LexFori

LUOGO DI AGGIORNAMENTO ED INFORMAZIONE SULLE NOVITÀ NORMATIVE E GIURISPRUDENZIALI, NAZIONALI ED INTERNAZIONALI

1/2020

07 MAGGIO 2020

Smart Working. *Quante e quali informazioni conosciamo a riguardo?*

MARCO TRIPPODO*

La presente riflessione tende ad agevolare la consapevolezza e la padronanza nell'uso della tecnologia da parte degli operatori della giustizia, non sempre particolarmente "disinvolti" nel corretto uso di computer, telefonini e altri dispositivi tecnologici.

*****

La situazione di *lockdown* generata dalla pandemia di Covid-19 ha determinato il repentino passaggio delle attività quotidiane da un ambito "analogico" ad uno totalmente "digitale", costringendoci a fronteggiare tematiche e terminologie di carattere tecnico che, quando non del tutto sconosciute, non sono sempre padroneggiate con la necessaria competenza e dimestichezza.

Forzatamente siamo stati catapultati nel mondo dello "*smart-working*" o, nella sua traslitterazione italiana, del "*lavoro agile*".

Ma siamo sicuri di sapere **esattamente** cosa significhi?

Il concetto di *smart working* viene comunemente associato al lavoro effettuato a casa, con orari e metodologie flessibili, attraverso l'uso di tecnologie e dispositivi diversi, che consentono di rimanere in contatto con l'ambito lavorativo tradizionale (colleghi, clienti, uffici giudiziari, etc.) senza la necessità di essere *fisicamente* in un determinato luogo.

Se da una parte questa interpretazione è sicuramente corretta, dall'altra, non si pone sufficiente attenzione al reale significato del termine "*smart*" (intelligente), generando una fuorviante contrapposizione, legata principalmente al rispetto degli orari e dei luoghi, tra lo "*smart working*" casalingo e lo "*stupid working*" tradizionale.

Come stiamo imparando in queste settimane, il lavoro casalingo, spesso effettuato utilizzando dispositivi personali, attraverso linee domestiche di connessione ad internet,

* MARCO TRIPPODO vanta trentennale esperienza nel mondo dell'informatica. È esperto di IT che si occupa della realizzazione, gestione e mantenimento di siti e portali online; hosting alla configurazione del server, programmazione al design delle pagine web, dalla gestione dei contenuti al monitoraggio quotidiano delle attività di primari Studi Legali, catene della GDO.

pone seri problemi di sicurezza e riservatezza dei dati, esponendoci maggiormente alla possibilità di subire le spiacevoli conseguenze di un attacco informatico.

Di fatto, però, non è tanto il "lavorare da casa" il vero responsabile di tale rischio, quanto *la mancanza di una vera e propria* ***educazione*** *ad un approccio "smart" nell'utilizzo della tecnologia*, cosa che rende e ha reso molti ambienti lavorativi, tradizionali e non, vulnerabili e a rischio.

Molti studi legali, fiscali e tributari, medici e Pubbliche Amministrazioni, pur avendo attuato le "*best practices*" (tecniche per evitare situazioni spiacevoli), risultavano comunque vulnerabili ad attacchi di tipo più tradizionale, esponendosi al rischio concreto di furto dei dati che gestivano o accesso non autorizzato ai loro sistemi informatici.

Le conseguenze per molti sono state assai dolorose e non sempre risolvibili senza danno. Qualcuno ha "soltanto" visto tutti i propri dati crittografati e non più accessibili, qualcun altro ha perso migliaia di euro dal proprio conto bancario, qualcun altro ha rischiato di essere incriminato per ricettazione!

Il G.D.P.R. 679/2016 ha solo parzialmente aiutato a risolvere la situazione: in certi ambiti, se possibile, ha creato ulteriore confusione, gettando nel panico chi cercava di dare la corretta interpretazione al concetto di *"accountability"* [1].

Ancora oggi, a quasi due anni dall'entrata in vigore del Regolamento, assistiamo a sconcertanti episodi di *"data breach"*, come nei recenti casi del portale INPS mal configurato o in quello relativo al furto delle credenziali di accesso alle PEC degli Avvocati dei Fori di Roma, Napoli, Bari e Avellino[2].

L'inevitabile trasformazione che necessariamente subirà il nostro modo di lavorare, richiede l'adozione di un nuovo approccio, di nuove metodologie, ci impone – questo si – di essere realmente e costantemente *"smart"*.

Al di là degli aspetti più squisitamente tecnici, numerosi *"tips & tricks"* (consigli e trucchetti) consentono la compilazione di alcune semplici regole valide universalmente e che possono, se non eliminare del tutto, almeno aiutare a mitigare le criticità insite nell'uso non accorto della tecnologia.

Quello che segue è un insieme di consigli pratici pensato per una struttura articolata, con ruoli operativi differenti, amministratori di sistema che può facilmente essere adattato alla propria realtà lavorativa.

In generale, inoltre, tali regole possono considerarsi valide anche per i dispositivi mobili (smartphone, tablet), nell'uso dei quali dovrebbe essere posta una maggiore attenzione.

---

[1] Con tale termine, tradotto in italiano con "Responsabilizzazione", il Legislatore Europeo ha voluto richiamare l'attenzione sull'obbligo del Titolare del Trattamento dei Dati di porre in essere tutte le misure, tecnologiche e non, atte a garantire la corretta protezione dei dati trattati, in misura proporzionale alla *natura* e alla *concretezza dei rischi di accesso / utilizzo / furto* degli stessi. Rispetto alla "*lista della spesa"* dell'Allegato B – Disciplinare Tecnico In Materia Di Misure Minime Di Sicurezza – D.Lgs. 196/03, abrogato dall'articolo 27, comma 1, lett. d), del decreto legislativo 10 agosto 2018, n. 101, si tratta di un cambiamento epocale e di non facile recepimento, soprattutto in assenza di una reale competenza tecnica.

[2] Vedasi a riguardo: https://www.cybersecurity360.it/nuove-minacce/anonymous-e-mail-degli-avvocati-cambiare-le-password-non-basta-il-problema-e-piu-vasto/

1. *Regole per un uso consapevole degli strumenti informatici e di internet*

1.1. *Sicurezza fisica*

- **Non fornire mai le proprie credenziali di accesso ad altre persone.** L'amministratore del sistema o il responsabile designato potranno recuperare l'accesso al vostro sistema in caso di bisogno, in modo controllato e autorizzato.
- **Non lasciare la propria postazione non sorvegliata.** In caso di allontanamento attivare lo screen saver protetto da una password.
- **Evitare di salvare le proprie credenziali su fogli o altro lasciati in giro o in luoghi facilmente accessibili.**
- **Comportarsi con i propri dati sensibili come con il proprio Pin bancomat.**
- **In caso di trasmissione e/o di utilizzo dati sensibili via internet, prediligere un computer dotato di connessione di rete via cavo piuttosto che wi-fi.** Nonostante le protezioni, questo genere di reti è facilmente hackerabile senza dar luogo ad anomalie immediatamente evidenti.
- **Evitare di inserire nel pc supporti rimovibili che siano stati usati in modo promiscuo su più dispositivi.** Una chiavetta USB infetta è il modo più comune di trasferire virus e/o malware.
- **Preferire chiavette o dispositivi con il blocco di scrittura.** In questo modo si possono trasferire dati da un pc sano ad uno potenzialmente infetto, ma evitare che il pc infetto comprometta il dispositivo rimovibile.
- **Per copiare e spostare file prediligere sistemi basati sul cloud o mail**, in modo da sfruttare i controlli normalmente effettuati dai fornitori di servizio online (Dropbox, Google,Microsoft, etc)

1.2 - *Sicurezza logica*

- **Usare password "robuste" e, ove possibile, abilitare i sistemi di doppia autenticazione (sms o mail) ad ogni accesso ad un servizio.** È oramai prassi comune, soprattutto per i servizi più sensibili, l'utilizzo delle OTP (*One Time Password*), ovvero codici a scadenza, generalmente 30 secondi, inviati via SMS o generati da apposite applicazioni, da utilizzarsi una volta sola come ulteriore livello di sicurezza negli accessi oltre a username e password.
- **In generale scegliere di NON eseguire automaticamente alcunché.** Prestare attenzione ai file che possono contenere macro o altri meccanismi di esecuzione automatica di codice.
- **Ogni tipologia di file può essere un veicolo di infezione.** PDF, ZIP, JPEG, MP3, AVI, DOC (e molti altri) sono tutte tipologie di file attraverso i quali è possibile nascondere e veicolare un malware in modo assai semplice.

1.3. *MAIL*

• **Prestare sempre molta attenzione alle mail ricevute, per evitare il fenomeno del "PHISHING".** Le mail di *phishing* sono costruite in modo da apparire graficamente come legittimamente inviate da un determinato ente o soggetto. In tali mail viene richiesto di seguire un collegamento internet verso delle pagine web fasulle che, sebbene sembrino appartenere ad un organismo realmente esistente, in realtà servono a carpire informazioni di accesso. Verificare sempre esattamente il reale indirizzo web riportato sulla barra degli indirizzi del proprio programma di navigazione e, in generale, ricordarsi che NESSUNO RICHIEDE LA TRASMISSIONE VIA MAIL DEI PROPRI DATI DI ACCESSO.

• **Prestare particolare attenzione ad eventuali errori grammaticali nel testo del messaggio delle mail.** Spesso le mail fraudolente sono tradotte in modo automatico e contengono alcuni errori abbastanza evidenti. Prestare altresì attenzione ad eventuali riferimenti, quali numeri di telefono o utenze varie: verificare esattamente che ci sia corrispondenza con il proprio numero di telefono o di utenza.

• **Non aprire direttamente mail il cui mittente è sconosciuto, "strano", con un oggetto poco credibile o scritto in modo scorretto.** Utilizzare la tecnica di visualizzazione "sorgente del messaggio" per leggere il testo della mail senza correre rischi immediati.

• **Disattivare l'anteprima automatica dei messaggi di posta elettronica.** In alcuni casi, la composizione dei messaggi è tale da fare eseguire direttamente dei download di file malevoli alla sola apertura del messaggio. Disattivando l'anteprima, si potrà avere più tempo per decidere se aprire o eliminare il messaggio

• **Verificare la reale destinazione di eventuali link inseriti nelle mail.** In caso di URL compresse, utilizzare servizi online per verificarne la reale destinazione (http://www.checkshorturl.com/)

• **Non lanciare eventuali allegati direttamente dal messaggio** a meno che non si sia proceduto alla verifica EFFETTIVA del tipo di file.

• **Non dare mai nulla per scontato.** Non è detto che una mail mandata da un indirizzo di posta certificata (PEC) o da un ente conosciuto sia una mail "sicura"

1.4. *Navigazione internet*

• **Durante la navigazione internet prestare sempre la massima attenzione ai link seguiti e ai siti visitati.** Ricordarsi che anche attraverso un sito internet "innocente" è possibile scaricare in modo invisibile software malevolo in modo del tutto automatico.

• **Prestare attenzione a dove vengono fatti i click con il mouse.** In certi casi, siti internet appositamente preparati, aprono subdolamente delle finestre poco o del tutto invisibili nelle quali "girano" pagine preparate per compromettere il vostro computer.

• **Fare attenzione ai file scaricati da Internet,** soprattutto a quelli ottenuti da siti di materiale pirata (torrent, emule, etc.). Non sempre all'interno dei file compressi sono presenti SOLTANTO i file ricercati.

• **Diffidare di ogni richiesta di scaricare particolari "codec" per la visualizzazione di video o altro.** Normalmente i sistemi operativi sono già dotati di tutti i codec necessari per visualizzare i principali formati audio e video.

1.5. *Software e aggiornamenti*

• **Mantenere aggiornato il sistema operativo abilitando l'installazione automatica degli aggiornamenti.** Tutti i sistemi operativi sono imperfetti; per questo motivo sono costantemente sottoposti ad esami da parte degli stessi sviluppatori e dai cosi detti *"bug-hunters"* (cacciatori di errori), che aiutano ad identificare le vulnerabilità e ne permettono la risoluzione attraverso il rilascio di apposite *"patch"* e aggiornamenti.

• **Aggiornare con regolarità il proprio sistema operativo, secondo i canali ufficiali.** Sembra scontato ma non lo è: accertarsi sempre di eseguire le procedure di aggiornamento del proprio sistema operativo solo dai canali ufficialmente riconosciuti come validi ed autorizzati.

• **Dotarsi di un buon antivirus e mantenerlo aggiornato giornalmente.** Ogni giorno nascono circa 350.000 (350mila!) nuovi *malware*. Se pure è vero che molti derivano da entità note e riconosciute, moltissimi sono del tutto sconosciuti e sfruttano, o cercano di sfruttare, vulnerabilità appena scoperte e non risolte, o non ancora scoperte (le così dette vulnerabilità *"zero-day"*).

• **Non installare mai alcun programma se non si è assolutamente certi della sua provenienza e sicurezza.** In generale considerare sempre il dispositivo come strumento di lavoro e non di svago ma, soprattutto, strumento aziendale. In caso di necessità particolari, rivolgersi all'amministratore del sistema o al responsabile delegato.

• **Assicurarsi di attivare la visualizzazione delle estensioni dei file e dei file nascosti.** Questo accorgimento permetterà di identificare correttamente tutti i file, anche gli allegati di posta elettronica con estensione "fasulla". Spesso infatti, molti programmi malevoli vengono attivati direttamente dall'utente che, credendo di trovarsi davanti ad un file di un certo tipo (p. es. PDF o testo), in realtà aprirà un file eseguibile (programma) ritrovandosi, come nel caso dei famigerati *"ransomware"*, con molte tipologie di file criptati sul proprio disco rigido e con la richiesta di un esoso riscatto per la chiave di sblocco.

• **Ricordarsi che l'estensione REALE di un file** (cosa che, in Windows, ne determina la tipologia), **è sempre l'ultima parte del nome dopo l'ultimo punto.**

• **In caso sia necessario installare un software accertarsi che non vengano installati anche altri software aggiuntivi** quali barre del browser, estensioni "strane" etc. Meglio perdere qualche secondo in più durante l'installazione e disabilitare qualche casella, piuttosto che ritrovarsi poi con software e servizi non richiesti di difficile – se non impossibile – disinstallazione.

MARCO TRIPPODO