Ministerul Educației, Culturii și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

Facultatea Calculatoare Informatică și Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

la „Managementul și auditul securității informaționale”

Lucrarea de laborator Nr. 1

A efectuat: st. gr.SI-201 Cebotari Dan

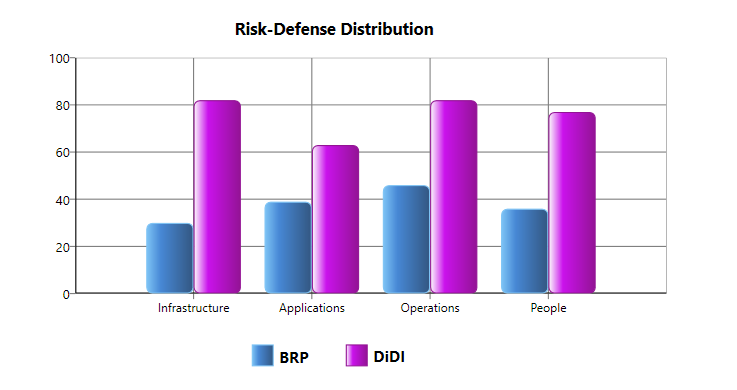
A verificat: asist. univ. Kunev I.

Chișinău 2022

În acest raport, voi analiza întreprinderea mea fictivă, numită „ITech”. Pentru el am întocmit un raport special despre datele aproximative ale unei întreprinderi IT medii în domeniul securității cibernetice. Raportul include: o comparație a riscurilor și protecției, nivelurile de securitate a infrastructurilor și a datelor personale, atât a întreprinderii, cât și a angajaților în special. Mai jos este afișat aplicația în care am făcut această analiză pe nume: *Microsoft Security Assessment Tool*.



**Fig. 1** – M.S.A.T.



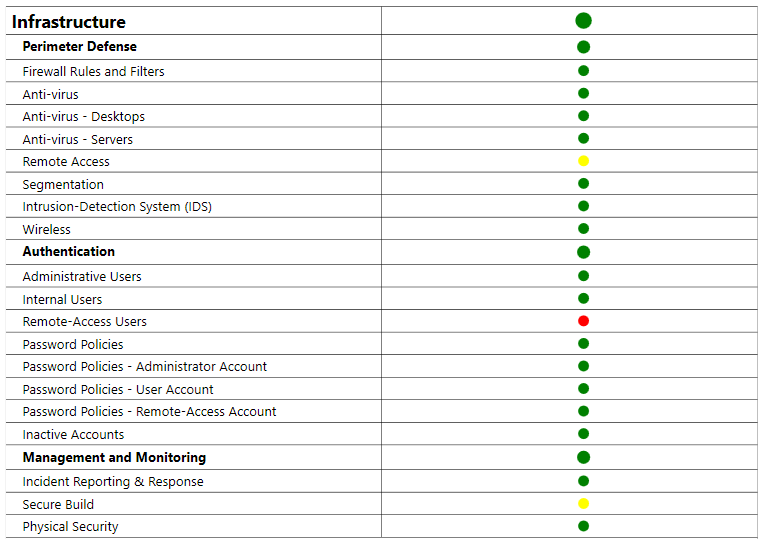
**Compararea riscului și a nivelului de protecție**

**BRP (Business Risk Profile)** variază de la 0 la 100, unde un scor mai mare implică o cantitate mai mare de risc potențial de afaceri pentru acel **AoA** (**Articles of Association**) specific. Este important de reținut că un scor de zero nu este posibil aici; desfășurarea afacerilor în sine implică un anumit nivel de risc. De asemenea, este important să înțelegeți că există unele aspecte ale conducerii unei afaceri care nu au o strategie directă de atenuare.

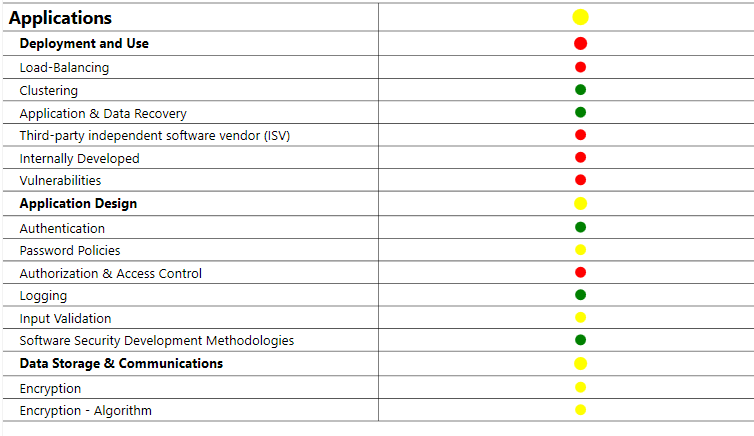
**DiDI** variază, de asemenea, de la 0 la 100. Un scor mare indică un mediu în care au fost luate un număr mai mare de măsuri pentru a implementa strategii de apărare în profunzime într-un anumit AoA. Scorul DiDI nu reflectă eficacitatea generală a securității sau chiar resursele cheltuite pentru securitate, ci mai degrabă este o reflectare a strategiei generale utilizate pentru apărarea mediului.

**Rezultatele obținute:**



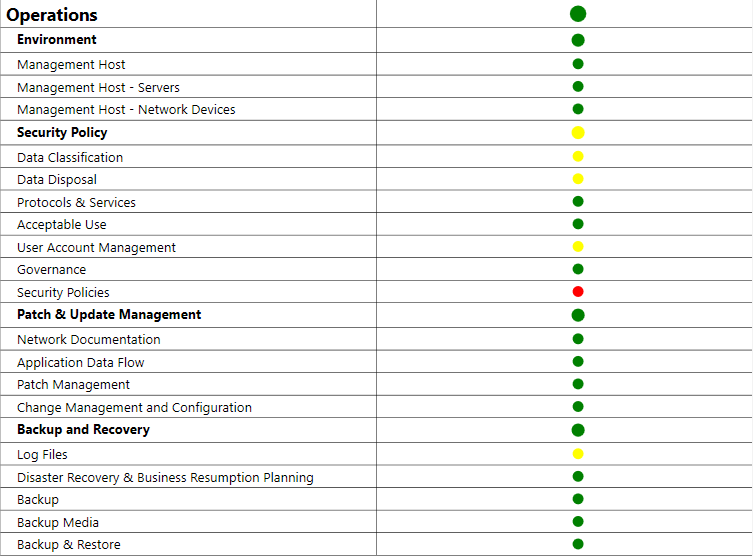


Pentru început avem datele despre securitate infrastructurei. Dupa cum vedem, analizele sunt foarte bune. Soluțiile de apărare, contul de administrator, răspunsul în timp util la apariția unei breșe de securitate și crearea de rapoarte privind problemele apărute sunt la un nivel înalt. Însă, în același timp observăm că accesul de la distanță pentru utilizatori este foarte slab și ar trebui îmbunătățit. În general: managementul și controlul, protecția prin parolă și autentificarea sunt la un nivel înalt, conexiunea remote este de nivel mediu și trebuie actualizată sau să întreprindem alte măsuri.

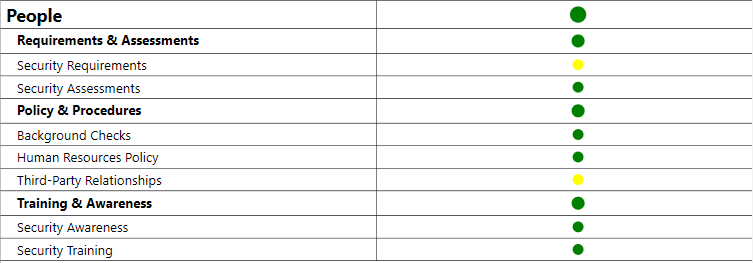


Aplicațiile utilizate de întreprindere au un rol important în securitate și confidențialitate. De exemplu, o întreprindere folosește în principal aplicații (software) de la furnizori terți, ceea ce nu garantează confidențialitatea datelor întreprinderii și ale clienților. De asemenea, recuperarea aplicațiilor și a datelor nu este configurată. Indicatorii stocării datelor criptate sunt, de asemenea, la nivel mediu. Pe lângă astea, nivelul de vulnerabilitate este la un nivel critic, ceea ce denotă faptul că trebuie de luat măsuri în cadrul schimbării procesului de securizare. Toate aceste note și evaluări se datorează următorilor factori:

* Prezența spațiilor vulnerabile în cadrul sistemului
* Să nu avem încredere în programele străine de la dezvoltatori independenți. Întreprinderea trebuie să-și dezvolte propria aplicație în rândul angajaților.
* Îmbunătățirea algoritmilor de criptare fiind la nivel mediu.



Operațiunile sunt acțiuni directe atât ale personalului, cât și ale angajaților întreprinderii în legătură cu siguranța. După cum vedem, nodurile de management atât ale serverelor, cât și ale dispozitivelor de rețea sunt foarte bine protejate, politica de securitate este la un nivel mediu, patch-urile și actualizările datelor întreprinderii au o rată ridicată. Arhivarea și restaurarea datelor la fel sunt la un nivel de securitate înalt. Există un singur lucru care ar trebui să fie îmbunătățit și acela fiind caracterizat de politicile de securitate, fiind la un nivel scăzut.



Personalul se descurcă perfect în confidențialitatea datelor. Toți angajații sunt instruiți și conștienți de posibilele amenințări care pot să apară în orice moment, precum și procedurile pentru apariția acestora sunt dezvoltate și perfecționate. Conturile angajaților care au părăsit întreprinderea sunt șterse, dar datele din cadrul companiei nu trebuie dezvăluite în niciun fel.

**Concluzie**

În această lucrare, în calitate de specialist în securitate cibernetică, am evaluat gradul de securitate și confidențialitate al datelor companiei folosind instrumentul de evaluare a securității Microsoft. Datorită interfeței ușor de utilizat, am putut înțelege rapid punctele forte și slabe ale protecției existente a companiei, precum și la ce ar trebui de lucrat și ce ar trebui să fie îmbunătățit din toate aspectele atât tehnic cât și legal. Cu ajutorul graficelor și tabelelor generate de program, precum și a unui studiu precis și amănunțit al tuturor aspectelor companiei, am putut obține o imagine completă a stării întreprinderii și a măsurilor necesare care trebuie luate.