PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5212 di Lunedì 25 luglio 2022

I rischi per la sicurezza delle informazioni nelle attività in smart working

Un documento del CNI sulle attività in smart working si sofferma sulla sicurezza delle informazioni. La normativa, il rispetto della privacy, le criticità connesse alla gestione impropria dei dati e le azioni strategiche possibili.

Roma, 25 Lug ? Con l'approvazione del D.Lgs. 8 giugno 2001 n. 231, il decreto che disciplina la responsabilità amministrativa delle persone giuridiche e delle associazioni, le imprese sono state sollecitate ad adottare "modelli e strumenti organizzativi per gestire, monitorare e controllare la protezione del proprio **patrimonio informativo**". E questo significa "assicurare un corretto utilizzo delle risorse tecnologiche e produrre le opportune evidenze che documentino via via l'efficacia dei controlli implementati".

Inoltre bisogna tener conto delle indicazioni del Regolamento Generale UE n. 2016/679 sulla Protezione dei Dati (GDPR), che prevedono:

- "la protezione dei dati fin dalla progettazione (Art. 25);
- l'adozione di criteri di *data loss* e *leak prevention* (DLP) sia per le funzioni sia per le modalità (Artt. 25 e 32);
- una forma di *application security* (Art. 25);
- la garanzia di sicurezza nel trattamento dei dati (Art. 32 commi 1 e 2);
- la definizione di una DPIA (*Data Protection Impact Assessment*) (Art. 35)".

Queste necessità e regole imposte dal legislatore italiano ed europeo "si fanno ancora più vive nel momento in cui la **realtà lavorativa subisce un repentino cambiamento** insieme ai suoi tradizionali modelli di gestione, assistendo alla **remotizzazione delle mansioni** e ad una sistematica **diffusione di informazioni** secondo canali non sempre protetti, controllati o monitorabili anche e soprattutto in rapporto all'imponente tasso di crescita dei crimini informatici".



A soffermarsi su questi importanti aspetti critici connessi da un lato alla diffusione dello smart working in seguito alla pandemia da COVID-19 e dall'altro alla crescita dei crimini informatici, è il documento CNI " Linee di indirizzo per la gestione dei rischi in modalità smart working", curato dall'Ing. Gaetano Fede (Consigliere CNI coordinatore GdL Sicurezza), dall'Ing. Stefano Bergagnin (GdL Sicurezza CNI) e del Gruppo Tematico Temporaneo "Smart working e lavori in solitudine". Il documento è stato presentato dal nostro giornale nell'articolo " Smart working e lavoro a distanza: criticità, vantaggi e prospettive future".

Riguardo al tema della **sicurezza delle informazioni nelle attività in smart working** l'articolo affronta i seguenti argomenti:

- La trasformazione digitale del lavoro e il rispetto della privacy
- I nuovi rischi connessi alla gestione impropria dei dati
- La sicurezza delle informazioni e le azioni strategiche possibili

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0499] ?#>

La trasformazione digitale del lavoro e il rispetto della privacy

Ricordando il crescente aumento per le aziende dei costi per la protezione e le conseguenze dei cyber-attacchi, che potrebbero incrementarsi anche in relazione alle tensioni e all'attuale situazione internazionale, il documento segnala come la **trasformazione digitale del lavoro** "renda ostico conciliare con immediatezza il lavoro agile (e/o il telelavoro) col diritto alla riservatezza dei lavoratori stessi nonché con la sicurezza delle informazioni/dati, specie in ambito pubblico"; anche ricordando che i controlli via web devono comunque "essere svolti nel rispetto della privacy e, prima ancora, secondo dinamiche coerenti con lo Statuto dei Lavoratori".

Detto tutto questo è utile delineare "il perimetro entro cui gli strumenti tecnologici di condivisione istantanea (es. videochiamate, conferenze a distanza, software che rilevano la presenza umana alla postazione remota, sistemi di tracciamento

delle attrezzature ecc.) agevolino la qualità delle funzioni di gestione e di comunicazione, ovvero costituiscano essi stessi delle **fonti di criticità e di stress**".

Una nota del documento ricorda come esista un "espresso divieto riguardo a qualunque uso di qualsivoglia mezzo che consenta il **controllo a distanza dei lavoratori**". In particolare - Art. 4 dello Statuto dei lavoratori, L. 20 maggio 1970, n. 300) - gli strumenti '*...dai quali derivi anche la possibilità di con-trollo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo*'.

I nuovi rischi connessi alla gestione impropria dei dati

Si indica poi che un'altra problematica da rilevare riguarda l'eventuale "**gestione impropria dei dati da parte di lavoratori** che, ad esempio, potrebbero accedere alle informazioni aziendali mediante i propri dispositivi privati (privi dei sistemi di protezione e/o del necessario aggiornamento che, generalmente, caratterizza le risorse informatiche professionali) creando molteplici criticità derivante dal fatto che questo frangente:

- consente all'impresa l'accesso a dati sensibili (es. pertinenti la sua sfera intima) del lavoratore e dei suoi congiunti (es. minorenni) che abbiano eventuale accesso ai medesimi dispositivi". Ad esempio con riferimento al cosiddetto "*sharenting*", un "neologismo derivante dall'unione dei termini '*sharing*' (condivisione) e 'p*arenting*' (genitorialità), ossia la condivisione sui social media di immagini dei propri figli";
- "genera una potenziale vulnerabilità ai danni dell'impresa in termini di perdita o furto di dati (es. dispositivi violati, smarriti o smaltiti senza prima cancellarne la memoria ecc.);
- coinvolge l'impresa nelle problematiche di natura etico-giuridica derivanti dall'accesso indesiderato ai dati di terzi", ad esempio per il lavoratore che "condivida immagini di estranei fotografati/ripresi volontariamente e/o accidentalmente", come nel caso di "un estraneo non consenziente ed accidentalmente ripreso in secondo piano nel corso di una videoconferenza avviata in un luogo pubblico".

La sicurezza delle informazioni e le azioni strategiche possibili

Partendo da queste considerazioni si sottolinea l'importanza di una "**revisione dei criteri di accessibilità e di gestione delle informazioni** condotta sia a livello materiale (es. la scelta della tipologia di dispositivi, es. privilegiando tecnologie dotate di protezioni biometriche) che procedurale, formando i lavoratori ad un nuovo modo di rapportarsi alla condivisione delle informazioni improntato ad una maggior tutela dei confini esistenti tra vita privata e professionale, resa ancor più cruciale da una modalità di lavoro che spesso annulla le medesime distinzioni sovrapponendo anzi l'ambito operativo e la compagine domestica".

E a questi presupposti strutturali "si legano, poi, alcune **azioni strategiche** ossia:

- prevedere e applicare un inventario dei dispositivi autorizzati;
- definire un inventario dei software autorizzati;
- proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server;
- attuare una valutazione e una correzione continua delle vulnerabilità;
- delineare un uso appropriato dei privilegi di amministratore (per i sistemi condivisi);
- prevedere opportune difese contro i malware;
- realizzare copie di sicurezza dei dati;
- attuare prassi di protezione dei dati;
- informare e formare i lavoratori riguardo le tecniche / contromisure sopraelencate".

Se poi si considerano che tra i settori d'impresa che ricorrono allo smart working figurano le banche, gli istituti finanziari ed altre realtà che trattano ogni giorno dati sensibili, "ecco che possiamo guardare" ? continuano gli autori del documento CNI ? "con altri occhi alla mole di indirizzi e-mail, codici, listini e report condivisi coi colleghi e gestiti, talvolta, attraverso i nostri stessi dispositivi privati" (BYOD - *Bring Your Own Device*). Queste situazioni "impongono una **maggior prudenza**, specie nel caso in cui più persone (es. fornitori, personale di servizio, corrieri, operai ecc.) abbiano normale, ancorché occasionale, accesso agli spazi di lavoro agile, in quanto una percentuale dei furti e delle violazioni informatiche denunciate ogni anno è messa in atto da estranei che hanno accesso fisico ad attrezzature lasciate incustodite (si tratta dei cosiddetti '*evil maid attacks*')".

In quest'ottica ? conclude il documento riguardo alla sicurezza delle informazioni ? "è ragionevole organizzarsi prevedendo appositi **spazi** dove riporre i dispositivi di lavoro, la memoria di massa (es. chiavette e hard-drive USB) e i documenti riservati. Ampliando ulteriormente la prospettiva, ed anche in base al valore delle attrezzature installate, è invece opportuno pensare di rivolgersi ad aziende specializzate per l'**installazione di impianti d'allarme e sorveglianza**, anche da remoto".

Per quel che concerne gli aspetti più operativi e metodologici di molte azioni strategiche descritte, il documento rimanda alle fonti specializzate e ai contributi condivisi dal Comitato Italiano dell'Ingegneria dell'Informazione (C3i) costituito presso il Consiglio Nazionale degli Ingegneri.

Tiziano Menduto

Scarica il documento da cui è tratto l'articolo:

Consiglio Nazionale degli Ingegneri, "Linee di indirizzo per la gestione dei rischi in modalità smart working", a cura dell'Ing. Gaetano Fede (Consigliere CNI coordinatore GdL Sicurezza), dell'Ing. Stefano Bergagnin (GdL Sicurezza CNI) e del Gruppo Tematico Temporaneo "Smart working e lavori in solitudine" del CNI, versione maggio 2021.

Scarica la normativa di riferimento:

Legge 22 maggio 2017, n. 81 - Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato.

Leggi gli altri articoli di PuntoSicuro su smart working e telelavoro

Licenza Creative Commons

www.puntosicuro.it