Testiamo in modo completo la sicurezza fisica della tua azienda

Per una sicurezza completa, non si possono trascurare gli attacchi che sfruttano tecniche di *ingegneria sociale* e *manomissione fisica* dei sistemi.

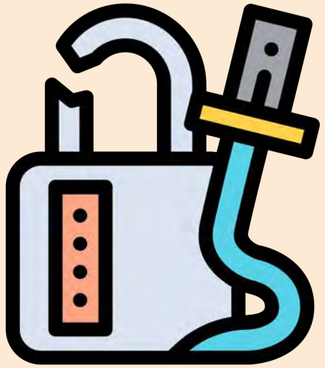
Mettiamo alla prova a 360° la sicurezza della tua azienda, testando la sua resilienza agli attacchi di sicurezza fisica.

Secure Online Desktop

Clusit
Associazione Italiana per la Sicurezza Informatica

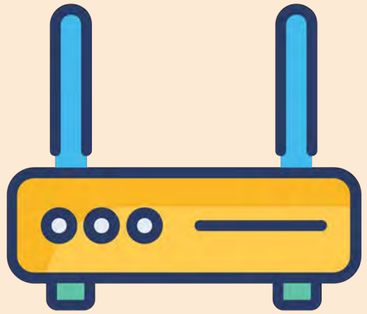
Ingegneria sociale

L'arte di imbrogliare le persone tramite empatia o vere e proprie truffe potrebbe essere la debolezza fatale della tua azienda.



Attacchi in loco

Non tutto passa per la rete. Alcuni attacchi potrebbero sfruttare punti deboli fisici dell'edificio o la leggerezza con cui i dipendenti usano i loro dati di accesso.



Rogue AP

Access point corrotti che vengono scambiati per legittimi. A volte non basta essere collegati a una certa linea WiFi per potersi dire al sicuro.

Cattura dati dalla rete

Le comunicazioni sulla rete sono davvero sicure? La VPN aziendale funziona correttamente? I dipendenti la usano sempre?

Dumpster diving

Non si fa quasi mai caso a quello che viene gettato nel bidone della spazzatura, invece è il caso di prestare attenzione a cosa e in che modo questo avviene.

Ingegneria sociale

È molto più facile e conveniente *hackerare* una persona piuttosto che una macchina.

Il *social engineering* è l'arte di manipolare le persone in modo che forniscano informazioni riservate. I tipi di informazioni possono variare e comprendere password, informazioni bancarie o informazioni di accesso a un computer da remoto.

Esempi di attacchi di ingegneria sociale

Incontri casuali

Con incontri che possono sembrare casuali, richieste di aiuto che puntano sull'empatia o raggiri verbali, gli hacker social possono farsi rivelare importanti informazioni sull'azienda. Non necessariamente informazioni sensibili come le password, ma anche informazioni sulla struttura dell'azienda che possono poi essere usate per portare avanti l'attacco.

Richieste via telefono

Le grandi aziende, che hanno decine o centinaia di dipendenti, magari suddivise in diverse sedi, dovrebbero prestare molta attenzione alle informazioni che sono comunicate telefonicamente. Sono noti i casi di hacker che fingendosi nuovi assunti di altre sedi riuscivano a farsi rivelare password di accesso o codici di sicurezza.

Assistenza online

Queste tecniche rientrano nel campo del phishing, per cui abbiamo un servizio dedicato. Si tratta di email, pagine web o comunque siti internet che assomigliano a portali legittimi, ma sono invece opera di hacker, che tramite queste copie riescono a ingannare gli utenti facendogli scaricare malware o inserire le proprie credenziali.

Installazione di Rogue Access Point

Una delle più comuni minacce alla sicurezza wireless è il *rogue access point*, usato in molti attacchi.

Per definizione un *rogue AP* si presenta come **un punto d’accesso wireless** che non fa parte della rete, ma potrebbe avere lo stesso nome della rete aziendale. Uno degli usi più comuni di un Rogue AP è quello di sostituirsi alla linea aziendale con una SSID identica (o apparentemente legittima). In questo modo i computer si collegano ad essa pensando di essere nella linea sicura dell’azienda e si comportano di conseguenza, abbassando la guardia.

Il rischio è che questi access point potrebbero essere usati per il furto di informazioni sensibili, quali password e dati degli utenti. Questi dati rubati possono poi essere usati per accedere alla vera rete aziendale per compiere attacchi mirati.

Con il nostro intervento possiamo individuare e analizzare i *Rogue AP* per poi prendere provvedimenti per mitigare il rischio.

Cattura dati sensibili dalla rete

Con l’uso sempre maggiore delle reti pubbliche o casalinghe, **il rischio di offrire i propri dati inconsapevolmente è aumentato molto**. Senza una VPN aziendale o comunque una cifratura della comunicazione, il furto di dati provenienti da comunicazioni tra dispositivi è un rischio concreto.

Tecniche comuni nel furto di dati dalla rete

Man in the Middle

Con **Man in the Middle** si intende un tipo di attacco con il quale l'hacker ritrasmette o altera i messaggi tra due utenti o macchine, ottenendo dalle risposte dei dati sensibili.

Wireless Sniffing

Analogamente agli attacchi Man in the middle, lo sniffing di una rete wifi intercetta i pacchetti tra i computer collegati e l'access point per poi cercare di decifrarli per ottenere dati sensibili.

In entrambi i casi, noi di SOD offriamo un servizio di test alla risposta di questo tipo di attacchi. Non ci limitiamo, però, nel provare a mettere in pratica questi attacchi. Tra i servizi di test con attacchi in loco, proponiamo anche un test sui dispositivi collegati solamente alle reti interne, come possono essere telecamere wifi a circuito chiuso e altri dispositivi IoT.

Attacchi in loco

Non sono solo le reti wifi a proteggere un’azienda, ma anche le infrastrutture fisiche. Con questi tipo di attacchi si sfruttano debolezze del personale di sorveglianza, della sicurezza delle centraline di rete ma anche del modo in cui vengono usati i dispositivi informatici dai dipendenti.

Cosa potrebbe accadere

Manomissione delle rete

Le aziende sono collegate alla rete telefonica e di internet come ogni altro edificio. Se si riesce ad avere accesso alle centraline e quindi alle **connessioni fisiche** dei cavi, è possibile installare dei dispositivi di intercettazione dei dati passanti per uno specifico cavo. L'accesso al cavo può avvenire per forzatura o sfruttando il *tailgating*.

Tailgating

Questa tecnica, usatissima nelle metropolitane di Londra e New York, consiste nell'**entrare in un edificio accodandosi a un dipendente** e sfruttando quel brevissimo lasso di tempo in cui la porta si sta chiudendo per evitare di usare campanelli o badge. Una volta dentro, le possibilità di attacco diventano molteplici.

Shoulder Surfing

Questa tecnica consiste nello spiare un utente che digita una password o un codice di accesso per poi riutilizzarlo in seguito. Per esempio: se le porte dell'azienda sono protette da un codice, potrebbe essere semplice aspettare che un dipendenti lo inserisca e guardare quali cifre compongono il codice.

Mitigazione del rischio per gli attacchi in loco

Solitamente non è sufficiente mettere in pratica **una sola tecnica** per completare un attacco, ma non è difficile usarne più di una per ottenere risultati sorprendenti.

Per proteggere *in modo completo* la vostra azienda, **bisogna pensare anche a questo tipo di attacchi che possono essere estremamente subdoli e difficilmente intercettabili**, facendo leva sull'empatia dei dipendenti e sulle debolezze fisiche dell'azienda.

Con i test di penetrazione fisica offerti da SOD, si individuano i punti deboli per prendere provvedimenti.

Dumpster diving

Il *dumpster diving*, chiamato anche *trashing* o *information diving*, è la pratica di **setacciare i rifiuti in cerca di documenti o dati sensibili** che possono poi essere usati per compiere attacchi informatici.

Quando si parla di *sicurezza fisica*, questo è un fattore che spesso si tende a scordare, ma **ogni documento ufficiale contiene informazioni riservate come l'indirizzo personale, il numero del conto corrente, il codice fiscale o altro.**

Con questo tipo di informazioni non è complicato rubare l'identità del malcapitato a cui sono state sottratte. Se succedesse in azienda? **Cosa potrebbe succedere se i dati bancari, codici di sicurezza o altre informazioni riservate e di valore cadessero in mani sbagliate?**

Non sarebbe bello scoprirlo.

Dal 2011 ci occupiamo di tecnologia Cloud e di sicurezza, affidati a professionisti esperti!

Scegli la sicurezza per la tua azienda

Scopri il servizio sul sito

Secure Online Desktop

Per ulteriori informazioni, i nostri contatti sono:
Via Statuto 3 c/o Impact Hub,
42121 Reggio nell'Emilia (RE)
www.secure-od.com

Tel. +39 0522 1685330
Fax. +39 0522 015371
E-mail: info@secure-od.com
Pec: secure-od@pec.it

Clusit
Associazione Italiana per la Sicurezza Informatica