XXX x.x.x.

Cyber Risk Assessment

XX/XX/XXXX

INDEX

ACRONIMI E TERMINOLOGIA

Nella tabella gli acronimi che possono essere utilizzati nel report.

Acronym	Description
RDP	Remote Desktop Protocol
CAPEC	Common Attack Pattern Enumeration and Classification
DMZ	Demilitarized Zone
WASC	Web Application Security Consortium
OWASP	Open Web Application Security Project
CVE	Common Vulnerabilities and Exposures
XSS	Cross-site scripting
ARP	Address Resolution Protocol
RFC	Request for Comments
NIST	National Institute of Standards and Technology

1.Introduzione

XXX s.p.a. (anche solo in seguito azienda, società, cliente) ha chiesto a Glue Labs s.r.l. (anche solo in seguito fornitore) un'attività di Cyber Risk Assessment per determinare in soli 2 giorni il livello di esposizione e di rischio per la sicurezza dei propri asset aziendali.

1.1.Ambito

L'ambito è stato definito come:

- Dominio: *.XXXXX

1.2.Obiettivi

- produrre un Cyber Risk Assessment di livello iniziale

1.1.3.Informazioni da includere

Le seguenti informazioni devono essere incluse:

- livello di rischio

2. Security Report

La fase iniziale di riconoscimento della rete del dominio *XXXX ha rivelato diverse vulnerabilità che potrebbero comportare la compromissione di dati degli utenti, le funzionalità dei server su cui risiedono.

Tali vulnerabilità sono parzialmente mitigate da firewall. Tali strumenti mitigano anche il rischio complessivo di esposizione.

Al fine di avere uno scenario di riferimento comune sono state rapportate le vulnerabilità riscontrate al framework OWASP[1] riconosciuto a livello internazionale come standard de facto per l'analisi dei rischi delle Web Application e che ha trovato spazio ed è diventato punto di riferimento per tutti i sistemi IT che espongono servizi online.

Inoltre come tabella di rischio per la relativa valutazione verrà utilizzata la seguente basata su 5 livelli di Probabilità e 5 di Impatto.

5 (altissimo)	5	10	15	20	25
4 (alto)	4	8	12	16	20
3 (medio)	3	6	9	12	15
2 (basso)	2	4	6	8	10
1 (bassissimo)	1	2	3	4	5
Impatto	**1(bassissima)**	**2 (bassa)**	**3 (media)**	**4 (alta)**	**5(altissima)**
	Probabilità				

Tabella di rischio

2.1 Injection

Sono stati riscontrati diversi possibili punti di injection sia su servizi Web based sia su servizi server side. Rischio **16**.

2.2 Broken Authentication

Alcuni servizi espongono punti di accesso poco protetti contro il brute forcing degli accessi. Rischio **9**.

2.3 Sensitive Data Exposure

Sono individuabili informazioni tecniche sensibili sui sistemi che possono essere utilizzate e sfruttate dagli hacker. Rischio **12**.

[1] https://owasp.org/www-project-top-ten/

2.4 XML External Entities (XXE)

Al momento non applicabile.

2.5 Broken Access Control

Una vulnerabilità riscontrata può comportare il bypass dell'autenticazione su un sistema del Cliente. Rischio **16**.

2.6 Security Misconfiguration

Sono stati utilizzati common pattern che permettono di scoprire ed allargare la superficie d'attacco per gli hacker, a titolo di esempio:

- XXXX
- XXXX

Inoltre su ogni sistema investigato dovrebbero essere applicate le opportune procedure di hardening per ridurre la superficie di attacco.

Rischio **25**.

2.7 Cross-Site Scripting XSS

Al momento non sono stati riscontrati XSS. Rischio **3**.

2.8 Insecure Deserialization

Al momento non sono stati riscontrati punti di Insecure Deserialization. Rischio **3**.

2.9 Using Components with Known Vulnerabilities

Sono stati riscontrati sia software sia librerie sia componenti con vulnerabilità note, alcune anche note da anni. Rischio **16**.

2.10 Insufficient Logging & Monitoring

I sistemi di logging e monitoring permettono di verificare le attività svolte dai sistemi e dagli utenti e di avere processi interni per gestire eventuali problemi riscontrati. Con le evidenze a disposizione è possibile prevedere che non ci siano sistemi efficienti di logging & monitoring. Rischio considerato **9**.

Nel caso in cui il Cliente abbia sistemi e processi di Logging & Monitoring dovrebbe essere riuscito ad individuare le attività svolte dal Fornitore per effettuare il presente Security Assessment. Qualora il Cliente abbia quanto indicato il rischio è diminuito a **6** altrimenti è aumentato a **16**.

3. Livello di rischio complessivo

Mettendo insieme le informazioni ricavate dalla fase di Information Gathering ed effettuando una media dei rischi delle vulnerabilità riscontrate il livello di rischio complessivo è **12** prodotto da:

- un livello di probabilità alto legato al fatto che l'azienda e le tipologie di vulnerabilità sono utilizzate comunemente dagli hacker e necessitano di un basso livello di preparazione per essere sfruttate. Tale probabilità viene mitigata dalla presenza di firewall e pertanto viene considerata di livello **medio(3)**;
- un livello di impatto **alto(4)** legato al fatto che le vulnerabilità scoperte e le evidenze riscontrate, qualora sfruttate dagli hacker, possono compromettere i sistemi del Cliente provocando danni rilevanti.

3.1. Esposizione al rischio nel tempo

In considerazione dei possibili vettori d'attacco, della continua esposizione delle vulnerabilità,della maggiore intensità delle attività degli hacker verso settori industriali prossimi a quelli del cliente che hanno comportato per diverse realtà aziendali la cifratura dei dati con la richiesta di riscatto, il Cliente ha un'**alta** probabilità di subire attacchi hacker.