Informatica

Dipartimento di Economia

Ing. Cristiano Gregnanin

Corso di laurea in Economia

19 novembre 2016

Sicurezza delle reti wi-fi

La protezione di una rete wifi è tipicamente demandata a:

- WEP: Wired Equivalent Privacy
- WPA: Wi-Fi Protected Access
- WPA2: Wi-Fi Protected Access2

Sicurezza delle reti wi-fi: WEP

Algortimo molto veloce ma poco sicuro. La crittografia a 64 bit si è rivelata poco sicura a seguito di numerosi attacchi informatici andati a buon fine nel 2001.

Sicurezza delle reti wi-fi: WPA e WPA2

Sono i successori del wep, utilizzano algoritmi con chiavi di sicurezza a 256 bit e sistemi di crittografia più avanzati.

Sicurezza delle reti wi-fi: Attacco war-driving

Consiste nell'utilizzare l'automobile per viaggiare in aree densamente popolate cercando reti non protette da utilizzare in modo illecito.

Sicurezza delle reti wi-fi: Attacco war-driving. Soluzioni

Utilizzare tecnologie che generino migliaia di punti d'accesso fasulli alla rete wi-fi confondendo quindi eventuali attaccanti.

Principali minacce alla sicurezza dei sistemi informativi

- Incidenti o disastri naturali
- Elementi interni (dipendenti e consulenti)
- Elementi esterni (hacker e cracker)
- Collegamenti con altre organizzazioni

Fra tutti si considerano molto rilevanti gli attacchi portati da individui esterni ed interni all'organizzazione: **accesso non autorizzato, negazione di servizio, virus, worm, spam, spyware, cookies**

Principali minacce alla sicurezza dei sistemi informativi: accesso non autorizzato

Ha luogo ogni volta che persone non autorizzate a vedere, manipolare o gestire informazioni sensibili consultano archivi elettronici o intercettano scambi di informazioni elettroniche.

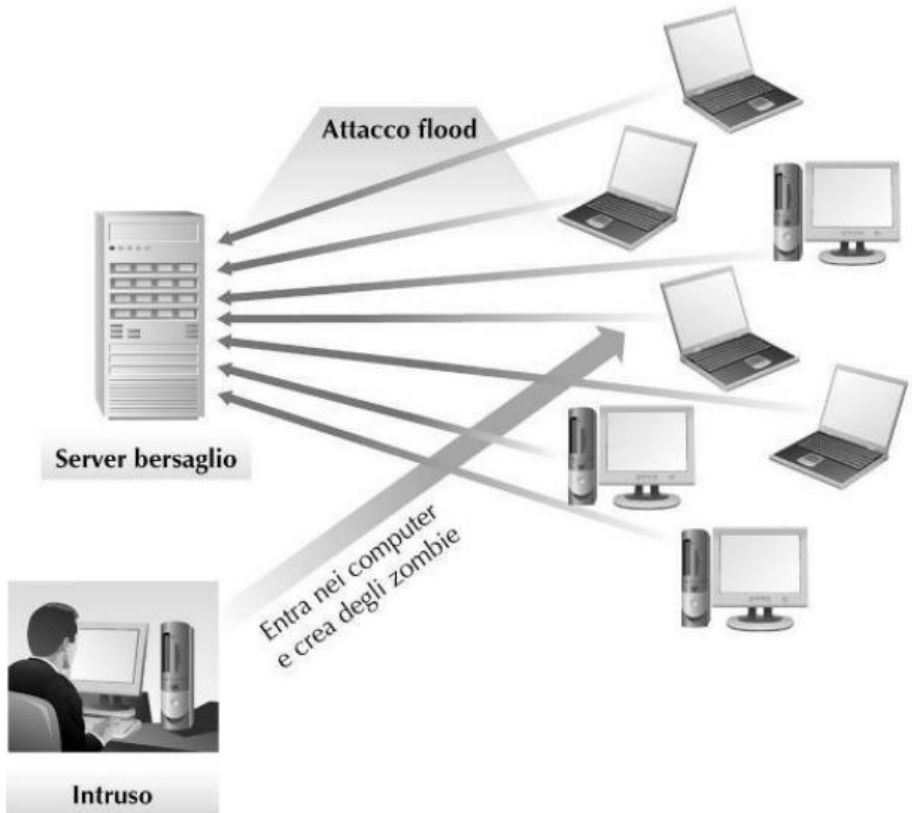
Principali minacce alla sicurezza dei sistemi informativi: negazione del servizio (DOS)

Gli attacchi vengono abitualmente attuati inviando molti pacchetti di richieste, di solito ad un server web, FTP o di posta elettronica saturandone le risorse e rendendo tale sistema "instabile".
Qualsiasi sistema collegato ad Internet e che fornisca servizi di rete basati sul TCP è quindi soggetto al rischio di attacchi DoS.

Principali minacce alla sicurezza dei sistemi informativi: negazione del servizio (DOS)

Per rendere più efficace l'attacco in genere vengono utilizzati molti computer inconsapevoli, detti zombie, sui quali precedentemente è stato inoculato un programma appositamente creato per attacchi DoS e che si attiva ad un comando proveniente dal cracker creatore. Se il programma maligno si è diffuso su molti computer, può succedere che migliaia di PC violati da un cracker, ovvero una **botnet**, producano inconsapevolmente e nello stesso istante un flusso incontenibile di dati che travolgeranno come una valanga anche i link più capienti del sito bersaglio.

Principali minacce alla sicurezza dei sistemi informativi: negazione del servizio (DOS)



Principali minacce alla sicurezza dei sistemi informativi: spyware

è un software che raccoglie informazioni sulle attività che un utente compie nel web senza che l'utente stesso ne sia a conoscenza

Principali minacce alla sicurezza dei sistemi informativi: compilazione web form robotizzata

Gli spammer creano spesso migliaia di account di posta elettronica presso provider gratuiti come Yahoo! o Hotmail. Le iscrizioni avvengono per mezzo di software che in modo automatico e sistematico compilano i form di iscrizione.

Principali minacce alla sicurezza dei sistemi informativi: compilazione web form robotizzata - soluzioni

il codice captcha è un'immagine distorta che per ora solamente gli esseri umani sono in grado di leggere. I form usano spesso dei campi captcha che l'essere umano deve necessariamente compilare.

Principali minacce alla sicurezza dei sistemi informativi: cookie

Sono una sorta di gettone identificativo, usato dai server web per poter riconoscere i browser durante comunicazioni con il protocollo HTTP usato per la navigazione web.
Tale riconoscimento permette di realizzare meccanismi di autenticazione, usati ad esempio per i login; di memorizzare dati utili alla sessione di navigazione, come le preferenze sull'aspetto grafico o linguistico del sito; di associare dati memorizzati dal server, ad esempio il contenuto del carrello di un negozio elettronico;

Principali minacce alla sicurezza dei sistemi informativi: cookie - problematiche

Il cookie è memorizzato nel client sottoforma di file di testo. Se un sito web è mal progettato potrebbe decidere di salvare nel cookie informazioni sensibili come ad esempio i numeri di carta di credito. Se un utente malintenzionato riesce ad accedere ai cookies salvati nel computer della vittima può potenzialmente conoscere tutto ciò che i siti web visitati dalla vittima hanno memorizzato.

Altre minacce alla sicurezza dei sistemi informativi

- Dipendenti che scrivono password su foglietti
- Non utilizzo di software antivirus
- password deboli
- lasciare la postazione di lavoro senza salvaschermo
- dare informazioni sensibili per telefono o email
- non avere un'adeguata politica di controllo degli accessi alla rete aziendale
- non utilizzare firewall

Soluzioni tecnologiche: limitazione all'accesso a dati e informazioni

- Limitazione fisica: proteggere i dispositivi con lucchetti o riporli in magazzino dopo l'utilizzo.
- Gestire l'autenticazione degli utenti quando effettuano l'accesso alla rete aziendale.

Soluzioni tecnologiche: strumenti per la limitazione di accesso

- Password, PIN, combinazioni di sblocco
- Chiavi, carte identificative con foto, smart card
- impronte digitali, timbro della voce, caratteristiche morfologiche del viso o della retina

Soluzioni tecnologiche: VPN

è una connessione di rete realizzata dinamicamente all'interno di una rete esistente. Si creano tunnel cifrati per inviare dati sicuri attraverso la rete internet. Si crea quindi un tunnel privato in una rete pubblica

Soluzioni tecnologiche: crittografia

è la branchia della matematica che studia la codica e decofica dei messaggi. Il mittente codifica il messaggio utilizzando un algoritmo che garantisce che solamente il destinatario possa decodificare il messaggio

Soluzioni tecnologiche: crittografia - chiave simmetrica

Si usa una chiave che permette di cifrare e decifrare il messaggio. Se la chiava usata dal mittente e dal destinatario è la medesima si parla di **chiave simmetrica**. Se troppe persone usano la stessa chiave il sistema può diventare inefficace. Inoltre serve un preventivo scambio della chiave attraverso un canale sicuro.

Soluzioni tecnologiche: crittografia - chiave pubblica

Si usano 2 chiavi: una pubblica e una privata. La chiave pubblica è distribuita liberamente, mentre la segreta è tenuta privata.
Il mittente codifica il messaggio usando la chiave pubblica del destinatario. Il destinatario usa la sua chiave privata per decodificare il messaggio. **il messaggio è decodificabile solo ed esclusivamente dal possessore della chiave privata**

Soluzioni tecnologiche: crittografia - chiave pubblica e privata. firma digitale

Un mittente può codificare il messaggio con la propria chiave privata. A quel punto chi è impossesso della chiave pubblica può decodificarlo. In questo modo si realizza la **firma digitale:** un ricevente può verificare che il messaggio proviene da un certo destinatario se può utilizzare la sua chiave pubblica per decifrarlo.