# Măsuri de securitate Hosting WEB/VPS, Colocare, Virtual PBX

## Introducere

Infrastructura S.A. Moldtelecom este concepută și proiectată în straturi progresive începând de la securitatea fizică a centrelor de date, continuând cu securitatea hardware și software și în cele din urmă tehnici și procese documentate menite pentru a sprijini securitatea operațională, astfel încât să ofere securitate și siguranță pentru platformele clientului, care includ dar fără a se limita la - stocarea securizată a datelor, comunicații securizate între platforme, operare securizată și transparentă de către administratori și garanții de confidențialitate pentru utilizatorul final.

Notă: Măsurile de securitate și informații referitoare la practicile de securitate specifice platformei Client, sunt disponibile doar de la Client.

## Cultura de securitate

În cadrul S.A. Moldtelecom preocuparea pentru a menține o cultură de securitate în cadrul companiei se începe încă de la procesul de recrutare, etapă în care angajații sunt verificați în mod rezonabil, în măsura în care este permis legal și în conformitate cu reglementările legale și legislația locală a muncii aplicabilă.

S.A. Moldtelecom implementează și menține programe de formare continuă (instruire și conștientizare) în domeniul securității pentru toți angajații (dependent de sarcini și atribuții), inclusiv teste a nivelului de înțelegere a responsabilităților și riscurilor de securitate aplicabile fiecărui domeniu de activitate.

Toți angajații S.A. Moldtelecom au semnat un acord de confidențialitate prin care confirmă înțelegerea și respectarea politicilor de confidențialitate, fapt care evidențiază angajamentul S.A. Moldtelecom de a păstra în siguranță informațiile despre clienți.

## Securitatea fizică și a mediului

S.A. Moldtelecom pentru prestarea serviciilor de tip Hosting VPS/WEB, Colocare și Virtual PBX utilizează exclusiv centre de date proprii gestionate intern care încorporează mai multe straturi de protecție fizică de securitate cibernetică.

Accesul la facilitățile centrelor de date este asigurat prin utilizarea sistemelor de control acces cu card magnetic și doar pentru un număr limitat de angajați autorizați.

Centrele de date sunt asigurate cu sisteme anti-incendiare, de monitorizare a mediului (temperatură, umiditate, etc.), antiseismic, pază tehnică (ex. video monitorizare) și fizică, sisteme de control al accesului.

Pentru asigurarea disponibilității sistemelor și eliminarea punctelor unice de eșec, S.A. Moldtelecom asigură redundanță pentru sistemele de alimentare cu energie electrică (alimentare din mai multe surse, sisteme UPS și generatoare electrice), sisteme de ventilare și condiționare, inclusiv personal (personal cu program de lucru 24/24 și standby).

Hardware-ul utilizat în Centrele de date este certificat și acreditat privitor la protecția mediului, iar pentru minimizarea emisiilor de căldură în atmosferă, dar și pentru minimizarea spectrului de vulnerabilități, în acestea sunt utilizate doar componentele necesare scopului acestora. Spre exemplu pe servere nu sunt instalate componente precum: plăci video, adaptoare fără fir sau echipamente periferice de stocare.

## Gestionarea acceselor

S.A. Moldtelecom are implementată o procedură de acordare și retragere a acceselor la sistemele informaționale, aplicată pentru toate sistemele din gestiune.

Accesul de management la platformele Hosting VPS/WEB este acordat doar unui grup restrâns de angajați - administratori. Drepturile și nivelurile de acces fiind acordate în baza funcției și rolurilor lor de serviciu, utilizând principiul de privilegiu minim.

Accesul la platformele clienților Hosting VPS/WEB și Virtual PBX este acordat printr-un proces standardizat și securizat (protocoale securizate și reguli de acces specifice), agreat cu clientul în contract, acordându-i acestuia posibilitatea de a accesa și de a efectua distant anumite sarcini în consola de administrare a platformei sale printr-un canal securizat. Accesul la contentul și datele clientului este gestionat individual de client, accesarea și prelucrarea din partea S.A. Moldtelecom limitând-se la exclusiv la sarcinile de administrare a platformei asigurarea funcționalului acesteia și back-up.

Accesul clienților la sălile de colocare este asigurat într-un mod documentat, securizat, fiind respectate toate procedurile și cerințele de pază, protecție a muncii și securitate anti incendiară. Accesul fizic este asigurat în baza solicitărilor din partea și pentru persoanele autorizate din partea clientului.

Sistemele clienților în sălile de colocare sunt amplasare în rack-uri sau în dulapuri personalizate dependent de forma de colocare agreată cu clientul în contract. Accesul între sisteme fiind posibil doar prin interconectare, evitându-se conectările directe între clienți.

Accesul la datele clientului amplasate în sălile de colocare oferite de S.A. Moldtelecom, îl deține în exclusivitate clientul, responsabilitatea S.A. Moldtelecom se limitează la asigurarea condițiilor fizice de funcționare și conectare la infrastructura de rețea, fără a avea acces la sistemele sau datele clientului.

Platformele Hosting VPS/WEB și Virtual PBX ale S.A. Moldtelecom sunt concepute astfel încât datele fiecărui client sunt izolate logic de cele ale altor clienți și utilizatori, chiar și atunci când sunt stocate pe același server fizic.

Accesul la datele clienților finali de pe platformele de Hosting VPS/WEB (în cazul în care platforma reprezintă de exemplu o pagină web sau un sistem de tip client-server) este gestionat exclusiv de Client.

Accesul direct la datele clienților este restricționat, iar în cazul în care accesul este necesar, drepturile de acces și instrucțiunile de prelucrare sunt stabilite de client și aplicate numai personalului autorizat corespunzător.

**Accesul la distanță**

Accesul la consola de administrare a platformei de Hosting VPS/WEB și Virtual PBX (excepție accesul clienților la consolele și platformele proprii) este limitat exclusiv la accesul local. În cazul necesității conectării distant, accesul este asigurat prin intermediul conexiunilor securizate (VPN), cu utilizarea sistemelor de tip ”jump server” și cu documentarea logarea detaliată/suplimentară a evenimentelor și acțiunilor utilizatorului conectat.

Accesul distant la platformele clientului amplasate în sălile de colocare este gestionat exclusiv de client. Rețeaua de management a sistemelor monitorizare a sălii de colocare DataCity este o rețea închisă, accesibilă exclusiv local.

**Redundanță**

Platformele de Hosting, Virtual PBX și sălile de colocare S.A. Moldtelecom beneficiază de o infrastructură complet redundantă atât la nivel conexiune de acces la Internet, a platformelor de stocare a datelor precum și redundanță alimentare cu energie electrică.

- Redundanța infrastructurii este asigurată prin utilizarea sistemelor în ”cluster” ce asigură funcționarea platformelor chiar și în cazul ieșirii fizice din funcțiune a câtorva servere;
- Redundanța de rețea este asigurată prin canale optice diferite cu implicarea echipamentului intermedia diferit cu acces direct către furnizorii de servicii Internet mondiali.

- Redundanța alimentarii cu energie electrica este asigurata prin conectarea echipamentelor și sistemelor la cel puțin doua surse de alimentare cu energie (UPS de mare capacitate)

S.A. Moldtelecom pentru toată infrastructura critică (inclusiv sistemele Hosting VPS/WEB și Virtual PBX) efectuează backup-uri în mod regulat folosind o combinație de controale tehnice și fizice. În cazul în care sistemele de producție vor fi indisponibile, S.A. Moldtelecom va aplica procedura de recuperare pentru a restabili funcționalul sistemelor în timp util.

**Incidente**

S.A. Moldtelecom are definit un proces riguros de gestionare a incidentelor, inclusiv incidente de securitate, care pot afecta securitatea (confidențialitatea, integritatea și disponibilitatea) sistemelor sau a datelor. Incidentele care au un impact direct asupra clienților primesc cea mai mare prioritate. Programul S.A. Moldtelecom de gestionare a incidentelor de securitate este bazat pe seria de standarde ISO 27001 și include atât instrucțiuni și procese de gestionare a riscurilor și incidentelor de secretate cât și programe de control al eficienței acestora.

S.A. Moldtelecom aplică abordarea ”zero trust” care impune controale de acces la toate nivelele fiind monitorizate atât rețelele interne, cât și cele externe. Acest lucru permite administratorilor de sisteme să identifice și să reacționeze în timp util și eficient în caz de urgență.

**Registre de Audit**

S.A. Moldtelecom are implementate sisteme colectare a evenimentelor din sistemele de monitorizare a traficul intern și extern, a evenimentelor și acțiunilor angajaților asupra sistemelor de Hosting și de rețea, pentru a detecta comportamente suspecte, cum ar fi prezența traficului care ar putea indica conexiuni botnet, activități ale angajaților neordinare, activități ale aplicațiilor malefice.

Aceste instrumente, suplimentar înregistrărilor de sistem, de asemenea înregistrează în registrele de audit modificările setărilor de autorizare din procesul de gestiune a conturilor de acces.

S.A. Moldtelecom are definite și aplică proceduri de evidență a acceselor fizice în sălile de colocare, care includ registre de acces fizic, evidență evenimente sisteme de acces și misiuni de control al respectării cerințelor de securitate.

**Gestiunea securizată a inventarului**

S.A. Moldtelecom are implementate sisteme și proceduri de gestiune a inventarului software și hardware care permit identificarea și gestiunea ușoară a componentelor și sistemelor la fiecare etapă a ciclului de viață a sistemelor. De exemplu evidența și inventarierea componentelor hardware și a sistemelor fiind asigurată prin utilizarea bar-codurilor.

S.A. Moldtelecom duce evidența echipamentelor clienților amplasate în sălile de colocare dependent de tipul de colocare ales de client (colocare în rack sau în dulap propriu), pentru fiecare client fiind documentat atât tipul de echipament colocat cât și numărul de unități, amplasare, interconectare, etc. fiind asigurat un control eficient a locației echipamentului clientului și al accesului la acesta.

S.A. Moldtelecom are implementate proceduri stricte de eliminare a componentelor hardware proprii cum ar fi: ștergerea contentului de pe HDD scoase din uz sau dacă formatarea contentului nu este posibilă se aplică distrugerea fizică a componentei, astfel încât să nu fie posibilă restabilirea informației de pe ea.

Platforma de Hosting VPS/WEB și Virtual PBX S.A. Moldtelecom este implementată pe baza sistemelor de operare (OS) și softurilor cu cod deschis (open-source), dar care este actualizată și se află în continua dezvoltare din partea comunității OpenSource Internet.

**Protecția sistemelor și infrastructurii**

**Protecția Malware**

S.A. Moldtelecom are implementate sisteme și instrumente comerciale de protecție împotriva softului malefic, instrumente care permit protejarea atât a infrastructurii S.A. Moldtelecom dar și a clientului.

Cu toate acestea, dependent de platforma aleasă de client, S.A. Moldtelecom nu poate asigura protecția anti malware pentru anumit content al clientului, în speță traficul din circuitele securizate, datele criptate de pe platforma client, echipamentul clientului amplasat în sălile de colocare, echipamentul și sistemele clientului amplasate în afara zonei de protecție S.A. Moldtelecom. Pentru aceste date/sisteme clientul este singurul responsabil de asigurarea securității anti malware pe platforma sa.

**Protecția la nivel de rețea**

S.A. Moldtelecom pentru protejarea împotriva atacurilor de rețea și detectarea intruziunilor, tentativelor de acces neautorizat și inclusiv oferirea posibilității de a izola rapid sursa și zona de atac, a implementat și utilizează mai multe straturi de dispozitive și instrumente de rețea:

- sisteme și servicii de protejare Anti-DDoS:
    - Network Based Anti-DDoS – Protecție oferita implicit tuturor clienților S.A. Moldtelecom împotrivita atacurilor internaționale.
    - Dedicated Inline Anti-DDoS – Protecție pentru orice atac, la toate nivelele stivei OSI, cu filtrarea traficului pana la 1Gbps utilizînd o soluție in-line, configurată personalizat pe IP adresele clientului. Aceasta soluție este recomandată pentru clienții care doresc sa-și asigure la maxim infrastructura și asigură filtrarea traficului internațional și MDIX.

- tehnici de segregare a rețelelor și izolare a platformelor precum zone demilitarizate (DMZ) și ”boundary networks”, pentru care au fost definite reguli de control și securitate adiționale (FW-IPS).

- protecție împotriva atacurilor și tehnicilor de exploatare DNS

- sisteme de monitorizare și detecție a intruziunilor și mecanisme de detectare a intruziunilor, cum ar fi firewall-uri, utilizarea unor controale inteligente de detecție la punctele de intrare a datelor și utilizarea tehnologiilor care remediază automat anumite situații periculoase.

S.A. Moldtelecom blochează traficul neautorizat către și în centrele de date folosind o varietate de tehnologii precum firewall-uri, NAT-uri, rețele locale partiționate și separarea fizică a serverelor back-end de interfețele orientate către public.

Nivelele de securitate de nivel ]nalt, nu sunt aplicabile pentru sistemele clientului amplasate în sălile de colocare, în speță pentru sistemele interconectate prin BlackFiber sau prin circuite și canale VPN. Pentru aceste tipuri de interconectare S.A. Moldtelecom poate asigura o protecție de bază doar de nivel 2 și 3 pe stiva OSI, clientul fiind responsabil să își asigure singur securitatea de nivel înalt dependent de necesitățile și capacitățile sistemului propriu.

Clientul, pentru asigurarea unui nivel de securitate adecvat al conexiunilor internet, suplimentar protecției asigurată de S.A. Moldtelecom, poate implementa pe platforma sa orice nivel de protecție adițională precum implementarea unor ecrane de protecție proprii, criptarea datelor și a canalelor de comunicare.

**Managementul Vulnerabilităților**

S.A. Moldtelecom are implementate proceduri de management al vulnerabilităților, care permit identificarea și gestionarea breșelor și riscurilor de securitate într-un mod sigur. Regulat, cu instrumente specializate, sunt lansate scanări a nodurilor din gestiune pentru identificarea problemelor de securitate.

**Hardening**

Fiecare sistem/echipament nou ce este lansat în producție este securizat cu utilizarea tehnicilor si recomandărilor CIS și anume:

- Dezactivarea porturilor și serviciilor neutilizate,
- Protecție împotriva tentativelor de autentificare eșuate repetate,
- Filtrarea conexiunilor pe porturile de management,
- Limitarea duratei sesiunilor de acces la consola de management,
- Setarea expedierii centralizata a evenimentelor către servere dedicate (log-server),
- Etc.

**Dezvoltarea continuă**

S.A. Moldtelecom pune un accent prioritar pe calitatea și dezvoltarea serviciilor presate, de aceea la implementarea programelor de dezvoltare continuă în domeniul securității (care implică actualizarea procedurilor de reacție la incidente, dezvoltarea personalului și a sistemelor și instrumentelor tehnice utilizate), ține cont permanent de toate domeniile de activitate, de experiența cumulată (incidente și cazuri proprii, de la parteneri sau companii specializate de dezvoltare profesională), rapoartele în urma controalelor de securitate și analiza de risc.