Il Regolamento Digital Operational Resilience Act (DORA)

Il Regolamento DORA

Impatti ed opportunità dei Regulatory Technical Standards (RTS) DORA

I ***Regulatory Technical Standards*** **(RTS)** del DORA dovranno essere considerati dalle **entità finanziarie** come elementi di **reale valore.**

Come CDP sta rispondendo agli RTS?

1. ***Information sharing***
2. ***Risk Management***
3. ***Incident Management e Reporting***
4. ***Supply chain management***
5. ***Threat-Led Penetration Testing***

IMPATTI

1. **CDP** esegue **attività di Threat Intelligence** e **scambio di Informazioni sulle minacce informatiche** (sessioni di confronto, ad esempio «5+1»).

   CISO CDP Community

2. **CDP identifica** le **aree** in cui è necessario **migliorare la sicurezza informatica** e sviluppa **piani di mitigazione** per ridurre l'impatto delle minacce informatiche.

3. **CDP** definisce e implementa una **cybersecurity dashboard** idonea a rilevare **vulnerabilità**, **minacce**, **incidenti** e **attacchi informatici.**

4. **CDP esternalizza i servizi ICT** in un'ottica di **gestione del rischio terze parti**, formalizzando la **Governance** del processo e utilizzando un **Framework documentale** predisposto ad hoc.

5. **CDP** sta incrementando le attività di **Pentesting e Security Assessment**, già orientate all'esecuzione di verifiche di sicurezza sulla base del **Threat Landscape attuale.**

OPPORTUNITA'

- ***Innalzamento dei presidi di sicurezza*** *organizzativi, procedurali e tecnologici e definizione di un* ***Modello Operativo*** *per la sicurezza* ***di Gruppo.***
- ***Incremento degli investimenti destinati alla sicurezza*** *al fine di rafforzare il sistema di Governance e di Operations della Cybersecurity dell'intera organizzazione.*
- *Implementazione di un* ***modello architetturale Zero Trust*** *come strategia per la modernizzazione della difesa dei sistemi.*

Quali strumenti utilizzare per monitorare e mantenere la conformità

L’approccio di CDP per il mantenimento della conformità

CYBER SECURITY FRAMEWORK DI CDP

CDP ha finalizzato un proprio Framework di Cybersecurity utilizzando un **approccio integrato** a partire **dall’adozione** di **standard**, **normative** e **best practices** su base **progressiva** e **volontaria** (e.g. **la Circolare 285/2013** e ss.mm.ii. della **Banca d’Italia; NIST Cybersecurity Framework; COBIT; ISO/IEC 270001;** etc).

CDP si serve di una **strategia di cybersecurity** che le consente di mettere in campo le **giuste contromisure** per la **gestione del rischio cyber**:

ZERO TRUST

Applichiamo il **Paradigma Zero Trust,** basato sul principio che **nessuno** dei **dispositivi**, **utenti** o **applicazioni** all’interno della **rete aziendale** deve essere considerato **affidabile** fino a quando non **vengono verificati o autenticati.** Tale paradigma è stato approvato all’interno del **Piano della Sicurezza 2022-2024.**

RISK ANALYSIS

Abbiamo strutturato un processo periodico di **analisi del rischio cyber**, con l’obiettivo di **monitorare** e **prevenire** le **minacce informatiche** a cui siamo esposti. In particolare, abbiamo avviato **specifiche progettualità** anche presso le Società del Gruppo CDP in ambito ***«Security Information Risk»***.

SECURITY BY DESIGN

Applichiamo la metodologia **Security by Design**, che prevede **l’integrazione** della sicurezza in tutte le iniziative di business fin **dall’inizio** del **processo** di progettazione dei sistemi o applicativi, finalizzato a rendere fin da **subito sicuri** i nostri **sistemi** e le nostre **applicazioni (es. Progetto «Mobile Security Strategy»).**

GESTIONE DEI RISCHI DI TERZE PARTI

Applichiamo un solido processo di verifica e monitoraggio delle **Esternalizzazioni e dei Servizi ICT forniti da Terze Parti, in linea con le indicazioni della Circolare 285/2013 di B.I.** Effettuiamo **controlli ex ante** per valutare l’adeguatezza dei fornitori e **controlli ex post** per verificare il mantenimento dei requisiti di sicurezza.

Come si configura un’azienda resiliente

La Resilienza Operativa Digitale

6 aspetti che rendono un'azienda «*Cyber resiliente*»

La **cyber-resilienza** è la **capacità di un'organizzazione di gestire** al meglio la **propria attività durante una violazione** dei dati o un cyber attacco. Al fine di garantire **l'adeguatezza dell'intero sistema ICT è necessario:**

Condurre, almeno annualmente, **un adeguato numero di test** di sicurezza e resilienza sui propri **sistemi e applicazioni ICT critici**.

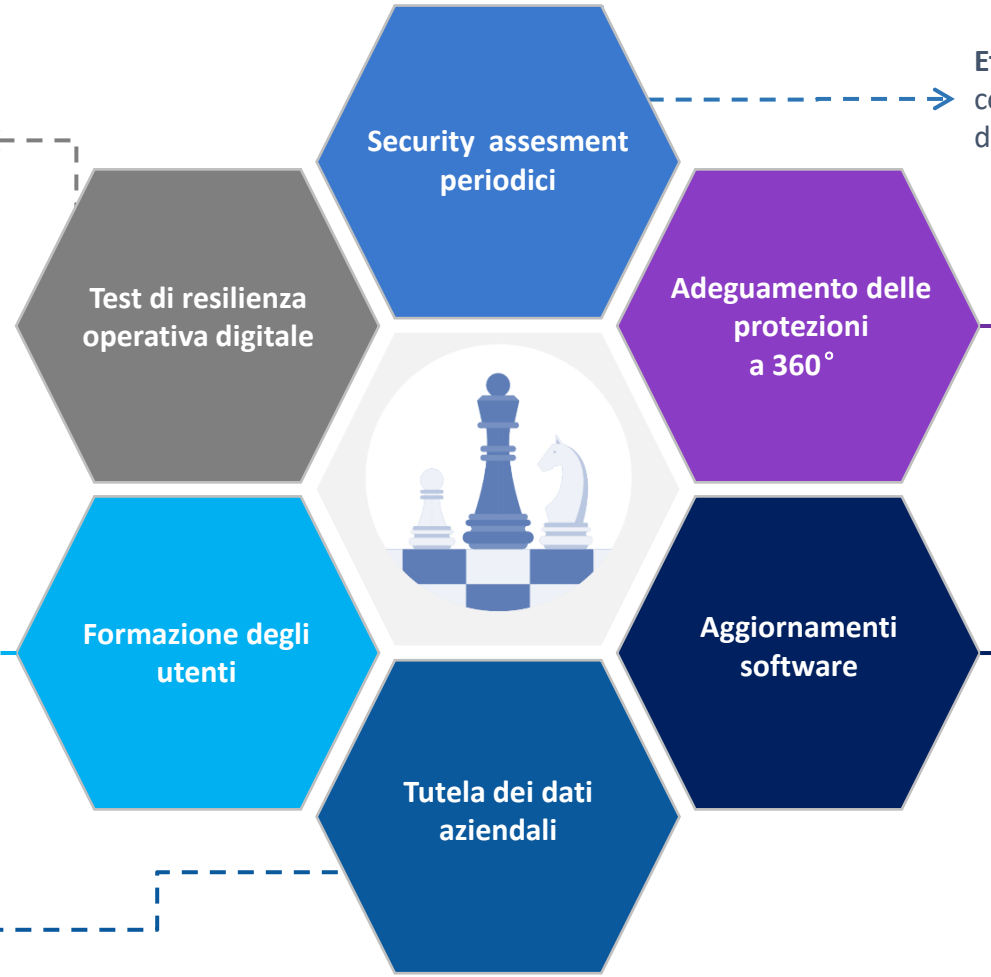
Effettuare assessment periodici del rischio, al fine di conoscere le vulnerabilità aziendali in funzione dell'emergere di nuove minacce.

Svolgere programmi di sensibilizzazione al fine di **accrescere il grado di consapevolezza** sulla sicurezza.

Adeguare le linee di difesa dell'intera organizzazione, garantendo la **compliance normativa** e la **sicurezza** delle **architetture**.

Adottare strumenti di **classificazione** delle **informazioni** aziendali (data security) e **sistemi di Data Loss Prevention.**

Utilizzare **software sempre aggiornati,** tramite un sistema di **patch management efficace**.



Come implementare DORA su tutti i dipendenti

Come implementare DORA su tutti i dipendenti?

L'art. 5 del **Regolamento DORA** prevede, appositamente per le Entità Finanziarie, un **programma di sensibilizzazione e formazione obbligatoria** sulla **gestione dei rischi ICT**, con un livello di complessità commisurata alla funzione svolta da ciascun dipendente. In particolare, i programmi e le attività di formazione dovranno:

1. Rappresentare **moduli obbligatori;**
2. **Riguardare tutti i dipendenti** e gli **alti dirigenti**;
3. Presentare un **livello commisurato** alle rispettive **funzioni**;
4. Essere rivolti **anche verso i fornitori di servizi ICT**.

Per implementare la DORA sui dipendenti di un'azienda, è necessario seguire un percorso di adeguamento che prevede i seguenti passi:

- **Definire** una **politica** di **governance** che **assegni ruoli** e **responsabilità** chiari in materia di resilienza operativa digitale e prevedere una specifica **struttura organizzativa**, coinvolgendo il management e il consiglio di amministrazione.
- **Formare** e **sensibilizzare** i **dipendenti** sulle **norme** e le **procedure** da seguire per garantire la **conformità** alla **DORA** e per gestire efficacemente gli incidenti ICT.
- **Investire** sulla **formazione** dei **dipendenti**, sulla sicurezza aziendale e su quella rivolta alle **terze parti** (**Supply Chain**).

CDP affianca alle sessioni di ***security awareness*** tradizionali, ***modalità innovative basate sull'interazione del dipendente***.