Social Engineering Awareness

CORSO DI FORMAZIONE

Come identificare e difendersi dagli attacchi di Social Engineering

Nel 2016 è cresciuta del 117% la "guerra delle informazioni": è a quattro cifre l'incremento degli attacchi compiuti con tecniche di Phishing / Social Engineering (+1.166%)
Fonte: Rapporto Clusit 2017

Nel 2016, 37,3 milioni di persone a livello mondiale sono state vittime di phishing.
Fonte: social-engineer.org

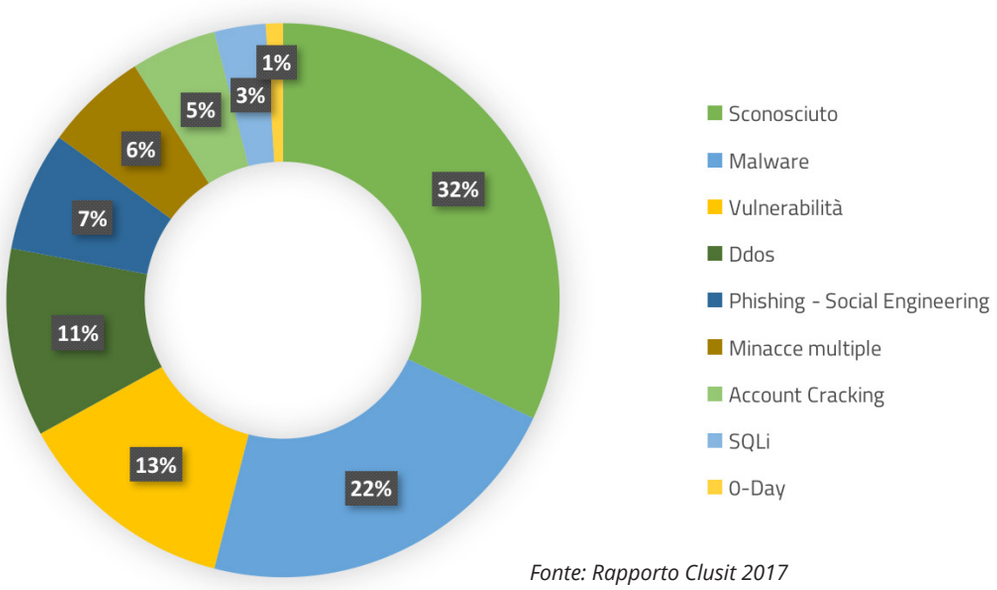
I canali di comunicazione più usati per gli attacchi di social engineering sono il telefono (46%), conversazioni con sconosciuti (37%) email (17%). Le figure professionali più coinvolte: impiegati (43%), personale addetto al desk informazioni (33%), addetti call center (8%)
Fonte: Verizon

Gli attacchi phishing crescono del 50% anno su anno.
Fonte: Verzion

600.000 profili Facebook vengono compromessi ogni giorno da attacchi di social engineering.

Fonte: Heimdal Security

Tipologia e distribuzione delle tecniche d'attacco



Fonte: Rapporto Clusit 2017

Gli attacchi cyber-criminali assumono forme diverse e vengono perpetrati con tecniche molto sofisticate. Vanno dai ransomware (un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto - ransom in inglese) al social engineering, ossia tecniche di attacco basate sulla raccolta di informazioni mediante studio - interazione con una persona.

Tutti sfruttano i punti deboli a livello tecnico, di processo, organizzativo e anche culturale.
Gli obiettivi di questi attacchi sono mirati a estorcere dati ed informazioni o addirittura a danneggiarli colpendo così una parte importante degli asset aziendali.

Questi attacchi impattano tutta l'azienda, sottovalutarli sarebbe molto grave, a rischio della stessa sopravvivenza dell'impresa.
Gli attacchi di phishing e social engineering stanno crescendo esponenzialmente, nel 2016 sono passati dal 1% al 7% (Fonte Rapporto Clusit sulla Sicurezza ICT in Italia).

Per ottenere le informazioni esistono molti metodi, uno dei quali è appunto il social engineering che si avvale sia di tecnologie ma anche tecniche psicologiche puntando sul fattore umano, quando i sistemi aziendali non hanno criticità o falle da sfruttare.

Chi vuole mettere in atto un un furto di dati aziendali si avvale di tanti espedienti, anche senza aver bisogno di un computer, come fa? Cerca carta nei cassonetti dell'immondizia (dumpster diving): stampe di elenchi clienti, estratti conto, ordini di acquisto, documenti contabili e altro.

Phishing, vishing e smishing

Altre tattiche sono invece rappresentate da phishing e vishing che si presentano entrambi come un email da parte di un ente, un istituto bancario, o altre istituzioni che usano tecniche psicologiche adottate per risolvere falsi problemi e per spingere l'utente a rilasciare le proprie credenziali per riattivare, ad esempio, un conto corrente.

Il tutto parte da un email falso, nel caso del vishing viene chiesto di contattare un numero telefonico a cui comunicare credenziali o dati.
Le truffe smishing arrivano via un sms che chiede di cliccare su un link per atterrare su una pagina web lasciando i propri dati o credenziali.

Contromisure
Il percorso formativo di Social Engineering di AD Consulting

Come identificare e proteggersi da questo tipo di attacchi?
Il percorso formativo di Social Engineering Awareness offerto da AD Consulting ha l'obiettivo di fornire al personale aziendale gli strumenti per riconoscere i tentativi di attacco perpetrati dai moderni ingegneri sociali.

Partendo dalla definizione di ingegneria sociale, gli studenti saranno introdotti ai principi psicologici normalmente abusati durante questo genere di attacchi ed alle tecniche di manipolazione impiegate per estorcere informazioni aziendali riservate.

Il docente mostrerà diversi casi di studio reali utili a comprendere il fenomeno del Social Engineering e sviluppare strategie di difesa a tali attacchi.

Percorso Formativo

Modulo 1

- Cos'è il Social Engineering
- Cronistoria del Fenomeno dell'Ingegneria Sociale
- Obiettivi di un Attacco di Social Engineering

Modulo 2

- Il funzionamento del sistema operativo "uomo"
- Principi psicologici abusati nell'Ingegneria Sociale
- Moderni attacchi di Social Engineering

Modulo 3

- La gestione della sicurezza "umana"
- Incrementare il livello della human security
- Progettare ed implementare policy di sicurezza

Modulo 4

- Difendersi dagli attacchi di Social Engineering
- Proteggere le "chiavi" del regno
- Comprendere gli indicatori di un attacco
- Come reagire ad un attacco

Il corso di Social Engineering può essere erogato presso le sedi AD Consulting oppure On Site con un intervento di formazione ad hoc secondo le diverse esigenze.
Per informazioni: 059 7470500 o info@adcsrl.it