**Evaluarea Amenințărilor MSD - Analiză STRIDE**

**1. Companie și Active Cheie**

**Companie: MSD (Merck Sharp & Dohme)**

* **Sector**: Farmaceutic
* **Apartenența**: Multinațională americană

**Active Cheie**:

1. **Proprietate intelectuală R&D**
   * Date de cercetare pentru medicamente în dezvoltare
   * Formule și procese de fabricație patentate
2. **Sistemul de gestionare a lanțului de aprovizionare**
   * Infrastructura IT pentru producția globală
   * Sisteme de control pentru calitatea produselor
3. **Baza de date pentru studii clinice**
   * Date medicale ale pacienților din studii
   * Informații demografice și dosare medicale

## 2. Potențiali Atacatori

### Atacator 1: Grupuri APT Sponsorizate de State

**Exemple reale**: APT41 (China), Lazarus Group (Coreea de Nord)

**Motivație**:

* Furtul proprietății intelectuale pentru medicamente
* Avantaj competitiv pentru industria farmaceutică națională

**TTP-uri (MITRE ATT&CK)**:

* **Inițial Access [TA0001]**: Spear-phishing (T1566)
* **Execution [TA0002]**: Exploatarea aplicațiilor client (T1203)
* **Persistence [TA0003]**: Crearea conturilor (T1136)
* **Defense Evasion [TA0005]**: Obfuscarea fișierelor (T1027)
* **Exfiltration [TA0010]**: Exfiltrare prin canal alternativ (T1048)

**Caz real**: În 2017, grupul Lazarus a vizat companii farmaceutice pentru a fura proprietate intelectuală legată de vaccinuri și tratamente.

### Atacator 2: Grupuri Criminale Cibernetice

**Exemple reale**: REvil, DarkSide

**Motivație**:

* Profit financiar prin ransomware
* Vânzarea datelor medicale pe piața neagră

**TTP-uri (MITRE ATT&CK)**:

* **Initial Access [TA0001]**: Phishing (T1566)
* **Execution [TA0002]**: PowerShell (T1059.001)
* **Privilege Escalation [TA0004]**: Exploatarea pentru elevarea privilegiilor (T1068)
* **Lateral Movement [TA0008]**: RDP (T1021.001)
* **Impact [TA0040]**: Criptarea datelor pentru impact (T1486)

**Caz real**: În 2017, MSD a fost afectat de atacul NotPetya care a perturbat operațiunile globale cu pierderi estimate la $870 milioane.

### Atacator 3: Competitori Corporativi

**Exemple reale**: Cazuri documentate de spionaj corporativ în sectorul farmaceutic

**Motivație**:

* Accelerarea dezvoltării propriilor medicamente
* Acces la rezultatele studiilor clinice

**TTP-uri (MITRE ATT&CK)**:

* **Initial Access [TA0001]**: Compromiterea lanțului de aprovizionare (T1195)
* **Collection [TA0009]**: Colectarea datelor din baze de date (T1213)
* **Command and Control [TA0011]**: Protocoale criptate (T1573)
* **Exfiltration [TA0010]**: Transferul programat (T1029)
* **Reconnaissance [TA0043]**: Scanarea activă (T1595)

**Caz real**: În 2018, mai multe companii farmaceutice au raportat încercări de compromitere a proprietății intelectuale prin atacuri cibernetice sofisticate.

## 3. Analiza STRIDE pentru Active Selectate

### Activ 1: Proprietate intelectuală R&D

| **Amenințare** | **Vulnerabilități** | **Măsuri de reducere** |
| --- | --- | --- |
| **Spoofing** | - Credențiale slabe- Lipsa MFA | - Implementare MFA obligatorie- Sistem IAM robust |
| **Tampering** | - Control inadecvat al versiunilor | - Semnături digitale- Control de integritate |
| **Repudiation** | - Logging insuficient | - Logging centralizat (Splunk)- Monitorizare în timp real (SIEM) |
| **Information Disclosure** | - Criptare insuficientă | - Criptare end-to-end- Clasificare riguroasă a datelor |
| **Denial of Service** | - Lipsa redundanței | - Sisteme redundante (arhitectura AWS sau Azure)- Planuri de continuitate testate |
| **Elevation of Privilege** | - Principiul privilegiului minim neaplicat | - Implementare strictă a principiului- Revizuiri trimestriale (Scanari prin Tenable) |

### Activ 2: Baza de date studii clinice

| **Amenințare** | **Vulnerabilități** | **Măsuri de reducere** |
| --- | --- | --- |
| **Spoofing** | - Politici slabe pentru parole | - Autentificare biometrică- Politici granulare de acces(RBAC) |
| **Tampering** | - Validare inadecvată a datelor | - Controale de integritate (hashing SHA256) - Validare riguroasă |
| **Repudiation** | - Jurnalizare insuficientă | - Jurnal de audit inalterabil- Marcaje temporale certificate |
| **Information Disclosure** | - Proceduri inadecvate de anonimizare | - Criptare end-to-end- Controale DLP |
| **Denial of Service** | - Backup insuficient | - Plan de recuperare după dezastru- Sistem multi-nivel de backup (3-2-1) |
| **Elevation of Privilege** | - Segregare inadecvată a rolurilor | - Segregare strictă a rolurilor- Audituri de securitate periodice |

## 4. Recomandări Cheie

1. **Implementare Zero Trust**
   * Verificarea continuă a tuturor utilizatorilor și sistemelor
   * Principiul "never trust, always verify"
2. **Protecție avansată împotriva amenințărilor**
   * EDR/XDR pentru detecția rapidă a comportamentelor suspecte
   * Monitorizare continuă a tranzacțiilor de date sensibile
3. **Segmentare și izolare a rețelei**
   * Separarea rețelelor de cercetare de alte sisteme
   * Micro-segmentare pentru limitarea mișcării laterale
4. **Program de conștientizare a securității**
   * Instruire țintită pentru cercetători și personal clinic
   * Simulări regulate de phishing și exerciții de răspuns la incidente
5. **Managementul accesului privilegiat**
   * Soluții PAM pentru controlul accesului la sisteme critice
   * Monitorizarea sesiunilor privilegiate