

Politica privind securitatea informatiei

Politica privind securitatea informației

S.C. FILTRE AER CURAT S.R.L.

Cuprins

SCOP 4
SECURITATEA SISTEMELOR INFORMAȚIONALE 4
MĂSURI NECESARE PENTRU ASIGURAREA SISTEMELOR INFORMATICE 6
SECURITATEA FIZICĂ 6
Inventarierea echipamentelor autorizate și neautorizate 6
Inventarierea aplicațiilor și sistemelor de operare autorizate și neautorizate 7
Controlul echipamentelor wireless 8
Proiectarea securității rețelelor 8
Limitarea și controlul porturilor de rețea, a protocoalelor de comunicație și a serviciilor 9
Protejarea zonelor de perimetru (sau boundary defense) 9
Accesul fizic în locații 10
Securitatea logică 11
Configurații de securitate a componentelor hardware pentru echipamente mobile, stații de lucru și servere 11
Configurații de securitate pentru echipamente de rețea – Firewall, Router, Switch 12
Modalități de protejare împotriva malware-ului 13
Securitatea aplicațiilor 14
Securitatea personalului 15
Utilizarea controlată a privilegiilor de administrare 15
Controlul accesului în baza principiului “Need to Know” 16
Monitorizarea și controlul conturilor de utilizator 17
Evaluarea abilităților și instruirea de securitate 17
Asigurarea continuității afacerii 18
Prevenirea pierderii datelor și capabilitatea de recuperare 19
Capabilitatea de a răspunde la incidente 20
Mentenanta, monitorizarea și evaluarea jurnalelor de audit 20
Teste de penetrare 21
Evaluari de securitate periodice și modalități de remediere 21

Atacuri cibernetice și măsuri de prevenire 22
ANGAJAMENTUL SOCIETĂȚII 23
CONSECINȚE 24
COMUNICAREA POLITICII 24

SCOP

Prezenta Politică are drept scop implementarea măsurilor necesare pentru securitatea adecvată a sistemelor informatice și protecția datelor cu caracter personal la standardele europene pentru a evita incidentele de securitate și asigura protecția necesară datelor cu caracter personal și drepturilor persoanelor la viața privată, precum și pentru a evita prejudiciile de imagine care pot fi aduse Societății ca urmare a vulberabilității sistemelor informatice

SECURITATEA SISTEMELOR INFORMAȚIONALE

Securitatea sistemului informațional trebuie să fie o responsabilitate asumată de către structurile de conducere ale S.C. FILTRE AER CURAT S.R.L. .

Structurile de conducere trebuie să asigure o direcţie clară şi gestionată corespunzator pentru indeplinirea obiectivelor stabilite prinpolitica de securitate, având în vedere următoarele elemente:

a) revizuirea și aprobarea politicii de securitate şi stabilirea de responsabilităţi legate de aceasta;

b) monitorizarea schimbărilor semnificative de expunere a sistemului informațional la ameninţări majore;

c) revizuirea și monitorizarea incidentelor de securitate a sistemului informațional;

d) aprobarea măsurilor de sporire a securității informațiilor.

În vederea stabilirii și menținerii politicilor de securitate este esențială implicarea specialiștilor din domeniu în vederea adoptării deciziilor privind securitatea sistemului informațional.

Accesul la echipamentele de prelucrare informaţiilor S.C. FILTRE AER CURAT S.R.L. de către terţe părţi trebuie să se facă sub supraveghere. Pentru accesul terţilor, o evaluare a riscului ar trebui să fie efectuată pentru a stabili implicaţiile de securitate şi cerinţele de control.

Măsurile de protecție trebuie să fie puse de acord şi incluse într-un contract cu terțele părți. De asemenea în acordurile/contractele de externalizare ar trebui să se abordeze riscurile, controalele și procedurile de securitate pentru sistemele informatice, rețelele şi / sau echipamentele de birou. Toate activele sistemului informațional ar trebui să fie contabilizate şi să aibă un responsabil desemnat. Responsabilitatea pentru active ajută să se asigure că protecția corespunzătoare este menținută. Responsabilul unui element din sistemul informațional trebuie să poată fi identificat pentru toate activele majore și să aibă responsabilități pentru menținerea și implementarea de controale adecvate. Responsabilitățile pentru control pot fi delegate.

Informațiile trebuie să fie clasificate pentru a indica prioritățile și gradul de protecţie necesare. Informațiile au diferite grade de sensibilitate și de importanţă, unele dintre acestea necesitând un nivel suplimentar de protecţie sau o manipulare specială. Un sistem de clasificare a informațiilor ar trebui să fie utilizat pentru a defini un set adecvat de niveluri de protecţie, precum și necesitatea de a institui măsuri speciale de manipulare.

Pentru a reduce riscurile de eroare umană, furt, fraudă sau de abuz de încredere, responsabilităţi de securitate trebuie să fie implementate încă din etapa de recrutare, incluse în contractele de muncă şi monitorizate în timpul activității la locul de muncă. Toți angajații proprii sau terțele persoane care au acces la sistemul informațional S.C. FILTRE AER CURAT S.R.L. ar trebui să semneze un acord de confidențialitate.

Pentru a ne asigura că utilizatorii sunt conştienţi de ameninţările de securitate a informațiilor şi sunt pregătiți pentru a sprijini politica de securitate organizațională în cursul activităţii lor la locul de muncă, angajații proprii sau terțele persoane ar trebui să fie instruiți cu privire la procedurile de securitate și utilizarea corectă a sistemelor de prelucrare a informațiilor.

Toate incidentele de securitate trebuie raportate și în acest sens trebuie implementat un sistem eficient și rapid de raportare a incidentelor de securitate, care să fie cunoscut de către toți angajații.

Informațiile de business critice sau sensibile trebuie să fie adăpostite în locuri sigure, protejate într-un perimetru de securitate adecvat, cu bariere de securitate corespunzătoare și controale de acces. Acestea ar trebui să fie protejate fizic împotriva accesului neautorizat, deteriorare şi interferențe. Protecția oferită trebuie să fie proporţională cu riscurile identificate. Echipamentele IT&C trebuie să fie protejate fizic împotriva ameninţărilor de securitate şi de pericolele de mediu.

Responsabilități și proceduri pentru gestionarea și exploatarea tuturor sistemelor de prelucrare a informațiilor ar trebui să fie stabilite. Aceasta presupune dezvoltarea unor instrucţiuni de utilizare şi proceduri de răspuns la incidente aprobate de conducerea unității și cunoscute de către tot personalul S.C. FILTRE AER CURAT S.R.L. . Măsuri de precauţie sunt necesare pentru a preveni şi detecta introducerea de software rău intenţionat. Software-ul și echipamentele de calcul sunt vulnerabile la introducerea de software rau intentionat, cum ar fi viruşi, viermi de rețea, cai troieni. Utilizatorii ar trebui să fie conştienți de pericolele software-ului neautorizat sau rău intenţionat şi managerii ar trebui, acolo unde este cazul, să introducă controale speciale pentru a detecta sau a preveni introducerea de software rău intenționat. În special, este esențial să se ia măsuri de precauţie pentru a detecta şi a preveni infectarea cu viruşi informatici ale calculatoarelor angajaților. Proceduri de rutină ar trebui să fie stabilite pentru efectuarea de back-up-uri strategice, simularea periodică a restaurării de pe copiile

realizate, logarea evenimentelor și a defectelor, acolo unde este posibil și monitorizarea permanentă a echipamentelor critice. Schimburile de informații și de software între organizații ar trebui să fie controlate, și trebuie să fie conforme cu legislația în vigoare. Proceduri și standarde care să protejeze informațiile și datele în tranzit ar trebui să fie stabilite iar acestea să fie parafate în acorduri semnate de toate părțile implicate.

MĂSURI NECESARE PENTRU ASIGURAREA SISTEMELOR INFORMATICE

SECURITATEA FIZICĂ

Inventarierea echipamentelor autorizate și neautorizate

O practică frecventă a grupurilor infracționale constă în utilizarea tehnicilor de scanare continuă a spațiilor de adrese IP ale organizațiilor țintă, urmărind conectarea sistemelor noi și/sau neprotejate, ori laptop-uri cu definiții sau pachete de securitate (patch-uri) neactualizate datorită faptului că nu sunt conectate frecvent la rețea. Unul din atacurile comune profită de sistemele nou instalate și care nu sunt configurate și securizate din punct de vedere al pachetelor de securitate decât în ziua următoare, fiind ușor de identificat și exploatat prin intermediul Internetului de către atacatori. În ceea ce privește sistemele informatice aflate în interiorul rețelelor protejate, atacatorii care au obținut deja acces pot viza și compromite acele sisteme insuficient sau necorespunzător securizate.

O atenție deosebită trebuie acordată de către S.C. FILTRE AER CURAT S.R.L. echipamentelor și sistemelor care nu sunt incluse în inventarul organizațiilor, cum ar fi diversele dispozitive mobile personale, sisteme de test, etc. și care nu sunt conectate în mod permanent la rețea. În general, aceste tipuri de echipamente tind să nu fie securizate în mod corespunzator sau să nu aibă controale de securitate care să răspunda cerințelor de securitate. Chiar dacă aceste echipamente nu sunt utilizate pentru a procesa, stoca sau accesa date sau informații critice, odată introduse în rețea, pot oferi atacatorilor o cale de acces spre alte resurse și un punct de unde pot fi lansate atacuri avansate. Menținerea de către S.C. FILTRE AER CURAT S.R.L. a unui inventar precis și actual, controlat prin monitorizare activă și managementul configurației, poate reduce șansele ca atacatorii să identifice și să exploateze sistemele neprotejate. Procedurile de inventariere stabilesc proprietarii de informații și sisteme informatice, documentând responsabilitățile pentru menținerea inventarului pentru fiecare componentă a sistemelor.

De asemenea, S.C. FILTRE AER CURAT S.R.L. poate utiliza instrumente de identificare pasivă a resurselor (care "ascultă" în mod pasiv la interfețele de rețea echipamentele care își anunță prezența prin modificarea traficului). Aceste instrumente de monitorizare și inventariere ar trebui să includă funcționalități precum:

- Identificarea echipamentelor noi neautorizate conectate la rețea într-un interval de timp predefinit;
- Alertarea sau transmiterea mesajelor de notificare către o listă predefinită cu personal administrativ;
- Izolarea sistemului neautorizat;
- Identificarea locației în care s-a efectuat conectarea.

Inventarierea aplicațiilor și sistemelor de operare autorizate și neautorizate

Grupurile infracționale utilizează tehnici de scanare a spațiilor de adrese ale organizațiilor vizate în scopul de a identifica versiuni vulnerabile de software care pot fi exploatate de la distanță. Astfel de atacuri pot fi inițiate prin distribuirea de pagini de web ostile, documente, fișiere media și alte tipuri de conținut web prin intermediul propriilor pagini web sau al altor pagini web demne de încredere. Atacurile complexe pot fi și de tipul zero-day, exploatând vulnerabilități în aceeasi zi sau înainte ca acestea sa fie cunoscute public. Fără cunoștințele corespunzătoare sau controlul software-ului implementat, S.C. FILTRE AER CURAT S.R.L. nu poate asigura protecția necesară pentru resursele informatice. Capacitatea de inventariere și controlul neadecvat asupra programelor care sunt instalate și autorizate a rula pe echipamentele organizațiilor, fac mai vulnerabile aceste medii informatice. Astfel de echipamente inadecvat controlate sunt pasibile să execute software care nu este necesar pentru specificul activității, inducând breșe potențiale de securitate sau rulând programe de tip malware induse de către un atacator, după ce sistemul a fost compromis. Odată ce un echipament a fost exploatat, adesea este utilizat ca și un punct de plecare pentru atacuri ulterioare și pentru colectarea de informații sensibile din sistemul compromis și din alte sisteme conectate la acesta. Echipamentele vulnerabile sunt utilizate ca puncte de lansare pentru "avansarea" în rețea și rețele partenere. Organizațiile care nu utilizează inventarierea completă a pachetelor software nu vor reuși să descopere sistemele pe care rulează software vulnerabil sau malițios și mai departe să reducă problemele sau atacurile. Software-ul comercial și instrumente specializate de inventariere a resurselor informatice sunt utilizate pe scară largă pentru a facilita verificarea simultană a aplicațiilor utilizate în organizații, extragând informații despre nivelul pachetelor de update al fiecărui program software instalat pentru a se asigura utilizarea celei mai recente versiuni. Sistemele de monitorizare utilizate de S.C. FILTRE AER CURAT S.R.L. ar trebui să includă și funcționalități precum:

- Capacitatea de identificare a software-ului neautorizat prin detectarea tentativelor de instalare sau executare a acestuia;
- Alertarea personalului administrativ într-un interval de timp predefinit;
- Blocarea instalării, prevenirea executării sau trecerea în carantină.

Controlul echipamentelor wireless

În absența unor măsuri eficiente de securitate implementate pentru rețelele fără fir, se pot iniția atacuri care vizează în principal furtul de date importante pentru orice tip de organizație. Deoarece rețelele fără fir nu necesită conexiuni fizice directe, echipamentele wireless oferă atacatorilor un vector convenabil pentru obținerea accesului în mediul țintă.

Tehnicile de atac dezvoltate pot fi inițiate din exterior, evitandu-se perimetrele de securitate ale organizațiilor. Astfel, echipamentele portabile pot fi infectate prin exploatare la distanță în intervalul în care acestea sunt scoase din perimetrul de securitate în afara organizației și apoi utilizate ca „back doors" odată intoarse în organizație și reconectate la rețea.

Măsurile de protejare impotriva atacurilor desfășurate prin intermediul rețelelor fara fir vizează utilizarea atât a instrumentelor de scanare, detectare și decoperire a rețelelor cât și a sistemelor de detectare a intruziunilor. S.C. FILTRE AER CURAT S.R.L. trebuie să efectueze captura traficului wireless desfășurat în zonele de perimetru pentru a determina dacă sunt utilizate protocoale mai permisive de transmitere sau criptare decât cele impuse. În plus, se pot utiliza instrumente de administrare de la distanță în cadrul rețelelor pentru a colecta informații despre capabilitățile wireless ale dispozitivelor conectate la sistemele administrate. Instrumentele utilizate trebuie să includă următoarele funcționalități:

- capacitatea de a identifica configurațiile dispozitivelor autorizate sau dispozitivele wireless neautorizate din cadrul ariei de acoperire a organizației și care sunt conectate în aceste rețele;
- identificarea dispozitivelor fără fir noi, neautorizate, conectate recent;
- alertarea personalului administrativ; ▫ identificarea zonei și izolarea punctului de acces în rețea.

Proiectarea securității rețelelor

Măsurile de securitate, chiar bine implementate la nivelul sistemelor informatice, pot fi eludate în rețele concepute deficitar. Fără o arhitectura de rețea atent planificată și implementată în mod corespunzător, atacatorii pot ocoli măsurile de securitate din diferite sisteme, pătrunzând în rețea pentru a obține acces către sistemele țintă. Atacatorii vizează în mod frecvent hărțile rețelelor pentru a identifica conexiuni neutilizate între sisteme, filtrare necorespunzătoare și rețele fără segregare. Prin urmare, o arhitectură

de rețea robustă și securizată poate fi realizată prin implementarea de către S.C. FILTRE AER CURAT S.R.L. a unui proces care să furnizeze și măsurile de securitate necesare. Pentru a se asigura un mediu robust și ușor de securizat, arhitectura fiecărei rețele trebuie să se bazeze pe modele care descriu structura generală a acesteia și a serviciilor pe care le oferă. S.C. FILTRE AER CURAT S.R.L. ar trebui să documenteze diagrame pentru fiecare rețea în care să fie evidențiate componentele de rețea împreună cu grupurile semnificative de servere și sisteme client.

Limitarea și controlul porturilor de rețea, a protocoalelor de comunicație și a serviciilor

Atacurile pot fi lansate și prin intermediul serviciilor de rețea accesibile de la distanță care sunt vulnerabile în fața exploatărilor. Exemple comune includ servere web configurate neadecvat, servere de email, servicii de fișiere și imprimare, servere DNS instalate în mod prestabilit pe o varietate de echipamente, de multe ori fără a se ține cont de nevoia de business pentru serviciile oferite. Multe pachete software instalează și pornesc servicii ca parte a instalării pachetului de bază fără a informa utilizatorul sau administratorul despre faptul că serviciile au fost activate. Atacurile urmăresc descoperirea de conturi, parole sau coduri prin scanări și încercări de exploatare a serviciilor expuse.

Asemenea tipuri de atac pot fi preîntâmpinate prin utilizarea de instrumente de scanare a porturilor pentru a determina serviciile care „ascultă” rețeaua pentru o serie de sisteme țintă. Pentru a determina porturile deschise, instrumentele de scanare pot fi configurate pentru identificarea versiunii de protocol și serviciul care „ascultă” pe fiecare port deschis descoperit. Serviciile descoperite și versiunile acestora sunt comparate cu inventarul serviciilor necesare S.C. FILTRE AER CURAT S.R.L. pentru fiecare echipament.

Protejarea zonelor de perimetru (sau boundary defense)

Atacurile pot fi concentrate asupra exploatării sistemelor care pot fi accesate din Internet, inclusiv sistemele aflate în DMZ (termen derivat din „Demilitarized Zone”, cunoscut și ca „perimeter networking”), cât și asupra sistemelor client (stații de lucru, laptop) care accesează conținut din Internet prin zona de perimetru a rețelei.

Tehnicile de atac lansate de grupurile criminale uzează de punctele de slăbiciune din configurarea sau arhitectura perimetrului, a sistemelor de rețea și a echipamentelor client pentru a obține acces inițial în interiorul organizației. Odată obținut accesul, atacatorii vor pătrunde mai adânc în interiorul rețelei în vederea furtului sau schimbului de informații, ori de a stabili o bază pentru atacuri ulterioare împotriva sistemelor gazdă interne. În multe cazuri, atacurile apar între rețele ale partenerilor de business, uneori calificate ca și „extranet”, atacurile mutându-se din rețeaua unei organizații în rețelele altor organizații,

exploatând sistemele vulnerabile găzduite în perimetrele din extranet. Pentru a controla fluxul de trafic efectuat prin rețelele de perimetru și a asigura evidențele în vederea depistării atacurilor efectuate pe sistemele compromise, protejarea zonelor de perimetru trebuie să fie multi-stratificată, utilizând echipamente și aplicații Firewall, Proxy, rețele DMZ, sisteme de prevenire și detectare a intruziunilor la nivel de rețea tip IPS și IDS, precum și filtrarea traficului în și dinspre interiorul rețelelor.

Sistemele de prevenire și detectare a intruziunilor S.C. FILTRE AER CURAT S.R.L. la nivel de perimetru trebuie să includă urmatoarele caracteristici:

- să aibă capacitatea de identificare a pachetelor neautorizate/nelegitime trimise înspre sau primite dinspre o zonă sigură;
- blocarea pachetelor neautorizate/nelegitime;
- alertarea personalului administrativ.

Accesul fizic în locații

Asigurarea unui mediu de securitate adecvat, începe chiar de la accesul fizic în clădireile/spațiile/locațiile S.C. FILTRE AER CURAT S.R.L. care trebuiesc protejate.

Pentru eficientizarea sistemelor de pază și apărare împotriva pătrunderii neautorizate, măsurile de securitate fizică ar trebui cuprinse într-un Plan de securitate fizică, iar implementarea acestor măsuri să fie bazată pe principiul „apărării în adâncime”, urmărindu-se stabilirea:

- spațiului care trebuie protejat;
- unor dispozitive exterioare de securitate destinate să delimiteze zona protejată și să descurajeze accesul neautorizat (gardul de perimetru, barieră fizică care protejează limitele locației, pază cu personal specializat);
- unor dispozitive intermediare de securitate destinate să descopere tentativele sau accesul neautorizat în zona protejată (sisteme de detectare a intruziunilor - SDI, iluminat, televiziune cu circuit închis - TVCI);
- unor dispozitive interioare de securitate destinate să întârzie acțiunile eventualilor intruși (controlul accesului - electronic, electromecanic sau prin alte mijloace).

Controlul accesului personalului S.C. FILTRE AER CURAT S.R.L. în zonele protejate se efectuează de personal de pază sau prin sisteme electronice, avându-se în vedere următoarele:

- accesul fiecărui angajat se realizează prin locuri anume stabilite, pe baza permisului de acces;
- permisul de acces poate specifica în clar identitatea organizației emitente sau locul în care deținătorul are acces, însă acest aspect nu este recomandat pentru zonele în care sunt gestionate

infromații clasificate (Practic la nivelul fiecărei persoane juridice care gestionează informații clasificate se pot stabili reguli suplimentare proprii privind accesul);

- pentru accesul angajaților agenților economici contractanți care efectuează diverse lucrări de reparații și întreținere a clădirilor sau mentenanță, organizațiile beneficiare vor elibera, pe baza actelor de identitate, la solicitarea reprezentanților autorizați ai agenților în cauză, documente de acces temporar.

Planul de securitate fizică cuprinde descrierea tuturor măsurilor de securitate fizică implementate pentru protecția locațiilor și poate fi structurat astfel:

- delimitarea, marcarea și configurația zonelor care trebuiesc protejate; ▫ sistemul de pază și apărare; ▫ sistemul de avertizare și alarmare;
- controlul accesului, al cheilor și combinațiilor de cifru;
- modul de acțiune în situații de urgență; ▫ modul de raportare, investigare și evidență a încălcării măsurilor de securitate;
- responsabilitățile și modul de implementare a măsurilor de pregătire și instruire pe linie de securitate fizică;
- responsabilitățile și modalitățile de realizare a verificărilor, inspecțiilor și controalelor sistemului de securitate;
- măsuri suplimentare de protecție fizică.

Securitatea logică

Configurații de securitate a componentelor hardware pentru echipamente mobile, stații de lucru și servere

Asupra rețelelor Internet cât și a celor interne deja compromise de atacatori, programe automate de atac informatic caută în mod constant rețele țintă pentru a găsi sisteme care au fost configurate cu software vulnerabil instalat. Configurațiile implicite sunt adesea orientate pentru a ușura exploatarea, utilizarea sistemelor, nefiind însă securizate și lăsând servicii inutile exploatabile în starea implicită a acestora. Tehnicile de atac, încearcă să exploateze în acest fel atât serviciile accesibile via rețea, cât și software-ul de navigare al clientului.

Măsurile de protecție împotriva acestor tehnici de atac includ achiziția de componente pentru sisteme și rețea cu configurații de securitate deja implementate, instalarea sistemelor preconfigurate pentru securitate, actualizarea configurațiilor periodic și urmărirea acestora în cadrul unui sistem de management al configurațiilor.

Aceste măsuri se pot implementa de către S.C. FILTRE AER CURAT S.R.L. prin crearea de imagini ale sistemelor și stocarea pe servere securizate împreună cu utilizarea instrumentelor de management al configurațiilor. În funcție de soluția adoptată, aceste instrumente pot monitoriza în mod activ devierile de la configurațiile implementate, furnizând informațiile necesare pentru asigurarea utilizării configurațiilor stabilite și vor include următoarele funcționalități:

- Identificarea oricăror modificări/schimbări în cadrul unei imagini securizate care pot include modificări aduse pentru fișiere cheie, porturi, fișiere de configurații sau pentru software-ul instalat;
- Compararea imaginii fiecărui sistem cu imaginea oficială stocată în mod securizat în cadrul sistemului de management al configurațiilor;
- Blocarea instalării și prevenirea executării odată cu alertarea personalului administrativ.

Configurații de securitate pentru echipamente de rețea – Firewall, Router, Switch

Atacatorii profită de o practică des întalnită în configurarea nivelului de securitate pe anumite echipamente de rețea: utilizatorii solicită excepții temporare din considerente specifice, de business, aceste excepții sunt aplicate dar nu și îndepărtate imediat ce necesitatea de business dispare. În unele situații și mai grave, riscul de securitate al unei astfel de excepții nu este nici analizat corespunzător nici evaluat din punct de vedere al necesității.

Atacatorii caută breșele din firewall-uri, routere și switch-uri și apoi le folosesc în scopul penetrării sistemului. Atacatorii au exploatat deficiențele acestor echipamente de rețea pentru a obține accesul în mediile vizate, pentru a redirecta traficul înspre o altă rețea sau un sistem malițios ce se anunță ca un sistem de încredere, și pentru a intercepta și altera informații pe măsură ce acestea sunt transmise. Cu astfel de acțiuni atacatorul obține acces la date sensibile, alterează informații importante sau chiar utilizează un sistem compromis pentru a „poza” într-un alt sistem de încredere din rețea.

Anumite organizații utilizează unelte comerciale de evaluare a setului de reguli de pe echipamentele de filtrare din rețea, cu scopul de a determina măsura în care acestea sunt consistente sau conflictuale. S.C. FILTRE AER CURAT S.R.L. va face astfel o verificare automată a stării filtrelor de rețea și se caută erori în seturile de reguli sau în listele de control al accesului (Access Control List - ACL) care ar putea permite servicii nedorite pe acele echipamente. Astfel de unelte ar trebui utilizate la fiecare modificare semnificativă a setului de reguli de pe firewall-uri, a ACL-urilor de pe router sau pe alte tehnologii de filtrare. Funcționalitățile minim recomandate pentru menținerea unui control optim la nivel de echipamente de rețea:

- Identificarea oricărei modificări la nivel de echipamente de rețea, inclusiv routere, switch-uri, firewall-uri și sisteme IDS și IPS (orice schimbare în fișierele cheie, servicii, porturi, fișiere de configurație sau orice alt software instalat pe echipamente
- Configurația fiecărui sistem trebuie comparată cu baza de date master cu imagini pentru a verifica orice modificare în configurație din punct de vedere al impactului asupra securității.

Modalități de protejare împotriva malware-ului

Software-ul malițios constituie un aspect periculos al amenințărilor din mediul Internet, care vizează utilizatorii finali și organizațiile prin intermediul navigării, atașamentelor email, dispozitivelor mobile precum și prin utilizarea altor vectori. Codul malițios poate să interacționeze cu conținutul sistemului, să captureze date sensibile și să se răspândească la alte sisteme.

Malware-ul modern urmărește să evite detectarea bazată pe semnături și cea comportamentală și poate dezactiva instrumentele anti-virus care rulează pe sistemul țintă. Software-ul anti-virus și anti-spyware, denumite colectiv ca instrumente anti-malware, ajută la apărarea împotriva acestor amenințări prin încercarea de a detecta programele malware și blocarea executării acestora. Instrumentele anti-malware, pentru a fi eficiente, necesită actualizări periodice. Bazându-se pe politici și acțiuni ale utilizatorilor pentru menținerea instrumentelor anti-malware actualizate, acestea au fost discreditate pe scară largă deoarece mulți utilizatori nu s-au dovedit capabili să aplice în mod consecvent aceste sarcini. Pentru a asigura actualizarea periodică și eficientă a intrumentelor anti-malware, sunt utilizate soluții care automatizează aceste sarcini. Aceste soluții, numite și suite de end-point security, utilizează funcționalități de administrare integrate pentru a verifica activitatea instrumentelor anti-virus, anti-spyware și host-based IDS pe fiecare sistem gestionat. Zilnic sau la intervale predefinite, rulează evaluări automate și efectuează revizuiri ale rezultatelor pentru identificarea sistemelor care au dezactivate instrumentele de protecție, precum și a sistemelor care nu sunt actualizate cu ultimele definiții malware.

Pentru creșterea nivelului de siguranță pentru sistemele protejate, cât și pentru sistemele care nu sunt acoperite de soluțiile de management ale organizațiilor, se folosesc tehnologiile de control al accesului în rețea prin intermediul cărora sunt testate echipamentele din punct de vedere al conformității cu politicile de securitate înainte de a permite accesul în rețea. Unele organizații implementeaza honeypot-uri comerciale sau gratuite și instrumente de „ademenire” – cunoscute ca „tarpit tools” pentru a identifica atacatorii în mediul lor.
S.C. FILTRE AER CURAT S.R.L. trebuie să monitorizeze permanent aceste instrumente pentru a determina când traficul este direcționat către atacatori și sunt efectuate tentative de conectare. Odată identificate

aceste evenimente, personalul de securitate trebuie să obțina sursa adreselor de unde este generat traficul și alte detalii asociate atacului pentru a furniza datele necesare activităților de investigare.

Instrumentele anti-malware vor include următoarele funcționalități:

- Identificarea instalării de software malițios, a tentativelor de instalare, executare sau a tentativelor de executare;
- Blocarea instalării și prevenirea executării sau trecerea în carantină a software-ului malițios odată cu alertarea personalului administrativ.

Securitatea aplicațiilor

Printre prioritățile recente ale grupurilor criminale se numără atacurile asupra vulnerabilităților aplicațiilor webbased precum și asupra aplicațiilor în general. Aplicațiile care nu fac verificări asupra volumului intrărilor generate de utilizator, nu reușesc să „sanitizeze" intrările prin filtrarea secvențelor de caractere care nu sunt necesare sau potențial malițioase sau nu inițiază „curățarea" variabilelor în mod corespunzator, fiind astfel vulnerabile la compromiterea de la distanță.

Atacurile pot fi efectuate prin „injectarea" de exploatări specifice incluzând buffer overflows, atacuri de tip SQL injection, cross-site scripting, cross-site request forgery, și click jacking de cod pentru obținerea controlului asupra sistemelor vulnerabile.

Pentru prevenirea unor asemenea atacuri, aplicațiile dezvoltate intern cât și aplicațiile third-party trebuie testate riguros de către S.C. FILTRE AER CURAT S.R.L. pentru a identifica deficiențele de securitate. Pentru aplicațiile third-party, S.C. FILTRE AER CURAT S.R.L. trebuie să se asigure că furnizorii au efectuat testări riguroase de securitate pentru produse, iar pentru aplicațiile dezvoltate intern, S.C. FILTRE AER CURAT S.R.L. trebuie să efectueze testările de securitate sau să angajeze servicii de specialitate pentru efectuarea de astfel de testări. Tool-urile ce testează cod sursă sau acelea pentru scanarea securității aplicațiilor web s-au dovedit a fi utile în vederea securizării, alături de verificările de securitate tip penetration testing efectuate manual de specialiști cu vaste cunoștințe de programare și expertiză în testarea de aplicații.

Funcționalități recomandate în sistemul de securitate al aplicațiilor:

- Detectarea și blocarea încercărilor de atac la nivel de aplicație;
- Testarea periodică, săptămânal sau chiar zilnic;
- Mitigarea tuturor vulnerabilităților cu risc mare din aplicațiile web accesibile din Internet - identificate cu scannere de vulnerabilități, instrumente de analiză statice și instrumente de

revizuire a configurațiilor automate din bazele de date – fie prin modificarea fluxului, fie prin implementarea unui control compensatoriu.

Securitatea personalului

Utilizarea controlată a privilegiilor de administrare

O primă metodă de atac cu scopul de a se infiltra în rețeaua unei organizații o reprezintă utilizarea eronată a privilegiilor administrative. Două metode comune de atac profită de lipsa de control asupra acestor privilegii administrative: În prima metodă, un utilizator al unei statii de lucru, folosind un cont privilegiat, este păcălit să deschidă un atașament malițios din email, descărcând și deschizând un fișier de pe un website malițios, sau pur și simplu navigând pe un site web ce găzduiește conținut periculos care poate exploata browserul. Fișierul sau exploit-ul conține cod executabil ce ruleazp pe mașina victimei fie automat, fie convingând utilizatorul sp execute conținutul. Daca acest cont de utilizator are privilegii administrative, atacatorul poate prelua complet controlul asupra sistemului victimei și poate instala tool-uri precum keystroke loggers sau keyloggers (aplicație ce reține într-un fișier tot ce se tastează), sniffers (interceptează și decodifică traficul de rețea) și software de control la distanță pentru a identifica parole de administrare și alte informații sensibile.

Atacuri similare au loc și prin intermediul emailului: un administrator deschide un email ce conține un atașament infectat, acesta fiind mai apoi utilizat pentru a obține un punct de acces în rețea și de a ataca și alte sisteme. O a doua metodă o reprezintă elevarea de privilegii ghicind și „spărgând” o parolă a unui cont administrativ, pentru a obține acces la o mașină țintă.

Dacă privilegiile administrative sunt folosite pe scară largă în interiorul S.C. FILTRE AER CURAT S.R.L., atacatorul va obține mai usor și mai repede controlul asupra sistemelor, întrucât sunt disponibile mai multe conturi cu privilegii administrative de încercat. O situație comună specifică unui astfel de atac este aceea a privilegiilor administrative de domeniu în mediile complexe Windows, atacatorul având astfel un control semnificativ asupra unui număr mare de mașini și asupra datelor conținute de acestea. Un management optim al conturilor administrative se realizează cu o serie de funcționalitati sau activități precum:

- extragerea listei de conturi privilegiate, atât pe sistemele individuale cât și la nivel de controllere de domeniu și verificarea periodică în lista cu servicii active dacă vreun browser sau serviciu de email folosește privilegii ridicate (utilizarea de scripturi ce caută anumite browsere, servicii de email și programe de editare a documentelor);

- conturile administrative pot fi configurate să utilizeze un proxy web în anumite sisteme de operare și să nu aibă acces la aplicația de poștă electronică.
- Setarea lungimii minime acceptabile a parolei de exemplu la 12 caractere, setarea unui algoritm de complexitate corespunzator.

Controlul accesului în baza principiului "Need to Know"

Unele organizații nu își identifică și separă cu atenție datele sensibile de cele mai puțin sensibile sau disponibile public în rețelele interne. În multe medii, utilizatorii interni au acces la toate sau la majoritatea informațiilor din rețea. Odată ce atacatorul a penetrat o astfel de rețea, pot găsi și transmite în exterior informații importante, fără eforturi considerabile.

Chiar în câteva situații de pătrundere din ultimii ani, atacatorii au reușit să obțină accesul la date sensibile cu același cont de acces ca și pentru datele obișnuite, stocate pe servere comune.

Este vital ca S.C. FILTRE AER CURAT S.R.L. să înțeleagă care sunt informațiile sale importante, unde sunt situate și cine are nevoie să le acceseze. Pentru a ajunge la nivelele de clasificare, S.C. FILTRE AER CURAT S.R.L. trebuie să treacă în revistă tipurile cheie de date și importanța lor la nivel de organizație. Această analiză poate fi utilă în creionarea schemei de clasificare a informațiilor la nivelul întregii organizații. În cel mai comun caz, schema de clasificare conține două nivele: informații publice (neclasificate) și private (clasificate). Odată ce informațiile private au fost identificate, acestea pot fi ulterior împărțite pe subclase în funcție de impactul în organizație, dacă ar fi compromise.

Ce putem face pentru a aplica principiul cât mai eficient:

- Identificarea datelor, clasificarea pe nivele, corelarea cu aplicațiile de business; segmentarea rețelei astfel încât sisteme de aceeași sensibilitate să fie pe același segment de rețea; accesul la fiecare segment de rețea trebuie controlat de firewall și eventual criptat traficul de pe un segment de rețea cu acces nesecurizat;
- Fiecare grup de utilizatori sau angajați ar trebui să aibă clar specificate în cerințele postului ce tip de informații trebuie sau au nevoie să acceseze în scopul îndeplinirii atribuțiilor. În funcție de cerințele postului, accesul se va permite doar pe segmentele sau serverele necesare pentru fiecare post în parte. Fiecare server ar trebui să înregistreze logurile detaliate, astfel încât accesul să poată fi urmărit, iar situațiile în care cineva accesează date la care nu ar trebui să aibă acces să poată fi examinate;
- Sistemul trebuie să fie capabil să detecteze toate încercările de acces fără privilegii corespunzatoare și să aibă capabilități de alertare.

Monitorizarea și controlul conturilor de utilizator

Atacatorii descoperă frecvent și exploatează conturi de utilizator legitime dar nefolosite pentru a impersona utilizatorii legitimi, făcând astfel dificilă depistarea atacului de către sistemul de securitate al rețelei. Sunt des întâlnite cazurile în care conturile de utilizator ale contractorilor sau angajaților care au finalizat colaborarea cu organizația rămân active. Mai mult, actualii angajați rău voitori sau foști angajați au accesat conturile vechi și mult după expirarea contractului, menținand accesul la sistemele organizației și la datele sensibile, în scopuri neautorizate și uneori malițioase.

Monitorizarea și controlul conturilor de utilizator sunt activități ce revin personalului administrativ al S.C. FILTRE AER CURAT S.R.L. și au în vedere cel puțin funcționalități precum:

- Activarea funcției de logare a informațiilor legate de utilizarea conturilor, configurarea astfel încât să genereze date coerente și detaliate;
- Folosirea de scripturi sau instrumente dedicate pentru analiza de log astfel încât să se poată evalua profilul accesării pe anumite sisteme;
- Managementul conturilor, cu atenție sporită pe cele inactive; ▫ Sistemul trebuie să fie capabil să identifice conturile de utilizator neautorizate, atunci când acestea există în sistem.

Evaluarea abilităților și instruirea de securitate

Fiecare organizație ce se crede pregatită să identifice și să reacționeze eficient în fața atacurilor este datoare în fața angajaților și contractorilor să observe deficiențele în cunoștințe și expertiză, și să susțină acoperirea acestora prin exercițiu și instruire. Un program solid de evaluare a abilităților poate oferi managementului informații solide despre zonele în care trebuie îmbunătățită conștientizarea în domeniul securității, și devine util pentru determinarea alocării optime a resurselor limitate cu scopul de a îmbunătăți practicile de securitate.

Strâns legată de politici și conștientizare este și activitatea de instruire a personalului S.C. FILTRE AER CURAT S.R.L. . Politicile comunică angajaților ce sa facă, instruirea le oferă metodele și abilitățile în vederea îndeplinirii, iar conștientizarea schimbă atitudini și comportament astfel încât personalul să urmeze prerogativele politicilor. Instruirea trebuie întotdeauna corelată cu necesitățile de cunoștințe pentru a îndeplini o sarcină dată. Dacă după instruire, utilizatorii nu respectă o anumită politică, aceasta ar trebui evidențiată prin conștientizare.

Asigurarea continuității afacerii

Orice organizație depinde de resurse, personal şi activități care sunt efectuate zilnic, în scopul de a rămâne operațională şi profitabilă. Cele mai multe organizații au resurse tangibile, proprietăți intelectuale, angajați, calculatoare, legăturile de comunicare, clădiri pentru sedii principale și puncte de lucru. Dacă oricare dintre aceste elemente este deteriorat sau inaccesibil pentru un motiv sau altul, compania și serviciile furnizate de aceasta pot fi grav afectate. În funcție de gravitatea cazurilor, S.C. FILTRE AER CURAT S.R.L. poate reveni la capacitatea de funcționare normală mai repede sau mai greu, dar există și situații în care companiile nu sunt niciodată în măsură să își reia activitatea și să-și mențină clienții în urma diferitelor dezastre care pot apare. Ca o consecință benefică implementării planului de recuperare în caz de dezastru, s-a constatat că organizațiile care au planificate măsuri de recuperare în caz de dezastru au o șansă mult mai mare de a-și relua activitatea în timp util şi de a rămâne în piață.

Scopul implementării de către S.C. FILTRE AER CURAT S.R.L. a unui plan de recuperare în caz de dezastru este acela de a minimiza efectele unui dezastru și pentru a se asigura că resursele, personalul, şi operațiunile își vor relua funcționarea într-un timp util. Un plan de recuperare în caz de dezastru este aplicat atunci când intervine o situație de nefuncționare și tot personalul este preocupat de a repune sistemele critice din nou online.

Un plan de continuare a afacerii (BCP), are o abordare mai largă a problemei. Acesta include activarea și funcționarea sistemelor critice în altă locație în timp ce se lucrează la rezolvarea problemelor și repornirea sistemelor în locația principală. De asemenea, este important de notat că o societate poate fi mult mai vulnerabilă, după un dezastru, pentru că serviciile de securitate folosite pentru protecția fizică sau logică pot fi indisponibile sau într-o stare de operare la capacitate redusă. Disponibilitatea este una dintre temele principale ale planificării continuității (planului de recuperare în caz de dezastru și a planului de continuarea afacerii) în care se asigură că există resursele necesare pentru a menține operaționalitatea organizației în orice condiții

Atunci când se are în vedere planificarea continuității activității, unele companii se concentrează în principal pe backup de date şi existența hardware-ului redundant. Deși aceste elemente sunt extrem de importante, ele sunt doar părți mici din imaginea de ansamblu. Echipamentele au nevoie de oameni pentru a le configura şi le utiliza, iar datele sunt de obicei nefolositoare dacă nu sunt accesibile pentru alte sisteme și entități, eventual, din exterior. Planificarea trebuie să aibă în vedere prezența oamenilor potriviți la locul potrivit, documentarea configurațiilor necesare, stabilirea de canale alternative de comunicații (voce și date), puterea de alimentare necesară și asigurarea că toate dependințele, inclusiv procesele și aplicațiile, sunt corect înțelese şi luate în considerare

De exemplu, în cazul în care liniile de comunicație sau în cazul în care un serviciu este indisponibil pentru orice perioadă semnificativă de timp, trebuie să existe o modalitate rapidă și testată de restabilire a comunicațiilor și serviciilor afectate.

Incidentele și întreruperile pot apare din multe cauze:

- Umane – angajați nemulțumiți, revolte, vandalism, accidente, furt, etc;
- Tehnice – întreruperi, viruși, viermi, hackeri, probleme de alimentare cu energie electrică, fiabilitatea echipamentelor, etc;
- Naturale – cutremure, furtuni, incendii, inundații, etc.

Fiecare din aceste situații pot cauza probleme de funcționare de tipul:

- Minor – operațiunile sunt indisponibile pentru o perioadă redusă de timp, de până la câteva ore, sau mai puțin de o zi;
- Mediu – operațiunile sunt indisponibile pentru mai mult de o zi. În acest caz o locație secundară poate fi utilă pentru continuarea operațiunilor;
- Major – acest tip de eveniment apare în urma unei catastrofe iar locația principală nu mai poate fi utilizată. Este necesară o locație auxiliară pentru continurarea operațiunilor până se va reactiva locația principală

Cele mai importante operațiuni care trebuiesc luate în considerare de către S.C. FILTRE AER CURAT S.R.L., în procesul de funcționare normală sunt următoarele:

Prevenirea pierderii datelor și capabilitatea de recuperare

În cadrul operațiunilor zilnice ale S.C. FILTRE AER CURAT S.R.L. este foarte important să se aibe în vedere securitatea și protecția datelor prelucrate. Datorită faptului că siguranța datelor procesate este esențială în orice organizație, prevenirea pierderii datelor și recuperarea acestora în caz de dezastru este critică. Obiectivul principal al unui plan de salvare a aplicațiilor și datelor critice este acela de a permite restaurarea acestora într-un timp foarte scurt și cu pierderi minime. În cadrul unui astfel de plan vor fi incluse următoarele puncte:

- Identificarea datelor și aplicațiilor care trebuiesc salvate;
- Tipul de salvare pentru diferite seturi de date (salvare completă, parțială, incrementală, continuă); ▫ Regularitatea cu care se vor face salvările;
- Unde vor fi păstrate salvările;
- Cine are acces la salvările efectuate; ▫ Perioada de timp necesară pentru a fi păstrate datele până vor fi distruse.

Salvările efectuate trebuiesc depozitate, iar accesul la acestea trebuie sa fie rapid și ușor. Locația în care sunt depozitate salvările de siguranță poate avea un impact major în procesul de restaurare a datelor și a serviciilor afectate. Din acest motiv este util ca salvările de siguranță să se regăsească în două locații diferite, astfel încât riscul de pierderea a lor să fi diminuat semnificativ.

Capabilitatea de a răspunde la incidente

În crearea planului de răspuns în cazul unui dezastru trebuie avută în vedere atât capabilitatea de a răspunde la incidente cât și identificarea obiectivelor pe termen scurt și pe termen lung, după cum urmează:

Identificarea funcțiilor critice și prioritățile pentru restaurare;

- Identificarea sistemelor suport necesare funcțiilor critice;
- Estimarea potențialelor probleme care pot apare și identificarea resurselor minime necesare pentru recuperare în caz de dezastru;
- Alegerea strategiei de recuperare și identificarea elementelor vitale necesare pentru reluarea activității (personal, echipamente, sisteme, etc);
- Identificarea persoanei (persoanelor) care vor conduce reluarea activității și procesul de testare;
- Calcularea fondurilor necesare pentru atingerea acestor obiective.

Planul va trebui sa detalieze și modul de contactare și mobilizare a angajaților, comunicarea între angajați, interfațarea cu furnizori externi.

Mentenanta, monitorizarea și evaluarea jurnalelor de audit

După finalizarea procedurilor de testare a planului de recuperare în caz de dezastru, este important ca acesta să fie întreținut, actualizat și evaluat în continuu. Aceste activități constau în:

- Responsabilizarea personalului S.C. FILTRE AER CURAT S.R.L. – fișa postului a persoanelor responsabile de planul de recuperare în caz de dezastru trebuie să conțină detalii despre responsabilitățilre acestor în cadrul planului de recuperare în caz de dezastru;
- Revizuirea performanțelor – realizarea (sau nerealizarea) acțiunilor de întreținere a planului de recuperare în caz de dezastru în cadrul unor întâlniri bianule cu persoanele responsabile;
- Auditare – echipa de auditare trebuie sa verifice planul și să se asigure că este actualizat și în conformitate cu realitatea.

Totodată, echipa de audit va trebui să inspecteze toate locațiile suplimentare în care sunt depozitatea copiile de siguranță, politicile de securitate, configurațiile, etc.

De asemenea, implicațiile planului de recuperare în caz de dezastru în cazul intreținerii, monitorizării și recuperării trebuie luate în considerare de către S.C. FILTRE AER CURAT S.R.L. în orice discuții referitoare la achiziționarea de echipamente noi, modificarea celor existente sau a infrastructurilor critice ale S.C. FILTRE AER CURAT S.R.L.

Teste de penetrare

Testarea securității reprezintă un element important în procesul de asigurare a continuității activității S.C. FILTRE AER CURAT S.R.L. și constă într-o analiză cuprinzătoare a comportamentului sistemelor și aplicațiilor organizației în condițiile unor scenarii prestabilite de atac informatic.

Scopul testelor de penetrare este acela de a analiza comportamentul aplicațiilor în contextul diferitelor atacuri informatice, fiind analizate vulnerabilitățile care pot exista în aplicațiile dezvoltate sau utilizate. Un test de penetrare complet cuprinde atât teste automate cât și manuale. Testele automate identificâ neglijențe sau erori de programare în aplicațiile utilizate și sunt efectuate cu ajutorul unor programe specializate (vulnerability scanners, fuzzers, code scanners, etc). Testele manuale sunt folosite pentru a analiza aspecte ale aplicațiilor care necesită intuiția umană, identificându-se erori logice de programare

. Este recomandat ca un test de penetrare (extern și intern) să fie efectuat anual de către S.C. FILTRE AER CURAT S.R.L.

Testele de penetrare nu rezolvă problemele aplicațiilor și sistemelor informatice, ci doar le identifică. După fiecare test de penetrare sunt necesare acțiuni de corectare și actualizare a sistemelor și aplicațiilor în testate.

Evaluari de securitate periodice și modalități de remediere

Lumea securității informatice este în continuă dezvoltare. Există o multitudine de metode de atac și apărare care pot fi utilizate atât pentru a ataca un sistem informatic cât și pentru apărarea acestuia. Evaluarea securității sistemelor informatice se poate realiza prin:

- Revizuirea politicilor de securitate – politicile de securitate sunt utilizate pentru a verifica prezența și rigurozitatea controalelor de securitate implementate;

- Scanare periodică pentru identificarea vulnerabilităților informatice (vulnerability scanning) – aceste programe sunt utilizate pentru a descoperi problemele aplicațiilor informatice, configurații eronate și vulnerabilități de securitate;
- Remedierea problemelor de securitate – se realizează pe baza rapoartelor rezultate în urma testelor de scanare periodică de securitate. Remedierea se realizează prin implementarea patch-urilor de securitate furnizate de catre producătorii de software, actualizarea la ultima versiune a aplicațiilor, reconfigurarea sistemelor informatice vizate, etc.

Teste de penetrare – sunt utilizate în principal pentru evaluarea măsurilor de remedierilor implementate în urma scanărilor de securitate.

Atacuri cibernetice și măsuri de prevenire

România se confruntă în prezent cu amenințări provenite din spațiul cibernetic la adresa infrastructurilor critice, având în vedere interdependența din ce în ce mai ridicată între infrastructurile cibernetice și infrastructuri precum cele din sectoarele energie, telecomunicații, transport, financiar-bancar, și apărare națională.

Globalizarea spațiului cibernetic este de natură să amplifice riscurile la adresa acestora afectând în aceeași măsură atât sectorul privat, cât și pe cel public. Amenințările specifice spațiului cibernetic se caracterizează prin asimetrie și dinamică accentuată și caracter global, ceea ce le face dificil de identificat și de contracarat prin măsuri proporționale cu impactul materializării riscurilor. Amenințările la adresa spațiului cibernetic se pot clasifica în mai multe moduri, dar cele mai frecvent utilizate sunt cele bazate pe factorii motivaționali și impactul asupra societății

. În acest sens, putem avea în vedere criminalitatea cibernetică, terorismul cibernetic și războiul cibernetic, având ca sursă atât actori statali, cât și non-statali.

Amenințările din spațiul cibernetic se materializează – prin exploatarea vulnerabilităților de natură umană, tehnică și procedurală – cel mai adesea în:

- atacuri cibernetice împotriva infrastructurilor care susțin funcții de utilitate publică ori servicii ale societății informaționale a căror întrerupere / afectare ar putea constitui un pericol la adresa securității naționale;
- accesarea neautorizată a infrastructurilor cibernetice;
- modificarea, ștergerea sau deteriorarea neautorizată de date informatice ori restricționarea ilegală a accesului la aceste date;

- spionajul cibernetic;
- cauzarea unui prejudiciu patrimonial, hărțuirea și șantajul persoanelor fizice și juridice, de drept public și privat.

Pericolele și amenințările din spațiul virtual vizează, în general, rețelele, nodurile de rețea și centrele vitale, mai exact, echipamentele și sistemele fizice ale acestora (calculatoare, providere, conexiuni și noduri de rețea etc.), precum și celelalte infrastructuri care adăpostesc astfel de mijloace (clădiri, rețele de energie electrică, cabluri, fibră optică și alte componente). În aceeași măsură, ele vizează și centrele de date, sistemele de înmagazinare, de păstrare și de distribuție a informației, suportul material al bazelor de date și multe altele.

Însă, înainte de toate, asemenea pericole și amenințări vizează sistemele IT (întreprinderi, linii de producție, sisteme de aprovizionare cu materiale strategice, infrastructuri de resurse și de piețe, institute de cercetări, sisteme de comunicații).

Din categoria pericolelor și amenințărilor împotriva infrastructurilor critice ale spațiului cibernetic fac parte și următoarele:

- dezvoltarea rețelelor subversive și neconvenționale IT;
- activitatea tot mai intensă a hacker-ilor;
- ciberterorismul.

Fără un sistem de securitate implementat și funcțional, sistemele informatice, de telecomunicații și datele prelucrate, stocate sau trasportate de acestea pot fi oricând supuse unor atacuri informatice. Unele atacuri sunt pasive - informațiile sunt monitorizate sau copiate, iar alte atacuri sunt active - fluxul de informații este modificat cu intenția de a corupe sau distruge datele sau chiar sistemul sau rețeaua în sine. Sistemele informatice și de telecomunicații, rețelele formate de acestea și informațiile pe care le dețin sunt vulnerabile la numeroase tipuri de atacuri dacă nu sunt apărate de un plan de securitate informatică eficient.

ANGAJAMENTUL SOCIETĂȚII

Societatea își ia angajamentul să implementeze măsuri care să asigure securitatea informațiilor pentru a proteja scurgerile neautorizate de date cu caracter personal.

Prezenta politică trebuie respectată de către toți angajații S.C. FILTRE AER CURAT S.R.L. și alți terți care au acces la datele personale ale organizației sau interacționează într-un fel sau altul cu persoanele fizice vizate și/sau sistemele informatice ale Societății

CONSECINȚE

Nerespectarea prezentei Politici de către angajații companiei poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă) și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse ca urmare a nerespectării prezentei Politici.

Nerespectarea prezentei Politici de către partenerii de afaceri poate conduce către rezilierea contractelor comerciale și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse S.C. FILTRE AER CURAT S.R.L. ca urmare a nerespectării prezentei Politici.

Prezenta Politică va fi comunicată de către S.C. FILTRE AER CURAT S.R.L. tuturor angajaților, colaboratorilor, partenerilor de afaceri sau a altor terți.

Politică aprobată de:	
Semnătura:	
Următoarea revizuire:	

Anexa I

COMUNICAREA POLITICII

Declar că am citit că sunt de acord și că mă oblig să respect prezenta Politică

Numele și Prenumele/Denumirea Societății/ Funcția	Semnătura
Exemplu #1 Ion Ionescu/manager HR	
Exemplu #2 ABC SRL prin administrator Ion Ionescu	
Numele și Prenumele/Denumirea Societății/ Funcția	Semnătura

Crearea acestei Politici a fost posibilă multumită ANSSI și materialelor publicate pe http://anssi.ro/