CYBERSECURITY, ISTRUZIONI PER L'USO

ANGELO CRESTA*, DIRETTORE DELL'IT DI BANCA DEL SEMPIONE, FORNISCE ALCUNI SPUNTI DI ATTENZIONE AI MENO ESPERTI PER GESTIRE AL MEGLIO IL TEMA DELLA CYBERSECURITY. ASPETTO SEMPRE PIÙ CENTRALE SIA NELLA "VITA DIGITALE" CHE IN QUELLA "ANALOGICA".

Come responsabile dell'IT di Banca del Sempione potreste essere portati a pensare che io voglia fare un'analisi più o meno tecnica della questione. Mi terrò invece alla larga dai tecnicismi e da termini riservati "agli addetti ai lavori", cercando di rendere più evidente e comprensibile il parallelismo tra consuetudini che osserviamo quando trattiamo questioni tradizionali rispetto a quelle digitali.
La nostra vita digitale sta diventando sempre più predominante a discapito di quella analogica, ed è per questo che non la si deve contrapporre ad una vita "reale" perché anch'essa lo è.
Fin qui tutto chiaro: non scriviamo più lettere con carta e penna, ma email; non sempre ci svaghiamo uscendo di casa fisicamente, ma lo facciamo sempre più spesso in maniera virtuale, dal gioco online fino a vivere una vita virtuale alternativa. Perfino il lavoro, "grazie" alla pandemia, è diventato smart!
La problematica, vista da una certa angolazione, è esattamente questa: siamo "stati educati" a comportarci nella nostra vita fisica (analogica) fin da bambini, siamo attenti a cosa firmiamo - perché ci hanno sempre insegnato a leggere tutto prima di firmare - non concediamo l'uso di casa nostra, della nostra auto o di una semplice bicicletta a persone che non conosciamo, ma ci assicuriamo che siano persone sicure, conosciute e di fiducia.
Bene, questo comportamento lo disattendiamo sistematicamente più o meno tutti nella nostra vita digitale…
Quanti di voi leggono le clausole di utilizzo software? Quanti controllano davvero i permessi che le applicazioni ci richiedono per funzionare sui nostri telefonini? L'attendibilità dei siti? Diciamo in pochi, e l'elenco di domande potrebbe essere lungo …
Ma cosa c'entra il phishing? Che cosa è? Iniziamo con la seconda domanda, e riporto quanto scritto da Wikipedia, diventata anch'essa una delle fonti primarie di informazioni. «Il phishing è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale». Dove "phishing", variante di fishing (letteralmente "pescare" in lingua inglese), allude all'uso di tecniche sempre più sofisticate per "pescare" dati finanziari (e non) di un utente.
Adesso che sappiamo di cosa parliamo, cosa c'entra l'educazione che ho ricevuto da bambino? Vi ricordate la "storia del non accettare le caramelle" o "non aprire la porta" agli sconosciuti? Vi arriva un'e-mail, che vi dice di aver vinto qualcosa, di poter avere un oggetto che desiderate perché "trendy" (caramella), l'intestatario sembra essere affidabile, ma sembra solamente, perché se analizzato meglio non lo è (lo sconosciuto) e vi chiede di cliccare su qualcosa che vi rimanda a un sito internet dove vi chiedono i vostri dati personali e di accesso per poter ricevere l'oggetto del desiderio super scontato... avete appena abboccato! Questa, come altre, sono tecniche ampiamente studiate nella vendita che cercano di creare esigenze o urgenze: è successo qualcosa ai vostri averi, ai vostri soldi, entrate a controllare! … e insieme a noi è "entrato lo sconosciuto".
Il numero di questi attacchi sta crescendo in maniera importante, basti pensare che la cifra richiesta da Ransomware, programmi informatici malevoli che rendono inaccessibili i file dei computer infettati e chiedono il pagamento di un riscatto per ripristinarli, è duplicata tra il 2020 ed il 2021, e, dopo gli enti statali il settore finanziario è tra i più colpiti ((ENISA Threat LANDSCAPE 2021 - https://www.enisa.europa.eu).
Cosa possiamo fare? Come possiamo difenderci? Dobbiamo apprendere, imparare, fare pratica sul come muoverci e comportarci per mettere in atto e mutuare tutte quelle misure che abbiamo già appreso nella vita "analogica".
Infatti, è il nostro atteggiamento, ma soprattutto la mancanza di "educazione", ad esporci maggiormente ai rischi di truffe informatiche. Detto così sembra semplice … ma lo è tanto quanto capire se possiamo fidarci o meno di qualcuno, anche se qui siamo facilitati dalla tecnologia e da corsi che ci aiutano a capire cosa controllare e a smascherare gli impostori.
Ma l'antivirus? Il primo e più efficace antivirus siamo noi con la nostra attenzione … infatti gli strumenti tecnici di prevenzione, anche se aggiornati e validi, nella stragrande maggioranza dei casi, non permettono di difenderci da attacchi nuovi e non "censiti", riconoscendo solo quelli di cui hanno già registrato le caratteristiche.
Siamo noi stessi ad azionare qualcosa, ad inserire i nostri dati, ad aprire le porte, e, pertanto, siamo noi a dover essere "aggiornati" per riconoscere queste minacce…
Le istituzioni, le banche, come fanno? In Banca del Sempione questa tematica viene affrontata applicando alcuni principi cardine come la "Security in Depth". In questo modello il collaboratore non è lasciato mai solo ma è parte di uno dei molteplici livelli di sicurezza utilizzati per salvaguardare le attività della banca e dei suoi clienti. Queste misure di protezione funzionano a strati concentrici, proprio come una cipolla, utilizzando una combinazione di diverse tecnologie per proteggersi dalle minacce. Il principio base da cui partire è comunque quello conosciuto come "Zero Trust", il "non ti fidare, controlla sempre" e se vogliamo ritornare al parallelismo, si tratta dell'espressione massima della tradizione.

BANCA DEL SEMPIONE
SIMPLON BANK
BANQUE DU SIMPLON

*Angelo Cresta – CISSP (Certified Information Systems Security Professional)