UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

uniMC

Cyber security pre-assessment audit

Flavio Tonetto

Sinergia EPC srl

www.sinergia.it

ftonetto@sinergia.it

Martedì 19 settembre 2023

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

Definizioni

Definizione di rischio

Con il termine di “**rischio**” si indica la potenzialità che una determinata azione possa avere un esito negativo e portare a un danno, una perdita o un evento indesiderato.

Nell’ambito della valutazione dei rischi di tipo informatico per la sicurezza delle informazioni, l’obiettivo è la conservazione della RID dei dati ovvero della **Riservatezza**, **Integrità** e **Disponibilità** delle informazioni trattate dai sistemi informatici aziendali, tenendo conto, allo stesso tempo, della necessaria operatività a cui sono sottoposte dette informazioni per il raggiungimento degli obiettivi di business di una organizzazione.

In senso operativo, infatti, le informazioni devono essere al sicuro in **tutto il ciclo di vita aziendale**: quando sono ferme, o in trasferimento, quando sono accedute e/o modificate.

Calcolo del rischio

Il calcolo del livello di Cyber Risk di una organizzazione è basato sulla seguente formula:

$$\text{RISCHIO} = \frac{(Minaccia\ potenziale) * (Probabilit\grave{a}\ evento) * (Conseguenze\ evento)}{(Misure\ di\ sicurezza\ implementate)}$$

ossia il prodotto tra il numero di potenziali minacce, la probabilità che un evento dannoso si verifichi e l’impatto che genera, diviso il numero di controlli di sicurezza in essere.

Pre-assessment audit

Definizione di Pre-assessment

Un assessment iniziale permette di identificare le informazioni, la loro tipologia e le correlazioni con gli asset aziendali ovvero alle risorse soggette a rischio, ma soprattutto ne **misura il livello iniziale di esposizione**.

Una volta individuati i rischi, ogni organizzazione ha quattro possibili scelte da fare:

- **evitarli**: eliminare/rinunciare al rischio;
- **contenerli**: ridurre probabilità o impatto del rischio;
- **trasferirli**: trasferire il rischio ad una terza parte;
- **accettarli**: riconoscere e tollerare il rischio.

Obiettivi pre-assessment

L'obiettivo del pre-assessment consiste nella valutazione di due parametri:

- **il livello di appetibilità cyber aziendale**
- **il livello della complessità IT aziendale**

Andando a combinare questi due elementi, è possibile determinare quale standard/framework di cybersecurity adoperare, per eseguire in un secondo momento una valutazione dei rischi tramite gap analysis, ossia mediante un processo che va a determinare lo scostamento tra le misure tecnico organizzative effettivamente implementate dall'organizzazione rispetto ai requisiti previsti dal framework.

Livello appetibilità cyber - Definizione

La probabilità che un'organizzazione subisca un incidente informatico deve essere determinata considerando la sua appetibilità cyber, ovvero quanto l'azienda risulti redditizia in termini economici dal punto di vista di un criminale informatico.

Sono stati previsti **3 livelli** di appetibilità cyber:

- **ALTO**: probabilità elevata che l'organizzazione possa essere vittima di un incidente informatico causato da un cyber criminale o un insider.
- **MEDIO**: buona probabilità di essere vittima di un attacco cyber.
- **BASSO**: probabilità molto bassa che l'organizzazione possa rimanere vittima di un attacco cyber.

Livello appetibilità cyber – Base dati

- **Settore in cui opera l’organizzazione**: gli attacchi hacker alle imprese italiane coinvolgono tutti i settori, ma alcuni sono più bersagliati di altri. Inoltre, la violazione di dati personali può portare a sanzioni da parte del Garante della Privacy per cui l’azienda che ha subito il data breach è maggiormente indotta a pagare il riscatto.
- **Fatturato aziendale**: le cifre richieste per i riscatti a seguito di un attacco informatico, sono spesso calcolate sul fatturato della vittima, proprio allo scopo di richiedere un importo proporzionato che possa essere pagato. Anche le realtà più “piccole” rappresentano un potenziale bersaglio
- **Essere fornitore di servizi ICT o software**: Molti attacchi partono dalle aziende della catena di approvvigionamento (supply-chain). Nonostante le aziende target di dimensioni maggiori, adottino rigorose misure di sicurezza, spesso consentono l’accesso ai propri sistemi a fornitori legittimi. In questo modo i fornitori entrano a far parte della rete aziendale target e, di conseguenza, la espongono a potenziali attacchi

Livello complessità IT aziendale

Il livello di complessità IT di un’organizzazione è definito come l’insieme degli elementi tecnologici interdipendenti di un dato perimetro IT, dove più sono le variabili e la loro interdipendenza, maggiore è la complessità da gestire.

Sono stati previsti **3 livelli** di complessità IT:

- **ALTO**: infrastruttura avente un perimetro IT molto esteso, un’architettura di rete articolata e dislocata in diverse aree geografiche, un numero elevato di asset tecnologici e di servizi supportati e gestiti internamente.
- **MEDIO**: infrastruttura avente un’ architettura complessa, un discreto numero di asset tecnologici e di servizi supportati e gestiti internamente.
- **BASSO**: infrastruttura semplice, numero ristretto di asset tecnologici e di servizi supportati.

Livello complessità IT aziendale – Base dati

Elenco dei dispositivi hardware presenti all’interno del perimetro IT da analizzare: rientrano in questo elenco i personal computer, i dispositivi mobile, i dispositivi di rete, i server, i dispositivi IoT, i terminali VoIP:

- **Elenco dei software utilizzati all’interno del perimetro IT da analizzare**: rientrano in questo elenco i sistemi operativi, le macchine virtuali, i container, le applicazioni web aziendali.
- **Elenco dei servizi Cloud che rientrano del perimetro IT da analizzare**: fanno parte di questo elenco i sevizi IaaS, PaaS e SaaS aziendali.
- **Gestione del reparto IT**: riveste un ruolo centrale in qualsiasi organizzazione e i processi che supporta sono trasversali a tutte le aree aziendali.

Pre-assessment audit – IMPRONTA srl

Descrizione società - SERVIZI

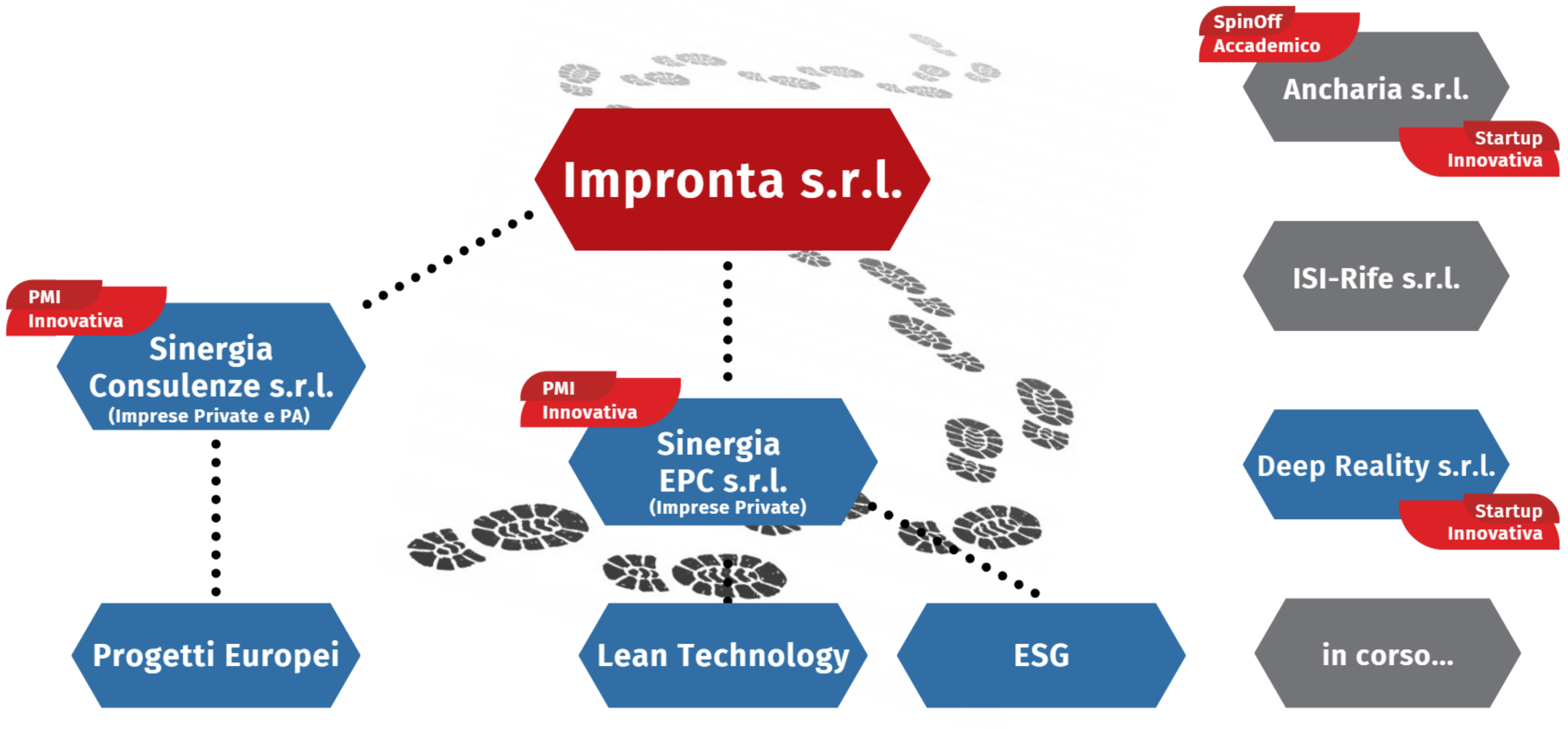
La società in oggetto, eroga 3 servizi:

- Lean Technology (LT)
- Progetti Europei, Sviluppo e Innovazione (PE)
- Sistemi di controllo Interno e Gestione Rischi (SCI-GR)

Oltre ai servizi sopra elencati, l’azienda offre anche un prodotto software per il Sistema di Gestione Integrato chiamato SGIA.

È inoltre presente un ulteriore software aziendale, un ERP per società di servizi, che per ora è a solo uso interno ma che la società intende far diventare un prodotto da offrire ai propri clienti.

Il gruppo



Legenda colori:
- Impronta Srl ha la maggioranza
- Impronta Srl ha la minoranza

Descrizione società - INFRASTRUTTURA

L’azienda oltre ai dati personali di dipendenti e collaboratori, tratta dati comuni dei propri clienti.

- Tutta l’infrastruttura documentale aziendale è in Cloud su piattaforma **Microsoft Office 365**; I soci sono gli unici amministratori della suite.
- All’interno dei PC dei consulenti della società, sono memorizzati alcuni dati aziendali ed è installato il client per la sincronizzazione degli stessi sul Cloud aziendale (**OneDrive**).
- All’interno della sede aziendale, è presente un Server utilizzato principalmente per il backup della web application SGIA eseguito due volte al giorno. Tale server è collegato ad un sistema RAID 1 (mirroring) e ad un UPS.
- Il Server consente l’accesso da remoto tramite una VPN le cui credenziali sono in possesso di alcuni dipendenti aziendali. Tuttavia l’uso è limitato e saltuario.

Informazioni acquisite durante l’audit

Domanda	Risposta	Note
Tipologia di organizzazione	Privata	
Settore	Servizi Tecnologici	Anche Consulenza
Fatturato ultimo anno	<3 mln di €	
Fornitore per grandi organizzazioni	Accesso alla infrastruttura IT	
Frequenza audit di sicurezza informatica	Mai svolti	

Informazioni acquisite durante l’audit

Domanda		Risposta	
Numero di IP pubblici	IP statici	**1**	46.37.24.186(server aruba)
Numero di personal computer	Include anche quelle in smart working	**Da 11 a 50**	
Numero dispositivi mobile che si collegano alla rete aziendale	Tablet, smartphone	**Da 11 a 50**	
Numero dispositivi di rete	Server, firewall, router, switch, ids/ips, hub	**Da 1 a 10**	No firewall
Numero di dispositivi IoT connessi alla rete aziendale	Dispositivi IoT su tecnologia IP	**Da 1 a 10**	Per gestione della temperatura ambientale
Dispositivi su rete di produzione industriale (OT)	Dispositivi connessi alla rete OT su tecnologia IP	**Nessuno**	
Terminali VoIP	-	**Da 1 a 10**	
Numero di Reti/sottoreti	Comprese le reti Wireless	**1**	
Numero di connessioni dall'esterno	Include VPN, RDP, SSH, Telnet, FTP, ecc	**Da 4 a 10**	

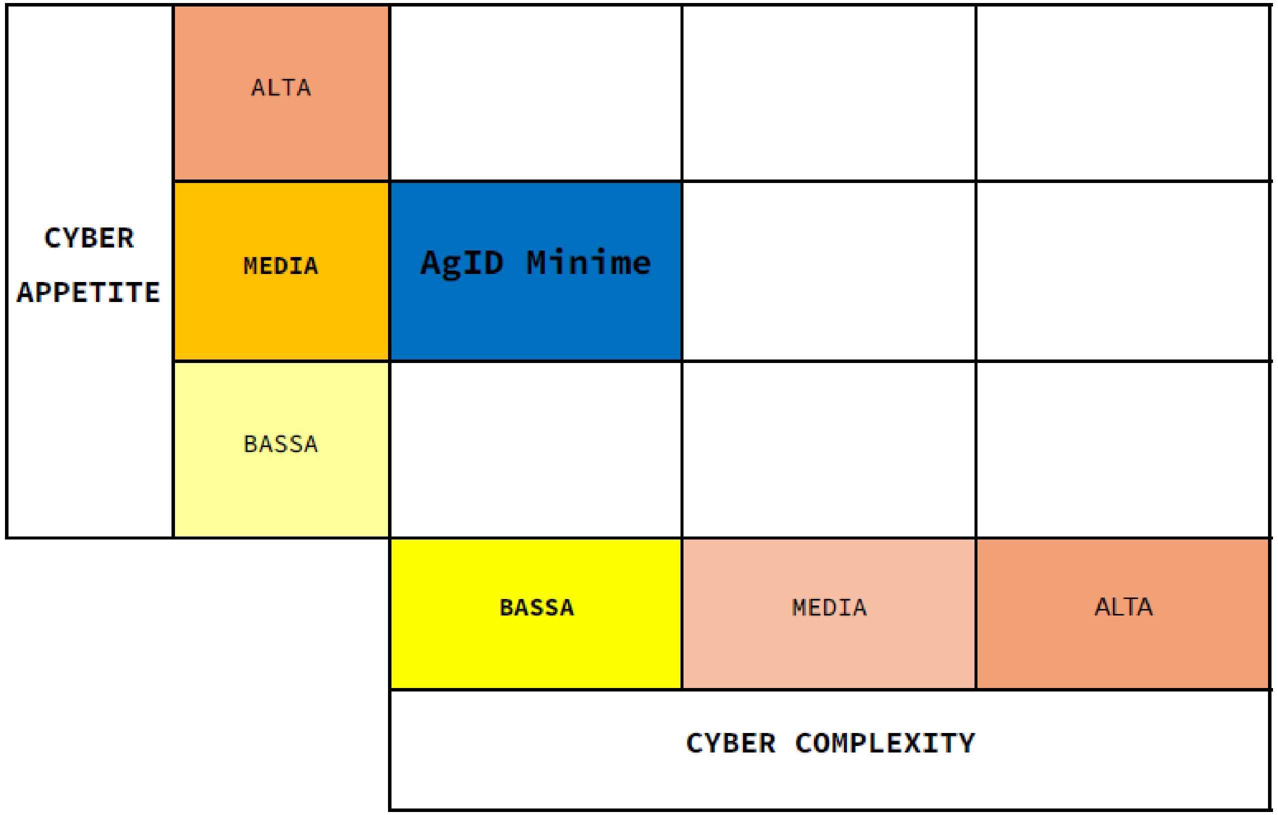
Informazioni acquisite durante l'audit

Domanda		Risposta	
Sistemi Operativi	Per PC e Server	**Più del 90% degli host hanno lo stesso SO con la stessa versione**	Server Aruba (WS2012); Server on-premise di backup (WS2008R2)
Numero di macchine virtuali/container	Sia quelle presenti nella Intranet, sia quelle nella DMZ	**Da 1 a 5**	Una su Azure e una su AWS
Numero di applicazioni web aziendali	Quelle presenti nella Intranet, nella DMZ e su Internet	**Da 1 a 3**	
Numero di servizi IaaS	Es: Computer Engine di Google Cloud Platform, AWS, Oracle, EC2 Amazon, ecc	**Da 1 a 3**	
Numero di servizi PaaS	Es: Google App Engine, Azure, ecc.	**1**	
Numero di servizi e SaaS	Es: Google Workspace, Dropbox, Office365, SalesForce	**Da 1 a 3**	
Reparto IT	Personale dedicato alla gestione dei sistemi informatici	**I sistemi informatici sono quasi tutti gestiti da personale dedicato interno specializzato**	

Risultati

- <u>Livello di cyber appetite</u>: **MEDIO** (pesa molto il fatto che la società ha accesso all'infrastruttura IT di clienti importanti)
- <u>Livello di complessità IT</u>: **BASSO**

Di conseguenza il framework di riferimento per la valutazione del livello di maturità cyber è rappresentato dalle **misure minime di sicurezza dell'AgID**.



Considerazioni finali

- Media complessità dell'ambiente cloud Microsoft 365
- Elevato turnover
- Il cerchio si chiude con la formazione. Il mondo del cybercrime è in costante evoluzione e le tecniche mutano e si perfezionano ogni giorno.

UNIVERSITÀ POLITECNICA DELLE MARCHE

DII
Dipartimento di Ingegneria dell'Informazione

unIMC

Cyber security pre-assessment audit

Grazie!

Martedì 19 settembre 2023