Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

**Raport**

la Managementul și Auditul Securității Informaționale

*Tema: „Metodologia Microsoft”*

Efectuat: st.gr. SI-201 Cebotari Dan

st.gr. SI-201 Roman Nicoleta

A verificat: lect.univ. Bulai Rodica

|  |  |
| --- | --- |
| ***Asset Name*** | ***Asset Classification (High, Medium, or Low Business Impact)*** |
| 1. ***Work Station*** | ***Mediu*** |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Defense-in-Depth**  **Layer** | **What You Are Afraid of or Are Trying to Avoid:**  **(Threats)** | **How It May Happen:**  **(Vulnerabilities)** | **Exposure Level (H,M,L)** | **Current Controls Descriptions** | **Probability (H,M,L)** | **Control Concerns, Potential New Controls** |
| Physical | Acces liber, defectarea intentionata PC, utilizarea necorespunzatoare a angajatilor nepregatiti. | Permiterea utilizarii calculatoarelor personale (nonorganizationale) | Mediu | Impartirea statiilor dupa destinatie/sectii in incaperi individuale | Mediu | Elaborarea unei politici stricte in baza contractelor. |
| Application | Virusi, Troieni, utilizarea irationala a resurselor. | Aplicatii netestate , posibilitatea de butare de pe oricare dispozitiv periferic | Mediu | folosirea programelor din surse nesigure, | Mediu | Procurarea programelor licentioate in baza unor contracte, evitarea utilizarii suportuerilor de stocare personale. |
| Network | Exploatarea neautorizata a canalelor | Porturi libere, deschise | Mediu | Utilizarea scanerelor de retea | Mediu | Configurarea avansata a scanerelor. |
| Data | Interceptarea pachetelor de date. | Utilizarea dispozitivelor periferice de stocare | Jos | Utilizarea accounturilor de utilozator cu parola | Mediu | Aplicarea unei politici avansate de parole |

|  |  |
| --- | --- |
| ***Asset Name*** | ***Asset Classification (High, Medium, or Low Business Impact)*** |
| ***2. Sistema de operare (OS)*** | ***Mediu*** |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Defense-in-Depth**  **Layer** | **What You Are Afraid of or Are Trying to Avoid:**  **(Threats)** | **How It May Happen:**  **(Vulnerabilities)** | | **Exposure Level (H,M,L)** | **Current Controls Descriptions** | **Probability (H,M,L)** | | **Control Concerns, Potential New Controls** |
| Physical | Deterioararea cablurilor, plug-urilor și conectorilor. | Lipsa echipamentuli anti-incendiu, lipsa echipamentelor de rezerva in caz de deteriorare | | Inalt | Aducerea la cunostina administratiei despre starea monitorului | Mediu | | Cumpararea echipamentelor de rezervă. |
| Application | SO neestetic, puncte slabe ale sistemului | Folosirea actualizărilor vechi a SO | | Înalt | Accesarea periodică a actualizărilor | Mediu | | Imbunatatirea configuratiei. |
| Network | Conectarea neautorizata. | Porturi libere | | Jos | Utilizarea unui model avansat | Mediu | | Configurarea avansată |
| ***Asset Name*** | | | ***Asset Classification (High, Medium, or Low Business Impact)*** | | | |
| ***3. Router*** | | | ***Inalt*** | | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Defense-in-Depth**  **Layer** | **What You Are Afraid of or Are Trying to Avoid:**  **(Threats)** | **How It May Happen:**  **(Vulnerabilities)** | **Exposure Level (H,M,L)** | **Current Controls Descriptions** | **Probability (H,M,L)** | **Control Concerns, Potential New Controls** |
| Physical | Conectarea neautorizata la porturile fizice | Acces liber la dispozitiv. | Mediu | Rezervam adrese dupa MAC. | Inalt | Amenajarea unui loc sigur pentru aplsare |
| Application | Exploatarea punctelor slabe a SO | SO mai veche | Inalt | x x x | Medie | Instalarea unui SO nou |
| Network | Atac de retea (Ddos, MITM) ,caderea retelei. | Configurare incompleta a routerului. | Mediu | Limitarea folosirii capacitatii benzii. | Jos | Cumpararea unui model de router mai avansat. |
| Data | Deteriorarea logurilor | Lipsa unei copii de rezerva logurilor, stergerea logurilor anterior mai vechi. | Mediu | Monitorizarea evenimentelor | Jos | Redirectionarea logurilor vechi pe server. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | ***Impact Rating Reference*** | | |
| **Asset Class** | **HBI** | Moderate Impact | High Impact | High Impact |
| **MBI** | Low  Impact | Moderate Impact | High Impact |
| **LBI** | Low  Impact | Low  Impact | Moderate Impact |
|  |  | **Low** | **Medium** | **High** |
|  |  | **Exposure Level** | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Information Collected During Data Gathering Process** | | | | | | | |
| **Asset** | | | | **Exposure** | | | |
| **Date Identified** | **Asset Name/Desc.** | **Asset Class** | **Applicable Defense-in-Depth  Layer(s)** | **Threat Description** | **Vulnerability Description** | **Exposure Rating (H,M,L)** | **Impact Rating (H,M,L)** |
| Data | Work Station | Impact Înalt (HBI) | Physical, Application, Host, Network, Data | Acces liber, introducerea virusilor, troienilor,  exploatarea neautorizata,  modificarea pachetelor de date. | Permiterea utilizarii calculatoarelor personale (nonorganizationale)  Porturi libere, deschise  Utilizarea dispozitivelor periferice de stocare | Mediu | Mediu |
| Data | Sistema de Operare | Impact Mediu (HBI) | Physical, Application, Host, Network, Data | Conectarea utilajului neautorizata la porturile fizice, deteriorarea plug-urilor | Acces liber la dispozitiv,  SO neactualizat, introducerea dispozitivelor neutorizate în porturi | Mediu | Mediu |
| Data | Router | Impact Jos (LBI) | Physical, Application, Host, Network, Data | Distrugerea echipamentului, tastelor | Acces liber la dispozitiv,  Configurare incompleta a routerului. | Mediu | Inalt |

|  |  |  |
| --- | --- | --- |
| ***Probability Rating Reference*** | |  |
| **Qualitative Rating** | **Description** | |
| High | Likely, one or more impacts expected within one year | |
| Medium | Probable, impact expected within two to three years | |
| Low | Not probable, impact not expected to occur within three years | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | ***Summary Level Risk Rating*** | | |
| **Impact  (from Impact Table above)** | **High** | Moderate Risk | High Risk | High Risk |
| **Med** | Low  Risk | Moderate Risk | High Risk |
| **Low** | Low  Risk | Low  Risk | Moderate Risk |
|  |  | **Low** | **Medium** | **High** |
|  |  | **Probability Value** | | |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Information Collected During Data Gathering Process*** | | | | | | | |  |  |
| **Asset** | | | | **Exposure** | | |  |  |  |
| **Date Identified** | **Asset Name** | **Asset Class** | **Applicable Defense-in-Depth Layer(s)** | **Threat Description** | **Vulnerability Description** | **Exposure Rating (H,M,L)** | **Impact Rating (H,M,L)** | **Probability  (H,M,L)** | **Summary Risk  Level (H,M,L)** |
| Data | Work Station | Impact Înalt (HBI) | Physical, Application, Host, Network, Data | Acces liber, introducerea virusilor, troienilor,  exploatarea neautorizata,  modificarea pachetelor de date. | Permiterea utilizarii calculatoarelor personale (nonorganizationale)  Aplicatii netestate , posibilitatea de butare de pe oricare dispozitiv periferic  Drepturi importante pentru functionari, lipsa configurarilor dedicate de firewall in domeniu | Mediu | Mediu | Mediu | Mediu |
| Data | Sistema de Operare | Impact Mediu (MBI) | Physical, Application, Host, Network, Data | Acces liber la dispozitiv  Acces ilegal a personelor neautorizate | SO neactualizat, introducerea dispozitivelor neutorizate. | Inalt | Inalt | Inalt | Inalt |
| Data | Router | Impact Jos (LBI) | Physical, Application, Host, Network, Data | Conectarea neautorizata la porturile fizice  Exploatarea punctelor slabe a SO  Atac de retea (Ddos, MITM) ,caderea retelei | Acces liber la dispozitiv,  Configurare incompleta a routerului.  Lipsa unei copii de rezerva logurilor, stergerea logurilor anterior mai vechi | Mediu | Inalt | Mediu | Inalt |

|  |  |
| --- | --- |
| **Exposure Rating** | **Confidentiality or Integrity of Asset** |
| 5 | Severe or complete damage to asset, e.g. externally visible and affects business profitability or success |
| 4 | Serious but not complete damage to asset, e.g. affects business profitability or success, may be externally visible |
| 3 | Moderate damage or loss, e.g. affects internal business practices, causes increase in operational costs or reduction of revenue |
| 2 | Low damage or loss, e.g. affects internal business practices, cannot measure increase in costs |
| 1 | Minor or no change in asset |

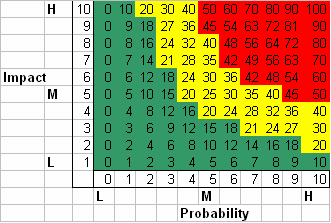
|  |  |  |
| --- | --- | --- |
| **Exposure Rating** | **Availability** | **Description** |
| 5 | Work stoppage | Substantial support costs or business commitments canceled. |
| 4 | Work interruption | Quantifiable increase in support costs or business commitments delayed. |
| 3 | Work delays | Noticeable impact to support costs and productivity. No measurable business impact. |
| 2 | Work distraction | No measurable impact, minor increases in support or infrastructure costs. |
| 1 | Absorbed by normal business operations | No measurable impact to support costs, productivity, or business commitments. |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Baseline Risk (Current)** | | | | | | | | | |
| **Asset** | | **Exposure** | | | |  |  |  |  |
| **Asset Name** | **Impact Class Rating (V)** | **Defense in Depth Layer** | **Threat Description** | **Vulnerability Description** | **Exposure Rating (1-5)**  **(EF)** | **Impact Rating (1-10)**  **IR=(V \* EF)/5** | **Current Controls Description** | **Probability Rating w/Control**  **(PR) (1-10)** | **Risk Rating w/Control (0-100)**  **(IR\*PR)** |
| *Description of digital asset to business.* | *Impact Class* | *Technical area(s) where exposure occurs* | *Storyline of what threat you are afraid of or are trying to avoid* | *Storyline of how a threat may occur* | *Exposure Rating* | *The level of damage to the asset through the defined exposure.* | *Impact occurring.* | *Probability of the exposure succeeding to impact the asset with current controls* | *Product of impact and probability rating.* |
| Work Station | 10 | Physical, Application, Host, Network, Data | Acces liber, introducerea virusilor, troienilor,  exploatarea neautorizata,  modificarea pachetelor de date. | Permiterea accesării serverului de catre persoanele neautorizate (nonorganizationale),  aplicatii netestate , lipsa configurarilor | 5 | 10 | Utilizarea unei politici de securitate.  Utilizarea accounturilor de utilozator cu parola | 9 | 90 |
| OS | 5 | Physical, Application, Host, Network, Data | Acces liber la sistem. Exploatarea punctelor slabe a SO | SO neactualizat, introducerea dispozitivelor neutorizate în porturi | 4 | 4 | Rezervăm și încărcăm în memoria RAM a calculatorului.  Menținem securitatea și drepturile de acces ale utilizatorilor. | 6 | 24 |
| Router | 3 | Fizic, aplicatie, retea, data | Conectarea neautorizata la porturile fizice  Atac de retea (Ddos, MITM) ,caderea retelei.  Deteriorarea logurilor | Acces liber la dispozitiv.  SO mai veche  Configurare incompleta a routerului.  Lipsa unei copii de rezerva logurilor, stergerea logurilor anterior mai vechi. | 3 | 6 | Rezervam adrese dupa MAC.  Limitarea folosirii capacitatii benzii.  Monitorizarea evenimentelor | 6 | 36 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Impact rating \* Probability rating = Risk Level** |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **Impact Rating Ranges** | | **\*** | **Probability Ranges** |  | **Overall Risk Rating** | **Risk level** |
| High | 10 -- 7 |  | 10 -- 7 |  | High | 41-100 |
| Medium | 6 -- 4 |  | 6 -- 3 |  | Medium | 20-40 |
| Low | 3 -- 0 |  | 3 -- 0 |  | Low | 0-19 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualitative Rating** | **Description** | **ARO Range** | **Description Examples** |
| High | Likely | >= 1 | Impact once or more per year |
| Medium | Probable | .99 to .33 | At least once every 1-3 years |
| Low | Not probable | < .33 | Less frequent than every 3 years |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Impact Class** | **Impact Class  Value (V)** |  |  |  |
| HBI | 10 |  |  |  |
| MBI | 5 |  |  |  |
| LBI | 2 |  |  |  |
|  |  |  |  |  |

******

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Exposure Factor Rating** | **Exposure  Factor (EF)** | **Impact Rating (V \* EF)** | **Impact Range** | **Summary Level Comparison** |
| 5 | 100% |  | 7 - 10 | High |
| 4 | 80% |  | 4 - 6 | Medium |
| 3 | 60% |  | 0 - 3 | Low |
| 2 | 40% |  |  |  |
| 1 | 20% |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| High Business Impact Value **= $10000** |  |  | **Exposure  Rating** | **Exposure Factor %** |
|  |  | 5 | 100 |
| **Asset Class** |  | 4 | 80 |
| HBI Value | 10000 lei | 3 | 60 |
| MBI Value | 5000 lei | 2 | 40 |
| LBI Value | 2000 lei | 1 | 20 |
| **Estimated Risk Value =** | Asset Class Value \* Exposure Factor % = SLE |  | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risk Description** | **Asset Class Value** | **Exposure Rating** | **Exposure Value** | **SLE** | **ARO** | **Quantitative Estimate (ALE=SLE\*ARO)** |
| Work Station | 10000 lei | 4 | 80 % | 8000 lei | 0.5 | 4000 lei |
| OS | 10000 lei | 3 | 60 % | 6000 lei | 0.5 | 3000 lei |
| Router | 2000 lei | 1 | 20% | 400 lei | 0.5 | 200 lei |

Calcule:

SLE = (10000\*80)/100 = 8000;

ALE = 8000\*0.5 = 4000