ROTARY INTERNATIONAL
ROTARY CLUB DI ABBIATEGRASSO – DISTRETTO 2050
(Anno di fondazione: 1968) - Club cod. n° 0012213
Anno rotariano 2019-2020

Ufficio di segreteria: Enrico Massimo Maiocchi
Via Alessandro Lamarmora. N 6 - 20081 Abbiategrasso MI
Tel +39 0294969962 - cell +39 366 671 8858
e.mail: emmaiocchi@gmail.com

Abbiategrasso, 26 Maggio 2020

A tutti i soci del RC Abbiategrasso

Oggetto: **BOLLETTINO N. 23 DEL 26 MAGGIO 2020 –** Caminetto - La sicurezza dei sistemi informatici in smart working - Relatore: Dott. Gianluigi Monti.

Cari soci,
vi trasmetto il report del caminetto tenutosi il 26 Maggio sulla sicurezza dei sistemi informatici alla luce del forte implemento dello smart working.

Dopo aver onorato le bandiere il Presidente ha salutato le autorità Rotariane, le gentili signore e gli ospiti presenti. Un particolare benvenuto a Georg socio del Club gemello di Donauwörth e Lucy Brown, originaria del Sudafrica, attualmente ospite in Italia attraverso il programma Scambio Giovani.

Relatore della serata, il Dott. Gianluigi Monti fondatore di NETECH. Società che si occupa di integratori di sistemi (SYSTEM INTEGRATOR)**,** servizi di consulenza e progettazione su misura. La mission della società consiste nell'affiancare il cliente nel processo di innovazione tecnologica; dalla fase di analisi delle necessità, alla ricerca delle soluzioni software, hardware e cloud più adatte ad ogni specifica esigenza. Garantendo continuità al business, la sicurezza dati e una gestione efficiente dei sistemi IT.

L'emergenza coronavirus ha contribuito a "sdoganare" lo smart working.
In molti casi, tuttavia, visto lo stato di contingenza, le aziende potrebbero non aver prestato la dovuta attenzione agli aspetti legati alla cyber security e protezione dei dati personali.
In questi giorni di emergenza, le organizzazioni stanno spingendo i dipendenti a "lavorare da casa": si è quindi in un certo qual modo, "sdoganato" il lavoro "agile" o smart working. Per trarre il massimo vantaggio da questa opportunità, generata da eventi del tutto straordinari, occorre però dare la giusta attenzione ad aspetti non certo secondari, quali la sicurezza delle informazioni. Pur senza sminuire la gravità della situazione e le difficoltà connesse, vogliamo quindi evidenziare le opportunità che questo complesso scenario emergenziale può offrire.

Proveremo perciò ad esplorare le misure di sicurezza sia dal punto di vista organizzativo, che dal punto di vista del dipendente — autorizzato — ponendo l'accento sulle:

- misure relative alla sicurezza dei sistemi utilizzati da remoto;
- politiche delle organizzazioni per l'applicazione del lavoro agile;
- misure a carico del lavoratore agile.

Vediamo quali sono le principali criticità, consigliando alcuni semplici comportamenti.

Si dà per scontato che lavorare all'esterno dell'azienda (da casa) sia sicuro come lavorare in ufficio, ma ragioniamo su alcuni aspetti che dimostrano esattamente il contrario.

Le aziende più "strutturate" che hanno già adottato un regime di smart working, hanno strumenti per rispondere pienamente a tutte le necessità di questa modalità lavorativa. Hanno cioè dotato i dipendenti di dispositivi appositamente predisposti, con applicativi pronti per una fruizione remota, dispositivi telefonici virtuali (software) adeguati allo scopo, se non anche portali per la gestione del tempo lavorativo (rilevazione presenze, ecc.), in un contesto gestito in modo formalmente ineccepibile.

Molte altre aziende, invece, hanno sperimentato il ricorso all'attività lavorativa da remoto in casi sporadici e non l'hanno pertanto mai regolamentata a sufficienza, dal punto di vista informatico, non pensando ai risvolti di sicurezza e all'uso di strumenti idonei. In più stanno, quindi, spingendo i dipendenti all'attività in smart working senza avere idea di come affrontare in modo serio la questione, mettendo di fatto a rischio i dati aziendali.

Cercando di semplificare un tema che semplice non è, ci pare corretto affermare che la maggiore criticità sia data dal fatto che i dipendenti usino i loro dispositivi personali per accedere ai sistemi aziendali, incluse le connessioni di rete (ADSL, WiFi, ecc.) dove a volte non si sono modificati i parametri standard (incluse le password amministrative, disponibili con una semplice ricerca su Google).

Molto spesso a casa non si adottano (o non in maniera adeguata) sistemi antivirus/antimalaware, e si sottovalutano i piccoli rischi normalmente connessi alla navigazione in rete e accettati con ingenuità (accesso a siti pericolosi, download, ecc.).In tale scenario, è quindi alta la possibilità che i computer abbiano *malware* attivi, o che qualcuno possa intercettare le nostre comunicazioni senza particolari difficoltà: uno scenario seriamente pericoloso se si accede, in questo modo, ai sistemi aziendali.

Ecco, quindi alcuni suggerimenti pratici da adottare:

- Non usare sistemi personali, neppure per leggere la posta elettronica, ma ricorrere sempre a dispositivi forniti dall'azienda, sui quali dovrebbero essere attivi e verificati con regolarità sistemi di sicurezza adeguati.
- In caso contrario, installare almeno un buon sistema antivirus (magari quello aziendale messo a disposizione per l'emergenza) ed effettuare un'accurata scansione preventiva.
- Sempre se possibile è molto utile un sistema di gestione remota del PC, con il quale i colleghi tecnici possano monitorare e gestire eventuali problemi (come ad esempio piattaforme Kaseya, Solarwind, ManageEngine).

Da ultimo, resta ancora un aspetto assai delicato che è quello legato all'accesso (il login). Se non si usano adeguati sistemi di protezione (come protocolli sicuri e software di protezione adeguati) è possibile che le utenze e le password digitate vengano carpite. L' utilizzo di sistemi di autenticazione a due fattori (con l'uso di codici o token, in aggiunta alla normale password), risolve questo problema.

In caso contrario, si consiglia di aumentare il grado di complessità delle password utilizzate e di forzarne il cambiamento molto più frequentemente di quanto si faccia normalmente (possibilmente anche una volta alla settimana, predisponendo

tuttavia un servizio di supporto per chi inevitabilmente farà pasticci e resterà bloccato).

Nello specifico, è opportuno che l'organizzazione aziendale:

- definisca e condivida un regolamento/procedura sullo smart working nel rispetto dei principi juslavoristici;
- fornisca ai dipendenti/autorizzati i necessari mezzi per operare in modalità di lavoro agile;
- favorisca, anche alla luce delle considerazioni precedenti, l'utilizzo di dispositivi a uso aziendale, consapevole che l'assenza di tale modalità presenta tutta una serie di rischi;
- renda disponibili tecnologie e formazione proattiva nella condivisione "sicura" di documenti;
- chiarisca nell'informativa all'autorizzato quali potrebbero essere i trattamenti dei dati pertinenti ai lavoratori, sempre nel rispetto della normativa della tutela dei medesimi, che potrebbero essere trattati nell'ambito dell'attività di telelavoro;
- attivi un piano di lavoro condiviso per sapere "chi fa, che cosa" alla luce di un cronoprogramma comune facilitato dall'uso di strumenti (es. Microsoft Outlook, o Google Calendar, ecc) tali da consentire da un lato la pianificazione del lavoro, e dall'altro la visibilità di ciascuno, coinvolto da remoto;
- preveda un Team Leader per coordinare i gruppi di lavoro operativa in smart working o in formule miste (collaboratori in smart working e collaboratori presenti nei siti dell'Organizzazione);
- individui una modalità che faciliti la rendicontazione delle attività in smart working, senza sovraccaricare e talvolta ingolfare l'aspetto burocratico, pur nel rispetto dei principi che vietano il controllo a distanza. In ogni caso, i controlli nel rispetto della normativa, sono utili, necessari, e dimostrativi dell'attuazione della sicurezza in modo serio ed efficace, come si dirà.

Dal punto di vista della privacy, i progetti di smart working implicano il coinvolgimento di tutta l'organizzazione e comportano una maggiore responsabilizzazione dei lavoratori/autorizzati caratterizzata non solo da maggiore autonomia, ma anche da un orientamento ai risultati più forte rispetto al lavoro tradizionale. Il lavoro agile se da un lato consente di migliorare la produttività delle imprese e di usufruire di diversi incentivi fiscali nonché di permettere ai lavoratori una migliore conciliazione tra lavoro e famiglia, producendo pertanto maggiori

opportunità per le imprese e i lavoratori, dall'altro espone anche a maggiori rischi informatici. Il lavoro agile, o smart working, rappresenta una delle "modalità di esecuzione del rapporto di lavoro subordinato, caratterizzato dall'assenza di vincoli orari o spaziali nonché una organizzazione per fasi, cicli ed obiettivi"

Per concludere, la situazione che stiamo vivendo in questi giorni, ci insegna – oltre a mantenere la calma e a non farsi prendere da forme di psicosi eccessiva – a considerare una (qualunque) epidiemia/pandemia come un evento in grado di minare la *Business Continuity* e conseguentemente i sistemi informativi.

Allora, è bene porre in essere tutta una serie di mitigazioni di queste come di altre minacce. Le politiche – se presenti, eventualmente potenziate – di smart working ne sono senz'altro un esempio.

Una volta che avremo superato questa emergenza e saremo tornati ad una normale operatività, occorrerà:

- pensare di pianificare delle simulazioni in cui ipotizzare scenari con una disponibilità ridotta di lavoratori sia in presenza che da remoto, ovvero la mancanza di fornitori strategici;

- verificare con regolarità l'efficienza degli apparati tecnologici utilizzati per lo smart working;

- tornare a lavorare sull'analisi dei rischi, facendo tesoro dell'esperienza e delle criticità superate. L'analisi del contesto, che è il momento iniziale da cui scaturisce la consapevolezza che guiderà il modello di analisi, non potrà non considerare questa nuova grande minaccia come un fattore ad alto rischio per il sistema aziendale. Solo così saremo in grado di aumentare il livello di sicurezza dei sistemi, includendo la valutazione di una nuova minaccia (come quella del coronavirus per l'appunto, o di ogni simile evento), attivando sistemi efficaci al fine di rendere maggiormente operativa l'azienda anche in momenti di crisi, mantenendo la piena sicurezza. La serata si conclude con una serie di domande alle quali il Dott. Monti risponde in modo esaustivo, sottolineando la sua competenza in materia.

Il suono della campana conclude la serata.

Il Segretario

Enrico Massimo Maiocchi