Raccomandazioni base per l'utilizzo consapevole dei sistemi informatici

Attacchi

Sempre più spesso gli attacchi informatici si basano su fenomeni d'ingegneria sociale e non su attacchi ai sistemi. Questo significa che i malintenzionati cercano di far cadere in trappola l'utente in modo da poter attaccare dall'interno il suo sistema o l'intera infrastruttura, sfruttando la conoscenza totale o parziale d'informazioni e comportamenti individuali (es. il nome della compagnia telefonica, banca, assicurazione malattia, ecc.).

È quindi importante adottare un comportamento attento per tutelare la propria privacy, i propri dati personali e l'integrità dell'infrastruttura in cui ci si trova, sia sul posto di lavoro che a casa. I costi causati per il rispristino dei dati, quando possibile, possono essere molto elevati.

Password differenti

La password personale è una vera e propria chiave d'accesso ad una vasta parte di informazioni personali confidenziali. È quindi consigliato:

1. non comunicare mai la propria password personale ad amici e colleghi
2. cambiare le proprie password a cadenza regolare
3. digitare le password evitando che terze persone ci osservino
4. evitare password contenenti informazioni personali come ad esempio data di nascita, nome del figlio, nome del gatto, luogo di nascita, il numero di targa, ecc.
5. ideare password diverse per ogni servizio, per evitare che la scoperta di una sola password permetta ad un malintenzionato di ottenere l'accesso completo a tutti i dati personali:
    a. email di lavoro
    b. email privato
    c. account accesso PC
    d. account GAGI
    e. accesso a piattaforme didattiche o private (es. telebanking)
    f. accesso ai siti web, ecc.

Password sicure

Ecco alcuni sistemi semplici per ideare password lunghe e sicure e facili da memorizzare:

1. pensare a tre o quattro parole scelte casualmente, seguite da cifre e segni
   esempio: `Gattoelefantebicchiere3$`

2. pensare ad una frase facile da memorizzare (canzone, poesia, citazione) e terminare o iniziare con il numero di parole presenti e un segno di punteggiatura:
   esempio: "*Mi ritrovai per una selva oscura*" corrisponde a: `Mrpuso6!`

Archiviazione delle password

Per risolvere la difficoltà di memorizzazione delle password, possiamo affidarci a programmi quali *KeePass* (Windows) o *1Password* (Mac, iPhone, Windows e Android). Queste vengono racchiuse in una cassaforte personale sicura, accessibile unicamente tramite un'unica password segreta che non andrà mai dimenticata o comunicata a terzi. L'uso di questi applicativi semplifica e rende sicura la gestione delle password personali.

Ricezione delle email

Gli allegati email sono uno dei principali canali di distribuzione di virus destinati al furto dei dati, alla loro distruzione o al loro recupero previo pagamento di un riscatto (*ransomware*, descritto più avanti).

1. Gli enti che offrono servizi online, non inviano mai richieste d'inserimento password ai propri utenti. Questo tipo di richieste sono unicamente frutto di attività illecite. Ogni giorno vengono inviate oltre 100 miliardi di email apparentemente reali, destinate al furto di dati (fonte: *phishing.org*). Oltre il 20% vengono cliccate dagli utenti, con i conseguenti danni.

   Si raccomanda dunque sempre la massima prudenza durante la lettura di email che invitano a cliccare collegamenti o ad effettuare accessi online. In questi casi consigliamo di collegarsi al sito dell'ente che ci ha contattato (es. banca, GAGI, azienda, ecc.) inserendo manualmente l'indirizzo web "*www...*" nel browser di navigazione (Firefox, Safari, ecc.).

2. Si raccomanda l'apertura di allegati unicamente da mittenti noti e esclusivamente se si stava già aspettando un allegato dal mittente.

3. È utile verificare l'indirizzo email e i collegamenti web presenti nella mail, che spesso vengono camuffati in modo da assomigliare a nomi legittimi. Ad esempio email in arrivo da *paypal.ppl.com* nulla hanno a che fare con il reale sito *paypal.com*.

Ransomware

È un tipo di virus che cripta tutti i documenti e le foto presenti sul computer rendendoli irrimediabilmente illeggibili e inutilizzabili. Non si limita solo al computer ma riesce a criptare anche tutti i dati presenti sui dischi di rete collegati al PC di casa o in ufficio. La semplice apertura di un allegato email contenente questo tipo di virus può avviare il processo di criptaggio dei dati, recuperabili previo pagamento di un riscatto che può arrivare a costare anche diverse migliaia di franchi. In alcuni casi però i malintenzionati che si celano dietro a questa truffa, non permettono il recupero dei dati nemmeno dopo il pagamento del riscatto. Per questi motivi, ci si protegge in questo modo:

1. effettuando regolari copie di sicurezza dei dati personali su supporti esterni, ad esempio dischi o penne USB che vanno scollegati da PC e conservati al sicuro
2. aggiornando regolarmente antivirus, PC e apparecchi elettronici
3. mettendo sempre in dubbio la legittimità di tutte le email che giungono ogni giorno nelle caselle email, in particolare quelle con allegati inattesi.

Il team del centro informatica ICEC resta a disposizione per qualsiasi dettaglio complementare.