Sefin e la tutela dello spazio cibernetico

13 Settembre 2021 in **Sicurezza**

0

Lock on the converging point on a circuit, security concept - 3D Rendering

Il cyberspazio rappresenta un sistema delicato che è posto a rischio di continui attacchi da parte dei cybercriminali e ciò può essere affrontato solo adottando un forte sistema di protezione dei sistemi informatici.

Gli attacchi alla sicurezza dei sistemi informatici possono avvenire in diversi modi. Per questo motivo sarà necessario dotarsi di molteplici linee difensive in modo da poter scongiurare le situazioni di criticità a cui si è esposti.

La Cyber Security è un punto cardine per SEFIN SpA, società informatica che gestisce dati e informazioni per il mondo finanziario e creditizio e che negli anni ha costruito un forte sistema di monitoraggio e protezione, realizzando soluzioni di Credit

Management System, tools per le segnalazioni verso gli Enti di Vigilanza e servizi di conservazione digitale e dematerializzazione dei processi documentali a norma.

Affrontiamo la tematica con Marco Losa, Responsabile del Dipartimento Sistemi Informativi, e Mark Barlow, collaboratore in ICT Security presso SEFIN, che ci aiuteranno a capire il valore della sicurezza informatica, le sue politiche e le best practices attraverso cui SEFIN ha avviato un efficace e affidabile percorso di Digital Transformation.

In che modo sono organizzate le responsabilità in materia di sicurezza delle informazioni in SEFIN?

La funzione ICT Security è composta secondo una struttura organizzativa denominata "Sistemi Informativi". Inoltre, all'interno di un'altra struttura organizzativa aziendale separata, vengono gestiti gli aspetti di Risk Management, Compliance, Data Protection e Privacy che prevede anche una delega ad una terza parte specializzata per gli adempimenti GDPR. Tutti i collaboratori delle funzioni mantengono i più elevati standard e qualifiche per i ruoli assegnati, anche per quanto riguarda i processi di assunzione e di gestione delle prestazioni.

Relativamente alla governance e agli ordini di servizi ICT & Cyber, in che misura sono disponibili le politiche di sicurezza delle informazioni? E fino a che punto viene gestita la sicurezza delle informazioni all'interno dell'organizzazione?

SEFIN è certificata UNI CEI EN ISO/IEC 27001:2017dal 2019 e dispone di una regolamentazione interna esaustiva in termini di sicurezza ICT.

UNI CEI EN ISO/IEC 27001:2017è uno standard internazionale relativo alla gestione della sicurezza delle informazioni e delle comunicazioni. Lo standard è stato pubblicato congiuntamente dall'International Organization for Standardization (ISO) e dalla International Electrotechnical Commission (IEC) nel 2005 e poi rivisto nel 2013, e un aggiornamento europeo dello standard è stato pubblicato nel 2017. Questa certificazione specifica i requisiti per stabilire, implementare, mantenere e migliorare continuamente un sistema di gestione della sicurezza delle informazioni (ISMS) – il cui scopo è aiutare le organizzazioni a garantire che le risorse informative in loro possesso siano più sicure anche all'interno di un approccio CQI (Continuous QualityIm provement).

Sul tema di IAM (Identity Access Management), come viene gestito l'uso dei mezzi di identificazione? E fino a che punto è protetto l'accesso degli utenti ai servizi di rete, ai sistemi IT e alle applicazioni IT? Come vengono assegnati e gestiti i diritti di accesso?

Le misure IAM (Identity Access Management) sono pienamente in atto, sia in termini di accesso fisico che di accesso logico, incluso l'accesso remoto. Le policy IAM sono coerenti con la Certificazione ISO/IEC 27001. L'accesso fisico alle strutture è multiplo, coinvolgendo un token fisico e un codice personale.

Le misure IAM (Identity Access Management) sono pienamente in atto per salvaguardare l'accesso a sistemi e reti. Inoltre, è in atto un accesso controllato da Cisco VPN (Virtual Private Network) per gli utenti remoti in merito alle misure di sicurezza.

I livelli di accesso sono controllati e monitorati centralmente. Gli account utente vengono creati, mantenuti e cancellati centralmente secondo i principi 4-eyes e 6-eyes.

Le password sono regolate da politiche e regole specifiche e devono essere modificate con una frequenza predeterminata.

I diritti di accesso sono assegnati centralmente in SEFIN e sono strettamente monitorati. I diritti sono determinati, assegnati e monitorati in base a ruoli e livelli di responsabilità, in particolare valutando le esigenze di conoscenza. Gli utenti privilegiati sono pochi e assegnati e autorizzati con molta attenzione.

In che misura viene presa in considerazione la protezione dei dati personali nell'attuazione della Cyber Security ed è organizzata l'attuazione della protezione dei dati?

La protezione dei dati e la privacy hanno la massima priorità, sia per i collaboratori interni che per i clienti di SEFIN e sono in linea con le leggi e le normative applicabili, in particolare alla luce degli obblighi del GDPR (Regolamento generale sulla protezione dei dati).

All'interno di SEFIN, il Responsabile Risk&Compliance gestisce le responsabilità in materia di Data Protection per la Società e le responsabilità del DPO (Data Protection Officer) sono state delegate a un soggetto terzo specializzato in Data Protection.

Come vengono adottate le misure organizzative per garantire che i dati di identificazione personale siano trattati in conformità con la legislazione?

La protezione dei dati è presa molto sul serio all'interno di SEFIN, in termini di strategia, documentazione, responsabilità, istruzioni operative, obblighi di terze parti, amministrazione e gestione delle risorse umane, considerazioni sull'accesso e sulla sicurezza, nonché valutazioni, controlli periodici e monitoraggio.

Le diverse certificazioni, come UNI EN ISO 9001:2015 e UNI CEI EN ISO/IEC 27001:2017, entrambe ottenute da SEFIN, tengono tutte in considerazione l'organizzazione e le tutele della protezione dei dati; inoltre, SEFIN Strategies e il progetto Innovation Manager mantengono l'obiettivo del miglioramento continuativo in questo ambito.

I sistemi IT in che modo sono protetti dalle minacce Cyber e malware?

Il software di protezione dal malware è presente in SEFIN per la protezione dai diversi tipi di malware, inclusi spyware, ransomware e molte altre forme. Sono inoltre in essere misure anti-phishing, nonché una formazione specifica del personale, al fine di tutelarsi da tali rischi Cyber. Un Corso di sicurezza informatica ai colleghi ha affrontato in modo specifico i Rischi Cyber e Operativi, sia Impatti Attesi che Scenari Estremi. Inoltre, SEFIN mantiene un monitoraggio degli eventi esterni per capire la posture e gli eventuali rischi.

Tags: cyber security sefin

Relativi Post

SICUREZZA

Metaverso: rischi per sicurezza e AML

21 DICEMBRE 2021

'Oggi, con 2,9 miliardi di utenti dichiarati, Facebook si appresta a divenire un Metaverso dalle fondamenta assai piu' solide rispetto...

LEGGI ANCORA

ICT & CyberSec elementi di Sicurezza Sistemica /Ransomware Case Study

15 DICEMBRE 2021

CRIF-MISTERCREDIT, +8,7% FRODI IN I SEM 2021, MA CALA L'IMPORTO MEDIO

13 DICEMBRE 2021

Il datasharing e le nuove opportunità tecnologiche per le imprese

30 NOVEMBRE 2021