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”

„Utilizarea instrumentului CSET Stand Alone”

Lucrarea de laborator Nr. 3

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

A verificat: asist. univ. Kunev I.

Chișinău 2022

**Conținutul raportului:**

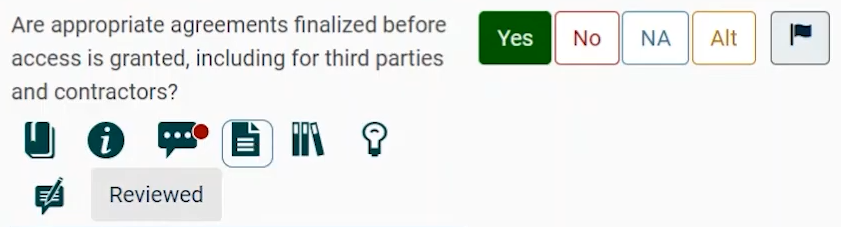
În acest raport, voi lua în considerare întreprinderea mea fictivă, numită „CibisDev”. Pentru a face acest lucru, folosesc programul CSET ediția Stand Alone (Figura 1), care analizează datele de specialitate, răspunzând la întrebări despre diverse aspecte ale securității (criptarea datelor, backup, protecție împotriva malware etc.).

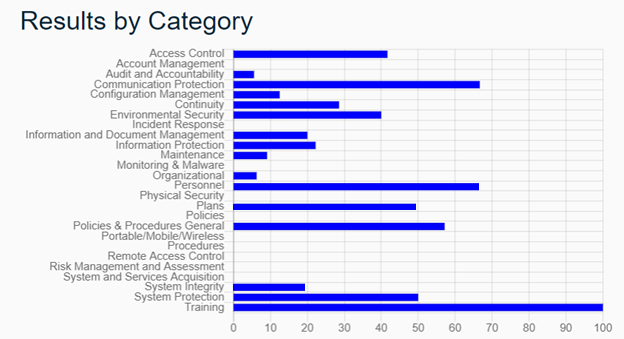


Fig. 1 – Aplicația CSET

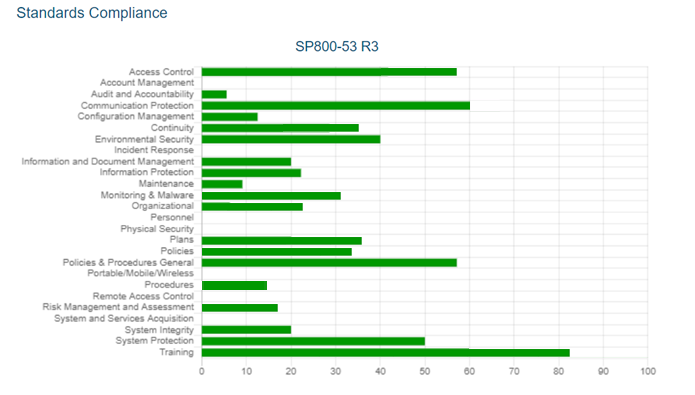
O evaluare bazată pe standarde CSET se bazează pe standarde industriale, cum ar fi seria NIST SP 800, CSF, NERC, NISTIR și alte autorități din industrie. Evaluarea examinează postura de securitate cibernetică a organizației în raport cu standardul, îi testează controalele de securitate și măsoară modul în care acestea se raportează la vulnerabilitățile cunoscute. Pot fi selectate mai multe standarde, astfel încât utilizatorul să poată facilita o combinație de standarde în timpul unei evaluări CSET.

Pentru analiza securității întreprinderii, am folosit standardul NIST SP 800. Să presupunem că mă gândesc la o afacere mică și că întreprinderea SMSI nu a fost încă planificată și configurată.





După cum puteți vedea din diagrama de mai sus, observam categorii precum managementul contului, răspunsul la incidente, monitorizare și programe malware, planuri, politici, securitate fizică și multe altele sunt complet neprotejate.



Cum poate fi corectată situația actuală? Pentru a înțelege cum trebuie să asigur securitatea fiecărei categorii neprotejate, ar trebui să parcurg prin fiecare articol:

* Account Management - controlul contului utilizatorului. Conturile foștilor angajați ar trebui șterse, exact ca toate datele lor, și ar trebui create altele noi. Specialistul trebuie să aibă acces la toate conturile, să le monitorizeze constant și să asigure confidențialitatea corespunzătoare
* Incident Response - ca răspuns la un incident, toate serviciile întreprinderii trebuie să continue să funcționeze, personalul trebuie să fie informat și pregătit pentru o astfel de situație.
* Physical Security – este necesară asigurarea protecției serviciilor la nivel fizic – răcire server, izolarea stocării datelor etc.
* Portable/Mobile/Wireless - lucrul la distanță al angajaților, acces la distanță, acces de pe dispozitive mobile, asigurând funcționarea constantă a internetului și securitatea acestuia.
* Remote Access Control - acces securizat la datele serverului, accesul utilizatorului la datele altor utilizatori printr-o rețea comună

**Concluzie:**

În această lucrare, în numele unui specialist în securitate cibernetică, am evaluat gradul de securitate și confidențialitate al datelor întreprinderii folosind aplicația CSET (Cyber ​​​​Security Evaluation Tool). După ce am răspuns la întrebări, am primit un grafic conform căruia pot observa punctele slabe ale întreprinderii, în care sunt specialist. Drept urmare, pe baza datelor primite, am notat la ce puncte trebuie acordate atenție, la ce să remediez și la ce să adăugați.