PARALEGALE IT S.R.L.

OUTSOURCING MANAGEMENT

Cyber Security in *outsourcing*

- **Cyber Security services**

- **GDPR compliance**

PARALEGALE IT S.R.L.
OUTSOURCING MANAGEMENT

- Nel 2018 gli attacchi informatici gravi sono aumentati globalmente del 38% rispetto all'anno precedente*, con gravissime ricadute economiche sulle aziende colpite e i diritti dei soggetti violati.

Ddos

Ransomware

Cyber espionage

0-day attach

Phishing

- Complice anche l'intervento di potenti attori governativi, gli attacchi alle aziende e al comparto pubblico sono divenuti più letali, subdoli e difficili da arginare, tendenzialmente diretti al trafugamento di dati rilevanti o estorsione di denaro.

Di fronte alla rapida avanzata ed evoluzione dei cybercriminali, i dati ci dicono che le aziende italiane non sono corse per tempo ai ripari e gli investimenti nella cyber security sono ancora insufficienti e sottovalutati.

Fonte: rapporto Clusit 2019 sulla sicurezza informatica

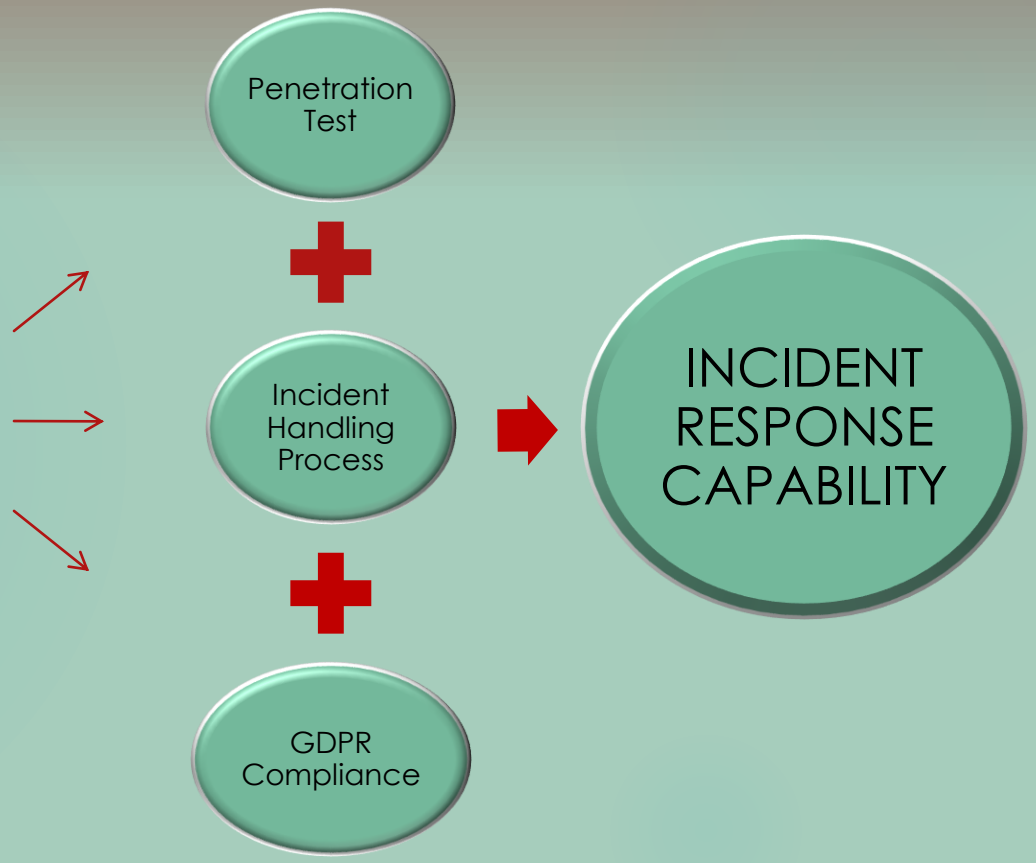
PARALEGALE IT S.R.L.

OUTSOURCING MANAGEMENT

Soluzione -> Cyber resilience

Assicurare la capacità dell'organizzazione di saper preventivamente individuare un incidente di sicurezza e resistere all'attacco informatico, in modo da ripristinare in tempi brevi la propria operatività.

Attraverso tre fasi parallele e connesse, è possibile assicurarsi che la propria azienda sia adeguata alle moderne linee guida in tema di Cyber Security



PARALEGALE IT S.R.L.
OUTSOURCING MANAGEMENT

RED TEAM

- **Penetration Test**

La parola chiave è **PREVENZIONE**.
L'unico modo che una azienda ha per difendersi dagli attacchi informatici, è verificare preventivamente quali vulnerabilità essa presenta e se le misure di difesa sino ad ora adottate sono sufficienti e funzionanti.

Passaggio oramai obbligato per dirsi conformi all'art. 32 c. 1 lett. d) del GDPR!*

* una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

PARALEGALE IT S.R.L.
OUTSOURCING MANAGEMENT

RED TEAM

L'attività di *Penetration Test*, con le sue fasi dislocate lungo la Cyber Kill Chain, costituisce un'attività concordata con il cliente e condotta simulando un realistico attacco hacker contro il target, al fine di rilevare vulnerabilità, misconfigurations, impreparazioni del personale, disclosure di informazioni e così via.

Reconnaissance

- Quali dati sono disponibili pubblicamente sull'azienda?
- Quali sono le risorse raggiungibili dai potenziali attaccanti?

Vulnerability Assessment

- Vi sono punti di accesso alla rete interna dell'organizzazione?
- Vi sono vulnerabilità dovute a mancanza di patch, misconfigurations, codice insicuro e così via?

Exploitation

- Le vulnerabilità riscontrate consentono di accedere alle risorse dell'azienda?
- L'azienda è vulnerabile a tecniche di Social Engineering?

Post-Exploitation

- Quali informazioni è possibile trafugare?
- E' possibile infettare ulteriori risorse mediante lateral movement?

Preparation

Occorre innanzitutto procedere all'implementazione delle misure di difesa necessarie (firewall, antivirus, IDS, IPS, Updates…), nonché ad istruire il personale affinché sappia riconoscere attacchi di social engineering. In tale fase è altresì fondamentale predisporre tutti i documenti necessari per gestire le procedure da attuare in caso di rilevato attacco, in particolare il comunication plan.

Detection & Analysis

Questa è la fase delicata in cui il monitoraggio della rete e degli hosts, mediante gli strumenti a tal fine installati (IDS, IPS…), deve permettere di rilevare prontamente comportamenti sospetti. Conseguentemente, il personale competente ed istruito dovrà verificare l'esistenza o meno di un security incident.

Containment, Eradication & Recovery

Rilevato un attacco, compito dell'Incident Response Team, a tal fine istruito, sarà primariamente quello di contenere l'infezione ed evitare la sua diffusione. Quindi, si potrà procedere alla disinfezione totale del sistema (se possibile) ed al suo reintegro nel processo produttivo, una volta accertata la sua sicurezza e monitorata comunque la sua attività.

Post-Incident activity

Le attività compiute e le lezioni apprese non vanno disperse, al contrario devono essere oggetto di analisi e studio in modo da migliorare il sistema difensivo e tenerlo aggiornato.

PARALEGALE IT S.R.L.
OUTSOURCING MANAGEMENT

3. GDPR Compliance

- Un CSIRT (*Computer Security Incident Response Team*) necessita di competenze multidiscplinari, inclusa quella legale diretta a verificare le conseguenze giuridiche di un *Data Breach*.

- E' fondamentale verificare l'adeguatezza, informatica e legale, dell'organizzazione rispetto alla normativa *Privacy*. La Paralegale offre tale servizio in forma integrata e collegata con la Cyber Security.

PARALEGALE IT S.R.L.
OUTSOURCING MANAGEMENT

Contatti

Paralegale IT s.r.l.

Indirizzo: Via Musumeci n. 137 - 95129 Catania

Tel: 0958361648, 0958361649

Fax: 09522463194

Mail: info@paralegale.it