DRV CONSULTING SRL
Via Ca' Nave, 30 - 35013 CITTADELLA (PD)
Tel. 049 5972788 - Cell. 3473140082
Uffici: Via degli Alpini, 2b
Loc. Belvedere TEZZE SUL BRENTA (VI)
Tel. 04241750143
www.drvconsulting.it - info@drvconsulting.it
PEC: info@pec.drvconsulting.it
C.F. e P.I. 05156950288
Registro Imprese PD-0515650288 – REA PD-447548
Cap. Sociale € 2500,00

L'importanza di una scrivania pulita

A volte bastano poche, semplici regole di comportamento e di buon senso per prevenire molti degli incidenti di sicurezza che, spesso, portano anche a una violazione di dati personali. Partiamo da una delle cose più facili: tenere pulita la propria scrivania.

Cosa troviamo sulla scrivania? Documenti sparsi dappertutto oppure uno sopra l'altro a formare una pila di cose da fare o da archiviare, post-it con username e password di accesso ai computer e alle applicazioni web, numeri di telefono, nomi, password relative alla rete Wi-Fi. Sono solo alcune delle cose che di frequente si notano presso le postazioni di lavoro dentro gli uffici.

Le ragioni che portano una persona a trovarsi in queste situazioni sono sicuramente le più svariate: dalle questioni organizzative alla mancanza di direttive o di linee guida da parte della direzione, dall'eccessiva mole di lavoro cui il lavoratore è sottoposto durante la giornata alle continue interruzioni che causano cali di attenzione. Ce ne sono sicuramente molte altre, ma non è questa la sede per elencarle; ciò su cui si focalizza l'attenzione in questa riflessione è valutarne le conseguenze e i possibili rimedi.

Non sempre viene attribuito il giusto valore e prestata la necessaria attenzione alla sicurezza delle informazioni che si trattano: sono proprio le informazioni che, da tempo e di fatto, costituiscono il vero tesoro da salvaguardare. Infatti, molte aziende hanno nel tempo cercato di migliorare le proprie infrastrutture informatiche con strumenti ad alto contenuto tecnologico, con l'obiettivo di contrastare in maniera efficace gli eventuali attacchi che possono arrivare da malintenzionati all'esterno del perimetro dell'organizzazione. Consapevoli di ciò gli "hacker cattivi" (o *black hat*) hanno cercato di migliorare i loro attacchi indirizzandoli verso i punti più vulnerabili delle aziende, le persone. Ecco perché lasciare incustoditi documenti riservati sopra la scrivania, password scritte su post-it attaccati al monitor, rappresentano uno scenario in cui un potenziale attaccante (persona non autorizzata a trattare tali informazioni) potrebbe fisicamente sottrarre alcuni documenti piuttosto che aprire le danze a tecniche di "ingegneria sociale" per perpetrare vere e proprie ricognizioni ai sistemi informatici e scovare le vulnerabilità sul fronte tecnologico dell'azienda.

Alcuni esempi di queste tecniche possono essere tentativi di phishing, che spesso arrivano via e-mail (anche via SMS o via Whatsapp, ecc.) e cercano di cogliere impreparati gli utenti, che presi da mille cose da fare abbassano l'attenzione e inavvertitamente aprono la mail malevola con conseguenze spesso nefaste (primi tra tutti i *ransomware* perché potenzialmente tra i più impattanti sui sistemi informativi).

Non vanno sottovalutati nemmeno i rischi della comunicazione tra colleghi oppure con i familiari, quindi anche al di fuori della sfera stretta dell'ufficio; infatti un'altra freccia nell'arco di un attaccante può essere l'*eavesdropping*, una tecnica che consiste nell'ascoltare furtivamente o segretamente una conversazione senza avere l'autorizzazione. Lascio immaginare quali potrebbero essere le

conseguenze se le informazioni possano riguardare aspetti relativi alla sfera sanitaria oppure situazioni finanziarie di terzi.

Chiaramente tenere in ordine le postazioni di lavoro, archiviando diligentemente i documenti, adottando piccoli accorgimenti nelle attività ordinarie, non risolve i problemi di sicurezza nella loro globalità, ma contribuisce sensibilmente alla riduzione della superfice di attacco o delle vulnerabilità, aiutando nel contrasto degli incidenti relativi alla sicurezza dei dati personali e delle informazioni più in generale.

Misura che fornisce un notevole contributo al rafforzamento della *business continuity* e della sicurezza delle informazioni è senza dubbio l'implementazione di soluzioni di sicurezza. Inoltre, poiché le persone sono sempre le prime risorse che ogni organizzazione deve salvaguardare e tutelare, è consigliabile adottare tutti gli strumenti che un'organizzazione può permettersi; un esempio di tutela su tutti è rappresentato dalla formazione per sensibilizzare le persone sulle minacce alla sicurezza dei dati e sul corretto utilizzo degli strumenti di lavoro. Questa è diventata importante soprattutto negli ultimi tempi in cui l'innovazione tecnologica evolve repentinamente, destabilizzando talvolta le metodologie di lavoro, vedi ad esempio il tele-lavoro. La formazione sull'utilizzo degli strumenti di lavoro dovrebbe essere, infine, accompagnata dalla predisposizione di linee guida comportamentali (nello specifico una *clean desk policy*) che ogni lavoratore dovrà applicare per salvaguardare la sicurezza dei dati, non solo di quelli in formato elettronico.

Enrico Munaro

Information Security e Privacy Consultant