Social engineering

Per ottenere informazioni riservate i criminali sfruttano spesso la buona fede, la disponibilità o l'insicurezza delle persone. Che si tratti di telefonate fittizie, falsi agenti di polizia o attacchi di phishing, nel social engineering il mirino è sempre puntato sulla persona. La protezione migliore è la «sana sfiducia».

Proteggetevi dagli attacchi di social engineering così:

- Comunicate il minor numero possibile di informazioni personali su di voi. Sulle reti sociali, in particolare, è opportuno agire con grande cautela nella pubblicazione di informazioni.
- In generale non comunicate mai password o codici TAN a un'altra persona, nemmeno a un amministratore di sistema o al vostro capo. Una password appartiene solo e soltanto a voi!
- Siate sospettosi quando ricevete richieste di informazioni via e-mail o al telefono. Anche le e-mail di mittenti conosciuti e le telefonate da numeri noti possono essere falsificate!

Gli attacchi di social engineering mirano a strapparvi informazioni personali o riservate (come dati di accesso, password ecc.) per utilizzarle poi illecitamente.

I criminali cercano come prima cosa di raccogliere la maggior quantità possibile di informazioni sulla vittima. Servendosi di queste informazioni sarà infatti più semplice ingannarla. Per esempio, il criminale potrebbe poi presentarsi come una persona che conoscete.

Lo strumento ideale per raccogliere informazioni è Internet. Soprattutto su reti sociali (https://www.ebas.ch/it/media-e-reti-sociali/) come Facebook, Xing, Instagram ecc. si trovano enormi quantità di informazioni personali che possono essere utili a chi sferra l'attacco per avvicinarsi a una persona in modo mirato e apparire affidabile.

Come potete proteggervi efficacemente?

Purtroppo non ci sono provvedimenti tecnici che offrano una protezione dal social engineering. Poiché chi sferra un attacco sfrutta in modo mirato qualità umane come la disponibilità, l'insicurezza, la buona fede e – in definitiva – la fiducia verso le altre persone, è molto difficile scoprire e sventare un attacco di social engineering.

In generale, solo una «sana dose di sfiducia» protegge contro le persone che non si conoscono – ma anche contro quelle che si pensa di conoscere. Spesso è utile chiedersi che tipo di informazioni si rendono pubbliche su di sé e a chi.

In caso di dubbio informate il vostro istituto finanziario

In caso di sospetti sul servizio e-banking non comunicate nulla e informate immediatamente il vostro istituto finanziario. I recapiti si trovano qui (https://www.ebas.ch/it/partner/).

Esempi di attacchi di social engineering

- Una persona si presenta come un tecnico (p. es. di una società telefonica o di fornitura di elettricità) e tenta di introdursi in casa vostra o nella sede della vostra impresa.

- Ricevete un'e-mail che vi invita ad aprire un link ed effettuare l'accesso su un sito Internet, oppure a fornire informazioni personali.
- Una persona vi telefona e desidera porvi certe domande per un sondaggio (p. es. sul reddito, sulle misure di sicurezza adottate per il vostro computer ecc.).
- Un hacker falsifica il mittente di un'e-mail presentandosi come una persona nota (è possibile che l'allegato contenga un malware).
- Alla vostra postazione di lavoro si presenta una persona che si spaccia per un tecnico e vi fa credere di dover eseguire dei lavori di manutenzione sul vostro computer.
- Chi sferra un attacco di social engineering può giungere persino al punto di candidarsi per ottenere un impiego mirato in un'impresa e impadronirsi poi di informazioni specifiche.

Il social engineering è un metodo diffuso per l'acquisizione di informazioni riservate. Nel mirino ci sono sempre i singoli individui. Non esistono forme tecniche di protezione. In generale è quindi sufficiente un po' di «sana sfiducia».