UPNET

AUDIT A INFRASTRUCTURII IT ICS BM Technotrade SRL

Data: 27.06.23(actualizat 11.07.2025)

Efectuat de: UPNET

1. Introducere

Scopul acestui document este de a prezenta managementului Technotrade SRL rezultatul auditului infrastructurii de servere din prisma securității informaționale cît și descrierea riscurilor identificate precum și soluții de remediere a acestora.

Auditul a fost efectuat din prisma asigurării principiilor de bază a securității informaționale:

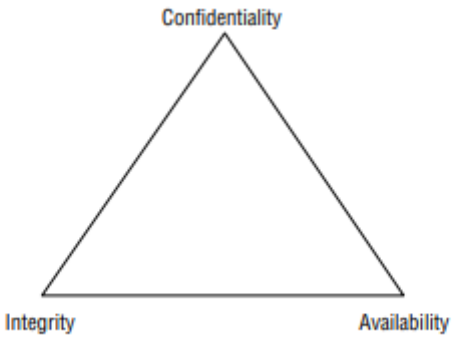


Fig 1. Triada securității informaționale.

Confidențialitate: Reprezintă principiul care trebuie să garanteze că informația este disponibilă doar persoanelor autorizate să aibă acces la ele, acest lucru se face prin mecanisme de verificare a autorizării și aplicarea procedurilor de limitare a accesului conform autorizării pe care o are utilizatorul.

Integritatea: Reprezintă pilonul care ar trebui sa garanteze ca informația este păstrată în forma sa inițiala și nu este distorsionată cumva în timpul mișcării printre sistemele informaționale, sau în timpul stocării acesteia pe servere.

Disponibilitatea: Reprezintă principiul prin care se garantează că informația este disponibilă atunci cînd este necesară și de acolo de unde este necesară.

Aceste 3 principii stau la baza fiecărei infrastructuri IT și sunt strîns legate între ele, nu pot fi aplicate mecanisme doar pe o direcție, această triadă garantează o infrastructură funcțională și securizată. Pentru fiecare principiu în parte sunt aplicate mecanisme IT de implementare a acestuia, prin aceste mecanisme această triadă este integrată în infrastructura IT.

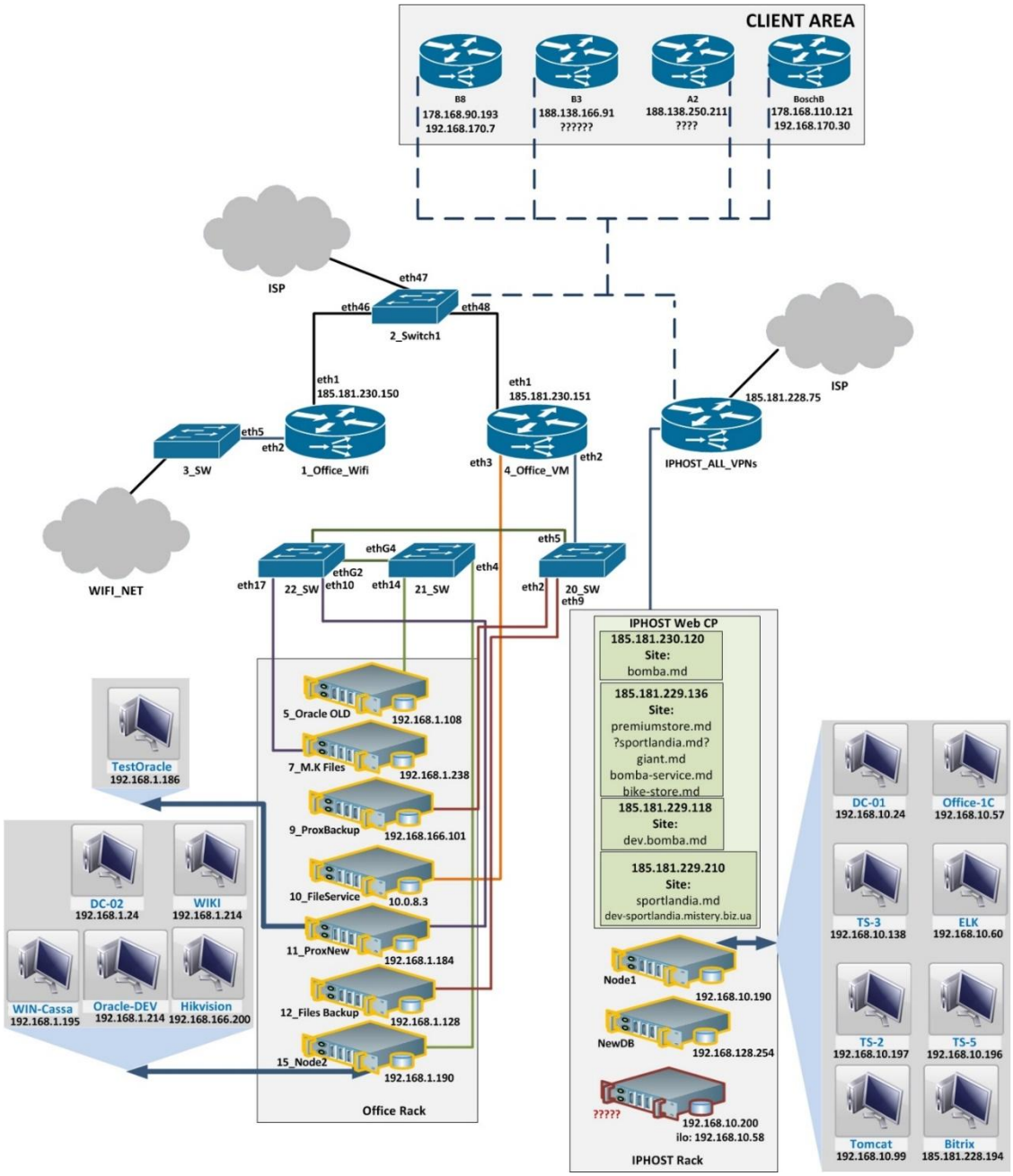
2. Rezumat

Echipa Upnet pe parcursul a cîtorva săptămîni a efectuat un audit tehnologic a infrastructurii IT a companiei Technotrade SRL.

Ca obiectiv de bază a fost evaluarea situației curente a Infrastructurii IT prin prisma tehnologiilor folosite și cum sunt astea folosite pe intern cît și care sunt riscurile aferente acestor tehnologii ce pot afecta funcționalitatea serviciilor.

Acest audit a fost împărțit în 2 componente Rețea, Server Hardware și reprezintă partea 1 de optimizare a infrastructurii, acest raport nu include o analiza.

Fig. 1. Infrastructura existentă.



2.1 Identificările auditului

Nr	Nume	Identificare	Risc	Nivelul Riscului
1. Securitatea informațională				
1.1.	Lipsa politicelor de securitate informațională	Am identificat ca în cadrul companiei Technotrade SRL nu este prezentă nici un fel de politică a securității informaționale care ar defini deciziile managementului.	Lipsa unei politici de securitate informațională poate duce la incapacitatea personalului de a estima rezultatul acțiunilor sale, care pot duce la expunerea companiei unui risc a securității informaționale.	High
1.2.	Lipsa politicii de confidențialitate semnată cu fiecare angajat	Am identificat ca in cadrul companiei nu sunt semnate careva clauze de confidențialitate	Nu exista un document juridic care să oblige angajatul ca informația confidențială a companiei sa fie păstrată confidențială	High
2. Procesele IT și probleme tehnice				
2.1.	Lipsa unui sistem de monitorizare a infrastructurii	A fost identificat ca nu este prezent nici un sistem de monitorizare a serviciilor.	In cazul in care un serviciu devine offline atunci nimeni nu va fi înștiințat	High
2.2.	Proces de backup Incomplet	Serverul Oracle nu foloseste instrument recomandat de backup RMAN, care permite backupul complet al bazelor inclusiv structura	În cazul unui incident major cu un serviciu exista riscul pierderii informației.	Critical
2.3.	Lipsa linkului de rezerva	NU exista un backup a conexiunii la internet	In cazul in care prestatorul principal de servicii are probleme atunci compania rămâne fără conexiune la internet.	High
2.4.	Folosirea unei singure subretele pentru oficiu/vpn/servere	La proiectarea rețelelor se dedica cite o subrețea si/sau Vlan pentru fiecare trafic sau scop. In cazul dat s-a folosit u singura subrețea pentru toate echipamentele absolut cu unele	Aceasta abordare este incorecta din motiv ca in așa caz compania este in primul rând lipsita de posibilitatea de a limita accesul anumitor persoane/departamente la informație, in așa caz, implicit toți au acces peste tot si la toata informația.	High

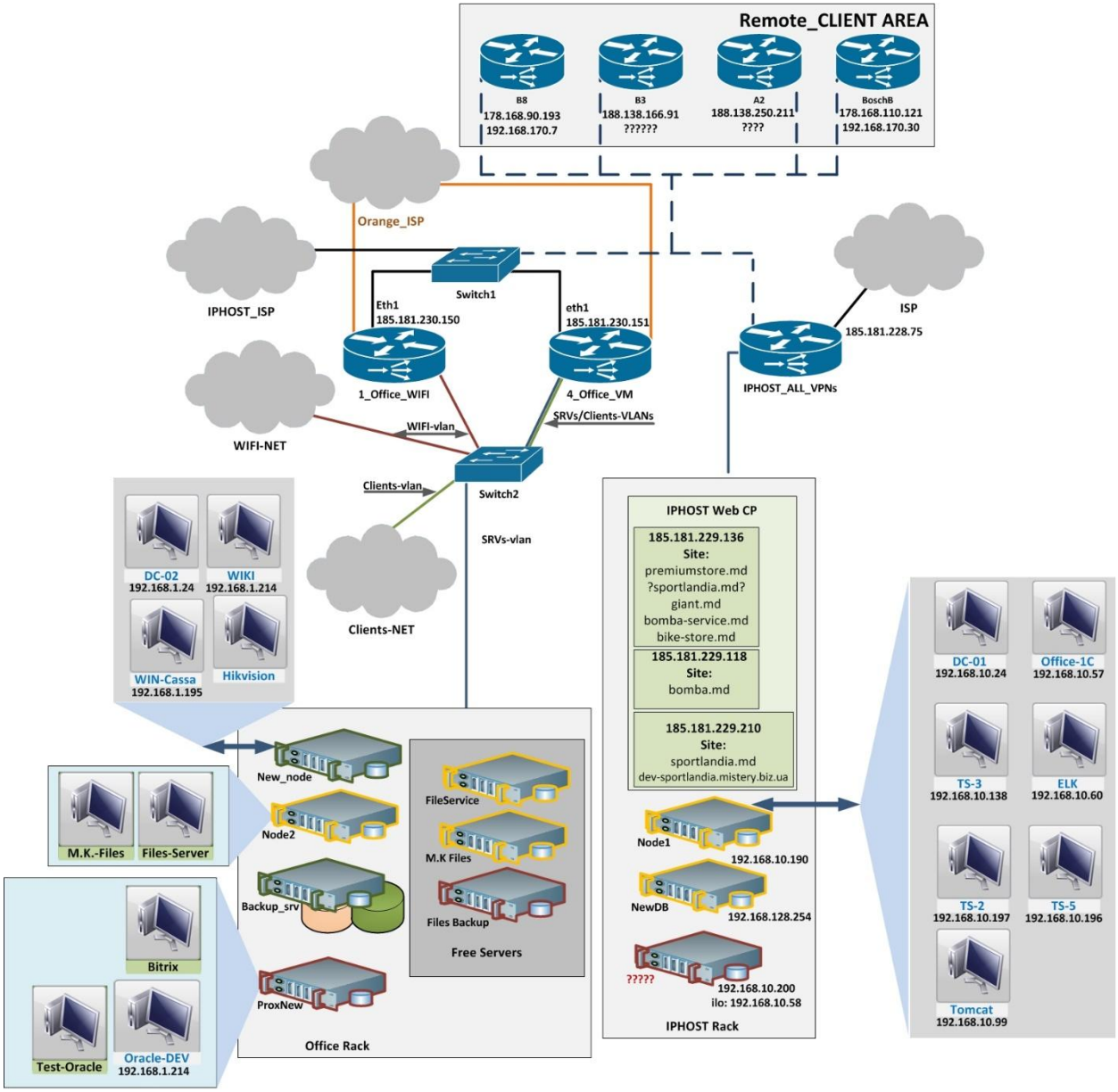
		excepții unde s-a dat acces dedicat pe rețea wireless.	De asemenea aceasta abordare este incorecta din punct de vedere a proiectării rețelelor, din motiv ca o așa subrețea duce la conflicte de IP adrese, lipsa acestora, din cauza ca subrețeaua este limitata la 253 ip adrese. Este de asemenea imposibil de a controla accesul la server si la alte resurse precum shared folders	
2.5.	Serverul fizic IPhost Proxomox Node1	Serverul are resursele la limita. Partitiile root sunt full	Pe acest server sunt păstrate mașinile virtuale ale companiei, in caz de suprasolicitare a resurselor fizice a acestui server este posibila o frinare a restul serviciilor, precum baze de date.	High
2.6.	DNS server	Serverul de domain/active directory, nu are nici o rezerva. Sunt prezente 2 servere de domain insa fiecare cu domainul sau, ele nu lucreaza ca pereche.	Serverele de domain sau active directory trebuie sa lucreze in pereche, iar in caz ca replica principala din oarecare motive este deconectata, rezerva va prelua încărcătura, astfel serviciile nu vor avea de suferit.	Medium
2.7.	Database Server	Serverul Oracle database este un single node pe care sunt hostate toate bazele de date	Serverul Oracle este unul stand alone, care hosteaza toate bazele de date, ce prezinta un risk de Single point of failure, in cazul in care acest server e afectat de un incident de natura hardware.	High
2.8.	Aplicatia back office este expusa internetului	Serverul aplicatie back office Bitrix este expus rețelei publice fara a avea o oarecare limitare cine poate accesa aceasta aplicatie.	Riscul aici îl reprezintă accesul necontrolat la aceasta aplicație. Pe lingă toate exista riscul scurgerii de informație de business prin unul din angajați care le poate ulterior preda concurenților.	High
2.9.	Conturi administrative partajate	Pe parcursul analizei am identificat faptul ca conturile administrative la toate resursele sunt partajate intre diferiți angajați conform necesităților, precum si partenerilor	Riscul aici consta in faptul ca daca un angajat a plecat, toate conturile si informația la care a avut acces trebuie blocate, însă la moment acest lucru este greu de implementat fără o modificare a proceselor de lucru a angajaților companiei, fiecare utilizator trebuie sa utilizeze contul sau personal, si in caz ca pleacă sa i se blocheze doar acel cont. Aici miza ar fi pe integrarea cu serviciile Active Directory, ce ar oferi o flexibilitate ridicata asigurând securitatea informațională.	High

2.10.	Conexiuni spre aplicație folosite incorect	Am identificat conexiuni spre server folosind ip adrese, si credențele păstrate in format text.	Se recomanda utilizarea numelor de domain in locul IP adreselor, deoarece IP adresele se pot schimba in timp. Si căutarea soluțiilor pentru autentificare aplicațiilor folosind credențele in forma criptata.	Medium
2.11.	Oficiul central VLAN	Oficiul central folosește o singura subrețea partajata cu serverele.	Aceasta implementarea plasează câteva riscuri către companie: ○ Incapacitatea de a implementa mecanisme de securitate, in a limita accesul la unele resurse pentru anumite departamente. ○ O scalabilitate scăzută, compania unde o modificare în rețea necesită o schimbare globală.	High
2.12.	Oficiul central – Layer 2 security acces	La moment nu este prezent nici un mecanism de control a cine are voie si cine nu sa se conecteze la rețeaua corporativa	Nu este posibil de restricționat accesul la rețeaua locala, astfel odată ce cineva s-a conectat la rețeaua locala folosind un cablu, are acces la toate resursele companiei.	High
2.13.	E-mail	Serverul de mail nu este configurat pentru filtrare SPAM si asigurarea livrării mesajelor	Serverul de mail este configurat pe postfix, folosind domainuri multiple. Pagina web a serverului este disponibila din internet, astfel exista un risc ridicat ca aceasta poate fi sparta si serverul de mail astfel devine compromis. Încă un mare risc aici este spamul lupta cu care prezinta un challenge, care la moment nu este abordat de postfix, in general subiectul Spamului si livrarea virusilor prin email este un risk.	**High**
2.14.	VPN	Lipsa controlului asupra conturilor de VPN	Nu exista o procedura de autorizare a conexiunilor distante, sunt o lista de conturi VPN care sunt active la moment. Însă nu exista o procedura clara de autorizare a cine are nevoie de VPN si cine nu.	Medium
2.15.	Acces Control	Lipsa unui control de acces asupra infrastructurii IT, nu este descris cine si unde ar trebui sa	Nu a fost stabilit nici un mecanism de control a accesului către resursele IT a companiei. Astfel exista riscul ridicat ca persoane neautorizate au accesul la informație	**High**

		aibă acces. Astfel la momentul dat nu este clar cine și ce nivel de acces are.	confidențială precum și riscul unei scurgeri de informație.	
2.16.	Disaster Recovery	Lipsa unui plan de rezervă a ce va trebui de făcut și cine va fi responsabil în cazul unui dezastru major, precum un incendiu, inundație sau alte calamități naturale sau umane.	Există un risc major de pierdere totală a informației și infrastructurii in cazul unui dezastru major, sau chiar a unui incident legat de cedarea unui echipament fizic.	Medium
2.17.	Web servers	Serverul care hosteaza web situl companiei bomba.md a fost de fapt Dev server	Aici exista riscul ca o buna parte din module sa fie unele experimentale, si nu-i exclus ca nu sunt necesare. Plus acest server dat fiind faptul ca anterior era preconizat pentru dezvoltare poate avea resurse la limita.	**High**

3. Plan de remediere

Fig. 2. Upgrade infrastructură



3.1. Rețea

3.1.1. Conectarea unui provider de internet adițional pentru conexiune de backup.

3.1.2. Reconfigurarea rețelei de la zero, prin aplicarea politicelor de securitate și a politicii de backup a echipamentelor care ulterior să se copie pe backup server.

- Segregarea rețelei interne prin separarea în diferite Vlanuri ce ar permite construirea unei rețele securizate prin limitarea accesului către resursele companiei.
- Revizuirea conexiunilor VPN – deconectarea celor ne folosite, și schimbarea parolelor celor existente.
- Revizuirea Firewall – firewallul la momentul de față nu protejează infrastructura nici rețeaua internă.
- Blocarea tuturor conexiunilor neautorizate către servere, aplicații web, sau interne.

3.1.3. Schimbarea tuturor parolelor, din considerente de securitate.

3.1.4. Configurarea tuturor routerelor magazinelor conform standardelor expuse și securizarea acestora prealabilă.

3.2. Infrastructura de servere

3.2.1. UPS camera de servere oficiu – procurarea unui UPS de putere nominala 3-4kw ca sa poată acoperi toată sarcina cumulativă a serverelor.

3.2.2. Backup Plan – Crearea unui Backup Plan a informației, și configurarea joburilor de copiere a copiilor de rezervă pe un server destinat acestui proces.

3.2.3. Politici de securitate – crearea politicelor de securitate care să gestioneze abordarea companiei către securitatea informațională.

3.2.4. Monitoring – configurarea monitoringului pentru toate serverele și serviciile existente.

3.2.5. Achiziția unui nod Proxmox Adițional – Acest server urmează a fi configurat ca un nou nod proxmox pe care ulterior vor fi migrate mașinile virtuale din alte noduri. Din serverul eliberat cream un server de backup a informației care ar colecta copiile de rezerva de pe toate serverele.

- Configurare proxmox
- Migrare VM de pe node2
- Upgrade Node2
- Install proxmox on node2
- Migrarea VM de pe Proxnew pe node2
- Upgrade Proxnew and și instalare proxmox
- Virtualizarea MK files pe proxnew.
- Serverul ProxBackup de facut upgrade, resetat și de configurat ca server de arhiva a datelor de pe toate serverele.

3.2.6. Upgrade Terminal Services TS 3/4/5 la windows server 2012 sau mai sus

3.2.7. Configurare domain controller – adăugarea serverelor si PC la domain, crearea utilizatorilor și configurarea stațiilor de lucru ca parte a domainului.

3.2.8. Configurarea unui backup a domain controller.

3.2.9. Integrarea file service cu Active Directory, ca fiecare utilizator să poată accesa fișierele folosind username/password din domain.

3.2.10. Configurare firewall pe fiecare server care nu îl are.

3.2.11. Proxmox node1:

- Adăugarea a min 32Gb de RAM
- Adăugarea 2xSSD 1TB pentru mașinile virtuale.
- Configurare raid utility
- Cleanup and configure Tomcat VM.

3.2.12. Oracle Server:

- Upgrade +32GB memory
- Raid Utility
- Configurarea RMAN backups

3.2.13. Mail – problema de mail este una mai specifică, din simplu motiv că lupta cu spamul și o funcționalitate mereu online a acestui serviciu nu poate fi garantată prin modul în care este gestionată la moment. Cea mai bună opțiune aici este migrarea în servicii de cloud precum Google workspace, prin această soluție se rezolvă toate problemele de mail, cît și angajații obțin accesul la instrumentele google, precum google spreadsheed (xls, care pot fi editate

concomitent de mai multe persoane), word, power point, google meet (pentru ședințe online).

3.2.14. Disaster recovery – crearea unui plan de rezervă asupra cum compania va reacționa la evenimente neașteptate precum caderea unui server, a unui link sau in general in cazuri de forță majoră precum incendii, calamități naturale sau erori umane.

4. Concluzii:

Infrastructura analizată prezintă riscuri foarte ridicare a pierderii datelor din cauza redundanței infrastructurii cît și din motivul lipsei unui proces de backup bine pus pe roate. Rețeaua internă are anumite lacune de configurare cît și nu există divizare a serviciilor/hosturile pe nivele și izolarea acestora în Vlanuri sau rețele separate.

Pe servere lipsește complet Firewalul ceea ce le face vulnerabile la atacuri externe.

Din aceste motive considerăm ca compania Technotrade SRL se afla într-o zonă de risc Foarte Ridicat în ceea ce privește disponibilitatea serviciilor/confidențialitatea datelor/ Integritatea datelor.

Vă recomandam un upgrade a infrastructurii atît din punct de vedere a rețelei cît și a serverelor.