



CYBER RISK MANAGEMENT



STUDIO E REPORTISTICA DELLE PROBLEMATICHE AZIENDALI IN AMBITO DELLA SICUREZZA INFORMATICA, SUCCESSIVE CONTROMISURE O RISOLUZIONE DEGLI INCIDENTI CON RIGUARDO ALLE INTRUSIONI E AGLI ATTACCHI ESTERNI. PROPOSTE DI AFFIANCAMENTO IN AMBITO DI SOCIAL ENGINEERING E GESTIONE DELLE QUESTIONI FORENSI.

I SERVIZI OFFERTI 1/3



Information Security Assessment preliminare

- Analisi della sicurezza dei sistemi informatici rispetto alle male configurazioni e vulnerabilità più diffuse (un test preliminare che, pur non sostituendo un assessment completo, fornisce al management una fotografia della situazione dei sistemi ad un costo limitato).

Application Security Assessment

- Audit della sicurezza di applicazioni Web e native, con tecniche di analisi whitebox e blackbox (l'analisi consiste nella ricerca di vulnerabilità nel codice e nell'indicazione di eventuali misure correttive).

Incident Response e Digital Forensics

- Acquisizione dati e analisi forense di sistemi informatici compromessi (ricostruzione timeline incidente e stesura di reportistica utile in sede giudiziaria).

Monitoring

- Implementazione e gestione sistemi per il monitoraggio di tutti i parametri informativi dei sistemi informatici aziendali, con notifiche istantanee su malfunzionamenti e anomalie.



Information Security Assessment

- Valutazione dei rischi informatici attraverso l'assessment dell'infrastruttura aziendale, rispetto ad attacchi esterni ed interni (Penetration Test/ Vulnerability Assessment/ Social Engineering/ Reti wireless IEEE 802.11) con report tecnico ed esecutivo del lavoro svolto e definizione delle azioni correttive.
- Valutazione dell'incolumità fisica dei dati, rispetto a furto, distruzione o danneggiamento dei dispositivi di archiviazione.
- Definizione di un modello ciclico di controllo e sviluppo per la sicurezza informatica.

Monitoring delle risorse di rete utilizzate dagli utenti

- Allarmi su anomalie d'utilizzo, tra cui tentativi di accesso a risorse non autorizzate o fuori dagli orari di lavoro.
- Valutazione e pianificazione di miglioramenti funzionali per il sistema informativo aziendale.

IDS (Intrusion Detection System)

- Installazione, configurazione e mantenimento di sistemi per il rilevamento delle intrusioni (HIDS/NIDS), utili ad evidenziare compromissioni attraverso l'analisi delle anomalie di rete e di sistema.



I SERVIZI OFFERTI 3/3

Honeypot

- Installazione, configurazione e mantenimento di sistemi "trappola" (high/low interaction), volutamente vulnerabili e isolati, utili ad ottenere allarmi preventivi in caso di scansioni e attacchi verso il sistema informativo aziendale.

IsaaS (Information Security as a Service)

- Un pacchetto completo per la gestione della sicurezza informatica in outsourcing. Il servizio comprende audit periodici delle vulnerabilità, la gestione delle notifiche generate dai sistemi di monitoring/sicurezza e risposta rapida alle emergenze informatiche (CERT).

Seminari e corsi di formazione

- Aiutare le vostre risorse a capire la potenzialità del web e degli strumenti informatici.
- Aiutare le vostre risorse a capire come proteggersi dagli attacchi informatici.