

| Asset | Value | Objective |
|------------------------|------------------|---|
| Dati cliente | 300.000-500.000€ | Authentication, Integrity, Confidentiality, Availability |
| Dati GPS | 150.000-250.000€ | Integrity, Confidentiality, Availability |
| Dati corriere | 250.000-450.000€ | Integrity, Confidentiality, Availability |
| Dati pagamento | 600.000-750.000€ | Authentication, Integrity, Confidentiality, Accountability, Availability |
| Dati utente di sistema | 500.000-600.000€ | Authentication, Integrity, Confidentiality, Accountability, Authorization, Availability |

| Asset | Value | Spoofing | Tampering | Repudiation | Information disclosure | DOS | Elevation of privilege | Danger | Unreliability | Absence of Resilience | Exposure | Attack | Inherent Probability | Inherent Risk | Control | Cost | Feasibility | Residual Probability | Residual Impact | Residual Risk | R.o.C | Overall Cost |
|------------------------|------------------|----------|-----------|-------------|------------------------|-----|------------------------|--------|---------------|-----------------------|------------------|--|----------------------|----------------|--|----------------|---|----------------------|-----------------|---------------|--------------|-------------------|
| Dati utente di sistema | 500.000-600.000€ | X | | | | | | | | | 50.000-60.000€ | Authentication Abuse (CAPEC 114) | 40-60% | 20.000-36.000€ | • Autenticazione MFA | 5.000-10.000€ | Fattibile, sono disponibili librerie già testate e pronte all'uso | 4% - 6% | 20.000-36.000€ | 800-2.160€ | 2,84 - 2,38 | 5.800€ - 12.160€ |
| | | | | | | | X | | | | 150.000-250.000€ | Privilege Escalation (CAPEC 233) | 5-15% | 7.500-37.500€ | • Effettuare degli Audit del sistema • Controllare la configurazione del sistema • Mantenere aggiornati i programmi, librerie e framework • Implementare MFA per effettuare azioni privilegiate • Usare soluzioni anti-malware • Fare training sulla sicurezza informatica agli utenti del sistema • Segmentare la rete per limitare la diffusione del malware | 9.000-15.000€ | Fattibile, è richiesto un controllo continuo | 1% - 2% | 7.500-15.000€ | 75-300€ | -0,18 - 1,48 | 9.075€ - 15.300€ |
| | | X | X | X | X | X | X | X | X | X | 100.000-200.000€ | Targeted Malware (CAPEC 542) | 25-35% | 25.000-70.000€ | • Fare training sulla sicurezza informatica agli utenti del sistema • Segmentare la rete per limitare la diffusione del malware | 10.000-17.000€ | Fattibile, la parte si segmentazione della rete richiede competenze più elevate | 3% - 4% | 25.000-30.000€ | 750-1.200€ | 1,43 - 3,05 | 10.750€ - 18.200€ |
| | | X | | X | | | | | | | 40.000-50.000€ | Phishing (CAPEC 98) | 65-75% | 26.000-37.500€ | • Fare training sulla sicurezza informatica agli utenti del sistema • Usare soluzioni di sicurezza email e client di messaggistica | 7.000-12.000€ | Fattibile | 7% - 8% | 25.000-30.000€ | 1.750-2.400€ | 2,46 - 1,93 | 8.750€ - 14.400€ |
| | | X | X | X | | | | | | | 80.000-100.000€ | Adversary in the Middle (AITM) (CAPEC 94) | 10-20% | 8.000-20.000€ | • Usare protocolli di comunicazione crittografati (TLS/SSL, HTTPS) | 5.000-8.000€ | Fattibile | 1% - 2% | 8.000-20.000€ | 80-400€ | 0,58 - 1,45 | 5.080€ - 8.400€ |
| | | X | | | X | | | | | | 50.000-70.000€ | Reusing Session Id (Session Replay) (CAPEC 60) | 20-30% | 10.000-21.000€ | • Usare soluzioni di sicurezza per il browser • Ininvalidare i token di sessione dopo il logout • Autenticazione MFA | 8.000-11.000€ | Fattibile | 2% - 3% | 2.000-8.000€ | 40-240€ | 0,25 - 0,89 | 8.040€ - 11.240€ |
| | | | | X | | | | | | | 50.000-70.000€ | Password Brute Forcing (CAPEC 49) | 55-65% | 27.500-45.500€ | • Implementare un sistema di limitazione dei tentativi d'inserimento delle password • Usare password complesse • Autenticazione MFA | 7.000-10.000€ | Fattibile | 6% - 7% | 27.500-45.500€ | 1.650-3.185€ | 2,69 - 3,23 | 8.650€ - 13.185€ |
| | | X | | X | | | | | | | 50.000-70.000€ | Try Common or Default Usernames and Passwords (CAPEC 70) | 60-70% | 30.000-49.000€ | • Implementare un sistema di limitazione dei tentativi d'inserimento delle password e degli username • Usare password complesse • Autenticazione MFA | 8.000-11.000€ | Fattibile | 6% - 7% | 30.000-49.000€ | 1.800-3.430€ | 2,53 - 3,14 | 9.800€ - 14.430€ |
| | | X | | X | | | | | | | 50.000-70.000€ | Dictionary-based Password Attack (CAPEC 16) | 60-75% | 30.000-52.500€ | • Implementare un sistema di limitazione dei tentativi d'inserimento della password • Usare password complesse • Autenticazione MFA | 7.000-10.000€ | Fattibile | 6% - 8% | 30.000-52.500€ | 1.800-4.200€ | 3,03 - 3,83 | 8.800€ - 14.200€ |
| | | X | | X | | | | | | | 50.000-70.000€ | Credential Stuffing (CAPEC 600) | 70-80% | 35.000-56.000€ | • Implementare un sistema di limitazione dei tentativi d'inserimento delle password • Usare password complesse • Autenticazione MFA | 7.000-10.000€ | Fattibile | 7% - 8% | 35.000-56.000€ | 2.450-4.480€ | 3,65 - 4,15 | 9.450€ - 14.480€ |
| Dati GPS | 150.000-250.000€ | X | X | X | | X | X | | | | 30.000-40.000€ | Traffic Injection (CAPEC 594) | 20-30% | 6.000-12.000€ | • Implementare controlli sulla sorgente dei dati | 5.000-7.000€ | Fattibile, richieste competenze tecniche alte | 2% - 3% | 10.000-20.000€ | 200-600€ | 0,16 - 0,63 | 5.200€ - 7.600€ |
| | | X | X | | | | | | | | 40.000-70.000€ | Carry-Off GPS Attack (CAPEC 628) | 10-20% | 4.000-14.000€ | • Rotte con zone sicure • Autenticazione del segnale GPS | 2.000-6.000€ | Fattibile | 1% - 2% | 10.000-50.000€ | 100-1.000€ | 0,95 - 1,17 | 2.100€ - 7.000€ |
| | | | X | X | | | | | | | 50.000-70.000€ | Counterfeit GPS Signals (CAPEC 627) | 10-20% | 5.000-14.000€ | • Ricevitore resistente allo Spoofing (SPREE) • Procedure di recupero | 3.000-5.000€ | Fattibile | 1% - 2% | 10.000-50.000€ | 100-1.000€ | 0,63 - 1,60 | 3.100€ - 6.000€ |

| | | | | | | | | | | | | | | | | | | | |
|----------------|------------------|---|---|---|---|---|---|------------------|---|--------|------------------|--|---------------------|---|---------|-----------------|--------------|-------------|-------------------|
| | | X | X | X | | | | 50.000-60.000€ | Transaction or Event Tampering via Application API Manipulation (CAPEC 385) | 20-30% | 10.000-18.000€ | • Implementare sistemi di autenticazione per gli endpoint API • Implementare sistema di logging per richieste API | 9.000-12.000€ | Fattibile, richieste competenze tecniche alte | 2% - 3% | 10.000-20.000€ | 200-600€ | 0,09 - 0,45 | 9.200€ - 12.600€ |
| | | X | X | X | X | X | X | 90.000-120.000€ | Server Side Request Forgery (CAPEC 664) | 20-40% | 18.000-48.000€ | • Autenticare e validare ogni richiesta • Configurare correttamente il server • Implementare sistema di logging | 15.000-20.000€ | Fattibile, richieste competenze tecniche alte | 2% - 4% | 40.000-60.000€ | 800-2.400€ | 0,15 - 1,28 | 15.800€ - 22.400€ |
| | | | | X | X | X | X | 50.000-60.000€ | Input data manipulation (CAPEC 153) | 30-40% | 15.000-24.000€ | • Validare gli input | 10.000-15.000€ | Fattibile | 3% - 4% | 20.000-40.000€ | 600-1.600€ | 0,44 - 0,49 | 10.600€ - 16.600€ |
| | | | X | | X | | | 40.000-50.000€ | Fake the Source of Data (CAPEC 194) | 25-35% | 10.000-17.500€ | • Autenticare e validare i dati in ingresso • Implementare un sistema di logging | 8.000-10.000€ | Fattibile | 3% - 4% | 20.000-30.000€ | 600-1.200€ | 0,18 - 0,63 | 8.600€ - 11.200€ |
| Dati cliente | 300.000-500.000€ | X | | X | | | | 20.000-30.000€ | Phishing (CAPEC 98) | 40-50% | 8.000-15.000€ | • Fare training sulla sicurezza informatica agli utenti del sistema • Usare soluzioni di sicurezza email e client di messaggistica | 7.000-12.000€ | Fattibile | 4% - 5% | 8.000-15.000€ | 320-750€ | 0,10 - 0,19 | 7.320€ - 12.750€ |
| | | X | | X | | | | 80.000-100.000€ | Credential Stuffing (CAPEC 600) | 70-80% | 56.000-80.000€ | • Implementare un sistema di limitazione dei tentativi d'inserimento delle password • Usare password complesse • Autenticazione MFA | 7.000-10.000€ | Fattibile | 7% - 8% | 35.000-56.000€ | 2.450-4.480€ | 6,65 - 6,55 | 9.450€ - 14.480€ |
| | | X | X | | | | | 40.000-50.000€ | Content Spoofing (CAPEC 148) | 20-30% | 8.000-15.000€ | • Verificare l'autenticità dei dati • Implementare un sistema di logging | 5.000-7.000€ | Fattibile | 2% - 3% | 8.000-15.000 | 160-450€ | 0,57 - 1,08 | 5.160€ - 7.450€ |
| | | X | X | X | | | | 50.000-70.000€ | Adversary in the Middle (AITM) (CAPEC 94) | 15-25% | 7.500-17.500€ | • Usare protocolli di comunicazione crittografati (TLS/SSL, HTTPS) | 5.000-8.000€ | Fattibile | 2% - 3% | 25.000-30.000€ | 500-900€ | 0,40 - 1,08 | 5.500€ - 8.900€ |
| | | X | X | X | X | X | X | 90.000-120.000€ | Server Side Request Forgery (CAPEC 664) | 20-40% | 18.000-48.000€ | • Autenticare e validare ogni richiesta • Configurare correttamente il server • Implementare sistema di logging | 15.000-20.000€ | Fattibile, richieste competenze tecniche alte | 2% - 4% | 18.000-48.000€ | 360-1.920€ | 0,18 - 1,30 | 15.360€ - 21.920€ |
| | | X | X | X | X | X | X | 100.000-150.000€ | Targeted Malware (CAPEC 542) | 50-60% | 50.000-90.000€ | • Usare soluzioni anti-malware • Fare training sulla sicurezza informatica agli utenti del sistema • Segmentare la rete per limitare la diffusione del malware | 12.000-17.000€ | Fattibile, la parte si segmentazione della rete richiede competenze più elevate | 5% - 6% | 30.000-60.000€ | 1.500-3.600€ | 3,04 - 4,08 | 13.500€ - 20.600€ |
| Dati pagamento | 600.000-750.000€ | X | X | X | X | X | X | 170.000-200.000€ | Targeted Malware (CAPEC 542) | 60-70% | 102.000-140.000€ | • Usare soluzioni anti-malware • Fare training sulla sicurezza informatica agli utenti del sistema • Segmentare la rete per limitare la diffusione del malware | 12.000-17.000€ | Fattibile, la parte si segmentazione della rete richiede competenze più elevate | 6% - 7% | 60.000-80.000€ | 3.600-5.600€ | 7,20 - 6,91 | 15.600€ - 22.600€ |
| | | X | | | | | | 100.000-120.000€ | Identity Spoofing (CAPEC 151) | 40-50% | 40.000-60.000€ | • Verificare l'autenticità di ogni pagamento • Usare autenticazione MFA per effettuare i pagamenti | 10.000-13.000€ | Fattibile | 4% - 5% | 40.000-60.000€ | 1.600-3.000€ | 2,84 - 3,38 | 11.600€ - 16.000€ |
| | | X | | X | | | | 40.000-50.000€ | Phishing (CAPEC 98) | 65-75% | 26.000-37.500€ | • Fare training sulla sicurezza informatica agli utenti del sistema • Usare soluzioni di sicurezza email e client di messaggistica | 7.000-12.000€ | Fattibile | 7% - 8% | 25.000-30.000€ | 1.750-2.400€ | 2,46 - 1,93 | 8.750€ - 14.400€ |
| | | X | X | X | X | X | X | 90.000-120.000€ | Log Injection-Tampering-Forging (CAPEC 93) | 30-40% | 27.000-48.000€ | • Controlli di accesso rigorosi ai log • Protezione del formato dei log • Protezione dell'integrità dei log | 15.000-20.000€ | Fattibile, richieste competenze tecniche alte | 3% - 4% | 27.000-48.000€ | 810-1.920€ | 0,75 - 1,30 | 15.810€ - 21.920€ |
| | | X | | X | | | | 100.000-200.000€ | Clickjacking (CAPEC 103) | 40-50% | 40.000-100.000€ | • Utilizzo di Content-Security-Policy (CSP) Hardening | • UI 30.000-40.000€ | Fattibile | 4% - 5% | 75.000-100.000€ | 3.000-5.000€ | 0,23 - 1,38 | 33.000€ - 45.000€ |
| | | X | X | X | | | | 50.000-70.000€ | Adversary in the Middle (AITM) (CAPEC 94) | 15-25% | 7.500-17.500€ | • Usare protocolli di comunicazione crittografati (TLS/SSL, HTTPS) | 5.000-8.000€ | Fattibile | 2% - 3% | 25.000-30.000€ | 500-900€ | 0,40 - 1,08 | 5.500€ - 8.900€ |

| | | X | X | X | | | | 50.000-60.000€ | Transaction or Event Tampering via Application API Manipulation (CAPEC 385) | 20-30% | 10.000-18.000€ | • Implementare sistemi di autenticazione per gli endpoint API • Implementare sistema di logging per richieste API | 9.000-12.000€ | Fattibile, richieste competenze tecniche alte | 2% - 3% | 10.000-20.000€ | 200-600€ | 0,09 - 0,45 | 9.200€ - 12.600€ |
|---------------|------------------|---|---|---|---|---|---|------------------|--|--------|----------------|--|----------------|---|---------|----------------|--------------|-------------|-------------------|
| Dati corriere | 250.000-450.000€ | X | | X | | | | 20.000-30.000€ | Phishing (CAPEC 98) | 40-50% | 8.000-15.000€ | • Fare training sulla sicurezza informatica agli utenti del sistema • Usare soluzioni di sicurezza email e client di messaggistica | 7.000-12.000€ | Fattibile | 4% - 5% | 8.000-15.000€ | 320-750€ | 0,10 - 0,19 | 7.320€ - 12.750€ |
| | | X | X | | | | | 30.000-40.000€ | Content Spoofing (CAPEC 148) | 20-30% | 6.000-12.000€ | • Verificare l'autenticità dei dati • Implementare un sistema di logging | 5.000-7.000€ | Fattibile | 2% - 3% | 5.000-7.000€ | 100-210€ | 0,18 - 0,68 | 5.100€ - 7.210€ |
| | | X | X | X | | | | 50.000-70.000€ | Adversary in the Middle (AiTM) (CAPEC 94) | 15-25% | 7.500-17.500€ | • Usare protocolli di comunicazione crittografati (TLS/SSL, HTTPS) | 5.000-8.000€ | Fattibile | 2% - 3% | 25.000-30.000€ | 500-900€ | 0,40 - 1,08 | 5.500€ - 8.900€ |
| | | X | X | X | X | X | X | 90.000-120.000€ | Server Side Request Forgery (CAPEC 664) | 20-40% | 18.000-48.000€ | • Autenticare e validare ogni richiesta • Configurare correttamente il server • Implementare sistema di logging | 15.000-20.000€ | Fattibile, richieste competenze tecniche alte | 2% - 4% | 18.000-48.000€ | 360-1.920€ | 0,18 - 1,30 | 15.360€ - 21.920€ |
| | | X | X | X | X | X | X | 100.000-150.000€ | Targeted Malware (CAPEC 542) | 50-60% | 50.000-90.000€ | • Usare soluzioni anti-malware • Fare training sulla sicurezza informatica agli utenti del sistema • Segmentare la rete per limitare la diffusione del malware | 10.000-17.000€ | Fattibile, la parte si segmentazione della rete richiede competenze più elevate | 5% - 6% | 30.000-60.000€ | 1.500-3.600€ | 3,85 - 4,08 | 11.500€ - 20.600€ |