Telsy

SECURITY AWARENESS

CYBER SECURITY AWARENESS

Emergenza “Nuovo Corona Virus”

Stay cyber safe from home

15/03/2020

INDICE

TABELLA DELLE REVISIONI

Versione	Autore	Data
1.0	Emanuele De Lucia	15/03/2020

INTRODUZIONE

L'emergenza "nuovo corona virus" ha imposto a molte organizzazioni una repentina modifica nelle modalità di conduzione delle proprie attività giornaliere e professionali. Uno dei cambiamenti più importanti che sta interessando sempre più *forza-lavoro* del Paese è sicuramente lo *smart working* o *"lavoro remoto"*.

Lo *smart working* permette di condurre le attività professionali mediante l'utilizzo di tecnologie telematiche che ci permettono di essere virtualmente vicini a Clienti e colleghi e di scambiare con loro velocemente dati ed informazioni.

Tuttavia, l'adozione repentina di tali tecnologie ed il rapido cambio di paradigma nelle modalità di espletamento del lavoro può esporre a rischi di natura *"cyber"* considerevoli.

Tali rischi derivano principalmente dal fatto che gli utenti potrebbero trovarsi sprovvisti di quelle tecnologie di sicurezza che nel tempo sono state implementate all'interno dei perimetri informatici delle società di appartenza, trovandosi costretti a gestire carichi di lavoro considerevoli da PC e connessioni di rete originariamente pensate per un esclusivo utilizzo privato.

In questo scenario ed in considerazione del fatto che non esiste una soluzione tecnologica in grado di ridurre a zero la percentuale di rischio di ogni infrastruttura informatica, il comportamento umano resta l'elemento determinante per ridurre le probabilità di intrusioni.

Se da un lato le connessioni di rete casalinghe solitamente presentano una scarsa superficie di attacco esterna in virtù del fatto che non presentano erogazione di servizi quali web, trasferimento di file, posta elettronica, etc. etc. , dall'altro c' è la necessità di considerare che la maggior parte degli attacchi fanno leva sulla distrazione, il coinvolgimento emotivo o la scarsa conoscenza e/o disattenzione dei singoli individui al fine di indurli a compiere azioni di cui

non percepiscono il rischio. (c.d. Social Engineering).

È fondamentale perciò conoscere alcuni concetti utili a metterci in condizione di non cadere nelle trappole della rete e proteggere così la nostra privacy e quella delle nostre società.

SCOPO E DESTINATARI

Il presente documento si rivolge sia a singoli individui che a gruppi di gestione IT che vogliano incrementare la consapevolezza dei rischi *cyber* dei loro utenti.

SICUREZZA DELLE PASSWORD

Utilizzare credenziali facili da ricordare ma poco robuste mette a repentaglio la propria sfera privata (diventa molto facile indovinare le credenziali d'accesso come ad esempio quelle di una casella email, social network etc. etc.) fino a rendere potenzialmente possibile l'accesso a sistemi e servizi aziendali.

Anche l'utilizzo della medesima *password* per la gestione di diversi *account* rappresenta un comportamento comune. Sotto quest'ottica infatti, è consigliabile evitare l'utilizzo di una singola *password* di accesso per più servizi, siano essi aziendali che privati (es. non usare mai la *password* della propria posta elettronica aziendale anche per altre caselle esterne [Gmail, Yahoo, Hotmail, etc.]).

Per costruire una password robusta, evitare di usare dettagli facilmente riconducibili a termini comuni o alla propria vita (spesso ricostruibile tramite social network; ad esempio, spesso è semplice reperire dettagli personali come la propria data di nascita, nome dell'animale domestico, nome dei figli, etc. etc.).
Una password forte è composta da almeno 14 caratteri alfanumerici e risponde genericamente alle seguenti caratteristiche:

1. Presenta l'utilizzo di caratteri speciali quali @ , ! , _ , *, etc. etc.

2. Presenta l'utilizzo sia di lettere maiuscole che minuscule
3. Non presenta un senso logico nella sua composizione
4. Non presenta riferimenti a parole di senso compiuto
5. Non presenta riferimenti ad informazioni personali (per esempio, date o ricorrenze, nomi di persona o animali etc.etc.)

Esempi di password considerabili forti sono:

1. **JYsz7_jkSa@kW8**
2. **kAn4Z!h3@_3x78x**
3. **4Hx_9ds*sUkj@63**

E' buona pratica considerare la robustezza della propria password come una qualità inversamente proporzionale al tempo del suo utilizzo. Nella pratica, è bene cambiare la propria password a scadenze regolari.

L'utilizzo di un software c.d. *"Password Manager"* aiuta nella gestione delle stesse. Un esempio di software utile a questo scopo è PSAFE, disponibile al link https://pwsafe.org/
Tuttavia, sono disponibili innumerevoli tool alternativi in grado di gestire le password in maniera efficace.

Riassumendo, i seguenti punti sono utili a ridurre le probabilità di incidenti informatici derivati da *password* deboli:

1. Utilizzare password forti o, ancora meglio, passphrases (https://it.wikipedia.org/wiki/Passphrase)
2. Utilizzare password uniche per ogni account.
3. Utilizzare un software per la gestione delle proprie password.
4. Utilizzare l'autenticazione a due fattori su tutti i servizi che lo permettono.

PHISHING E SOCIAL ENGINEERING

Il phishing è una frode online che mira a rubare informazioni sensibili come numeri di carta di credito, password e dati relativi al conto bancario. Tipicamente inizia con una email e ci invita a scaricare od aprire contenuti e link.

Solitamente il messaggio ha tutto l'aspetto di una notifica ufficiale proveniente da una fonte attendibile (una banca, un amico, un college etc.etc.).
Molte volte il messaggio invita a collegarsi a un sito web graficamente simile a quello originale e ad inserire alcune informazioni personali come, per esempio, il numero di conto corrente o la password dello stesso. Queste informazioni vengono poi utilizzate per appropriarsi dell'identità di chi cade nella truffa. In qualche altro caso la mail potrebbe spingerci ad abilitare contenuti inseriti all'interno di allegati come file Word o Excel.

In via generale, le email devono essere considerate sospette se:

1. sono state ricevute da persone, aziende od organizzazioni non conosciute o con le quali non si hanno rapporti professionali.
2. Richiedono di impostare e/o re-impostare credenziali di accesso a servizi sia privati che aziendali, anche se da un mittente conosciuto.
3. Contengono indicazioni che vanno a richiamare un senso di "urgenza" del messaggio.
("Si prega di voler quanto prima…", "In accordo con il CEO della società…", "In relazione alla pratica urgente di…", "Sospensione dei servizi di…")

E' importante ricordare che il social engineering si basa sullo studio del comportamento dell'essere umano, al fine di manipolarlo e spingerlo a compiere azioni volute da malintenzionati, come fornire informazioni riservate o accessi a sistemi.
Tali pratiche spesso approfittano anche dei potenziali coinvolgimenti emotivi dell'utenza e l'emergenza COVID-19 ne è un chiaro esempio. Negli ultimi giorni infatti si stanno moltiplicando campagne ostili sia in ambito cybercrime che APT che mirano a sfruttare questo argomento per portare a compimento attacchi informatici.
Rif. https://www.poliziadistato.it/articolo/385e6120220066d414895301

E' bene inoltre tenere a mente che i social network (Facebook, Twitter, Instagram, ecc.) sono la principale fonte di informazioni sulla vittima, e permettono spesso di ottenere chiare indicazioni riguardo abitudini personali, preferenze, luoghi frequentati etc.etc.

Ad esempio, un malintenzionato, sapendo che il compleanno di qualcuno è vicino, potrebbe inviare una finta *email* impersonando la palestra in cui si è iscritti al fine di proporre offerte sull'abbigliamento, spingendo in realtà a fornire delle credenziali bancarie o password di accesso a vari servizi.
Adottare nelle abitudini quotidiane degli accorgimenti utili a tutelare la nostra *privacy* mediante comportamenti virtuosi aiuta a mitigare l'esposizione ai rischi di questa pratica.

Alcuni di questi comportamenti sono riportati di seguito:

1. Non confidare informazioni sulla tua vita privata a sconosciuti.
2. Controllare e verificare le impostazioni di privacy del tuo profilo sui social network e presta sempre attenzione a ciò che pubblichi.
3. Prestare attenzione alle applicazioni che installi all'interno dei dispositivi *mobile*.
4. Evitare la partecipazione a test di personalità online.
5. Non cliccare su link sconosciuti, non accettare offerte non richieste, non accettare nulla che tu non ritenga con certezza essere legittimo.
6. Prestare attenzione anche ai social c.d. *"professionali"*. Un malintenzionato potrebbe fingersi un ***recruiter*** di grosse società per poi inviare ***malware*** nascosto all'interno di documenti quali *job description, NDA,* etc. etc.

NAVIGAZIONE

Durante la navigazione prestare massima attenzione ai programmi eventualmente da scaricare ed installare (come ad esempio quelli di lettura / modifica di documenti PDF o altro). Scaricare contenuti da siti malevoli equivale ad infettare i nostri pc e comporta diversi rischi per la nostra *privacy* e potenzialmente per l'Azienda o l'organizzazione di cui facciamo parte.

In generale, i seguenti comportamenti sono da evitare:

1. Inserimento dell'email aziendale per l'iscrizione a servizi non strettamente relazionati all'attività professionale (social network, giochi di ruolo, download di contenuti, etc.etc.).
2. Installazione di programmi di dubbia provenienza.
3. Utilizzo di web browsers insoliti.
4. Continuare la navigazione su di un sito web di cui non si sia verificato visivamente l'indirizzo URL. (I malintenzionati potrebbero infatti registrare un nome a dominio malevolo del tipo ***www.bancasocura.it*** simulando il reale sito ***www.bancasicura.it*** confidando negli errori di battitura degli utenti. Il controllo visivo dell'URL digitato aiuta a riconoscere tali frodi.
5. Non navigare su siti che offrono gratuitamente software e servizi che solitamente sono disponibili a pagamento.
6. Adottare servizi di risoluzione dei nomi a dominio (DNS) orientati alla sicurezza. Tali servizi prevengono la navigazione ed il contatto dei nostri sistemi con siti internet che gruppi di esperti dedicati classificano come *"malevoli"*.

Per la configurazione di un servizio DNS sicuro è possibile fare riferimento alle FAQ presenti ai seguenti URL:

[Windows XP/Vista/7/10/Server]:
https://blog.telsy.com/free-secure-dns-telsy/

[Android]:
https://blog.telsy.com/strengthen-android-privacy-and-security-via-telsy-free-secure-dns-over-tls/

Le procedure descritte sono valide per qualsiasi servizio DNS sicuro si decida di utilizzare.

SICUREZZA DEI SISTEMI

E' importante che i sistemi operativi dediti alle attività professionali (ed in generale tutti quelli che utilizziamo) dispongando degli ultimi aggiornamenti e possano contare sugli ultimi rilasci *software* disponibili.

E' consigliabile pertanto verificare che il servizio di *aggiornamento automatico* del sistema sia correttamente avviato ed operativo. (*https://support.microsoft.com/it-it/help/875349/how-to-change-your-automatic-updates-settings-by-using-windows-securit*)

E' consigliabile inoltre:

1. Abilitare il firewall di sistema qualora non lo fosse (*https://support.microsoft.com/it-it/help/4028544/windows-10-turn-microsoft-defender-firewall-on-or-off*).
2. Assicurarsi che **Windows Defender** sia abilitato o, in alternativa, utilizzare un prodotto anti-virus fidato di terze parti.
3. Qualora possibile non utilizzare PC originariamente pensati per uso privato per espletare attività professionali o accedere a servizi aziendali (posta elettronica, VPN, condivisione di file etc.etc.).
4. In generale, NON utilizzare sistemi operativi obsoleti o il cui supporto da parte della software house di provenienza sia terminato.

RETI WI-FI

In linea generale la normale utenza in smart working non può disporre dell'aiuto di molti servizi di sicurezza implementati all'interno del perimentro informatico della propria azienda.

Considerando che la quasi totalità delle abitazioni dispone di copertura *wireless*, risulta estremamente importante adottare delle pratiche che puntino a garantire almeno i minimi livelli di sicurezza delle nostre reti *wi-fi*.

Di seguito alcuni consigli pratici utili per irrobustire la nostra rete:

1. Modificare le credenziali di accesso al pannello di amministrazione del nostro *access point* rimuovendo quelle impostate di *"default"*. Impostare una password di accesso forte (sez. *"Sicurezza delle password"*).
2. Assicurarsi di utilizzare gli standard crittografici più alti che il nostro *access point wi-fi* è in grado di supportare.
3. Qualora possibile, modificare il *"nome"* della nostra rete wi-fi (SSID).
4. Assicurarsi di adottare password forti (sez. "Sicurezza delle password") per l'accesso dei client alla propria rete.
5. Sostituire gli *access point wi-fi* che supportano solamente standard crittografici troppo deboli (es. WEP).
6. In considerazione del fatto che una rete casalinga può servire diverse tipologie di apparati (Smart TV, IoT etc.etc.), valutare la possibilità di creare diverse reti di accesso ed utilizzarne una ad esclusivo utilizzo professionale.

DISPONIBILITÀ DEI DATI

In caso di incidente informatico casalingo che veda l'utilizzo da parte degli attaccanti dei c.d. *ransomware* (malware progettato per impedire l'accesso a files e documentazione mediante utilizzo di algoritmi crittografici forti per poi chiedere un riscatto per riaverli indietro) e fortemente consigliabile avere una copia dei propri dati in una locazione protetta.

Le seguenti procedure aiutano a mitigare la minaccia della perdita dei dati:

1. Eseguire il backup dei propri dati ad intervalli regolari e prestabiliti.
2. Mantenere la locazione dei propri dati di backup in modo tale che non siano normalmente raggiungibili dalla postazione di lavoro che stiamo utilizzando (es. qualora utilizzassimo dischi esterni USB assicurarsi che questi non siano connessi con continuità alla nostra postazione di lavoro.) ATTENZIONE: In caso di incidente assicurarsi che la postazione di lavoro sia bonificata da personale esperto prima di inserire il disco di *backup* per il ripristino dei file.

3. E’ possibile utilizzare servizi in Cloud per il *backup* dei dati. Assicurarsi in questo caso che essi siano protetti e cifrati mediante password forti (sez. *“Sicurezza delle password”*) al fine di proteggere la nostra privacy prima di salvarli in rete.

MALWARE

Gli incidenti informatici che vedono l’impianto di software malevolo (aka malware) all’interno di reti e sistemi sono solitamente trattati da personale molto esperto e qualificato nel settore della cyber sicurezza.

Alla normale utenza, non viene infatti richiesto di “risolvere” tali problematiche ma di aiutare la propria società a prevenirle mediante l’adozione di semplici accortezze e buon senso nelle azioni quotidiane.

Alcune di esse sono:

1. Curare gli aggiornamenti del proprio software anti-virus ed assicurarsi periodicamente che sia attivo e funzionale.
2. Effettuare scansioni complete del proprio sistema operativo ad intervalli regolari tramite il proprio software anti-virus (on-demand scan).
3. Curare gli aggiornamenti del proprio sistema operativo (ref. Sicurezza dei sistemi).
4. Verificare la sorgente di provenienza di ogni software ed applicazione che si vuole installare sui propri sistemi.
5. Prestare attenzione agli URL e ai file allegati presenti nelle email (sez. Phishing e Social Engineering).
6. Prestare attenzione all’utilizzo di chiavette USB non fidate.
7. In caso di sospetta infezione, NON tentare di risolvere il problema ma contattare immediatamente i preposti reparti IT della propria società o organizzazione.

CONCLUSIONI

Il comportamento umano rappresenta in molti casi la prima linea di difesa contro gli attacchi informatici. Il buon senso di cui tutti noi siamo dotati può spesso fare la differenza fra un "*incidente*" ed un "*tentativo di intrusione non riuscito*". Tramite l'adozione di alcune semplici misure cutelative infatti non solo possiamo aiutare a proteggere la confidenzialità dei dati della nostra società ma anche la nostra stessa *privacy*.

AUTORE

Emanuele De Lucia è un professionista della sicurezza informatica e delle informazioni. E' attualmente responsabile della divisione Cyber Security e Cyber Threat Intelligence di Telsy S.p.A. ed è quotidianamente impegnato nell'analisi e nella ricerca di minacce informatiche emergenti. Ha lavorato come analista di secondo livello presso il Security Operation Center di TIM S.p.A, e come Cyber Security Manager presso l'Agenzia Spaziale Europea. Possiede diversi titoli accademici relativi a tale settore oltre numerose certificazioni di tipo professionale quali: CISSP, L|PT, E|CSA, C|HFI, C|EH, CEPT, CREA, CIFI.