Smart Working e Sicurezza delle Informazioni

Le misure globali di sicurezza adottate in questo periodo di crisi hanno dato un brusco impulso alla diffusione di pratiche di lavoro (o didattica) da remoto. Tale soluzione già presente in Italia da diversi anni, seppur con non pochi vuoti normativi, ha trovato solo in questa emergenza una vera e propria applicazione pratica.

La Legge n.81 del 22 maggio 2017 (anche detta Legge sul Lavoro Agile) ha finalmente regolato la materia del lavoro da remoto. La normativa definisce lo Smart Working in tutti suoi aspetti giuridici: diritti dello smart worker e controllo da parte del datore di lavoro, strumenti tecnologici e modalità con cui viene eseguita l'attività da remoto.

L'approccio emergenziale di tale soluzione ha creato confusione e incertezze in molte realtà private e pubbliche porgendo il fianco a numerose minacce, aggravate dalla scarsa presenza o, più frequentemente ancora, la totale assenza di piani e procedure predefinite. Bisogna sottrarsi dunque alla tentazione di *recitare a soggetto*, ma è necessario avanzare per procedure chiare e collaudate: non improvvisazione, ma preparazione. Il Presente documento vuole essere un aiuto per le aziende e le istituzioni nel concepimento di pratiche e procedure definite e collaudate

Renorm

COMPUT ELECTRONIC

Smart Working e Sicurezza delle Informazioni

Ero... rimasto senza benzina. Avevo una gomma a terra. Non avevo i soldi per prendere il taxi. La tintoria non mi aveva portato il tight. C'era il funerale di mia madre! Era crollata la casa! C'è stato un terremoto! Una tremenda inondazione! Le cavallette! Non è stata colpa mia! Lo giuro su Dio!
The Blues Brothers

Rischi e Problematiche di sicurezza

Molto spesso a casa nostra siamo portati a trascurare le misure di sicurezza più basilari come antivirus/antimalware e si sottovalutano i piccoli rischi connessi ad una navigazione ingenua. La possibilità che i computer abbiano malware già attivi è uno scenario seriamente pericoloso e con una probabilità molto alta.

Modelli di sicurezza

Garantire *riservatezza, integrità e disponibilità* dei dati coinvolti in pratiche di smart working impone un tempestivo aggiornamento delle prassi di cybersecurity. Qualora venisse a mancare una di queste caratteristiche della sicurezza delle informazioni avremo una violazione di tali informazioni.

Raccomandazioni pratiche

Quello che ci viene dunque richiesto, è un'attenta analisi dei rischi riguardante la sicurezza delle informazioni trattate. Tale analisi dei rischi non è solo a carico del datore di lavoro, ma dello stesso dipendete che viene maggiormente responsabilizzato. Andiamo a vedere nel pratico ciò che deve essere fatto.

Le restrizioni imposte in questi giorni dal Governo hanno spinto molte aziende, e la stessa Pubblica Amministrazione, a impiegare velocemente lo schema dello Smart Working generalizzato per proseguire le attività lavorative. Sono state adottate soluzioni di Digital Collaboration, Virtual Desktop Infrastructure (VDI), altre strutture si sono adeguate in corsa acquisendo prodotti per il remote working, anche open source, dotati di un minimo di sicurezza (Software per lo Smart Working, VPN, Autenticazione a due fattori e Strumentazione aziendale preconfigurata,) e, infine, le imprudenti si sono limitate ad abilitare i protocolli di Remote Desktop (RDP) sulle postazioni aziendali, per consentire ai propri collaboratori di collegarsi da remoto alle postazioni in ufficio, oppure sfruttano i programmi utilizzati ordinariamente per l'assistenza remota.

.1 Rischi e Problematiche di sicurezza

Esistono numerosi rischi connessi allo Smart Working, alcuni connaturati e altri indotti. Chiaramente, l'attività svolta in un luogo che normalmente non è adibito a tale funzionalità, (come il domicilio, un treno, un bar, ecc..) comporta di per sé un aumento importante delle minacce a cui i dati personali e le informazioni in generale sono sottoposti.

Ricordiamo che qualsiasi violazione della sicurezza che comporta, accidentalmente o in modo illecito, il venir meno di una o più delle proprietà della sicurezza delle informazioni (riservatezza, integrità e disponibilità).

Tale violazione può accadere sia accidentalmente che di proposito: le informazioni subiscono un trattamento non previsto dal Titolare, non preventivato dalla struttura e che le misure di sicurezza adottate non hanno potuto evitare. Questo può avvenire sia a causa di comportamenti dolosi di terzi che a seguito di un semplice errore da parte di una persona autorizzata al trattamento delle stesse.

Poiché le persone operano da remoto – in questo caso da casa propria - possono utilizzare sia dotazioni aziendali sia, in molti casi, dispositivi di loro proprietà: spesso si tratta di sistemi datati, privi di patch di sicurezza e di protezione e, quindi, maggiormente esposti alle vulnerabilità. Inoltre, i dati sensibili dell'organizzazione potrebbero muoversi al di fuori della rete aziendale (i dipendenti che lavorano da casa potranno salvare i dati sui propri dispositivi, non soggetti alle misure tecniche di protezione tipiche dell'organizzazione, così esponendoli al rischio di furti e hacking).

> Il software pericoloso non riguarda solo i computer, ma ogni dispositivo. Nel 2016, le prime versioni del popolarissimo gioco per dispositivi mobili Pokemon GO richiedeva accesso completo ai dati presenti sui dispositivi. La casa produttrice ha segnalato che si è trattato di un errore, in molti hanno sospettato che la Nintendo volesse raccogliere dati per fini di marketing.
>
> https://www.nowsecure.com/blog/2016/07/11/pokemon-go-security-risks-what-cisos-and-security-pros-need-to-know/

Tutto deve dunque partire da un'attenta e ponderata valutazione dei rischi connessi al paradigma dello Smart Working ed al conseguente trattamento di tali rischi.

Valutazione del rischio:

- **Contesto**: combinazione di fattori interni ed esterni che possono avere degli effetti sullo sviluppo e raggiungimento degli obiettivi di un'organizzazione
- **Identificazione del rischio**: processo di individuazione, riconoscimento e descrizione del rischio
- **Analisi del rischio**: processo di comprensione della natura del rischio e di del livello di rischio
- **Ponderazione del rischio**: processo di comparazione dei risultati dell'analisi del rischio rispetto ai criteri di rischio per determinare se il rischio è accettabile o tollerabile.
- **Trattamento del rischio**: processo per modificare il rischio. Il rischio successivo al trattamento è detto il rischio residuo.

Una sana dose di paranoia!

People think I'm insane because I am frowning all the time

All day long I think of things but nothing seems to satisfy

Think I'll lose my mind if I don't find something to pacify

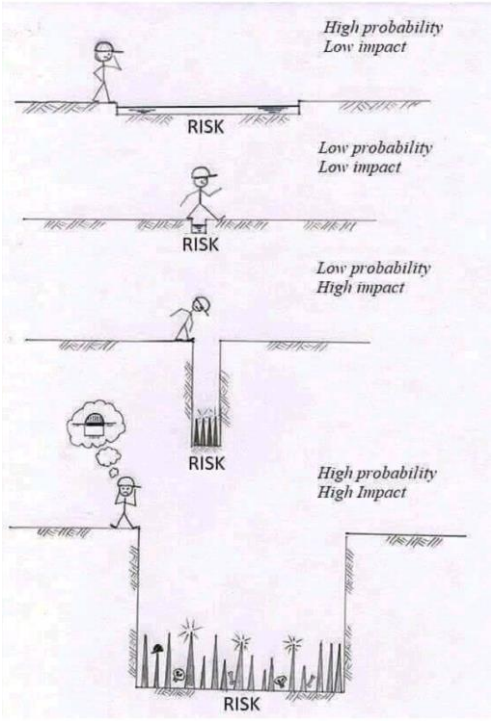
Can you help me, occupy my brain?

Black Sabbath, *Paranoid*

IL RISCHIO

ISO/IEC 27001: effetto dell'incertezza sugli obbiettivi.

- L'incertezza è dovuta a degli eventi, che possono avere degli effetti o conseguenze o impatti, negativi o positivi.



.2 Modelli di Sicurezza

Nessun sistema, informatico e non informatico, è immune da vulnerabilità. Oggi è sempre più diffuso il fenomeno detto *consumerization of IT* (COIT). Riguarda l'uso di strumenti hardware e software personali per attività lavorative (10 anni fa si aveva il problema dell'utilizzo del materiale aziendale per scopi personali, mentre oggi si ha l'inverso). Parte di questo fenomeno è noto come *bring your own device* (BYOD). In un sistema di Smart Working l'utilizzo di sistemi propri è portato all'esasperazione. L'uso di strumenti personali per le attività lavorative introduce vulnerabilità: molti non impostano le password e li fanno utilizzare da altre persone. In generale, l'uso di strumenti personali può portare alcune persone a ritenere come personali delle informazioni dell'organizzazione e quindi ad usarle in modo non corretto.

Gli obiettivi di sicurezza a cui un progetto di Smart Working deve puntare sono:

- **RISERVATEZZA**: assicurare che le comunicazioni tramite accesso remoto e i dati degli utenti interessati non possano essere acceduti da entità non autorizzate;
- **INTEGRITÀ**: rilevare qualsiasi cambiamento intenzionale o non intenzionale alle comunicazioni che avvengono durante il transito dei dati;
- **DISPONIBILITÀ**: assicurare che gli utenti possano accedere alle risorse tramite accesso remoto ogni volta che ne hanno bisogno.

Per fare ciò è necessario che tutte le componenti all'interno del sistema di trattamento delle informazioni (supporti informatici e cartacei) siano opportunatamente messe in sicurezza contro un insieme di minacce. le tecnologie di accesso remoto sono, per propria natura, maggiormente esposte a minacce esterne: per questo è necessario, *by design e by default*, prevedere un'opportuna modellizzazione delle minacce cyber che sarà inevitabile affrontare. Le principali fonti di rischio includono aspetti di sicurezza fisica, delle reti e dei devices utilizzati dai lavoratori, oltre a inevitabili problematiche di accesso. Di seguito facciamo alcuni esempi:

- **MANCANZA DI CONTROLLI DELLA SICUREZZA FISICA**: I dispositivi tramite cui il dipendente può connettersi alle risorse dell'organizzazione sono utilizzati in una estrema varietà di luoghi tutti al di fuori del perimetro di controllo dell'organizzazione
- **RETI INSICURE**: I sistemi di comunicazione utilizzabili comprendono reti a banda larga, ADSL e meccanismi wireless quali Wi-Fi e reti cellulari. È necessario assumere che le reti esistenti tra il dispositivo usato dal dipendente per operare in Smart Working e l'organizzazione non possono essere considerate affidabili.
- **DISPOSITIVI INFETTI**: La possibilità che i computer abbiano malware già attivi è uno scenario seriamente pericoloso e con una probabilità molto alta. Le organizzazioni devono assumere che i dispositivi client prima o poi si infetteranno e devono pianificare conseguentemente i propri controlli di sicurezza.
- **ACCESSI ESTERNI A RISORSE INTERNE**: L'accesso remoto fornisce a entità esterne un accesso diretto a risorse interne e protette, ad esempio server o applicativi aziendali. Le aziende dovrebbero bilanciare molto attentamente i benefici correlati all'accesso remoto con il potenziale impatto derivante dalla compromissione di tali risorse.

Attenzione!

Stai attenta, stai attenta almeno a te

Non dar la colpa a me, la colpa a me

Negramaro, *Attenta*

.3 Raccomandazioni pratiche

Quali sono le considerazioni pratiche che deve fare un'azienda?

- Dare per assodato che le reti utilizzate per l'accesso da remoto non sono sicure e agire di conseguenza;
- Dare per scontato che i dispositivi client dei dipendenti in Smart Working siano infettati da malware, predisponendo di conseguenza i relativi controlli di sicurezza;
- Cercare di posizionare le infrastrutture di accesso remoto sul perimetro della propria rete, tenendo in considerazione fattori quali le prestazioni richieste, la capacità di analisi del traffico e la gestione del NAT;
- Implementare meccanismi di autenticazione forte per validare l'identità del lavoratore remoto.
- Pianificare con attenzione le modalità di gestione e manutenzione dei client software per l'accesso remoto, ponendo attenzione che queste attività operative avvengano in maniera sicura, cifrando le comunicazioni di rete e applicando la mutua autenticazione tra gli endpoint;
- Proteggere la riservatezza e l'integrità di qualsiasi informazione sensibile che possa attraversare reti non trusted tramite l'utilizzo della crittografia;
- Mettere in sicurezza i dispositivi client devono mantenendo nel tempo un adeguato livello di protezione. Se possibile, i dispositivi client dei lavoratori remoti dovrebbero avere lo stesso livello di sicurezza dei dispositivi client aziendali.
- Avere una policy per gestire informazioni sensibili, come certi tipi di proprietà intellettuale o dati classificati, e fare uso di tecnologie appropriate (crittografia, DLP, Information Right Management);
- Definire una policy di sicurezza per lo Smart Working che individui quali sono le forme di accesso remoto consentite, quali tipologie di dispositivi sono permesse
- Disciplinare la gestione dei documenti cartacei e la conservazione di tali supporti nei luoghi esterni alla struttura
- Prendere le proprie decisioni basate sul rischio

In conclusione, conseguentemente a questa situazione di emergenza, le aziende hanno dovuto inglobare le *mura domestiche* all'interno del loro sistema di gestione dell'informazione attraverso lo Smart Working. Tale processo deve fondare su basi solide: valutazioni del rischio e ponderati sistemi di sicurezza finalizzati proteggere le informazioni aziendali. La stessa FBI mette in guardia le aziende come queste situazioni di emergenza e la conseguente soluzione dello Smart Working sia piena di insidie (https://www.ic3.gov/media/2020/200401.aspx) : l'Internet Crime Complaint Center (IC3) dell'FBI ha ricevuto ed esaminato oltre 1.200 reclami relativi alle truffe COVID-19.

Non ci facciamo fregare di nuovo!

I'll tip my hat to the new constitution

Take a bow for the new revolution

Smile and grin at the change all around

The Who, *Won't Get Fooled Again*

CRISI

Dal greco "κρίσις", che vuol dire «decisione». Gestire una "crisi", dunque, non vuol dire essere protagonisti di una catastrofe, ma governare una situazione traumatica. Le situazioni di crisi sono determinate dal verificarsi di un evento negativo indesiderato: ma indesiderato non vuol dire ignoto. Si tratta, quindi, del verificarsi concreto di un evento che prima consideravamo un RISCHIO.

Questa situazione di crisi se sfruttata può portare ad una rivoluzione digitale del nostro paese dando nuova forma e vigore al concetto di security.