adfor
Idee
Persone
Soluzioni

QUICK ASSESSMENT CYBER SECURITY

Perché governare il Cyber Risk?

Il rischio Cyber è diventato, negli ultimi anni, sempre più oggetto di interesse da parte delle istituzioni pubbliche e delle aziende private a causa della digitalizzazione di tutti i processi di business. Le minacce che si possono concretizzare, così come affermato nelle ultime edizioni del Global Risk Report del World Economic Forum, presentano un indice alto sia in termini di probabilità di accadimento, sia di entità dell'impatto. Tale rilevanza deriva dal fatto che il rischio cyber include uno spazio concettuale molto ampio, in cui le conseguenze di un attacco possono implicare **perdita di capacità operativa**, **furto di dati**, **danni di natura reputazionale**, **minore attrattività del Brand**, **tutela dei propri clienti**, **salvaguardia della proprietà intellettuale con conseguente riduzione dei vantaggi economici**.

Per questi motivi, il tema merita un'attenzione sotto differenti profili: tecnologico, giuridico, di analisi e valutazione del rischio, di conformità regolamentare e, non ultimo, di maggiore Awareness nei confronti del management aziendale.

Benefici e obiettivi

Obiettivo del Quick Assessment è quello di offrire all'azienda un approccio per affrontare la **Cyber Security**, al fine di ridurre il rischio legato alla minaccia **Cyber**. Questo approccio è legato a un'analisi dei rischi e non a standard tecnologici. L'approccio prende spunto dal Framework for Improving Critical Infrastructures Cyber Security emanato dal NIST (National Institute of Standards and Technology).

L'Assessment, così condotto, tende a dare risposta alle seguenti sei questioni centrali:

- Che cosa vogliamo difendere?
  Identificazione degli Asset
- Da chi o cosa lo vogliamo difendere?
  Identificazione delle Minacce
- Perché pensiamo di doverci difendere?
  Identificazione delle Vulnerabilità
- Come ci possiamo difendere?
  Identificazione delle Contromisure
- Come gestiamo un attacco?
  Incident Management
- Quanto sono riuscito a difendermi?
  Monitoraggio e Controllo

Adfor S.p.A. Str.3 Pal. B4 V.le Milanofiori, 20090 Assago MI Web: www.adfor.it Tel.: 02.25201411 Fax: 02.2550215 E-mail: info@adfor.it

adfor
Idee
Persone
Soluzioni

A chi si indirizza?

Le imprese di ogni settore di attività possono beneficiare del Quick Assessment. In particolare, si rivolge a chi in azienda è responsabile della comprensione e della gestione del rischio Cyber:

- i Responsabili IT e della Sicurezza Informatica (**CIO** e **CISO**);
- le Funzioni a presidio degli Operational Risk (**CRO**);
- fino ad arrivare ai vertici dell'impresa (**Top Management e Board**).

NIST Framework

Il Framework comprende cinque macro-funzioni che rappresentano l'intero ciclo di vita per una corretta gestione del rischio Cyber:

1. **Identify**
2. **Protect**
3. **Detect**
4. **Respond**
5. **Recover**

Le cinque macro-funzioni rappresentano il massimo livello di astrazione previsto dal Framework. Esse rappresentano la struttura del Framework attorno alla quale sono organizzati tutti gli altri elementi. Le cinque macro-funzioni si declinano infatti in 22 categorie e 98 sottocategorie.

La nostra proposta

L'intervento di Assessment inizia con un processo di **contestualizzazione del Framework** rispetto alla realtà della vostra azienda, prosegue con una serie di **interviste – di taglio "tecnico / operativo"** – da condurre con i Responsabili IT e con alcuni Key-Users, si conclude con la restituzione di un **Report** che documenta il **Maturity Level** della vostra organizzazione nella gestione del Cyber Risk. Nel report sono indicati quelli che potrebbero essere gli spunti di miglioramento e le iniziative progettuali – organizzate in un **Master Plan** – per colmare i Gap con un approccio Risk-Based.

Adfor si avvale, nella conduzione dell'Assessment, di specialisti che hanno maturato ampia e rilevante esperienza in ruoli di responsabilità all'interno di primarie aziende italiane.