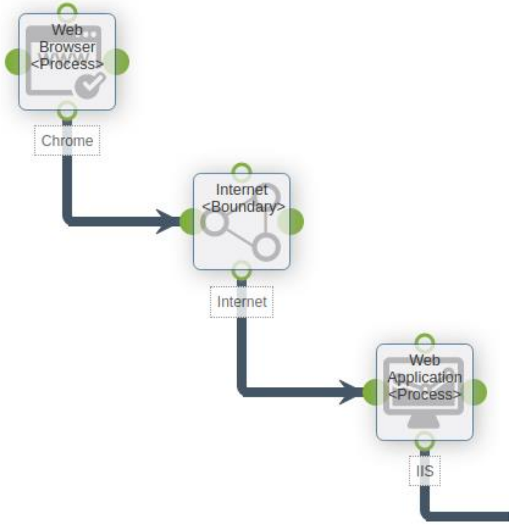
INADECO

Programación Segura

Presentación

Threat Modeling: cómo hacerlo

1. Scope: Diagrama de arquitectura
2. Threats STRIDE
   - Spoofing
   - Tampering
   - Repudiation
   - Information disclosure
   - Denial-of-service
   - Elevation privilege
3. Contramedidas o gestión del riesgo
4. Evaluar



Herramientas: Microsoft Thread Modeling Tool

https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

Demo de MS Threat Modeling Tool

Risk Rating

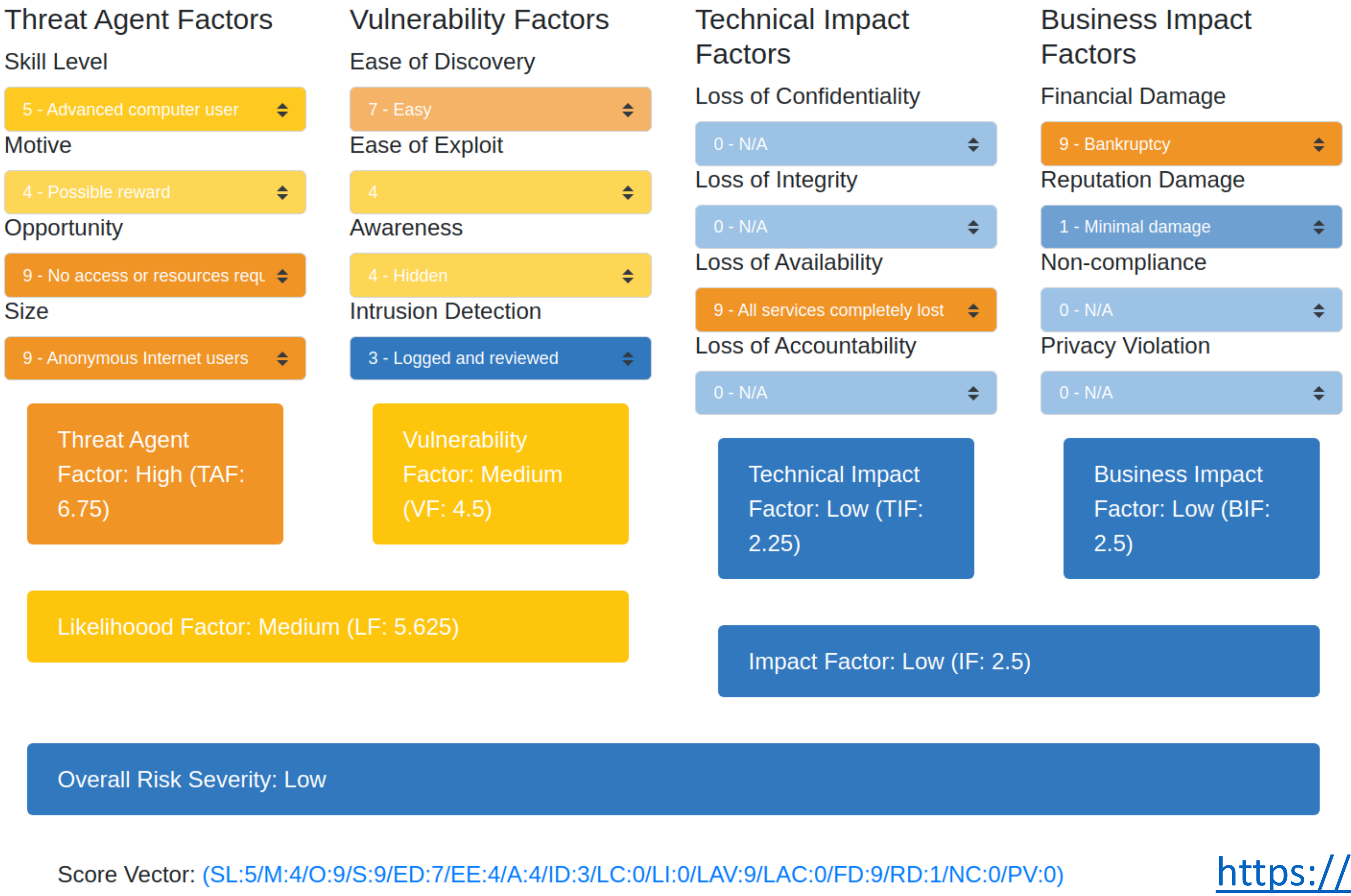
Risk = Likelihood * Impact

- Steps:
  1: Identifying a Risk
  2: Factors for Estimating Likelihood
  3: Factors for Estimating Impact
  4: Determining Severity of the Risk
  5: Deciding What to Fix
  6: Customizing Your Risk Rating Model
- Sacado del OWASP, así que empezemos a utilizarlo
  https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

Fuente: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology

Alternativas: NIST-800-30, Magerit

Calculadora de riesgos OWASP



Threat Agent Factors

Skill Level: 5 - Advanced computer user

Motive: 4 - Possible reward

Opportunity: 9 - No access or resources requ

Size: 9 - Anonymous Internet users

Vulnerability Factors

Ease of Discovery: 7 - Easy

Ease of Exploit: 4

Awareness: 4 - Hidden

Intrusion Detection: 3 - Logged and reviewed

Technical Impact Factors

Loss of Confidentiality: 0 - N/A

Loss of Integrity: 0 - N/A

Loss of Availability: 9 - All services completely lost

Loss of Accountability: 0 - N/A

Business Impact Factors

Financial Damage: 9 - Bankruptcy

Reputation Damage: 1 - Minimal damage

Non-compliance: 0 - N/A

Privacy Violation: 0 - N/A

Threat Agent Factor: High (TAF: 6.75)

Vulnerability Factor: Medium (VF: 4.5)

Technical Impact Factor: Low (TIF: 2.25)

Business Impact Factor: Low (BIF: 2.5)

Likelihoood Factor: Medium (LF: 5.625)

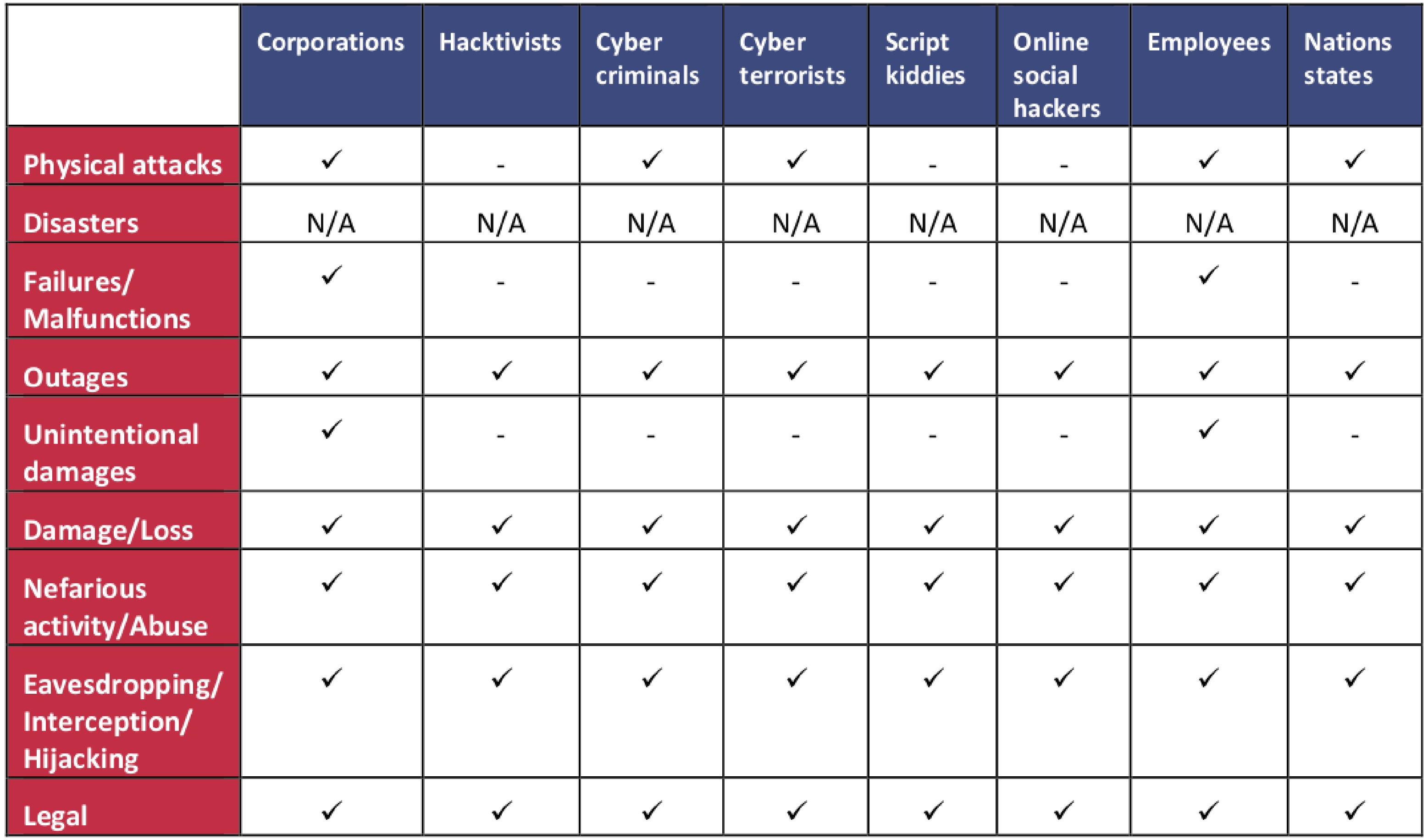
Impact Factor: Low (IF: 2.5)

Overall Risk Severity: Low

Score Vector: (SL:5/M:4/O:9/S:9/ED:7/EE:4/A:4/ID:3/LC:0/LI:0/LAV:9/LAC:0/FD:9/RD:1/NC:0/PV:0)

https://owasp-risk-rating.com/

Tipos de atacantes



	Corporations	Hacktivists	Cyber criminals	Cyber terrorists	Script kiddies	Online social hackers	Employees	Nations states
Physical attacks	✓	-	✓	✓	-	-	✓	✓
Disasters	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Failures/ Malfunctions	✓	-	-	-	-	-	✓	-
Outages	✓	✓	✓	✓	✓	✓	✓	✓
Unintentional damages	✓	-	-	-	-	-	✓	-
Damage/Loss	✓	✓	✓	✓	✓	✓	✓	✓
Nefarious activity/Abuse	✓	✓	✓	✓	✓	✓	✓	✓
Eavesdropping/ Interception/ Hijacking	✓	✓	✓	✓	✓	✓	✓	✓
Legal	✓	✓	✓	✓	✓	✓	✓	✓

Fuente: Thread landscape and Good Practice Guide for Internet Infraestructure
https://www.enisa.europa.eu/publications/iitl/view/++widget++form.widgets.fullReport/@@download/Threat+Landscape+and+Good+Practice+Guide+for+Internet+Infrastructure.pdf