LA SICUREZZA DIGITALE: INFORMATIZZAZIONE DEI PROCESSI E CONTROLLI DEGLI APPLICATIVI

POLITICHE E MISURE PER LA TUTELA DEL SISTEMA INFORMATIVO INAIL

Sulla base delle normative vigenti, degli indirizzi strategici dell'Ente, dei risultati delle analisi dei rischi (tecnologici e informativi) svolte negli anni, nonché delle attività per la gestione degli incidenti di sicurezza, l'Inail ha individuato e posto in essere nel tempo una serie di politiche e misure per la tutela del Sistema informativo, mettendo a punto criteri, regole e procedure e dotandosi di vari sistemi e apparati che ne consentono la gestione e l'amministrazione.

In particolare l'Istituto ha adottato due approcci:

1. Un approccio *top/down* volto a:
    - stabilire le strategie per allineare la sicurezza delle informazioni alla sicurezza attesa dal business;
    - garantire che la sicurezza delle informazioni sia gestita in maniera efficace in tutte le attività di fornitura e gestione dei servizi;
    - analizzare, valutare e gestire il rischio in ambito ICT (*Information and Comunication Technology*);
    - fornire informazioni a organismi di vigilanza interni ed interni, ove necessario;
    - progettare, realizzare e verificare un Piano di Continuità operativa divulgare la cultura della sicurezza attraverso piani di formazione o campagne informative.

    A supporto di questi obiettivi e per contribuire e diffondere tale approccio top/down, è stato costituito il Comitato Rischi e Sicurezza ICT (*Information and Comunication Technology*), con i seguenti compiti:
    - garantire l'integrità, la riservatezza e la disponibilità delle informazioni trattate nel Sistema Informativo dell'Istituto e nell'ambito dei processi della Direzione centrale organizzazione digitale;
    - garantire piena conformità alla normativa vigente con particolare riferimento alla normativa in ambito privacy;
    - promuovere le azioni finalizzate ad accrescere il livello di sensibilità e competenza del personale e degli utenti sulle tematiche della sicurezza delle informazioni e della *business continuity*, diminuendo il rischio di comportamenti non adeguati che possano compromettere il patrimonio informativo di Inail.
2. Un approccio *bottom/up* volto a:
    - implementare e gestire le misure di sicurezza tecniche necessarie alla mitigazione delle vulnerabilità individuate dal processo di analisi e valutazione

del rischio;

- verificare la conformità alle normative, alle policy e alle Linee guida definite dall'Istituto;
- effettuare verifiche tecniche sui sistemi - IT *(Informatici e Telematici)* - (*Vulnerability Assessment*, collaudi di sicurezza applicativa, *Penetration Test* applicativo a campione).

Relativamente al perseguimento dell'obiettivo di evitare le frodi, le misure in essere si sintetizzano di seguito:

a) per quanto concerne la sicurezza logica:

- un sistema per l'identificazione e autenticazione informatica (Access Management, Single Sign On, automatismi nella gestione delle password, autenticazione forte tramite smart card);
- una infrastruttura di Strong Authentication, basata su OTP (One Time Password);
- un sistema di gestione delle Identità Federate, conforme alle specifiche di SPID (il Sistema Pubblico delle Identità Digitali);
- un sistema di autorizzazione utenti interni/esterni (profilazione con possibilità di profili multipli per singolo utente);
- un sistema di autorizzazione in cooperazione (sistema di autorizzazione in cooperazione applicativa);
- un'infrastruttura di firma digitale centralizzata (utilizzato per DURC, GRA e Documentale);
- un servizio di test di vulnerabilità delle applicazioni;
- un servizio di tracciatura delle operazioni effettuate sui dati e sui sistemi;
- l'auditing operativo del traffico applicativo e segnalazione abusi;
- sistemi per la protezione delle comunicazioni (Sistemi Firewall per la sicurezza perimetrale, sistemi IPS (Intrusion Prevention System) per la rilevazione delle intrusioni, sistemi di monitoraggio degli accessi alle basi dati, in grado di segnalare trattamenti anomali sui dati, utilizzo del protocollo HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer) nella trasmissione dei dati in rete con cifratura del canale con SSL (Secure Socket Layer), sistemi per la raccolta del traffico per finalità forensi);
- soluzioni per la protezione dei sistemi (server, desktop, laptop, tablet, smartphone) quali antivirus, antimalware e anti intrusione;
- un servizio di verifica delle vulnerabilità dei sistemi (Vulnerability Assessment);
- sistemi per la protezione dei documenti con tecniche di crittografia e DLP (Data Loss Prevention) finalizzate a individuare e bloccare attività non autorizzate su documenti critici e riservati;
- un sistema per la correlazione dei log raccolti da fonti differenti (sistema di correlazione dati che aiuti a rilevare anomalie sulla base di eventi, spesso leciti se presi singolarmente, occorsi su piattaforme diverse o in tempi

differenti).

b) Per quanto concerne la sicurezza procedurale e organizzativa:

- norme, Linee guida e procedure di sicurezza e privacy (ad es. politiche di gestione delle password);
- il Piano per la sicurezza e privacy;
- la realizzazione di audit operativi interni;
- la definizione di un organigramma (ruoli e strutture) per la sicurezza e privacy che prevede anche la costituzione di uno specifico Comitato interno alla Direzione centrale organizzazione digitale;
- la presenza da diversi anni del Computer Emergency Response Team (CERT) Inail per la gestione degli incidenti di sicurezza, che collabora con il CERT-PA di AgID (Agenzia per l'Italia Digitale);
- la realizzazione, manutenzione e verifica del Piano per la continuità operativa.

LA METODOLOGIA ADOTTATA PER L'ANALISI DEI RISCHI DATI

L'analisi del rischio identifica le cause più probabili di rischio per un'azienda, valuta accuratamente il grado di esposizione ad esse e determina quali misure di sicurezza, quante, ed in che modo debbano essere realizzate.

L'analisi è quindi focalizzata sulle circostanze possibili o probabili che possono causare il verificarsi di rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta.

L'esame dei rischi, inoltre, viene effettuato tenendo conto della natura dei dati e delle caratteristiche del trattamento, in linea con le indicazioni contenute nelle normative di riferimento.

L'Inail, con l'obiettivo di manutenere un Sistema per la gestione della sicurezza delle informazioni (SGSI) in linea con le indicazioni dello Standard ISO 27001, effettua ogni anno, assieme alle altre iniziative correlate alle tematiche di sicurezza, l'analisi dei rischi.

La realizzazione e la gestione del Sistema per la gestione della sicurezza delle informazioni, consente all'Istituto di dimostrare la conformità e l'efficacia delle proprie scelte organizzative e delle attività operative poste in atto per garantire le tre proprietà fondamentali della sicurezza delle informazioni: la riservatezza, l'integrità e la disponibilità, nonché di assicurare la continuità delle attività istituzionali, la minimizzazione dei danni in caso di incidenti e la massimizzazione degli investimenti effettuati per l'implementazione e la gestione della sicurezza.

In siffatto contesto, per delineare le strategie di sicurezza più adeguate, l'Inail svolge l'attività di analisi con il supporto metodologico offerto da *RiskWatch*, scelta adottata anche da altre amministrazioni pubbliche e aziende private, in grado di elaborare i risultati dell'attività di *risk assessment*.

Tale processo di *risk assessment*, costituito dalle fasi di *risk analysis* e di *risk evaluation*, è condotto, con riferimento al "perimetro ICT (*Information and Comunication Technology*)" prescelto dall'Inail, utilizzando la metodologia qualitativa TLQE-QUAL, supportata dallo strumento *RiskWatch* e ritenuta più adeguata allo scopo e più semplice nella applicazione.

La metodologia TLQE-QUAL prevede che venga effettuata la valutazione dei "rischi

effettivi” elaborando il livello di protezione, inteso come “mancanza di protezione” (IRI

– *Impact Relative Index*) e del “rischio potenziale o intrinseco” che si avrebbe se non fossero presenti le salvaguardie/controlli a protezione dei beni compresi nell’ambito sotto analisi.

Il livello di protezione viene valutato tramite l’acquisizione di informazioni soggettive (risposte a questionari) e oggettive (risultati di *Vulnerability Assessment* sistemistico) che consentono di confrontare la situazione reale con la situazione di protezione ottimale costituita da un modello che comprende un insieme di controlli/criteri di sicurezza che dovrebbero essere attuati nell’ambito sotto analisi.

La scelta degli intervistati è fatta per aree funzionali e/o per singoli beni (*asset*) e il set di domande è scelto in fase di modellizzazione svolta dal team di analisi sulla base delle specifiche esigenze di conformità alle normative (d.lgs. n. 196/2003, provvedimenti del Garante, requisiti di sicurezza derivati dallo standard ISO 27001, ecc.).

Il rischio potenziale invece viene derivato dalle probabilità di accadimento e dall’impatto che si potrebbero avere per ciascuna minaccia, in base a valori statistici standard e a valori locali specifici dell’analisi in oggetto.

In particolare la valutazione del rischio potenziale in TLQE-QUAL viene fatta procedendo con l’analisi delle minacce; tale attività consente di mettere in relazione, acquisendo o confermando quanto già presente nello strumento, i valori di probabilità/frequenza annuale e di impatto di ciascuna minaccia sull’ambito sotto osservazione.

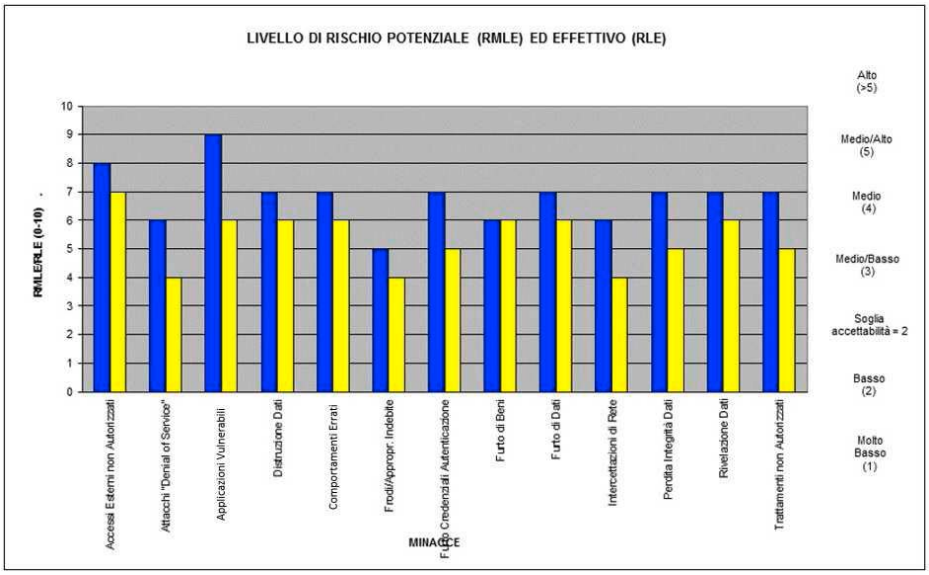
I risultati delle elaborazioni svolte con il supporto dello strumento *RiskWatch* sono riportate in un report di sintesi contenente indicatori e raccomandazioni utili per effettuare le scelte più adeguate per la sicurezza delle informazioni e per la protezione dei beni. Le analisi avvengono mediante campagne periodiche, l’ultima è stata svolta in ambiente sviluppo con lo scopo di controllare ed indirizzare i requisiti di sicurezza a partire dal primo anello del ciclo di vita del software, per evitare che le eventuali carenze di sicurezza vengano propagate fino all'esercizio.

Il perimetro dell’attività è stato identificato in un sottoinsieme consolidato di applicazioni. In particolare, per identificare il perimetro di riferimento sul quale condurre l'analisi dei rischi dell'area sviluppo, sono state svolte alcune attività mirate ad individuare un campione di applicazioni mediante:

- l'identificazione della tipologia dei dati trattati;
- la macro-categoria (istituzionale, gestionale);
- l'esposizione (internet-intranet);
- i risultati dell'attività di verifica della sicurezza applicativa.

L’analisi dei rischi è stata effettuata mediante la tecnica dell’intervista ai referenti di sviluppo delle applicazioni individuate.

Di seguito il grafico di riepilogo che riporta il livello di rischio potenziale e quello effettivo:



LA CREAZIONE DI UN SISTEMA STRUTTURATO DI MONITORAGGIO ATTO A RIDURRE IL RISCHIO DI UN UTILIZZO IMPROPRIO DELLE INFORMAZIONI

Per quanto concerne il monitoraggio della sicurezza e della riservatezza delle informazioni, si proseguirà ad agire nei seguenti ambiti:

- attività periodiche di *assessment*, analisi dei rischi di sicurezza, *penetration test* applicativo a campione;
- sviluppo e aggiornamento di norme, linee guida e procedure in materia di controllo su sicurezza e privacy;
- consolidamento delle attività del Computer Emergency Response Team (CERT) Inail per la gestione degli incidenti di sicurezza;
- svolgimento di specifiche attività di verifica;
- svolgimento della attività relative alla certificazione ISO 27001 (par. 6.1.4 del Piano).

I rischi connessi alla violazione delle normative in materia di sicurezza e privacy saranno gradualmente inseriti tra i rischi trasversali, oggetto di monitoraggio continuo nell'ambito del progetto di *risk management* generale dell'Istituto.

Contestualmente sarà avviato un programma di verifiche sul territorio finalizzate a rilevare sia lo stato di attuazione delle linee guida esistenti sia le possibili azioni di adeguamento.

Considerato, altresì, come la materia presuppone adeguati livelli di competenze tecniche negli operatori, saranno richiesti all'Ufficio Formazione specifici percorsi formativi destinati a tutto il personale.

CONTROLLO DELL'EFFICACIA DELLE MISURE DI SICUREZZA INFORMATICA E TELEMATICA (IT)

È stato intrapreso un percorso di "verifiche periodiche" per il controllo:

- dell'efficacia del Sistema di gestione della sicurezza delle informazioni (SGSI);
- dell'attuazione delle policy, delle Linee guida e dei requisiti cogenti in ambito IT;
- della conformità alle normative e allo standard di riferimento ISO/IEC 27001:2013 e 9001:2015.

Nei paragrafi successivi verranno illustrate le attività svolte e la pianificazione delle future azioni.

AVVIO DI ATTIVITÀ PERIODICHE DI VERIFICA DELL'EFFICACIA DEL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI

Security Assessment

La Direzione centrale organizzazione digitale (DCOD) di Inail ha intrapreso un'attività di verifica finalizzata a valutare, nell'ambito della propria organizzazione, il livello di maturità ed implementazione del Sistema di gestione della sicurezza delle informazioni (SGSI), con particolare riguardo allo stato di attuazione e all'efficacia dei controlli di sicurezza ad esso afferenti.

Una delle attività caratterizzanti di questo progetto è consistita nella conduzione di un *assessment* di parte terza, finalizzato a rilevare lo stato dei controlli per la sicurezza delle informazioni attualmente in esercizio nell'Istituto e dei relativi processi di gestione dei controlli stessi (da non confondersi coi processi di business previsti dall'attuale modello organizzativo delle attività). Tale verifica è stata intrapresa allo scopo di stabilire il livello attuale di efficacia delle misure di sicurezza logiche ed organizzative, individuare gli eventuali ambiti di miglioramento, suggerire gli opportuni piani di rientro laddove le condizioni lo richiedano.

Per la conduzione dell'attività di *assessment* è stata impiegata una metodologia, sviluppata a partire da consolidati standard internazionali, con il preciso obiettivo di consentire una rilevazione puntuale non solo dello stato delle contromisure tecniche e organizzative per la sicurezza delle informazioni, ma anche dello stato dei processi di gestione delle stesse in termini di efficacia e maturità dei medesimi.

Agendo su queste due dimensioni, una maggiormente tecnica e l'altra maggiormente gestionale, la valutazione si estende dal mero adempimento di soli fatti tecnici puntuali fino a comprendere le effettive capacità dell'organizzazione di prendere decisioni, adottare strategie, reagire al mutare delle situazioni; ovvero di governare consapevolmente la propria sicurezza delle informazioni.

Per conseguire tale risultato, la metodologia adottata ha coniugato due standard internazionali di eccellenza: da un lato la norma internazionale ISO/IEC 27001:2013 (Information technology - Security techniques - Information security management systems – Requirements) per la parte tecnica, e dall'altro la consolidata metodologia CMM (Capability Maturity Model) della Carnegie-Mellon University per la parte di governo dei processi.

In particolare la metodologia adottata ha preso come riferimento i 114 Controlli elementari di sicurezza previsti dalla norma ISO/IEC 27001:2013 e ha valutato, per ciascuno di essi, i seguenti tre parametri:

- il suo livello di applicabilità, inteso come la maggiore o minore misura in cui tale controllo risulta effettivamente applicabile alla realtà oggetto di valutazione;
- il suo livello di efficacia, inteso come la maggiore o minore misura in cui tale controllo raggiunge effettivamente gli obiettivi desiderati;
- il livello di maturità del processo che governa tale controllo, inteso come la maggiore o minore misura in cui tale processo è formalizzato, compreso, adottato e attuato dalle strutture preposte alla sua attuazione.

I risultati complessivi emersi dallo studio evidenziano un livello subottimale di performance dell'Organizzazione, con solo il 7% dei controlli caratterizzati da un livello di criticità bassa, molto bassa e bassissima e ben il 31% caratterizzato da un livello di criticità alta, molto alta e altissima (il rimanente 62% è caratterizzato dai tre livelli intermedi di criticità medio bassa, media e medio alta).

Questa attività sarà ripetuta periodicamente nel 2017 e negli anni.

Vulnerability Assessment e Penetration Test Applicativo

L'attività di *Vulnerability Assessment* e di *Penetration Test* è stata condotta in modalità *double-blind*, ossia il team di analisi non aveva alcuna informazione relativa alle tecnologie e ai sistemi di sicurezza adottati nel contesto Inail né le strutture preposte alla gestione dei processi di *Incident Handling* erano al corrente dell'attività, ad eccezione dei referenti di processo designati per valutare l'andamento dell'attività nel periodo di esecuzione.

Obiettivo dell'attività, oltre a valutare la presenza di eventuali vulnerabilità, era soprattutto la valutazione dell'*effort* necessario per eseguire attività di scansione preliminare, ricerca di vulnerabilità e attivazione delle stesse in una situazione "reale" con tutte le contromisure e i processi di sicurezza del contesto attivi.

Attraverso il suddetto metodo è stato possibile stimare più correttamente l'impatto reale causato da attacchi che potrebbero sfruttare le vulnerabilità rilevate; inoltre è stato possibile verificare gli obiettivi di business e di sicurezza, valutando il grado di attenzione e reattività di fronte ad una minaccia reale da parte dei gruppi interni di gestione della sicurezza preposti al monitoraggio dei sistemi Inail.

Per questa ragione il test non è da considerarsi esaustivo in logica di vulnerabilità rilevate e completezza delle prove effettuate, ma più orientato a comprendere il grado di preparazione necessario e il grado di profondità raggiungibile attraverso una simulazione di attacco il più realistico possibile.

Considerata la natura del test (*double-blind*) l'analisi si è svolta quindi in varie fasi, come di seguito elencate e brevemente descritte:

- *Information gathering*: ricerca di informazioni inerenti l'infrastruttura e i componenti (framework, piattaforme di pubblicazione siti, ecc.) in uso presso Inail;
- Mappatura dei servizi esposti dall'infrastruttura Inail: finalizzata alla rilevazione di siti non più utilizzati e probabilmente dimenticati all'interno del perimetro Inail;
- *Discovery*: vista la natura del test, contestualmente alle attività di *Information Gathering*, è stata eseguita una attività di *discovery* utilizzando strumenti semiautomatici sui servizi esposti in funzione delle limitazioni e delle soglie rilevate. In questa fase, oltre a identificare puntualmente i servizi, sono state effettuate le operazioni necessarie per individuare la versione di software utilizzato, la tipologia e la versione di sistema operativo e altre informazioni utili per portare a termine l'attività di *Vulnerability Assessment* e di *Penetration Test*;

- *Penetration Test*: l'ultima fase dell'attività è stata effettuata approfondendo manualmente quanto emerso nelle fasi precedenti, utilizzando le opportune tecniche e gli exploit adeguati al fine di validare la vulnerabilità stessa e certificare il grado di compromissione e le possibili modalità di utilizzo, in modo da avere una reale classificazione delle stesse anche in relazione al rischio reale di un'eventuale esposizione.

Attività analoga verrà svolta in modalità *cristal box* ovvero con la completa collaborazione di tutti gli attori e responsabili della sicurezza del sistema informativo.

ATTIVITÀ PERIODICHE DI VERIFICA DI ATTUAZIONE DELLE POLICY, DELLE LINEE GUIDA E DEI REQUISITI COGENTI IN AMBITO INFORMATICO E TELEMATICO (IT)

In relazione alla conformità alle normative vigenti, saranno svolte attività mirate a verificare che il SGSI (Sistema di gestione della sicurezza delle informazioni) in essere, ed il relativo sistema di controllo interno, indirizzino correttamente e pienamente i requisiti di sicurezza previsti dalle norme, quali:

- d.lgs. n. 196/2003 - Codice in materia di protezione dei dati personali, e successive modificazioni, integrazioni e provvedimenti del Garante applicabili al contesto di Inail;
- d.lgs. n. 231/2001 - Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300, relativamente agli articoli introdotti con la legge n. 48/2008, che inseriscono i reati informatici fra quelli presupposti dal decreto;
- d.lgs. n. 82/2005 - Codice dell'amministrazione digitale, e successive modificazioni ed integrazioni.