Tema 10 Managementul riscurilor

**Pasul 1: Identificarea activelor**

| **Nr.** | **Activ** | **Clasificare** | **Categorie** | **Descriere** | **Proprietar** | **Locație** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Sistemul ERP | Critic | Software | Gestionează producția, achiziții, finanțe | Departament IT | Sala serverelor |
| 2 | Sistemul MES | Critic | Software | Controlează procesele/echipamentele de producție | Departament Producție | Spații producție |
| 3 | Site-ul web public | Important | Software | Platformă prezentare companie | Departament Marketing | Furnizor hosting |
| 4 | Sistemul de e-mail | Critic | Software | Comunicare internă și externă | Departament IT | Infrastructură cloud |
| 5 | Sistemul SCM | Critic | Software | Gestionează lanțul de aprovizionare | Departament Logistică | Sala serverelor |

**Pasul 2: Analiza amenințărilor și vulnerabilităților**

| **Activ** | **Amenințări principale** | **Sursă (I/E)** | **Vulnerabilități identificate** | **Control existent** | **Instrument scanare/analiză** |
| --- | --- | --- | --- | --- | --- |
| Sistemul ERP | Ransomware, acces neautorizat, sabotaj | E/I | Software neactualizat, parole slabe | Firewall, backup | Nessus, audit intern |
| Sistemul MES | Defect hardware, manipulare date, sabotaj | I | Lipsă redundanță, control acces slab | Mentenanță, acces controlat | Audit manual |
| Site-ul web public | DDoS, defacement, injectare cod | E | Configurare slabă, lipsă WAF | CDN basic, backup | OpenVAS, pentest extern |
| Sistemul de e-mail | Phishing, spoofing, malware | E | Filtre anti-spam insuficiente, 2FA lipsă | Antivirus, filtre spam | Simulare phishing, scanare email |
| Sistemul SCM | Interceptare date, falsificare comenzi | E/I | Lipsă criptare, acces excesiv | VPN, autentificare | Nessus, audit acces |

**Pasul 3: Evaluarea riscurilor**

| **Activ** | **Amenințare principală** | **Probabilitate (S/M/R)** | **Impact (S/M/R)** | **Nivel risc (S/M/R)** | **Acceptabil? (Da/Nu)** | **Decizie (Accept/Tratare)** |
| --- | --- | --- | --- | --- | --- | --- |
| Sistemul ERP | Ransomware | Medie | Ridicat | Ridicat | Nu | Tratare |
| Sistemul MES | Defect hardware | Scăzută | Mediu | Mediu | Da | Accept |
| Site-ul web public | DDoS | Ridicată | Scăzut | Mediu | Da | Accept |
| Sistemul de e-mail | Phishing | Ridicată | Ridicat | Ridicat | Nu | Tratare |
| Sistemul SCM | Falsificare comenzi | Medie | Ridicat | Ridicat | Nu | Tratare |

**Pasul 4: Elaborarea strategiei de atenuare**

| **Activ** | **Măsuri tehnice propuse** | **Măsuri administrative propuse** | **Măsuri fizice propuse** |
| --- | --- | --- | --- |
| Sistemul ERP | IPS, backup automat, patch management | Politici acces, audit lunar | Acces fizic controlat la servere |
| Sistemul MES | Redundanță hardware, segmentare rețea | Proceduri urgență, training personal | Acces fizic restricționat la utilaje |
| Site-ul web public | WAF, monitorizare trafic, backup | Politici publicare, audit trimestrial | N/A (la furnizor) |
| Sistemul de e-mail | DMARC, filtre avansate, 2FA | Politici anti-phishing, training | N/A |
| Sistemul SCM | VPN, criptare date, patch management | Politici acces, audit lunar | Acces fizic controlat la servere |

**Pasul 5: Implementare și monitorizare**

| **Activ** | **Măsuri implementate** | **Responsabil** | **Termen finalizare** | **Monitorizare/Evaluare** | **Risc rezidual** |
| --- | --- | --- | --- | --- | --- |
| Sistemul ERP | Backup, IPS, patch management | Departament IT | 3 luni | Teste backup, revizuire loguri | Scăzut |
| Sistemul MES | Redundanță, segmentare | Dep. Producție/IT | 2 luni | Test failover, audit acces | Scăzut |
| Site-ul web public | WAF, backup, monitorizare | Dep. Marketing/IT | 1 lună | Monitorizare uptime, test penetrare | Scăzut |
| Sistemul de e-mail | 2FA, filtre, DMARC | Departament IT | 1 lună | Simulare phishing, audit loguri | Mediu |
| Sistemul SCM | VPN, criptare, patch management | Dep. Logistică/IT | 3 luni | Test criptare, audit acces | Scăzut |

**Pasul 6: Instruirea personalului**

| **Activ** | **Subiect training principal** | **Grup țintă** | **Frecvență** | **Metodă evaluare** |
| --- | --- | --- | --- | --- |
| Sistemul ERP | Securitate acces, parole, phishing | Utilizatori ERP/IT | Semestrial | Test online, simulare |
| Sistemul MES | Proceduri urgență, acces control | Personal producție | Anual | Test practic |
| Site-ul web public | Politici publicare, recunoaștere atacuri | Marketing/IT | Anual | Test online |
| Sistemul de e-mail | Phishing, parole, atașamente periculoase | Toți angajații | Trimestrial | Simulare phishing |
| Sistemul SCM | Acces date, bune practici securitate | Logistică/IT | Semestrial | Test online |