Google Chrome sau Safari au astfel de setări incluse. Mai mult, vă recomandăm să dezactivaţi în browser stocarea fişierelor de tip cookie deoarece acestea pot fi folosite cu intenţii maliţioase. Descărcaţi programe şi software numai de pe site-uri de încredere. Niciodată nu accesaţi ferestre pop-up nedorite. În schimb, închideţi-le cu click pe butonul X care apare cu culoarea roşie de regulă în partea dreaptă sus a ferestrei pop-up.

Instalaţi software anti-spyware şi actualizaţi-l periodic, la fel cum procedaţi şi cu software-ul antivirus. Rulaţi acest software în mod regulat. Programe precum SpyBot şi AdAware sunt gratuite şi fac o treabă excelentă în ceea ce priveşte protejarea sistemului de spyware. În acelaşi timp, instalaţi un pop-up blocker de tip AdBlock.

Sfaturi pentru utilizarea în condiţii de siguranţă a Internetului, prevenind pătrunderea spyware-ului în calculator:

- Nu descărcaţi niciodată deliberat, software de pe Internet pe staţia de lucru, indiferent cât de productiv sau interesant pare. Chiar şi inofensivele bare de instrumente sau utilităţi pot conţine spyware. Atenţie sporită la programe de tip file-sharing, pe care oricum nu ar trebui să le utilizaţi la birou;

- Stați departe de orice site-uri dubioase, inclusiv pornografie, jocuri de noroc, hacking sau alte site-uri suspicioase/ne-convenționale. În orice caz, nu ar trebui să vizitați astfel de site-uri în desfășurarea atribuțiilor de serviciu;

- Oricând apare o fereastră pop-up nedorită sau neașteptată, închideți-o imediat apăsând pe semnul X din partea dreapta sus a ferestrei. Niciodată nu dați click pe orice buton afișat, chiar dacă afișează mesajul "CANCEL" sau "CLOSE" pe fereastra în sine. Aceste butoane pot avea în spate o comandă pentru descărcare nedorită de spyware;

- Fiți suspicioși în momentul în care numeroase ferestre pop-up încep să se afișeze pe ecranul computer-ului, sau dacă performanța sistemului este sesizabil afectată. Din acel moment puteți presupune că ați fost infectat cu spyware și va trebui să vă adresați departamentului IT;

- Dacă folosiți Internet Explorer ca browser, schimbați setările pentru a bloca Active X. Mergeți la TOOLS > Internet Options > Security > Custom Level. În această fereastră există o secțiune în partea de sus, dedicată controalelor Active X. Aici vă sfătuim să dezactivați descărcarea de Active X cu sau fără semnătură, precum și cele marcate ca ''unsafe''. Unele obiecte Active X sunt spyware. Aceste setări le vor bloca.

Farse pe e-mail, Scam și Spam

Multe din incidentele de tip Scam vin sub forma unui avertisment despre un virus care poate să 'șteargă hard disk-ul' sau un mesaj similar. Mesajul îți va cere să contactezi toate persoanele din agenda dvs. pentru a-i avertiza. Aceste farse sunt extrem de comune, astfel că furnizorii de software antivirus au creat pagini web care raportează și urmăresc ultimele astfel de încercări.

Una dintre escrocheriile cele mai cunoscute și propagate via e-mail (SCAM) este cea care folosește mesajul 'You can be a millionaire' (Poți deveni milionar). Prin retransmiterea acestor e-mail-uri altor persoane, utilizatorul este convins că va primi o anumită sumă de bani pentru fiecare mesaj transmis. Au existat foarte multe persoane care au căzut pradă acestei scheme. Autorii acestui tip de e-mail caută adesea notorictate prin transmiterea mesajului lor, la cât mai mulți utilizatori.

O modalitate simplă de a sesiza o farsă sau înșelătorie este includerea unui atașament. La fel cum siteuri de încredere nu vor cere informații cu caracter personal prin e-mail, persoane de încredere sau instituții nu vă vor transmite printr-un atașament care trebuie folosit 'pentru eliminarea fișierelor infectate.

Așadar, este foarte important să nu deschideți niciodată un atașament de la un expeditor necunoscut sau un atașament pe care nu îl așteptați.

Țineți minte: În cazul în care mesajul sună prea frumos pentru a fi adevărat, atunci probabil că așa este. În cazul în care în corpul e-mail-ului se specifică faptul că urmărește numărul destinatarilor mesajului pe care ar trebui să îl transmiți mai departe, atunci este vorba de o înșelătorie. E-mail-urile nu pot fi urmărite în acest mod. Cel mai bun mod de a opri acest tip de farse și escrocherii, este de a te informa despre modul cum acestea operează. Informarea este cheia succesului în cazul eliminării campaniilor dăunătoare de pe Internet.

Spam-ul este adesea un efect secundar comun și adesea frustrant de a avea un cont de e-mail. Cu toate că nu vei putea niciodată elimina complet primirea unor astfel de mesaje, există totuși modalități de a reduce cantitatea de mesaje de tip spam primită.

Spam-ul este varianta electronică a junk mail-ului, termen referitor la mesaje nesolicitate şi adesea nedorite de către destinatar. Tendinţa este ca şi spam-ul să conţină un ataşament sau link maliţios.

Există câţiva paşi pe care puteţi să-i faceţi pentru a reduce semnificativ cantitatea de spam pe care o primiţi:

- Nu oferiţi adresa de e-mail în mod arbitrar – adresele de e-mail au devenit aşa de comune, încât au alocat un spaţiu special pe aproape orice formular. Pare inofensiv, astfel că o mulţime de oameni completează adresa lor de e-mail în spaţiul alocat de pe orice formular practic fără să realizeze ce se poate întâmpla cu aceasta. Spre exemplu, companiile de regulă introduc astfel de adrese de e-mail într-o bază de date pentru a putea ţine evidenţa clienţilor şi a datelor de contact aferente acestora. Uneori aceste liste sunt vândute sau partajate cu alte companii, astfel că din acel moment este posibil să primiţi mesaje nesolicitate;

- Verificaţi politicile de confidenţialitate – Înainte de a trimite o adresă de e-mail online, uitaţivă după o politică de confidenţialitate. Cele mai renumite site-uri au încorporat un link către politica de confidenţialitate pentru orice formular pe care vi se cere să îl completaţi cu date personale. Ar trebui să citiţi atent această politică de confidenţialitate înainte de a completa o adresă de e-mail sau orice alte informaţii personale;

- Raportaţi mesajele ca spam – Majoritatea clienţilor de e-mail (Thunderbird, Outlook etc.) oferă o opţiune de a raporta un mesaj ca spam sau junk. Dacă aveţi această opţiune puteţi profita de funcţionalitatea ei. Raportând mesajele de tip spam sau junk folosind această funcţionalitate, ajută la filtrarea corectă a mesajelor astfel încât e-mail-urile nedorite să nu mai fie afişate în Inbox. Cu toate acestea, instrumentele care fac această filtrare fiind automatizate, este de dorit să verificaţi frecvent directoarele de tip SPAM sau JUNK pentru eventualitatea în care mesaje legitime pot ajunge la rândul lor în acest spaţiu;

- Nu urmăriţi link-urile din mesajele de tip spam – Unele mesaje spam se bazează pe generatoare care încearcă diferite variaţii de adrese de mail pe anumite domenii. Mesajele nedorite care oferă o opţiune de dezabonare sunt deosebit de tentante, dar acest lucru este de multe ori o metodă de colectare a adreselor valide care sunt apoi folosite pentru a trimite alte mesaje de tip spam;

- Dezactivaţi descărcarea automată a graficii în e-mail-uri HTML – Mulţi dintre cei care trimit mesaje de tip SPAM trimit mesaje HTML cu un fişier grafic ataşat, iar acesta este utilizat pentru a urmări cine deschide mesajul. În cazul în care clientul de mail descarcă graficul de pe serverul de web, expeditorul ştie că mesajul a fost deschis. Dezactivarea afişării HTML cu totul şi vizualizarea mesajelor în text simplu previne această problemă;

- Pentru spaţiul personal, recomandăm deschiderea adiţională a unui alt cont de e-mail, majoritatea furnizorilor importanţi oferind conturi de e-mail gratis. Dacă o anumită adresă de e-mail este foarte des utilizată (pentru cumpărături online, pentru autentificarea pe anumite servicii, etc.), o adresă secundară de e-mail ar putea fi folosită pentru protejarea celuilalt cont utilizat. Totodată, aţi putea utiliza acest al doilea cont atunci când postaţi pe liste de discuţii publice, pe site-uri de social networking, bloguri, forumuri sau web. În cazul în care contul începe să se umple cu spam vă recomandăm să ştergeţi absolut toate mesajele şi să vă notificaţi contactele despre noua adresă de e-mail pe care aţi creat-o;

- Utilizaţi câmpul "BCC:" pentru a trimite e-mail-uri. Câmpul "Bcc:" ajută la protejarea caracterului confidenţial al adreselor altor destinatari şi să conferim mesajului nostru un caracter unic şi special;

- Nu folosiţi adresa de e-mail primită de la serviciu în interes personal. De exemplu înscrierea pe diferite forumuri, reţele de socializare sau alte site-uri, precum şi recepţionarea şi/sau redistribuirea de mesaje de genul filmuleţe comice, bancuri, fotografii sunt activităţi pentru care ar trebui utilizat un cont de e-mail personal.

Phishing

Phishing-ul este o metodă online folosită de către atacatori pentru a sustrage bani, credenţiale de acces la conturi online, parole sau alte informaţii personale şi/sau importante. De obicei, un atac de tip phishing reprezintă un e-mail deghizat ca un mesaj de la o sursă de încredere (bancă, companii de credit, comercianţi online etc.). Nu este un fapt neobişnuit ca personalul angajat să primească e-mailuri de tip phishing care par să vină din partea colegilor de birou sau din partea altor angajaţi din spaţiul public. Aceste conturi au fost de cele mai multe ori compromise în prealabil şi ulterior făcute să trimită e-mailuri de tip phishing către toate contactele înregistrate în lista lui de contacte.

Mesajul primit vă cere de regulă să verificaţi imediat datele contului dvs., ameninţând de regulă cu luarea unor măsuri negative împotriva dvs. în cazul în care nu vă conformaţi. Utilizatorii sunt astfel adesea păcăliţi în a furniza informaţiile cerute cu caracter personal sau confidenţial, cum ar fi numere de cont bancar sau de card de credit, codul numeric personal, parole, etc. Astfel de e-mail-uri pot conţine imagini, logo-uri texte şi link-uri către site-uri web ce par a fi legitime. De asemenea, este comun pentru astfel de e-mail-uri să includă ataşamente şi link-uri pentru documente false, care vă solicită să introduceţi numele de utilizator şi parola. Este foarte importantă verificarea legitimităţii oricăror ataşamente venite din partea colegilor de muncă, angajaţi din spaţiul public, sau din alte surse, înainte de a deschide documentul sau de a accesa link-ul transmis.

E-mail-urile legitime venite din partea instituţiilor financiare, angajaţi din domeniul public sau orice alt tip de organizaţie, nu îţi vor solicita NICIODATĂ informaţii personale.

Cum puteţi sesiza diferenţa dintre o înşelătorie de tip phishing şi un e-mail sau site legitim?

Din nefericire, incidentele de tip phishing sunt din ce în ce mai răspândite şi utilizate, dezvoltându-se şi fiind din ce în ce mai greu de identificat. Cu toate acestea, există multiple strategii pe care le puteţi utiliza pentru a recunoaşte acest tip de escrocherii.

Fiţi sceptic! Din moment ce realizaţi faptul că astfel de escrocherii de tip phishing există în lumea virtuală, fiţi sceptici cu privire la conţinutul fiecărui email pe care îl primiţi. A fost oare contul dvs. cu adevărat compromis? Aveţi cu adevărat nevoie să vă actualizaţi informaţiile contului? Majoritatea companiilor nu aşteaptă până în ultimul moment să-şi notifice clienţii despre o situaţie de urgenţă. Aceştia de regulă trimit mai multe notificări, de regulă prin intermediul serviciului poştal sau vă contactează prin telefon pentru a vă avertiza asupra potenţialelor încălcări ale securităţii. Dacă primiţi astfel de email-uri, verificaţi conţinutul pentru indicii care să demonstreze că acel mesaj este un fals.

Verificaţi atent adresa web şi adresa de email deopotrivă. Este o modalitate foarte bună de a descoperi o înşelătorie. Spre exemplu, în cazul în care o adresă web este afişată sub această formă (http://172.168.15.100/ebay/account/), atunci fiti sigur că site-ul pe care urma să îl accesaţi nu este unul legitim. Chiar dacă Ebay este parte a adresei afişate, după cum puteţi observa, prima parte conţine caractere numerice aranjate sub forma unei adrese IP. Acesta este un indiciu clar că ceva nu este în regulă.

Uitați-vă după semne clare de securitate. Site-urile corporațiilor, de regulă sunt atent securizate și folosesc pagini web criptate de fiecare dată când clienților li se cere să trimită informații cu caracter personal. În bara de navigare a browserului utilizat, verificați dacă adresa pe care doriți să o accesați începe cu 'https://'. Litera 's' reprezintă unul din semnele că această conexiune este securizată și vine din engleză de la termenul de 'security/secure'. Totodată, uitați-vă după o pictogramă cu un lacăt închis în partea de sus a ferestrei browserului. Dacă nu identificați aceste semne, atunci este posibil ca site-ul să fie unul fals.

Atenție la detaliile dubioase! Majoritatea email-urilor sau website-urilor venite din partea corporațiilor au un aspect profesional. Phishing-urile încearcă să te păcălească, copiind aspectul acestora. Pentru a detecta diferențele, căutați în text greșeli gramaticale, de ortografie sau chiar greșeli de design cu privire la aspectul site-ului. Dacă instinctul îți transmite că e ceva dubios, atunci cel mai probabil ai dreptate. După cum am mai afirmat, escrocheriile de tip phishing devin din ce în ce mai complexe pe zi ce trece, astfel că parcurgerea pașilor propuși nu este o modalitate 100% sigură de detectare a unui phishing, dar este un punct de început.

Folosiți telefonul pentru a vă asigura de legitimitatea conținutului. Sunați compania expeditoare a mesajului sau persoana în cauză, dar nu folosiți numărul de telefon afișat în corpul e-mail-ului. Contactați o persoană care ar putea cu adevărat să vă ajute să verificați legitimitatea mesajului primit.

Dacă simțiți că ați fi putut primi un e-mail de tip phishing, nu faceți click pe orice link-uri pentru a deschide atașamentele și nu transmiteți e-mailul mai departe.

Spear-phishing

Acest tip de phishing este o formă mai concentrată și vizează un anumit membru al unei instituții, care solicită accesul neautorizat la date confidențiale. Ca și în cazul mesajelor folosite în cazul campaniilor de tip phishing normale, mesajele de spear-phishing par că sunt expediate de la o sursă cunoscută și de încredere. În cazul spear-phishing-ului însă, sursa aparentă a e-mailului este cel mai probabil un individ din interiorul instituției recipientului sau dintr-o rețea de contacte de încredere, de regulă aflați într-o poziție de autoritate.

Încercările de spear-phishing nu sunt de regulă inițiate de către atacatori în mod aleatoriu, dar sunt mai degrabă conduse de "grupuri sofisticate ce caută câștiguri materiale, secrete comerciale sau informații militare".

Definiții și termeni

Administratorul sistemului informatic şi de comunicaţii – este o persoană investită cu responsabilitate privind crearea, modificarea, dezvoltarea şi administrarea sistemelor informatice.

Abuz de privilegii – reprezintă orice acţiune întreprinsă în mod voit de un utilizator, contrar prevederilor procedurilor şi legilor în vigoare.

Confidenţialitatea se referă la protecţia datelor împotriva accesului neautorizat. Fişierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia şi sub controlul Operatorului în condiţiile legilor în vigoare.

Informații confidențiale – acele informații generate, gestionate sau procesate în cadrul Operatorului, care nu pot fi furnizate către terți în formă brută (fără a fi prelucrate sau completate) sau care sunt marcate în consecință, în baza unor reglementări.

Disponibilitate – principiul securității informației, conform căruia utilizatorii au acces la informație atunci când au nevoie.

Echipament – În sensul prezentei proceduri, prin echipament se înțelege un calculator, hub, switch, antenă, modem, router, server, telefon, tabletă sau orice alt dispozitiv informatic.

Eveniment de securitate – orice fapt sau situație relevantă din punct de vedere al securității cibernetice, ce poate produce o schimbare a stării de normalitate în cadrul unui sistem informatic, poate indica o posibilă încălcare a politicii de securitate sau o deficiența a acesteia, sau inclusiv o deficiență în aplicarea masurilor de protectie stabilite prin politica de securitate ce poate fi pusă în evidență și documentată corespunzător;

Incident de securitate – prin incident se va înțelege orice eveniment, în legătură cu un sistem informatic, ale cărui consecințe pot afecta în mod negativ securitatea cibernetică a acestuia.

Integritatea - se referă la măsurile și procedurile utilizate pentru protecția datelor împotriva modificărilor sau distrugerii neautorizate.

Resurse informaționale – totalitatea datelor și informațiilor manipulate în cadrul instituției, procesate cu sau fără ajutorul sistemului informatic și de comunicații.

Rețea – reprezintă o structură interconectată de echipamente de comunicație (hub, router, switch etc.) și terminale (stații de lucru, telefoane, servere etc.) având ca scop utilizarea în comun a unor resurse software, dispozitive de intrare-ieșire, date și voce.

Serviciu – o componentă software care rulează în fundal (background) pe un sistem informatic (adesea server) și răspunde la cererile clienților (utilizatori, aplicații client etc.).

Sistemul informatic și de comunicații – reprezintă un sistem prin intermediul căruia se realizează colectarea, transmiterea, stocarea și prelucrarea informației în format electronic. Un sistem informatic poate avea diferite componente: calculatoare, dispozitive de rețea, medii de transmisie, aplicații informatice, tehnologii de securitate și chiar utilizatori.

Utilizator – este persoana care poate accesa datele cu caracter personal procesate de Operator.

Obligațiile operatorilor de date cu caracter personal

Persoana împuternicită de operator

În cazul în care prelucrarea urmează să fie realizată în numele unui operator, operatorul recurge doar la persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute în prezentul regulament și să asigure protecția drepturilor persoanei vizate.

Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal

În cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru au, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta autorității de supraveghere competente, fără întârzieri nejustificate și, dacă este posibil.

Evaluarea impactului asupra protecţiei datelor

Având în vedere natura, domeniul de aplicare, contextul şi scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operaţiunilor de prelucrare prevăzute asupra protecţiei datelor cu caracter personal

Procedura operaţională nr.1 - Intervenţii în cazul defecţiunilor hardware

În cazul în care a fost constatată o defecţiune sau o disfuncţionalitate a vreunui sistem de calcul şi/sau a unui periferic al acestuia (monitor, tastatură, mouse, imprimantă, etc) se va informa specialistul IT din cadrul Compartimentului de Informatică. Informarea se va face telefonic.

Poate exista şi cazul în care defecţiunea să fie constatată de către specialistul IT când acesta execută operaţiuni de întreţinere sau verificări de rutină, conform procedurii P0.7.

Specialistul IT va constata în ce constă defecţiunea şi dacă este posibil va proceda la remedierea acesteia.

În cazul în care nu este posibilă remediere de către specialistul IT, acesta va anunţa firma de service urmând procedura specifică P0.9.

Reprezentantul firmei de service va stabili dacă defecţiunea poate remediată pe loc, în cadrul instituţiei, sau este necesară deplasarea componentei hardware defecte la sediul firmei. În cel de-a doua situaţie se va urma procedura P0.10.

După remedierea defecţiunii se va respecta procedura P0.11, privind receptia componentelor hardware.

Procedura operaţională nr. 2 : Salvările de date, stocarea şi păstrarea acestora

Salvările de date în general se fac pe suport magnetic extern (dischete, CD, benzi magnetice, memory stick), sau pe suport magnetic intern (hard disk) în funcţie de instrucţiunile existente în manualele programelor informatice. De asemenea perioada de păstrare a acestor salvări se va face tot în funcţie de aceste instrucţiuni. Dacă nu există instrucţiuni în acest sens păstrarea se va face pe perioadă nedeterminată.

În cazul salvărilor efectuate pe harddiskurile serverelor prin opţiunile existente în cadrul programelor informatice, se vor efectua salvari complete de către o persoană desemnată în acest sens de către şeful departamentului respectiv.

În cazul schimbări unui sistem informatic cu unul şi în care au fost preluate datele existente în salvările efectuate anterior, vechile salvări vor fi distruse.

Persoanele care efectuează salvări vor avea un jurnal de evidenţă al acestor salvări în care se va specifica clar data şi ora când a fost efectuată salvarea.

Procedura operaţională nr. 3: Achiziţii echipamente hardware şi/sau software pe bază de referat de necesitate, altele decât prin licitaţii

Pentru achiziţionarea echipamente hardware şi/sau software pe bază de referat de necesitate, referatul de necesitate înainte de a fi trimis spre aprobare conducerii instituţiei va fi avizat de către specialistul IT pentru a stabili dacă necesitatea achiziţionării echipamentelor este justificată sau nu. În cazul unui aviz favorabil referatul de necesitate va fi aprobat ulterior de către conducătorii instituţiei (primar/viceprimar).

Referatele avizate şi aprobate vor fi retransmise Compartimetului de Informatică pentru a fi achiziţionate echipamentele.

Dacă cuantumul valorii echipamentelor depăşeşte plafonul legal privind achiziţia materialelor, acestea intrând pe lista de investiţii, referatul respectiv va fi trimis de către Compartimentul de Informatică departamentului care se ocupă cu achiziţiile publice, conform Procedurii P0.8.

Dacă suma este sub plafonul legal privind achiziţia materialelor acestea vor fi achiziţionate direct de la furnizor.

Recepţionarea acestora se va face respectând Procedura P0.11.

Procedura operaţională nr. 4 - Modificări sau defecţiuni ale aplicaţiilor software

În cazul în care sunt necesare modificări ale aplicaţiilor software (programe informatice) în urma modificărilor legislative sau datorită altor cauze, sau constatării funcţionării defectoase, sau a apariţiei unor erori de funcţionare se va anunţa în scris sau telefonic, sau prin email, sau prin fax, producătorul/autorul aplicaţiei sau firma care ofera asistenţă, după caz.

Departamentul care solicită modificările va furniza date cât mai amănunţite astfel încât modificările realizate să fie corecte.

Departamentul care solicită modificarea este răspunzător de datele furnizate.

Realizatorul modificărilor este răspunzător de modificările aduse în aplicaţia software. Acesta este obligat să informeze sau să instruiască utilizatorii aplicaţiilor despre modificările aduse.

În cazul defecţiunilor dacă se va constata că erorile de funcţionare se datorează unor defecţiuni ale echipamentului hardware se va anunţa specialistul IT şi se va urma procedura P0.1.

Procedura operaţională nr. 5- Exploatarea aplicatiilor informatice

Exploatare/utilizarea aplicaţiilor informatice se face doar de către personalul autorizat în conformitate cu instrucţiunile prevăzute în manualul aplicaţiei.

Utilizatorii noi care vor utiliza un program informatic vor fi instruiti de către persoanele abilitate în acest sens, de exemplu utilizatori cu vechime în exploatare acestuia sau de către un reprezentat al producătorului.

În cazul unui program informatic nou instruirea se face de către un reprezentant al producătorului programului informatic.

Dacă apar modificări din diverse motive se va urma procedura P0.4.

Procedura operaţională nr. 6 - Activităţi de mentenanţă privind componentele hardware

Activităţi de mentenanţă privind componentele hardware se vor executa cel puţin o data pe lună la staţiile de lucru de către firma de service, iar pentru servere se va executa cel puţin o data pe săptămână de către specialistul IT din cadrul Compartimentului de Informatică şi o dată pe lună de către firma de service.

Verificările de rutină efectuate se vor evidenţia într-un jurnal de activităţi.

În cazul constatării unor nereguli în funcţionarea echipamentelor în urma acestor verificări se va urma procedura P0.1, privind intervenţiile în cazul defecţiunilor hardware.

Procedura operaţională nr. 7 - Poşta electronică, mesajele primite din rubrica Contact de pe Site sau direct pe emailul de contact

Fiecare angajat al Operatorului are propria lui adresă de email, găzduită pe un server dedicat, securizat. Fiecare angajat este răspunzător păstrarea securităţii adresei de email primite de la Operator.

Un se vor transmite datele de accesare ale adresei de email personalizate primite de la Operator către terţi fie alţi angajaţi ai Operatorului fie persoane care un au legătură cu Operatorul.

Nu păstrați auto log-in pentru această adresă de e-mail și schimbații parola de cel putin 4 ori pe an, la intervale regulate de timp.

Fiecare angajat al Operatorului este raspunzătoar de modul în care gestionează datele cu caracter personal procesate prin intermediul adresei personalizate de email.

Toate solicitările venite pe adresa de email primită de la Operator trebuiesc salvate pe suport de hartie. Răspunsul se va transmite de pe adresa de email destinată transmiterii răspunsului conform procedurilor interne și apoi listat pe suport de hartie și atașat cererii primite.

Toate documentele primite pe adresa de email primită de la Operator trebuiesc salvate pe suport de hartie și păstrate în conformitate cu Legea Arhivării, legile specifice fiecărui tip de document în parte și conform procedurilor interne privind păstrarea fircărui tip de document în parte.

Nu este permisă folosirea adreselor de email personale pentru activităţile desfăsurate în cadrul Operatorului.

Nu este permisă accesarea adreselor de email personale de pe staţiile de lucru ale Operatorului.

Procedura operaţională nr. 8 - Rezolvarea mesajelor/cererilor

Modul în care sunt transmise datele către solicitanți ar trebui tratat punctual, de la caz la caz și dacă este necesar consultat responsabilul cu protecția datelor personale pentru stabilirea modului în care răspunsul va fi transmis și ce informații vor putea fi transmise.

Persoana care se ocupă de transmiterea răspunsului este răspunzătoare de modul în care a fost transmis acesta și de modul în care a respectat procedurile interne de lucru și normele de securitate interne.

De asemenea este răspunzătoare și de păstrarea unor copii neautorizate ale datelor cu caracter personal procesate. Păstrarea unor copii de siguranță a datelor cu caracter personal procesate se va face doar după consultarea responsabilului cu protecția datelor și a responsabilului IT și în conformitate cu instrucțiunile primite.

Procedura operațională nr. 9- Anunțarea defecțiunilor hardware/software firmei de service, garanții și/sau asistență

În cazul apariției unei defecțiuni care nu poate fi rezolvată de către specialistul IT din cadrul Compartimentului de Informatică, după cum este prevăzut și în procedura P0.1, se va contacta firma de service, garanții sau asistență hardware/software, după caz.

Anunțarea se va face telefonic, prin email, fax de către specialistul IT. Intervenția prestatorului de service se va face cu respectarea termenelor în cazul intervențiilor prevăzute în contractul de service.

Procedura operațională nr. 10 - Părăsirea temporara a calculatorului- Oprirea Calculatorului

În cazul în care utilizatorul părăsește temporar calculatorul este obligat să blocheze stația de lucru prin utilizarea opțiunii "Log Off", în cazul în care stația este utilizată de mai mulți utilizatori, sau prin utilizarea opțiunii "Lock Computer". De asemenea este obligatorie selectarea opțiunii "On resume, password protect" din cadrul sectiunii "Screen Saver".

Este interzisă cu desăvârșire părăsirea stației de lucru fără a închide aplicațiile în care se lucrează.

Procedura operațională nr. 11- Atribuirea/schimbarea/anularea utilizatorilor și a parolelor de access

Procedurile de schimbare a parolei asistate de administratorul de sistem trebuie să respecte următoarea procedură:

- Utilizatorul se va legitima, administratorul va verifica drepturile de acces a persoanei la contul utilizator;
- Se va genera o parolă care va fi comunicată utilizatorului
- Se va întocmi/actualiza fișa utilizatorului de către administrator.

În cazul în care un utilizator parasește definitiv sau temporar Operatorul, specialistul IT va recurge la ștergerea contului acestei persoane.

Președinte de ședință
Csizmár Antal-Tamás

ROMÂNIA JUDEȚUL SATU MARE CONSILIUL LOCAL COM. CAPLENI

Contrasemnează
Csizmar Erika
Secretar general

Anexa nr.3 la hotărârea nr.13/2021

Regulamentul de Securitate privind Sistemul Resurselor Informatice şi de Comunicaţii privind Protecția Datelor cu Caracter Personal din cadrul Primărie comunei Capleni, județul Satu Mare

Cuprins

Capitolul I

Introducere

În acord cu prevederile din prezentul document, Resursele Informatice şi de Comunicaţii sunt bunuri strategice ale Primărie comunei Capleni, județul Satu Mare care trebuiesc administrate ca resurse ale Primărie comunei Capleni, județul Satu Mare numită în continuare Operator.

Compromiterea securităţii sistemului RSRITC poate afecta capacitatea Operatorului de a oferi serviciile specifice, poate conduce la fraude sau distrugerea datelor, violarea clauzelor contractuale, divulgarea secretelor, afectarea credibilităţii Operatorului în faţa partenerilor săi.

RSRITC este stabilit astfel încât:

- ✓ Să fie în conformitate cu statutul, regulamentele, legile şi alte documente oficiale în vigoare privind administrarea resurselor informatice;
- ✓ Să stabilească practici prudente şi acceptabile privind utilizarea RSRITC ale Operatorului;
- ✓ Să instruiască utilizatorii care au dreptul de folosire a sistemului RSRITC privind responsabilităţile asociate unei astfel de utilizări;

Regulamentul de securitate a sistemului Operatorului se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii al Operatorului.

Următorii utilizatori sunt vizaţi în mod distinct de prevederile RSRITC:

- ✓ Angajaţii cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informaţional şi de comunicaţii;
- ✓ Colaboratorii Operator care au acces la sistemul RSRITC;

Scopul politicii de securitate

Politica de securitate a sistemului RSRITC are ca scop asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei.

Confidenţialitatea se referă la protecţia datelor împotriva accesului neautorizat. Fişierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia şi sub controlul Operatorului, sunt proprietatea instituţiei în condiţiile legilor în vigoare. Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la sistemul RSRITC.

Integritatea se referă la măsurile şi procedurile utilizate pentru protecţia datelor împotriva modificărilor sau distrugerii neautorizate.

Disponibilitatea se asigură prin funcţionarea continuă a tuturor componentelor sistemului RSRITC. Diverse aplicaţii au nevoie de nivele diferite de disponibilitate în funcţie de impactul sau daunele produse ca urmare a nefuncţionării corespunzătoare a sistemului RSRITC.

Politica de securitate are ca scop, de asemenea, stabilirea cadrului necesar pentru elaborarea regulamentelor şi procedurilor de securitate. Acestea sunt obligatorii pentru toţi utilizatorii sistemului RSRITC.

Definiţii folosite în politica de securitate şi regulamentul de utilizare

Resurse Informatice şi de Comunicaţii : toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unităţi de stocare, şi toate activităţile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepţioneze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (notebook-uri), calculatoare de buzunar, asistent digital personal (Personal Digital Assistant - PDA), pagere, sisteme de procesare distribuită, echipament de laborator şi medical conectat la reţea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicaţii, medii de reţea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentul, facilităţile, programele şi datele care sunt proiectate, construite, puse în funcţiune (operaţionale) şi menţinute pentru a creea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia.

Administratorul Resurselor Informatice şi de Comunicaţii (ARIC): Desemnarea ARSRITC are ca scop stabilirea în mod clar a responsabilităţii privind crearea, modificarea şi aprobarea regulamentelor privind activităţile de finanţare, administrare şi utilizare a RIC. Titlul este atribuit în mod automat şefului de departament IT, iar acolo unde nu există, se aplică ordonatorului de credit.

Ofiţer responsabil cu Securitatea IT (OSRIC): Răspunde direct doar în faţa ARSRITC privind administrarea funcţiilor de securitate al informaţiei în cadrul Operatorului. Este persoana de contact pentru orice problemă în legătură cu securitatea IT (specialistul IT din cadrul instituţiei).

Responsabilul cu protecţia datelor personale (RPD): Persoana responsabilă de monitorizarea şi implementarea controalelor de securitate, precum şi a procedurilor pentru sistemul RSRITC la nivelul Operatorului. Este persoana de contact al Operatorului pentru orice problemă în legătură cu protecţia datelor personale.

ANSPDCP: Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, în calitate de autoritate publică centrală autonomă cu competență generală la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.

Utilizator: O persoană, o aplicaţie automatizată sau proces utilizator autorizat de către Operator, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RSRITC.

Abuz de privilegii: Orice acţiune întreprinsă în mod voit de un utilizator, care vine în contradicţie cu regulamentele Operatorului şi/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acţiunii respective.

Furnizor: Persoană fizică/juridică care oferă bunuri şi/sau servicii Operatorului în baza unui contract comercial sau de colaborare.

Internet: Sistem global care interconectează calculatoare şi reţele de calculatoare. Acestea sunt deţinute de mai multe organizaţii, agenţii guvernamentale, societăţi, instituţii academice.

Intranet: Reţea privată destinată comunicaţiilor şi partajării informaţiilor, care, ca şi reţeaua Internet, foloseşte suita de protocoale TCP/IP, însă este accesibilă doar utilizatorilor autorizaţi din cadrul unei organizaţii (instituţii). În mod obişnuit, reţeaua Intranet a unei organizaţii este protejată printr-un sistem de protecţie (firewall).

Echipa de Răspuns la Incidentele de Securitate a RSRITC(ERIS): persoanele responsabile de acţiunile desfăşurate în scopul micşorării sau eliminării impactului negativ al unui incident de securitate. ERIS este formata din ARIC, OSRIC, RPD.

Virus: Un program care se auto-ataşează la un fişier executabil sau la o aplicaţie vulnerabilă şi care generează efecte de la cele deranjante până la cele distructive. Un virus se execută în momentul în care este accesat un fişier infectat. Un virus de macro infectează codul executabil încapsulat în pachetul de programe Microsoft Office (Word, Excel, PowerPoint) sau alte programe care permit utilizatorului să genereze macro-uri.

Vierme: Un program care se auto-copiază în oricare altă parte a unui sistem informatic. Aceste copii pot fi create pe acelaşi calculator sau pot fi trimise către alte calculatoare prin intermediul reţelei. Prima utilizare a termenului descria un program care s-a multiplicat într-o reţea de calculatoare, folosind resursele sau calculatoarele neutilizate din reţea pentru a distribui aceste copii. Unii dintre aceşti viermi reprezintă o ameninţare la adresa securităţii datorită faptului că folosesc reţeaua pentru a se împrăştia, împotriva voinţei proprietarilor de sisteme de calcul, cauzând astfel nefuncţionarea sau funcţionarea defectuoasă a reţelei. Un vierme este asemănător unui virus prin faptul că se auto-copiază, diferenţa constând în faptul că un vierme nu are nevoie să se ataşeze la anumite fişiere pentru a se multiplica.

Cal troian: de obicei un virus sau un vierme – care este ascuns sub forma unui program atractiv sau inofensiv, cum ar fi un joc, sau program de grafică (o felicitare în format electronic, un program tip screen-saver). Victimele pot primi un astfel de cal troian prin email sau pe o dischetă, adeseori de la o altă victimă necunoscută sau pot fi încurajate să descarce un fişier de pe o pagină Web sau un forum.

Incident de Securitate: În termeni informatici este definit ca un eveniment prin care se încearcă sau se realizează accesul la un sistem informatic, un atac asupra integrităţii şi/sau confidenţialităţii informaţiei de pe un sistem informatic automatizat. Aceasta include examinarea sau navigarea neautorizată, întreruperea sau anularea unui serviciu, date alterate sau distruse, prelucrarea (procesarea), stocarea sau extragerea informaţiilor, modificarea informaţiilor sistemului referitoare la caracteristicile componentelor hardware, firmware sau software cu sau fără ştiinţa sau intenţia utilizatorului.

Reţea locală (LAN): O reţea de comunicaţii de date ce este distribuită pe o zonă restrânsă (de regulă la nivelul unui grup de lucru). Reţeaua locală oferă comunicaţii între calculatoare şi periferice la o viteză de transfer mare şi cu puţine erori.

Server: Un program de calculator care oferă servicii altor programe aflate pe acelaşi calculator sau pe calculatoare diferite. Un calculator care rulează un program tip server este denumit în mod frecvent server, cu toate că pe acelaşi calculator mai pot rula şi alte programe de tip client sau server.

Gazdă (Host): Un sistem care oferă servicii pentru un anumit număr de utilizatori.

Copii de Siguranţă (backup): Copii ale fişierelor şi aplicaţiilor făcute pentru a evita pierderea datelor şi pentru a permite recuperarea în cazul unor evenimente care pot conduce la pierderi de date.

Firewall: Un mecanism de control al accesului care acţionează ca o barieră între două sau mai multe segmente ale unei reţele de calculatoare sau ale unei arhitecturi de tip client/server, folosit pentru a proteja reţelele interne sau segmente ale acestora împotriva utilizatorilor sau proceselor neautorizate.

Atac informaţional: O încercare de a trece peste măsurile şi controalele de securitate fizice sau informatice care protejează un sistem din cadrul sistemului de RSRITC. Atacatorul poate altera informaţiile, poate acorda sau refuza accesul la ele. Succesul unui eventual atac depinde de gradul de vulnerabilitate al sistemului în particular şi de eficacitatea contramăsurilor aplicate.

Protecţie informaţională: Acţiuni întreprinse în vederea afectării informaţiilor şi sistemelor informatice ostile, în timp ce protejează informaţiile şi sistemele informatice proprii.

Procedura - reprezintă modalitatea specifică de desfăşurare a unei activităţi sau a unui proces.

Confidenţialitate

Fişierele electronice create, trimise, primite sau stocate folosind sistemul RSRITC propriu, administrate sau în custodia şi sub controlul Operatorului nu au caracter personal şi pot fi accesate oricând de către angajaţii autorizaţi (specialistul IT/administrator reţea) fără înştiinţarea utilizatorului.

În scopul administrării RSRITC şi pentru asigurarea securităţii RSRITC personalul autorizat poate revizui sau utiliza orice informaţie stocată pe sau transportată prin sistemele RSRITC în conformitate cu legile în vigoare. În aceleaşi scopuri, este posibilă monitorizarea activităţii utilizatorilor.

Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul Operator, orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament (prin contactarea OSRSRITC- RPD).

Un mare număr de utilizatori, pot accesa diverse informaţii din sistemul de comunicaţii al Operatorului. În aceste condiţii este obligatorie păstrarea confidenţialităţii acestor informaţiilor transmise din exteriorul RSRITC şi a informaţiilor obţinute din interior.

Utilizatorii nu trebuie să încerce să acceseze informaţii sau programe de pe sistemele Operatorului pentru care nu au autorizaţie sau consimţământ explicit.

Nici un utilizator al sistemului RSRITC ale Operatorului nu poate divulga informaţiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilităţi a sistemului RSRITC. Această regulă se extinde şi după ce utilizatorul a încheiat relaţiile cu Operatorul, conform angajamentelor personale sau contractelor de munca semnate, existente in cadrul Serviciului Resurse Umane.

Confidenţialitatea informaţiilor transmise prin intermediul resurselor de comunicaţii ale terţilor nu poate fi asigurată. Pentru aceste situaţii, confidenţialitatea şi integritatea informaţiilor se poate asigura folosind tehnici de criptare. Utilizatorii sunt obligaţi să se asigure că toate informaţiile confidenţiale ale Operatorului se transmit în aşa fel încât să se asigure confidenţialitatea şi integritatea acestora.

CAPITOLUL II

Introducere

Regulamentele de Utilizare a Resurselor Informatice şi de Comunicaţii sunt elaborate pentru a stabili un cadru corect, legal şi eficient de utilizare a tehnologiei informaţiei şi comunicaţiilor pentru Operator. Acestea au ca scop principal protejarea utilizatorilor, colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea acestea au

ca scop protejarea imaginii instituţiei şi a investiţiilor acesteia pentru dezvoltarea sistemul informatic şi de comunicaţii.

În acord cu legislaţia în vigoare în România, Resursele Informatice şi de Comunicaţii sunt valori ale Operatorului care trebuie exploatate şi administrate ca resurse private în proprietatea Operatorului.

Scopul acestor regulamente este acela de a asigura:

- ✓ Stabilirea unor reguli corecte, echitabile şi eficiente pentru folosirea resurselor informatice şi de comunicaţii în vederea sprijinirii procesului educaţional şi a cercetării ştiinţifice;
- ✓ Protejarea imaginii Operatorului;
- ✓ Protejarea investiţiilor Operatorului pentru dezvoltarea sistemului informatic şi de comunicaţii propriu;
- ✓ Protejarea proprietăţii intelectuale şi a tuturor informaţiilor stocate şi transportate folosind Resursele Informatice şi de Comunicaţii ale utilizatorilor autorizaţi: membrii conducerii, personalul propriu, colaboratori etc.
- ✓ Educarea utilizatorilor resurselor informatice şi de comunicaţii în ceea ce priveşte responsabilităţile asociate cu utilizarea acestora;
- ✓ Compatibilitate cu regulamentele, statutul şi atribuţiile stabilite pentru administrarea resurselor informatice şi de comunicaţii.

Regulamentele de utilizare a resurselor informatice şi de comunicaţii ale Operatorului se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la acesta.

Regulamentele şi procedurile de lucru sunt elaborate de Compartimentul Informatică din cadrul instituţiei şi supuse spre aprobare conducerii.

Prevederile Politicii de Securitate şi Procedurile de Lucru aprobate vor fi aplicate tuturor entităţilor şi utilizatorilor după cum urmează:

- ✓ Angajaţii cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informaţional şi de comunicaţii;
- ✓ Colaboratorii Operatorului care au acces la sistemul RSRITC;

Modificarea regulamentului şi/sau a procedurilor generale de lucru se va face ori de câte ori este nevoie, iar aprobarea modificărilor se va face de către conducere la propunerea OSRIC.

Regulament de utilizare a RSRITC

Utilizarea sistemului RSRITC se face numai în interes de serviciu.

Utilizatorii trebuie să anunţe OSRIC- RPD în cazul în care se observă orice problemă/breşă în sistemul de securitate a RSRITC al Operatorului cât şi orice posibilă întrebuinţare greşită sau încălcare a regulamentelor în vigoare.

Utilizatorii, prin acţiunile lor, nu trebuie să încerce să compromită protecţia sistemelor informatice şi de comunicaţii şi nu trebuie să desfăşoare, deliberat sau accidental, acţiuni care pot afecta confidenţialitatea, integritatea şi disponibilitatea informaţiilor de orice tip în cadrul sistemului Operatorului.

Utilizatorii nu trebuie să încerce să obţină acces la date sau programe din RSRITC pentru care nu au autorizaţie sau consimţământ explicit.

Utilizatorii nu trebuie să divulge nimănui numerele de acces Dialup sau Dialback prin modem.

Utilizatorii nu trebuie să divulge sau să înstrăineze nume de cont-uri, parole, Numere de Identificare Personală (PIN-uri), dispozitive pentru autentificare (ex.: Smartcard) sau orice dispozitive şi/sau informaţii similare utilizate în scopuri de autorizare şi identificare.

Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright).

Utilizatorii nu trebuie să utilizeze programe de tip shareware sau freeware, fără aprobarea OSRIC, cu excepţia cazului în care acestea se găsesc pe lista programelor standard folosite de către Operator. Această listă va fi întocmită de către OSRSRITC împreună cu RPD în funcţie de necesităţile departamentelor.

Utilizatorii nu trebuie să se angajeze într-o activitate care ar putea hărţui sau ameninţa alte persoane.

Utilizatorii nu trebuie să degradeze performanţele RSRITC.

Utilizatorii nu trebuie să împiedice accesul unui utilizator autorizat la RSRITC.

Utilizatorii nu trebuie să obţină alte resurse în afara celor alocate.

Utilizatorii nu trebuie să ignore măsurile de securitate impuse prin regulamente.

Utilizatorii nu trebuie să exploateze defectuos componentele RSRITC.

Utilizatorii nu trebuie să utilizeze dischete, cd-uri, sau orice alt suport magnetic de stocare a informaţiei din exteriorul instituţiei fără acordul explicit al OSIRC - RPD;

Utilizatorii nu trebuie să descarce, instaleze şi să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilităţi ale securităţii RSRITC, care au capacitatea de a decripta parole sau informații stocate în mod criptat, care pot captura traficul în rețeaua internă sau care pot scana structura rețele interne sau orice alt program nepermis în mod explicit prin regulamente.

RSRITC ale Operatorului nu trebuiesc folosite pentru beneficiul personal.

Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care Operatorul le poate considera ofensive, indecente sau obscene.

Accesul la reţeaua Internet prin intermediul RSRITC se supune aceloraşi regulamente care se aplică utilizării din interiorul instituţiei şi Regulamentului pentru Utilizare Internet şi Intranet (cap.II subcap.14).

Angajaţii nu trebuie să permită membrilor familiei sau altor persoane străine neautorizate, care nu au aprobare explicită din partea ARIC, OSRIC, RPD sau a conducerii instituţiei accesul la RSRITC ale Operatorului. Utilizatorii care au acces la sistemul RSRITC al

Operatorului au obligaţia de a purta acte şi/sau legitimaţii/ecusoane care să ateste calitatea de utilizator autorizat în spaţiile Operatorului. Utilizatorii nu trebuie să se angajeze în acţiuni împotriva scopurilor Operatorului folosind RSRITC.

În cazul demisiei/plecării definitive din companie a unui utilizator acest lucru va fi comunicat OSRIC- RPD de către Serviciul Resurse Umane din Cadrul instituţiei. OSRSRITC va recurge la stergerea conturilor şi parolelor utilizatorului respectiv, iar accesul utilizatorului la RSRITC va fi interzis.

Este interzisă utilizarea RSRITC de către persoane neautorizate.

Utilizarea ocazională a RSRITC în scopuri personale

În aceste situaţii se aplică următoarele restricţii:

✓ Utilizarea personală ocazională a serviciilor de poştă electronică, acces internet, telefoane, fax-uri, imprimante, copiatoare, etc. este restricţionată la utilizatorii autorizaţi şi nu poate fi extinsă la membrii familiilor sau alte persoane.

✓ Utilizarea ocazională a RSRITC nu trebuie să aibă drept rezultate costuri directe pentru Operator. Utilizarea ocazională a RSRITC nu trebuie să afecteze activitatea normală a angajaţilor.

✓ Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni legale împotriva Operatorului sau prejudicierea, indiferent de formă, a intereselor acestuia.

✓ Stocarea mesajelor de email, a mesajelor de voce, a documentelor şi fişierelor personale din cadrul RSRITC trebuie să fie nominală.

✓ Toate mesajele, fişierele şi documentele – incluzând mesajele personale, fişierele şi documentele – localizate în cadrul RSRITC sunt proprietatea Companiei şi pot fi subiectul unor cereri de verificare/inspectare/accesare de către ARIC, OSRIC, RPD conform regulamentelor.

Accesul Administrativ

✓ Utilizatorii trebuie să cunoască şi să accepte toate regulamentele privind securitatea RSRITC înainte de a li se permite accesul la un cont.

✓ Utilizatorii care au conturi de acces administrativ trebuie sa aibă instrucţiuni de administrare, documentare, instruire şi autorizare a conturilor. Aceste instrucţiuni se vor elabora de către fiecare Departament şi vor fi incluse în fişa postului.

✓ Utilizatorii cu drepturi administrative sau speciale de acces nu trebuie să folosească în mod abuziv aceste drepturi şi trebuie să facă investigaţii numai sub îndrumarea OSRSRITC sau RPD.

✓ Cei care utilizează conturi de acces cu drepturi administrative sau speciale trebuie să folosească tipul de privilegiu cel mai potrivit activităţii pe care o desfăşoară.

✓ Accesul administrativ trebuie să se conformeze Regulamentului privind Parolelor.

✓ Parola pentru un cont cu acces privilegiat nu va fi utilizată de mai multe persoane decât cu acordul scris al OSRIC-RPD şi trebuie să fie schimbată atunci când

o persoana care utilizează acest cont îşi schimbă locul de muncă din cadrul Departamentului sau a Instituţiei, sau în cazul unei modificări a listei de personal ale terţilor (furnizor desemnat) în contractele cu Operatorul.

✓ Trebuie să existe o procedură prin care o altă persoană, în afară de administrator, să poată avea acces la contul administratorului în caz de forţa majoră. Această procedură va fi elaborată de către OSRSRITC şi comunicată ARSRITC- RPD.

✓ Unele conturi sunt necesare pentru audit (verificare, control) intern sau extern, pentru dezvoltare sau instalare de software sau alte operaţiuni definite. Acestea trebuie să îndeplinească următoarele condiţii:

- trebuie să fie autorizate;
- trebuie create cu dată de expirare specifică;
- contul va fi şters atunci când nu mai este necesar.

Accesul Fizic

✓ Accesul fizic la toate încăperile în care sunt instalate RSRITC trebuie să fie documentat şi monitorizat.

✓ Toate încăperile în care sunt instalate RSRITC trebuie să fie protejate fizic, în funcţie de importanţa acestora şi tipul datelor vehiculate sau stocate.

✓ Pentru fiecare încăpere în care sunt instalate echipamente ale sistemului RSRITC se aprobă accesul doar pentru personalul care răspunde de buna funcţionare a echipamentelor din încăperea respectivă şi, dacă este cazul, părţilor contractante, ale căror obligaţii contractuale implică acces fizic.

✓ Personalul care are drepturi de acces trebuie să deţină legitimaţie de serviciu şi acte de identitate care să-i ateste calitatea.

✓ Nu este permis transferul dreptului de acces indiferent de motiv.

✓ Accesul publicului, vizitatorilor, sau a persoanelor străine în cadrul instituţiei se va face doar pe baza actului de identitate. Vizitatorii/persoanele străine trebuie să fie însoţiţi în zonele cu acces restricţionat.

✓ Pentru fiecare spaţiu în care sunt instalate RSRITC se va păstra o evidenţă a accesului pentru verificări de rutină în situaţii critice.

Conectarea la Sistemul Resurselor Informatice şi de Comunicaţii

✓ Utilizatorilor le este permis să utilizeze pentru conectare la reţea numai parametrii specificaţi de către administratorul de reţea .

✓ Pentru fiecare sistem conectat trebuie să existe o persoană care să răspundă de acesta, numele şi datele de identificare ale acesteia se vor comunica către OSRIC.

✓ Conectarea sistemelor de calcul care nu sunt proprietatea Operatorului se face numai cu aprobarea în scris din partea conducerii instituţiei pentru reţeaua de producţie sau oricând consideră de cuviinţă utilizatorul în cazul reţelei pentru vizitatori.

✓ Accesul de la distanţă la reţeaua Operatorului se va realiza numai prin echipamente aprobate, sau prin intermediul unui Furnizor de Servicii Internet (Internet

Service Provider (ISP)) agreat de către Operator şi folosind protocoale aprobate de către OSRIC.

✓ Utilizatorii RSRITC din interiorul rețelei Operatorului nu se pot conecta la altă reţea.

✓ Utilizatorii nu trebuie să extindă sau să retransmită serviciile de reţea în nici un fel (pe nici o cale). Nu este permisă instalarea de conexiuni de reţea neautorizate indiferent de motiv. Autorizarea tuturor conexiunilor se face la propunerea Departamentelor de către Compartimentul de Informatică.

✓ Utilizatorii nu trebuie să instaleze echipamente hardware sau programe care furnizează servicii de reţea fără aprobarea Compartimentului de Informatică.

✓ Sistemele computerizate din afara Instituţiei care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei interne a Operatorului.

✓ Utilizatorii nu au dreptul să descarce din Internet, să instaleze sau să ruleze programe de securitate sau de altă natură care pot dezvălui slăbiciuni în securitatea unui sistem.

✓ Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de reţea, cabluri, prize de conexiuni.

✓ Serviciul de nume şi administrarea adreselor IP sunt deservite exclusiv de către Compartimentul de Informatică.

✓ Serviciile de interconectare a reţelei Operatorului cu alte reţele sunt realizate exclusiv de către Compartimentul de Informatică.

✓ Nu este permisă instalarea şi/sau modificarea echipamentelor utilizate pentru conectare la reţea (inclusiv plăci de reţea) fără aprobarea Compartimentul de Informatică. Tipul şi modelul plăcilor de reţea şi tuturor echipamentelor care se pot conecta în reţea trebuie să fie aprobate de către Compartimentul de Informatică.

Configurarea Parametrilor de Acces la Reţea

✓ Infrastructura de comunicaţii, reţeaua de comunicaţii digitale, a Operatorului este administrată de către Compartimentul de Informatică care este responsabil cu întreţinerea şi dezvoltarea acesteia.

✓ Pentru a furniza o infrastructură de comunicaţii unitară cu posibilităţi de modernizare toate componentele acesteia sunt instalate de către Compartimentul de Informatică sau de către un furnizor avizat explicit de către Compartimentul de Informatică

✓ Toate echipamentele, fără excepţie, conectate la reţeaua de comunicaţii trebuie configurate conform specificaţiilor Compartimentul de Informatică

✓ Orice dispozitiv hardware, inclusiv plăcile de reţea şi modemuri, care se va conecta la reţeaua Operatorului, trebuie să fie însoţit de o aprobare de tip (producător, model etc.) din partea Compartimentul de Informatică.

✓ Modificarea configuraţiei oricărui dispozitiv activ conectat la reţeaua de comunicaţii se face numai de către Compartimentul de Informatică.

- ✓ Toate conectările în reţeaua de comunicaţii a Operator sunt responsabilitatea Compartimentul de Informatică, conectarea se va face numai în baza unei cereri standard aprobată de către conducerea Companiei.
- ✓ Toate conectările dintre reţeaua de comunicaţii a Operatorului şi alte reţele de comunicaţii, publice sau private, sunt responsabilitatea exclusivă a Compartimentul de Informatică
- ✓ Echipamentele de protecţie a reţelei de comunicaţie ale Operator (firewall) se vor instala de către Compartimentul de Informatică.
- ✓ Utilizatorii nu au dreptul să extindă sau să retransmită în nici un fel serviciile reţelei (este interzisă instalarea unui telefon, fax, modem, router, switch, hub sau punct de acces la reţeaua Instituţiei) fără aprobare din partea Compartimentul de Informatică. Utilizatorilor li se interzice instalarea de dispozitive hardware de reţea sau programe care furnizează servicii de reţea fără aprobarea Compartimentul de Informatică.
- ✓ Utilizatorilor nu le este permis accesul la dispozitivele hardware ale reţelei.

Tratarea Incidentelor de Securitate şi de nerespectare a Politicii şi Regulamentului de Securitate

Membrii Echipei de Răspuns la Incidentele de Securitate (Membrii ERIS) ai Operatorului, au funcţii şi responsabilităţi pre-definite care pot fi prioritare îndatoririlor obişnuite.

Ori de câte ori un incident de securitate este suspectat sau confirmat, precum un virus, vierme, descoperirea unor activităţi suspecte, informaţii modificate etc., trebuie urmate procedurile standard specifice pentru micşorarea riscurilor.

OSRSRITC este responsabil cu înştiinţarea şi coordonarea echipei ERIS pentru tratarea incidentului.

OSRSRITC este responsabil cu strângerea dovezilor fizice şi electronice ce vor face parte din documentaţia pentru tratarea incidentului.

Folosind resurse tehnice speciale se va monitoriza nivelul daunelor şi gradul de eliminare sau atenuare a vulnerabilităţilor acolo unde este cazul.

OSRIC, în colaborare cu RPD va stabili conţinutul comunicatelor pentru utilizatori privind incidentele şi va determina nivelul şi modul de distribuire a acestei informaţii.

OSRSRITC şi RPD trebuie să comunice proprietarului sau producătorului resursei afectate de un incident informaţiile utile pentru eliminarea sau diminuarea vulnerabilităţilor care au cauzat incidentul.

OSRSRITC este responsabil cu documentarea anchetei privind incidentul cu asistenţă din partea ERIS.

OSRSRITC este responsabil de coordonarea activităţilor de comunicare cu terţi pentru rezolvarea incidentului.

În cazul în care incidentul nu implică acţiuni contrare legilor în vigoare RPD va recomanda ARSRITC sancţiuni disciplinare.

În cazul în care incidentul implică aplicarea legilor civile sau penale RPD va recomanda ARSRITC sesizarea organelor în drept ale statului şi va acţiona ca ofiţer de legătură cu acestea.

Monitorizarea Resurselor Informatice şi de Comunicaţii

Monitorizarea RSRITC se va face astfel încât să fie posibilă detectarea în timp util a atacurilor informatice şi a situaţiilor de încălcare a regulamentelor de securitate. Echipamentele utilizate pentru monitorizare (dedicate sau nu) vor urmări şi înregistra:

- ✓ Tipul traficului (ex. structura pe protocoale şi servicii) extern şi conţinutul acestuia în cazurile în care acest lucru se impune sau este ordonat;
- ✓ Tipul traficului în reţea, a protocoalelor şi a echipamentelor conectate la RSRITC, conţinutul acestuia în cazurile în care acest lucru se impune sau este ordonat;
- ✓ Parametrii de securitate pentru sistemele individuale (la nivelul sistemelor de operare).

Fişierele jurnal vor fi examinate regulat în vederea detectării eventualelor atacuri informatice şi abateri de la regulamentele de securitate ale Operatorului.

În această categorie intră următoarele (fără a se limita doar la acestea):

- ✓ Jurnale ale sistemelor de detectarea automată a intruşilor;
- ✓ Jurnale Firewall;
- ✓ Jurnale ale activităţii conturilor utilizator;
- ✓ Jurnale ale scanărilor reţea;
- ✓ Jurnale ale aplicaţiilor;
- ✓ Jurnale ale erorilor din sisteme şi servere.

Securitatea Serverelor

Un server nu trebuie conectat la reţeaua Operatorului până când nu se află într-o stare sigură acreditată de către OSRIC.

Procedura de securizare a serverelor trebuie să includă obligatoriu următoarele:

- ✓ Instalarea sistemului de operare dintr-o sursă aprobată;
- ✓ Aplicarea patch-urilor furnizate de producător;
- ✓ Înlăturarea programelor, a serviciilor sistem şi a driver-lor care nu sunt necesare;
- ✓ Setarea/activarea parametrilor de securitate, a protecţiilor pentru fişiere şi activarea jurnalelor de monitorizare;
- ✓ Dezactivarea sau schimbarea parolelor conturilor predefinite;
- ✓ Securizarea accesului fizic la aceste echipamente.

Compartimentul de Informatică va monitoriza obligatoriu pentru serverele principale (enterprise) procesul de instalare şi aplicare regulată a patch-urilor de securitate şi, prin sondaj, pentru serverele departamentale sau a grupurilor de lucru.

Crearea şi Utilizarea Copiilor de Siguranţă (Backup)

Frecvenţa, dimensiunea şi conţinutul copiilor de siguranţă trebuie să fie în concordanţă cu importanţa informaţiei şi cu riscul acceptat de proprietarul datelor.

Procedura de creare a copiilor de siguranţă şi de recuperare pentru fiecare sistem din cadrul RSRITC trebuie să fie documentată şi periodic revizuită.

Verificarea copiilor de siguranţă se va face după o procedură documentată şi revizuită periodic.

Copiile de siguranţă trebuie să fie periodic testate pentru a asigura faptul că informaţiile stocate sunt recuperabile.

Accesul la mediile de backup ale Operatorului se va face numai de personalul abilitat în acest sens.

Accesul trebuie interzis pentru persoanele autorizate care îşi schimbă locul de muncă.

Detectarea Tentativelor de Acces Neautorizat

Procesele de înregistrare şi verificare a activităţii sistemelor de operare, conturilor utilizator şi programelor trebuie să fie funcţionale pe toate sistemele active (host, server, echipamente de reţea).

Trebuie activate funcţiile de anunţare a persoanelor responsabile oferite de firewall-uri şi sistemele de control al accesului la reţea.

Trebuie activate funcţiile de înregistrare a evenimentelor pe dispozitivele firewall şi pe toate sistemele de control al accesului.

Înregistrările de verificare ale dispozitivelor de control al accesului trebuie monitorizate/revizuite (examinate) zilnic de către administratorul de sistem.

Verificările privind integritatea fiecărui sistem trebuie să se facă periodic. Această activitate este obligatorie şi pentru dispozitivele de tip firewall sau dispozitive de control al accesului.

Înregistrările de verificare pentru serverele şi host-urile din reţeaua internă trebuie revizuite cel puţin săptămânal.

Se vor verifica periodic (săptămânal) programele utilitare pentru detectarea tentativelor de acces neautorizat.

Toate rapoartele privind incidentele trebuie revizuite în vederea detectării de indicii ce ar putea implica o activitate de acces neautorizat.

Toate indiciile suspecte sau confirmate de accesări sau încercări de accesare neautorizate trebuie raportate imediat către OSRIC-RPD.

Utilizatorii sunt obligaţi să raporteze orice anomalii în performanţa sistemelor utilizate cât şi orice semne ale unor posibile infracţiuni la OSRSRITC- RPD.

Utilizarea Calculatoarelor Portabile

OSRSRITC–RPD trebuie să aprobe, în scris, conectarea dispozitivelor portabile la RSRITC ale Instituţiei.

Calculatoarele portabile trebuie să fie protejate prin parole.

Se va evita stocarea datelor care privesc Operatorul pe dispozitivele portabile. În cazul în care nu există o altă alternativă de stocare locală, toate datele care privesc Operatorul trebuiesc criptate.

Conectarea sistemelor de calcul care nu sunt proprietatea Operatorului se face numai cu aprobarea în scris a Compartimentul de Informatică la recomandarea Departamentelor.

Dispozitivele portabile de calcul neutilizate trebuie securizate fizic. Aceasta presupune încuierea lor într-un birou, într-un dulap.

Modificări şi Modernizări ale Sistemului Resurselor Informatice şi de Comunicaţii

Orice modificare asupra unei componente a RSRITC din cadrul Operatorului, cum ar fi: sisteme de operare, componente hardware, echipamente şi componente de reţea, aplicaţii, este supusă prezentului regulament şi trebuie să urmeze procedurile în vigoare.

Compartimentul de Informatică trebuie să fie anunţat de toate modificările care afectează mediul de funcţionare a sistemelor componente ale RSRITC.

Toate propunerile de modernizare şi extindere a elementelor de infrastructură a sistemului RSRITC vor fi documentate şi aprobate de către ARIC. Nu este permisă modificarea de către utilizatori a elementelor de infrastructură a RSRITC.

Modificările şi modernizările sistemelor de calcul vor fi documentate de către utilizator şi aprobate de către conducerea instituţiei.

Utilizare Internet şi Intranet

Programele pentru acces la reţeaua Internet sunt destinate utilizatorilor autorizaţi pentru a fi folosite în scopuri exclusiv de servici, cu excepţia situaţiei prevăzute în regulamentul Utilizarea ocazională a RSRITC în scopuri personale.

Toate programele utilizate pentru acces la reţeaua Internet trebuie să facă parte din pachetul de programe aprobat de către Compartimentul de Informatică. Aceste programe trebuie să includă toate patch-urile de securitate puse la dispoziţie de către producător.

Toate fişierele care provin din reţeaua Internet trebuie să fie scanate cu un program antivirus care să fie actualizat cel puţin o dată la 24 ore.

Toate programele pentru acces Internet/Intranet trebuie să permită folosirea sistemelor proxy şi/sau firewall.

Toate informaţiile accesate în reţeaua Internet trebuie să se conformeze Regulamentului de Utilizare Acceptabilă a RSRITC.

Orice activitate a utilizatorilor folosind RSRITC poate fi înregistrată şi ulterior examinată.

Nu se vor publica pe sit-urile web ale Operatorului materiale cu caracter ofensiv sau de hărţuire.

Nu se vor publica pe sit-urile web ale Operatorlui date ale Operatorului fără asigurarea că materialele sunt disponibile numai persoanelor sau grupurilor autorizate.

Nu este permisă utilizarea RSRITC al Operatorului în scop personal sau pentru solicitări personale ce nu au legătură cu Operatorul. Orice material confidenţial al Operatorului transmis prin reţeaua Internet trebuie criptat.

Fişierele electronice se supun aceloraşi reguli de păstrare ce se aplică şi altor documente şi trebuie păstrate în conformitate cu regulile stabilite prin prezentele regulamente şi regulamentele proprii fiecărui Departament.

Este interzisă accesarea site-urilor cu caracter pornografic.

Este interzisă folosirea programelor peer-to-peer.

Este interzisă descărcarea/instalarea programelor din reţeaua Internet.

Administrarea Conturilor

Prin acord individual, fişa postului şi/sau alte documente toţi utilizatorii acceptă prevederile regulamentelor privind securitatea sistemului RSRITC.

Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces.

Toate parolele pentru conturi trebuie să fie create şi folosite în conformitate cu Regulamentul privind Parolele de Acces.

Conturile utilizator ale persoanelor plecate din Instituţie pe timp îndelungat (mai mult de 90 de zile) vor fi dezactivate (conturile nu vor mai putea fi accesate).

Toate conturile utilizator care nu au fost accesate timp de 30 de zile vor fi dezactivate. După încă 30 zile conturile vor fi şterse dacă nu s-a solicitat accesul la acestea.

Administratorii de sisteme sau alt personal autorizat sunt responsabili de ştergerea conturilor persoanelor (utilizatorilor) care nu mai lucrează pentru Operator, sau care nu mai au relaţii cu Operatorul.

Parole de Acces

Toate parolele trebuie să îndeplinească următoarele condiţii:

- ✓ Să fie schimbate de utilizator în mod regulat, cel puţin o dată la 90 de zile;
- ✓ Să aibă o lungime minimă de 6 caractere;
- ✓ Să fie parole complexe;
- ✓ Reutilizarea parolelor este interzisă;
- ✓ Parolele stocate trebuie criptate;

Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaţilor care răspund de securitatea sistemelor informatice.

Dacă se suspectează că o parolă a putut fi divulgată aceasta trebuie schimbată imediat.

Administratorii de sistem nu trebuie să permită schimbarea parolelor utilizatorilor folosind contul administrativ.

Utilizatorii nu pot folosi programe de stocare a parolelor. Se pot face excepţii pentru anumite aplicaţii (precum backup automat) cu aprobarea OSRIC-RPD.

Dispozitivele de calcul nu trebuiesc lăsate nesupravegheate fără a activa un sistem de blocare a accesului la acestea; deblocarea trebuie să se facă folosind parolă.

Sistemul de Mesagerie Electronică

Următoarele activităţi sunt interzise de regulament:

- ✓ Trimiterea de mesaje cu caracter de intimidare sau hărţuire;
- ✓ Folosirea sistemului de mesagerie electronică în scopuri personale;
- ✓ Folosirea sistemului de mesagerie electronică în scopuri politice sau pentru campanii politice;
- ✓ Încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate;
- ✓ Folosirea altei identităţi decât cea reală atunci când se trimite email, exceptând cazurile când persoana este autorizată în scop de suport administrativ.
- ✓ Folosirea programelor de poştă electronică neautorizate.
- ✓ Trimiterea sau retrimiterea email-urilor în lanţ;
- ✓ Trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc interesele companiei;
- ✓ Trimiterea mesajelor de dimensiuni foarte mari;
- ✓ Trimiterea sau retrimiterea mesajelor ce pot conţine viruşi.

Toate informaţiile şi datele confidenţiale ale Operatorului, transmise către alte reţele externe, trebuie să fie criptate.

Toate activităţile utilizatorilor ce implică accesul şi/sau folosirea RSRITC ale Operatorului pot fi oricând înregistrate şi analizate.

Utilizatorii serviciilor de mesagerie electronică nu trebuie să dea impresia că reprezintă, că îşi spun opinia sau dau declaraţii în numele Operatorului, cu excepţia situaţiilor în care aceştia sunt autorizaţi în mod corespunzător (implicit sau explicit) să facă acest lucru. Atunci când este cazul, se va include o declaraţie explicită prin care utilizatorul specifică faptul că nu reprezintă Operatorul.

Utilizatorii nu trebuie să trimită, retrimită sau să primească informaţii confidenţiale sau senzitive ce privesc Operatorul, folosind conturi utilizator care nu sunt proprietatea Operatorului. Exemple de astfel de conturi, sunt (dar nu sunt limitate numai la acestea: Hotmail, Yahoo mail, AOL mail), precum şi adrese de email puse la dispoziţie de alţi Furnizorii de Servicii Internet.

Utilizatorii nu trebuie să trimită, retrimită, primească sau să stocheze informaţii confidenţiale sau nesigure, ce privesc Operatorul, folosind dispozitive de comunicaţii mobile care nu sunt autorizate de Operator. Exemple de astfel de dispozitive (dar nu sunt limitate numai la acestea) sunt: asistenţi digitali personali, pagere ce permit trimiterea/primirea de informaţii şi telefoanele mobile.

Detectarea viruşilor

Toate staţiile de lucru de sine stătătoare sau conectate la reţeaua de comunicaţii a Operatorului, trebuie să utilizeze programe antivirus aprobate de către OSRIC.

Programele antivirus nu trebuie dezactivate.

Configuraţia programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului.

Frecvenţa actualizărilor automate a programului antivirus trebuie asigurată de către utilizator.

Orice server de fişiere conectat la reţeaua Instituţiei trebuie să utilizeze un program antivirus aprobat în scopul detectării şi curăţirii viruşilor care pot infecta fişierele puse la dispoziţie.

Orice server sau gateway pentru e-mail trebuie să folosească un program antivirus pentru e-mail aprobat şi trebuie să respecte regulile de instalare şi utilizare a acestui program.

Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie raportat imediat OSRIC-RPD –ARIC- ANSPDCP.

Licenţe de utilizare

Toate aplicațiile folosite în interesul Operatorului atât sistemele de operare cât și aplicațiile specifice vor fi folosite cu licență.

Operatorul trebuie să se pună de acord în mod adecvat cu furnizorii implicaţi pentru obţinerea de copii adiţionale ale licenţelor dacă şi când acestea sunt necesare în activitatea instituţiei.

Copiile suplimentare ale materialelor protejate prin drepturi de autor nu vor fi stocate pe sistemele sau resursele reţelei Operatorului în situaţia în care nu există aprobări specifice. Administratorii de sistem vor şterge produsele şi toate materialele protejate prin drepturi de autor în situaţia menţionată, cu excepţia cazului în care utilizatorii implicaţi fac dovada autorizaţiei de folosire sau stocare de la producătorii de drept.

Programele sau alte bunuri informatice aflate sub incidenţa drepturilor de autor aflate în posesia Operatorului nu vor fi copiate, cu excepţia cazului în care această copiere este în concordanţă cu prevederile licenţei.

Relaţii cu terţi

Orice activitate desfăşurată de furnizor care implică acces la RSRITC trebuie să se conformeze cu regulamentele în vigoare ale Operatorului.

În toate convenţiile şi contractele încheiate cu Furnizori trebuie specificate următoarele:

Informaţiile din cadrul Operatorului, la care Furnizorul are drept de acces;

Modul în care informaţiile la care Furnizorul are drept de acces urmează a fi protejate de către acesta precum şi măsuri ce vor fi luate în cazul nerespectării clauzelor;

Metodele de predare, distrugere sau de transfer al drepturilor informaţiilor Instituţiei aflate în posesia Furnizorului, la încheierea contractului.

Furnizorul trebuie să folosească sistemul RSRITC din cadrul Operatorului numai în scopul stipulat în contract.

Orice altă informaţie din sistemul RSRITC al Operatorului obţinută de Furnizor pe durata contractului nu poate fi folosită în interes propriu de către Furnizor sau divulgată altora.

Toate echipamentele de întreţinere ale Furnizorului, aflate în reţeaua internă a Operatorului şi care se pot conecta în exterior prin intermediul reţelei, a liniilor telefonice sau a

liniilor închiriate, precum şi toate conturile de utilizator create temporar pentru Furnizor şi necesare pentru acces la RSRITC ale Operatorului, vor fi scoase din uz la încheierea relaţiilor contractuale.

Accesul Furnizorului trebuie să fie identificat în mod unic iar administrarea parolelor sau metodele de autentificare trebuie să fie în conformitate cu Regulamentul privind Parolele de Acces şi Regulamentul de Acces Administrativ.

Activităţile principale ale Furnizorului trebuie să fie documentate de acesta şi puse la dispoziţia conducerii Operatorului, la cerere. Acestea trebuie să cuprindă, dar să nu fie limitate la, evenimente precum: schimbări de personal, schimbări de parolă, schimbări majore în derularea proiectului, timpii de sosire, de plecare şi de livrare.

În cazul retragerii din contract a unui angajat al Furnizorului, indiferent de motiv, Furnizorul se va asigura că toate informaţiile sensibile sunt colectate şi predate Operatorului sau distruse în cel mult 24 de ore de la producerea evenimentului.

În cazul terminării/rezilierii contractului sau la cererea Operatorului, Furnizorul va preda sau distruge toate informaţiile ce aparţin Operatorului şi va oferi certificare în scris privind predarea sau distrugerea informaţiilor în decurs de 24 de ore de la producerea evenimentului.

În cazul încheierii contractului sau la cererea Operatorului, Furnizorul trebuie să predea imediat toate legitimaţiile, cartelele de acces, echipamentele şi stocurile Operatorului.

Echipamentele şi/sau stocurile care urmează a fi reţinute de către Furnizor trebuiesc documentate şi autorizate de Conducerea Operatorului.

Toate programele folosite de Furnizor în scopul furnizării serviciilor stipulate în contract către Operator trebuie să fie inventariate corespunzător si să posede drepturi de utilizare atestate prin Licenţe.

Avizat RPD

.....

Aprobat Primar

.....

Președinte de ședință
Csizmár Antal-Tamás

ROMÂNIA JUDEȚUL SATU MARE COM. CAPLENI CONSILIUL LOCAL

Contrasemnează
Csizmar Erika
Secretar general

Anexa nr.4 la hotărârea nr.13/2021

ANGAJAMENT DE CONFORMARE

Confirm faptul că:

am luat la cunoştinţă despre prevederile Regulamentului Primăriei Capleni privind protecţia datelor cu caracter personal.

Înţeleg că am obligaţia de a respecta dispoziţiile legale privind prelucrarea datelor cu caracter personal, precum şi Regulamentul Primăria Capleni privind protecţia datelor cu caracter personal. Voi procesa date cu caracter personal în vederea intocmirii lucrarii de licenta care are ca si titlu:"Aspecte privind auditul public intern la UAT Capleni"'.Îmi asum personal responsabilitatea pentru respectarea integrală a principiilor, cerinţelor şi obligaţiilor care rezultă din dispoziţiile legale privind prelucrarea datelor cu caracter personal şi Regulamentul Primăriei Capleni privind protecţia datelor cu caracter personal, elaborat în aplicarea prevederilor legale specifice si ma oblig sa procesez doar datele care sunt publice in cadrul primariei Capleni sau datele la care mi se da acces.Conform legii 679 din 27 aprilie 2016 sunt obligata sa nu instrainez datele cu caracter personal care urmeaza sa le procesez in cadrul primariei Capleni in vederea intocmirii lucrarii de liceenta.

Subsemnatul/subsemnata:

_____

Data :

Semnătura :

Președinte de ședință
Csizmár Antal-Tamás

ROMÂNIA JUDEȚUL SATU MARE COM. CAPLENI CONSILIUL LOCAL

Contrasemnează
Csizmar Erika
Secretar general