Managementul riscurilor tema capitol 5. Evaluare succintă a riscurilor pentru start-up-ul IT „InnoTech”

**1. Descrierea mediului intern și extern**

**Mediul intern:**

* Start-up IT cu 50 angajați în București, focusat pe dezvoltarea unei platforme cloud pentru managementul proiectelor.
* Cultura orientată spre inovație, dar cu resurse limitate în securitate IT.
* Infrastructură cloud în creștere, cu echipă tehnică dedicată, dar fără departament IT securitate dedicat încă.

**Mediul extern:**

* Piață competitivă, cu presiune pe securitatea datelor clienților.
* Reglementări stricte GDPR pentru datele europene.
* Amenințări cibernetice în creștere, inclusiv atacuri ransomware și phishing.
* Dependență de furnizori cloud și servicii terțe.

**2. Active cheie și rolul lor**

| **Activ Cheie** | **Rol în Afacere** |
| --- | --- |
| Platforma software cloud | Produsul principal, depozitează și procesează datele utilizatorilor |
| Datele clienților | Informații sensibile, esențiale pentru încrederea și funcționarea serviciului |
| Infrastructura IT (servere, cloud) | Asigură disponibilitatea și securitatea serviciilor |
| Echipa tehnică | Dezvoltare, mentenanță și răspuns la incidente |
| Politici și proceduri de securitate | Cadru pentru prevenirea și gestionarea riscurilor cibernetice |

**3. Identificarea riscurilor potențiale (tehnice, comerciale, juridice)**

| **Tip risc** | **Risc specific** |
| --- | --- |
| Tehnic | Atac ransomware, exfiltrare date, phishing, vulnerabilități software, atac DDoS, acces neautorizat intern, backup insuficient |
| Comercial | Pierdere încrederii clienți din cauza breșelor de securitate |
| Juridic | Neconformitate GDPR, amenzi, litigii privind protecția datelor |

**4. Analiza riscurilor (probabilitate și impact)**

| **Risc** | **Probabilitate** | **Impact** | **Observații** |
| --- | --- | --- | --- |
| Atac ransomware | Medie | Foarte mare | Poate bloca accesul la date și paraliza serviciul |
| Exfiltrare de date | Medie | Foarte mare | Amenzi GDPR, pierdere reputație |
| Phishing | Mare | Mare | Vulnerabilitate umană, necesită training |
| Vulnerabilități software | Medie | Mare | Necesită patch-uri și audituri regulate |
| Atac DDoS | Medie | Mediu | Afectează disponibilitatea, nu compromite datele |
| Acces neautorizat intern | Mică | Mare | Politici stricte pot reduce riscul |
| Backup insuficient | Mică | Foarte mare | Pierdere ireversibilă de date |
| Pierdere încrederii clienți | Medie | Foarte mare | Impact comercial și juridic |
| Neconformitate GDPR | Medie | Foarte mare | Amenzi și litigii |

**5. Riscuri acceptabile și riscuri ce necesită măsuri imediate**

| **Risc** | **Status** |
| --- | --- |
| Atac ransomware | Necesită măsuri imediate |
| Exfiltrare de date | Necesită măsuri imediate |
| Phishing | Necesită măsuri imediate |
| Vulnerabilități software | Necesită măsuri imediate |
| Atac DDoS | Necesită măsuri imediate |
| Acces neautorizat intern | Necesită măsuri imediate |
| Backup insuficient | Necesită măsuri imediate |
| Pierdere încrederii clienți | Necesită măsuri imediate |
| Neconformitate GDPR | Necesită măsuri imediate |

**6. Plan de acțiune pentru riscurile critice**

| **Risc** | **Măsuri propuse** |
| --- | --- |
| Atac ransomware | Backup criptat și offsite, soluții antivirus actualizate, plan de recuperare în caz de dezastru |
| Exfiltrare de date | Criptare date, control acces RBAC, monitorizare acces și audit continuu |
| Phishing | Training regulat angajați, autentificare multi-factor (MFA), simulări phishing |
| Vulnerabilități software | Patch management riguros, audituri de securitate externe, bug bounty |
| Atac DDoS | Servicii anti-DDoS, monitorizare traficului și alertare în timp real |
| Acces neautorizat intern | Politici stricte de acces, segregare responsabilități, audit accesuri |
| Backup insuficient | Politică clară de backup, testare periodică a restaurării, backup criptat și multiplă locație |
| Pierdere încrederii clienți | Comunicare transparentă, îmbunătățirea securității, suport clienți post-incident |
| Neconformitate GDPR | Numirea DPO, audituri GDPR, politici clare de protecție a datelor, training angajați |

**7. Procese de monitorizare și revizuire**

* Audituri trimestriale de securitate IT și GDPR.
* Monitorizare continuă uptime platformă (SLA ≥99,9%).
* Raportare lunară incidente securitate și timpi răspuns.
* Simulări phishing trimestriale și training angajați.
* Revizuire anuală a planului de gestionare a riscurilor.
* Indicatori cheie monitorizați:

| **Indicator** | **Frecvență** | **Obiectiv / Prag alarme** |
| --- | --- | --- |
| Număr incidente securitate | Lunar | Scădere continuă, zero incidente majore |
| Timp mediu răspuns incidente | Lunar | < 1 oră pentru incidente critice |
| Rata succes simulări phishing | Trimestrial | < 5% angajați păcăliți |
| Procent patch-uri aplicate | Lunar | ≥ 95% patch-uri aplicate în 7 zile |
| Uptime infrastructură | Continuă | ≥ 99,9% uptime |
| Număr accesări neautorizate | Lunar | Zero sau minimal |
| Rata restaurare din backup | Trimestrial | 100% restaurare testată |

**8. Concluzii și recomandări**

* Riscurile cibernetice sunt cele mai critice pentru „InnoTech”, având potențial de impact major asupra funcționării și reputației.
* Implementarea unui sistem robust de securitate IT, inclusiv backup-uri, monitorizare și training, este esențială.
* Conformitatea GDPR trebuie asigurată prin audituri și politici clare.
* Monitorizarea continuă și revizuirea periodică a planului de gestionare a riscurilor vor asigura adaptarea la noi amenințări.
* Recomandăm alocarea de resurse suplimentare pentru securitate cibernetică și formarea unei echipe dedicate.