Ministerul Educației și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

Departamentul Ingineria Software și Automatică

**RAPORT**

**Lucrarea de laborator nr.6**

**la Tehnologii ale Securității Informaționale**

*Tema: Crearea politicilor de securitate bazate pe SMSI.*

Grupa academică: TI-211  
 A efectuat: Budeanu Cristian  
 Popa Cătălin

**A verificat: Răducanu Octavian**

Chișinău 2023

**Tema:** Crearea politicilor de securitate bazate pe SMSI.

**Sarcina propusă**:

**1. Stabilirea contextului organizațional**

- Definirea unei organizații ce include, numărul de angajați, departamentele, domeniul de activitate, activele, etc.

- Stabilirea persoanelor responsabile, cerințele interne și față de parteneri.

- Stabilirea domeniului de activitate și potențialii beneficiari (clienți).

- Elaborarea politicilor interne ale organizației bazate pe standardele ISO 27001.

- Roluri organizaționale, responsabilități și planificare.

**2. Gestionarea Riscului**

- Stabilirea activelor și universul supus analizei de risc

- Utilizarea unei metode de analiză a riscurilor calitativă sau cantitativă (recomandat metoda calitativă)

- Propunerea unor măsuri de control pentru diminuarea riscului

- Verificarea eficienței controalelor

**3. Realizarea SMSI**

- Utilizarea Standardelor din familia ISO 2700x precum și recomandărilor de bune practici în elaborarea sistemului de gestiune al securității informaționale.

**1. Stabilirea contextului organizațional:**

Pentru lucrarea de laborator, am creat o organizație numită SC Synergy Softworks SRL, o companie de tehnologie cu sediul în Ialoveni, Republica Moldova. Compania este specializată în furnizarea unei game largi de servicii IT, inclusiv dezvoltare de software, consultanță IT, securitate cibernetică, suport și întreținere și alte servicii.

Compania a fost fondată în 2022 și de atunci și-a consolidat poziția pe piața locală, devenind un jucător de încredere prin furnizarea de soluții inovatoare și satisfacerea nevoilor clienților. Împreună cu echipa noastră talentată de specialiști IT, Synergy Softworks SRL oferă fiecărui client soluții personalizate, adaptate nevoilor și obiectivelor sale specifice.

Politica internă a companiei se concentrează pe asigurarea securității și confidențialității datelor clienților și se bazează pe standardul ISO 27001. Synergy Softworks SRL are o echipă dedicată de experți în securitate cibernetică care monitorizează constant amenințările și vulnerabilitățile și implementează măsuri avansate de securitate pentru a preveni incidentele de securitate.

Cu 70 de angajați, Synergy Softworks SRL are divizii specializate în dezvoltare de software, consultanță IT, securitate cibernetică și suport tehnic. Portofoliul de clienți al companiei se întinde pe o gamă largă de industrii, inclusiv bancar, asistență medicală și retail.

Synergy Softworks SRL se concentrează pe îmbunătățirea continuă a serviciilor și satisfacția clienților. Synergy Softworks SRL își propune să fie un partener de încredere pentru clienții săi și un jucător major pe piața de tehnologie a Moldovei și a regiunii, oferind soluții personalizate, de înaltă calitate și de înaltă performanță.

**2. Gestionarea Riscului:**

Compania Synergy Softworks SRL, este o organizație puternică, care se bazează pe suportul clienților și îmbunătâțirea serviciilor, dar pe lângă acestea, are și careva dezavantaje. Compania este noua și nu are multa experiență, a angajat mult personal și s-a implicat în multe proiecte, crezând că aceasta le vă ajuta la dezvoltare și obținerea unui venit valoros. De asemenea, compania întâmpină greutăți legate de baza de date, deoarece având puțin timp la dizpozitie, nu au reușit să creeze o baza de date bine stabilita și clasificata corespunzător. Respectiv noii utilizatori, dar și cei vechi, deseori întâmpină erori la autentificare sau alte procese legate de sistem. Pe lângă aceasta, având un buget mic inițial, compania s-a stabilit într-un bloc vechi, care nu suporta internet de viteza înalta, precum și deseori se confrunta cu probleme electrice, și sunt uneori în pană de curent. Respectiv, are loc pierderi de date și căderi sistematice de sistem. Pe lângă acestea, serverele companiei se afla în subsol, deoarece doar acolo este aerul rece, iar compania nu își permite alte sisteme de răcire. Din cauza aceasta, pe timp de ploaie, deseori se întâmplă și inundații mici în subsol, care duc la deconectări electrice și defectare de dispozitive importante. De asemenea, compania întâmpină greutăți cu criptarea datelor. A fost procurat un sistem de criptare puternic, dar instalarea lui incorecta la fel a dus la o eficienta mica și furt de date. Persistă, la fel, și probleme de securitate, deoarece compania nu are un sistem bine stabilit și instalat, foarte des au loc atacuri malware și furt de date. Compania a încercat până la moment să rezolve aceste probleme cât mai ieftin și rapid, dar aceasta nicicum nu îi ajuta, deoarece sau lucrul este efectuat de lucrători necalificați sau lucrul este realizat rapid și incorect.

Determinarea elementelor-cheie care constituie activele și universul analizei de risc într-o companie implică identificarea și evaluarea valorilor și vulnerabilităților potențiale asociate afacerii. Prin acest proces, compania poate înțelege și gestiona în mod eficient riscurile asociate acestor active. Apoi, urmează analiza de risc, care constă în evaluarea amenințărilor și vulnerabilităților potențiale ce pot afecta aceste active. Scenariile de risc pot include situații precum incendii, atacuri cibernetice, fraude sau alte evenimente neprevăzute. Identificarea activelor este prezentată în tabelul 1.

Scopul acestei analize este de a permite companiei să se reorganizeze în plan tehnic și securitate. Aceasta îi vă ajuta la menținerea forțelor de munca și atragerea de noi utilizatori. Schimbările ar putea include în primul rand găsirea unui nou loc de oficiu, unde este pofibilitate de a avea internet puternic și alte necesitați importante. De asemenea gestionarea corecta a forței de munca, precum și accentuarea muncii pe necesitățile clienților, dar nu pe venitul banilor.

**Tabelul 1.** Identificarea activelor companiei Synergy Softworks SRL.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Acțiune**  **(Resurse)** | **Atacuri malware** | **Cadere de tensiune** | **Probleme acces** | **Pierderi de date** | **Distrugeri și pagube** | **Instalare** | **Furt de date** | **Impact rezultat** |
| **Servere** |  | mediu, 3 |  |  | mediu, 3 |  |  | 6 |
| **Cladiri** |  |  |  |  | foarte scăzut, 1 |  |  | 1 |
| **Bazele de date** |  |  | foarte scăzut, 1 | scăzut, 2 |  |  |  | 3 |
| **Personalul** |  |  | mediu, 3 |  | ridicat, 4 |  |  | 7 |
| **Sisteme de criptare** |  |  |  |  |  | scăzut, 2 | scăzut, 2 | 4 |
| **Securitate** | scăzut, 2 |  |  |  |  |  | scăzut, 2 | 4 |
| **Serviciile acordate** |  |  | scăzut, 2 |  |  |  | mediu, 3 | 5 |
| **Total** | 0.1 | 0.5 | 0.3 | 0.3 | 0.44 | 0.3 | 0.37 | 0.33/29 |

Probabilitatea de apariție Synergy Softworks SRL: Impact:

**Foare scăzut** – (0%-20%) – prezenta neglijabila S-a intamplat o singura data in ultimii 3 ani, 1 – impact ( 1000 $ ),

**Scăzut** –(20%-40%) – prezenta putin probabila s-a intamplat 2-3 in ultimii 3 ani, 2 – impact minor ( 2000$ ),

**Mediu** - (40%-60%) – prezenta probabila S-a intamplat peste 5 ori in ultimii 3 ani, 3 – impact moderat ( 3500$ ),

**Ridicat** - (60%-80%) - prezenta foarte probabila Se intampla anual, 4 – impact considerabil ( 6000$),

**Foarte ridicat** – (80%-100%) - Se intampla cel putin o data la 3 luni. 5 – impact major ( 20000$ ).

**Pagube:**

Impact bugetar – 29 ~ 33000 $ Risc = 0.33 \* 29 \* 10 = 95.7

Valoarea maximă a riscului = 150

Valoarea nivelului de risc acceptat de organizație 50.

Orice risc sub această valoare este asumat de organizație.

Iată câteva exemple de măsuri de control pe care compania le poate utiliza pentru îmbunătățire:

1. Amplasarea incorectă – în primul rând, ce-l mai important este necesitatea de a schimba locația serverelor,, cu o încăpere mai mare. Unde nu au loc căderi de tensiune și probleme de inundații și este bine răcită.
2. Filtrarea proiectelor – implicarea în multe proiecte, fără cunoașterea sigură a succesului lor, s-a dovedit a fi o idee rea, respectiv este nevoie de a analiza mai întâi complex orice proiect în care compania se implică și mai bine să investești într-o compania bună, decât în multe și fără avantaje.
3. Actualizarea bazei de date – acest pas va îmbunătăți viteza de adăugare a clienților noi, precum și eliminarea problemei de autentificare.
4. Accesul la rețea – internetul este cel mai important pentru o companie respectivă, astfel este nevoie de cea mai mare viteză a lui.
5. Camera pentru servere – pentru o securitate corespunzătoare, serverele au nevoie de o încăpere specială, cu ventilare și sisteme de răcire.
6. Criptarea datelor – având un sistem puternic de criptare, este nevoie și de folosirea lui corespunzătoare. Respectiv, este nevoie de un specialist, care va configura corect sistemul de criptare a datelor, pentru a avea toată informația și transferul de date în securitate.
7. Securitate – un punct la fel de important, este securitate. Este nevoie de un sistem de securitate mai dezvoltat , care poate pune față la orice atac sau furt de date.

**Concluzii:**

În concluzie, raportul evidențiază importanța stabilirii contextului organizațional pentru o gestionare eficientă a securității informaționale. Prin definirea organizației, inclusiv a numărului de angajați, departamentelor, domeniului de activitate și a activelor, precum și prin stabilirea persoanelor responsabile și a cerințelor interne și față de parteneri, se poate obține o înțelegere mai clară a mediului în care organizația operează. Elaborarea politicilor interne ale organizației bazate pe standardele ISO 27001 asigură o abordare coerentă și consistentă a securității informaționale în cadrul organizației, contribuind la protejarea activelor și reducerea riscurilor. Gestionarea riscului, prin stabilirea activelor și a universului supus analizei de risc, utilizând o metodă de analiză calitativă sau cantitativă, permite identificarea și evaluarea riscurilor asociate securității informaționale. Propunerea măsurilor de control pentru diminuarea riscului și verificarea eficienței acestor controale asigură un nivel adecvat de protecție a informațiilor și a sistemelor organizației. Realizarea sistemului de gestiune a securității informaționale (SMSI) prin utilizarea standardelor din familia ISO 2700x și a recomandărilor de bune practici reprezintă un pas esențial în direcția asigurării securității informaționale în organizație. Aceasta oferă un cadru structurat și documentat pentru implementarea și menținerea unui nivel adecvat de securitate a informațiilor, protejând astfel organizația împotriva amenințărilor și riscurilor în domeniul informațional. Prin urmare, este recomandată adoptarea și implementarea acestor măsuri și practici în cadrul organizației pentru a se asigura un nivel înalt de securitate informațională și protecție a activelor organizaționale.

**Anexe:**

**1.**      **Manualul SMSI 27001,** [Resursă electronică]: [SMSI 27001](https://docs.google.com/document/d/1MJnmw6kkWNcAKIDmD01_sPMT59h3Sk9-/edit)