Agenzia Entrate

Divisione Risorse
Direzione Centrale Tecnologie e Innovazione

Settore Infrastrutture e sicurezza
Ufficio Sicurezza informatica

Ufficio del Direttore dell'Agenzia
Ufficio Comunicazione e Stampa
Divisioni
Direzioni Centrali
Direzioni Regionali
Direzioni Provinciali
Direzioni Provinciali di Bolzano e Trento
Centri Operativi
Sezioni di Assistenza Multicanale

OGGETTO: Emergenza COVID-19 e smart working. Regole e buone pratiche per la riduzione dei rischi di sicurezza nel lavoro agile emergenziale.

Finalità

Le misure straordinarie adottate per il contenimento dell'emergenza da COVID-19 hanno comportato il ricorso al cosiddetto *smart working* emergenziale o lavoro agile emergenziale. L'esigenza di consentire, in linea di principio, a tutto il personale di adottare questa modalità lavorativa in un lasso di tempo estremamente ridotto ha reso necessaria, tra le altre cose, la definizione di specifici requisiti tecnici di sicurezza, tipicamente meno vincolanti di quelli ordinariamente previsti.

Con la presente comunicazione si intende sintetizzare le peculiarità del contesto di *smart working* emergenziale nonché i conseguenti rischi relativi alla sicurezza informatica, e nel contempo promuovere tutte le buone pratiche che permettano di mitigare tali rischi con l'obiettivo di mantenere, anche nella situazione emergenziale, un livello di sicurezza elevato e quanto più possibile prossimo a quello corrispondente alle condizioni ordinarie di lavoro.

Contesto di lavoro agile emergenziale e rischi di sicurezza

Il contesto di lavoro agile richiede a ciascun lavoratore una particolare attenzione ad un comportamento responsabile, in considerazione del fatto che in tale modalità di lavoro l'attività viene svolta anche tramite l'utilizzo di dotazioni personali (PC, *smartphone*/*tablet*, connessione ad Internet domestica) spesso condivise con altri membri della famiglia.

È utile infatti evidenziare che lavorare in un ambiente al di fuori della sede dell'ufficio comporta intrinsecamente alcuni elementi di rischio, tra i quali:

- non si dispone di un'infrastruttura di sicurezza efficiente e aggiornata come quella che l'Agenzia garantisce per le proprie postazioni di lavoro, che offre una protezione a più livelli;
- in un ambiente domestico sono presenti una quantità di dispositivi connessi, che possono avere delle vulnerabilità, anche non rilevate, alla cui rimozione in ogni caso si può provvedere solo con un intervento manuale e in loco;
- con l'uso condiviso dei dispositivi informatici e di comunicazione aumentano i rischi di sicurezza complessivi, in quanto sono maggiori le probabilità che uno qualsiasi degli utilizzatori tenga un comportamento a rischio;

- si utilizza la stessa rete sia per lavoro che per le proprie attività personali, con il rischio che un problema di sicurezza possa propagarsi facilmente tra i due ambienti; se l'impatto di tali eventi può essere limitato nel contesto personale, può risultare grave quando esteso alla sfera lavorativa;
- spesso si utilizza il proprio computer tramite un'utenza con privilegi di amministrazione anziché una con privilegi ordinari[1].

È pertanto importante, per ognuno di noi, porre attenzione nel mantenere alto il livello di sicurezza del contesto lavorativo anche in modalità agile. È evidente, peraltro, che l'incremento dei livelli di sicurezza delle dotazioni informatiche personali e della rete domestica, oltre che rappresentare un requisito per un contesto sicuro di *smart working* emergenziale, offre una più alta protezione della propria sfera personale e familiare.

Raccomandazioni per la riduzione dei rischi di sicurezza nel lavoro agile emergenziale

I rischi richiamati nel paragrafo precedente si possono ridurre considerevolmente attraverso comportamenti vigili e responsabili, che prevedono l'adozione di alcune misure di sicurezza macroscopicamente raggruppabili in tre categorie:

a) regole comportamentali;

b) messa in sicurezza dei dispositivi personali eventualmente utilizzati;

c) messa in sicurezza della rete domestica.

Regole comportamentali

[1] L'uso del computer con un'utenza che ha privilegi di amministrazione è sempre rischioso perché, ad esempio, in caso di infezione può consentire al malware di avere il completo controllo del dispositivo disattivando i programmi antivirus, il firewall personale e gli altri eventuali programmi di protezione, cosa che non sarebbe possibile con i privilegi da utente ordinario.

1. Non condividere mai le proprie credenziali, in particolar modo quelle utilizzate per l'accesso alle risorse informatiche dell'Agenzia o per trattare dati e documenti dell'Agenzia.
2. Evitare l'utilizzo della stessa password per servizi diversi.
3. Accedere al dispositivo con l'utenza senza privilegi di amministrazione, limitando l'uso di quest'ultima solo ai casi di effettiva manutenzione del sistema.
4. Utilizzare password complesse[2] anche per i propri account di posta personale e dei social network.
5. Attivare, se possibile, l'autenticazione a due fattori[3] per i propri servizi internet.
6. Fare sempre attenzione alle mail sospette che possono essere riconducibili a messaggi di *phishing*, anche e soprattutto nella posta elettronica personale. A questo riguardo è utile consultare le informative ed i documenti emessi dall'Agenzia e riferiti nel prosieguo del documento.
7. Fare sempre riferimento a fonti di informazione affidabili, specialmente per quanto riguarda argomenti "sensibili" come le notizie sul COVID-19, prediligendo i canali ufficiali; non è infrequente imbattersi in pagine che, promettendo per esempio di rivelare "i veri fatti che non vi vogliono far sapere", portino poi a collegamenti che fanno scaricare software malevoli o tentano di carpire le credenziali utente.
8. Per la condivisione di documenti e per la videoconferenza utilizzare di preferenza i servizi, tra quelli di collaborazione online, forniti dall'Agenzia, evitando per quanto possibile altre piattaforme.

[2] Come riferimento per comporre password di buona complessità, si possono utilizzare le regole per la password di dominio dell'Agenzia (almeno otto caratteri, almeno tre caratteristiche fra lettere minuscole, maiuscole, numeri e caratteri speciali).
[3] L'autenticazione a due fattori richiede, oltre alla password, anche un secondo elemento di sicurezza (ad esempio il codice ottenuto tramite l'app Google Authenticator per alcuni i servizi WEB o il codice ricevuto via SMS per l'accesso allo *smart working* FULL dell'Agenzia).

9. Limitare l'uso di servizi di messaggistica privata (per es. WhatsApp) al solo scambio di messaggi semplici evitando di usarli per esempio per l'invio di documenti.

Messa in sicurezza dei dispositivi personali eventualmente utilizzati

10. Accertarsi che i dispositivi utilizzati abbiano un sistema operativo supportato dal produttore e mantenerlo regolarmente aggiornato.
11. Accertarsi che sui dispositivi, laddove applicabile, siano attivi ed aggiornati i software di protezione antimalware.
12. Attivare, se disponibile, il firewall del dispositivo.
13. Accertarsi che i programmi di navigazione Internet (*broswer*) siano aggiornati e se possibile attivare l'aggiornamento automatico. Disattivare nei *browser* i componenti aggiuntivi non necessari.
14. Attivare, se possibile, nei programmi di navigazione Internet le opzioni di navigazione sicura e protezione da contenuti ingannevoli.
15. Limitare, se possibile, le autorizzazioni concesse alle applicazioni installate sul dispositivo, utilizzando gli strumenti messi a disposizione dal sistema operativo.
16. Porre attenzione ai messaggi di sicurezza del sistema operativo, del browser e dei programmi di protezione e non proseguire nell'azione in caso di dubbio.
17. Modificare le password predefinite dei propri dispositivi scegliendone una complessa.
18. Utilizzare diversi utenze per ciascun membro della famiglia nel caso si usino gli stessi dispositivi.

Messa in sicurezza della rete domestica

19. Modificare la password predefinita di amministrazione del modem/router e quella del Wi-Fi, impostandone una complessa.

20. Realizzare la connessione tra PC e router preferibilmente via cavo, ovvero, laddove non sia possibile, anche tramite Wi-Fi avendo cura di verificare che siano impostati algoritmi di protezione di ultima generazione (almeno WPA2-PSK AES 256, impostazione tipicamente predefinita nei router di ultima generazione).
21. Modificare il nome della propria rete Wi-Fi domestica (SSID), modificando quello predefinito ed evitando di sceglierne uno "parlante" (riconducibile al dipendente, ad esempio il cognome o il luogo); come ulteriore misura di cautela si suggerisce inoltre di disattivarne la trasmissione rendendolo quindi non visibile.
22. Verificare ed eventualmente disattivare l'accesso da Internet all'interfaccia di configurazione del proprio modem/router.
23. Limitare l'accesso da Internet alla propria rete interna ai soli servizi personali indispensabili. Va evidenziato che i programmi dell'Agenzia utilizzati per il lavoro agile non richiedono tale accesso mentre può essere richiesto per i giochi on line ovvero per programmi di condivisione (ad esempio Bittorrent, …).
24. Disattivare sul proprio modem/router il protocollo UPnP, che consente ad esempio ai programmi installati sul computer di aprire automaticamente porte di accesso sul router (cfr. punto precedente).
25. Se possibile, consentire l'accesso alla rete Wi-Fi solo a dispositivi esplicitamente autorizzati, ad esempio impostando esplicitamente gli indirizzi autorizzati all'accesso e negando per definizione tutti altri (tramite filtraggio del MAC address).
26. Evitare il collegamento a reti Wi-Fi pubbliche ovvero reti Wi-Fi al di fuori del controllo del dipendente, a meno che non sia per brevi periodi e sia strettamente indispensabile per l'esecuzione di attività di ufficio non differibili.

Regole e prassi già in vigore

Nell'ottica di agevolare i migliori comportamenti da parte di tutti in questa fase di lavoro agile emergenziale, si ritiene utile richiamare le principali regole e prassi di sicurezza vigenti per il personale dell'Agenzia, pubblicate sulla intranet nella sezione *Gestione Uffici – Sicurezza – Informatica*. Opportunamente contestualizzate nell'ambito dell'utilizzo domestico, queste disposizioni rivestono comunque un'importanza fondamentale nella loro interezza.

In quest'ambito si evidenziano:

1. le "Regole per il corretto utilizzo delle risorse informatiche per i dipendenti dell'Agenzia delle Entrate" del 21 dicembre 2017;
2. le indicazioni per la protezione dai rischi connessi alla posta elettronica:
   - la "Procedura operativa per il trattamento dei messaggi di posta elettronica sospetti";
   - la procedura specifica per le PEC sospette "Messaggi di PEC contenenti allegati sospetti - Procedura di gestione nel sistema di protocollo";
   - le "Semplici regole da seguire per la propria sicurezza informatica – Phishing e Ransomware".

Inoltre, nella sezione "*Personale - Rapporto di lavoro - Telelavoro e smartworking*" del sito intranet e alla pagina "Misure di sicurezza per l'utilizzo degli strumenti tecnologici di lavoro agile" della sezione *Gestione Uffici – Sicurezza – Informatica*, sono disponibili le "Linee guida operative per la configurazione degli strumenti tecnologici a supporto dello svolgimento di lavoro agile relativo all'emergenza COVID-19", che includono tra le altre cose anche tutte

le istruzioni operative necessarie per la configurazione dei dispositivi aziendali e di quelli personali ed una sintesi delle misure di sicurezza da adottare.

°°°O°°°

In conclusione e sintesi, il mantenimento di un elevato livello di sicurezza del contesto lavorativo domestico non può prescindere dalla partecipazione attiva di ciascun lavoratore nell'adottare comportamenti corretti e applicare misure di sicurezza nell'utilizzo delle dotazioni informatiche a scopi lavorativi.

E' indispensabile pertanto, in particolar modo in questo periodo di emergenza, l'impegno e la massima attenzione da parte di tutti noi per garantire il conseguimento di questo obiettivo.

L'Ufficio Sicurezza Informatica resta disponibile per offrire ogni necessario supporto.

Si prega di dare massima diffusione alla presente, portandola a conoscenza di tutto il personale.

IL DIRETTORE CENTRALE
Giuseppe Buono
Firmato digitalmente