GETNUT

Manuale sicurezza delle comunicazioni elettroniche

La sicurezza informatica non è solo un acquisto, è più una conquista.

La maggior parte degli attacchi informatici, anche tra quelli più famosi e finiti sui media di massima diffusione, sono stati effettuati grazie al fattore umano, ossia ad errori da distrazioni o noncuranza delle persone preposte all'uso e con accesso ai sistemi informatici.

Per cui la prima avvertenza è non abbassare la guardia.

Un primo tipo di attacco si definisce "Man In The Middle" e descrive l'azione di una persona che si pone tra mittente e destinatario, riuscendo non solo a leggere le comunicazioni ma anche inserire e modificare a suo piacimento i contenuti che desidera.

In altre parole, l'hacker è in grado di leggere ovvero di sostituirsi in toto a uno solo od entrambi gli utenti, possibilmente coprendo le tracce della propria intrusione.

Quali risultati può ottenere il Man in the middle? Se è riuscito a porsi in mezzo, può sorvegliare ad esempio la comunicazione tra l'utente e la sua Banca e quando questa invia la chiave di accesso, intercettarla. In tal modo potrà accedere ai dati bancari o, peggio, agire al posto dell'ignaro utente effettuando bonifici. Per di più, avrà la possibilità di inviare messaggi di rassicurazione che appariranno come della Banca stessa.

Un metodo per evitare un attacco MITM è l'uso di chiavi firmate: se la chiave della Banca viene firmata da una terza parte, che si rende garante dell'autenticità, si può essere sufficientemente tranquilli.

Tuttavia, qualsiasi sistema presenta vulnerabilità e sono stati elaborati metodi per superare molti degli ostacoli difensivi. Come una gara, la tecnologia e gli hacker si sfidano a colpi di innovazione.

Per cui, rientra in gioco il fattore umano: un utente mediamente esperto, che sceglie sistemi e procedure avanzati, può (quasi) dormire sonni tranquilli. È sufficiente che adotti tali tecniche e le usi con attenzione e coscienza: ad esempio tenendo sott'occhio i suoi device, cambiando le pw, prestando attenzione ai messaggi e agli avvisi che riceve.

Se gestite milioni di Euro, dovete stare molto all'erta. Se siete nella media, è di solito sufficiente prestare attenzione.

Attenzione anche alla tecnologia usata e proposta: le soluzioni periodicamente adottate diventano obsolete con il tempo in quanto continuamente superate dalla tecnologia.

Non dimenticate, quindi, che spesso è la persona l'anello debole di un sistema. Rafforzate la sicurezza delle vostre abitudini e la sicurezza di tutto il sistema e dei vostri interessi sarà parimenti rafforzata.

Altro anello debole, spesso sottovalutato, sono i servizi liberamente accessibili, dai quali si possono trarre informazioni che, adeguatamente riunite, possono essere la base di attacchi informatici a sistemi maggiormente protetti, alle informazioni e ai dati riservati.

La posta elettronica come punto di vulnerabilità.

Attraverso i sistemi di mailing passano la gran parte delle informazioni personali e aziendali. Va da sé, pertanto, che siano una importantissima porta di accesso per i malintenzionati.

I protocolli di messaggeria (SMTP, POP3, IMAP4) sono quelli di gran lunga più diffusi e la posta elettronica è il servizio più usato su internet. L'instradamento (routing) della posta avviene attraverso protocolli sicuri o non sicuri.

Sono protocolli insicuri: http, POP, IMAP, SMTP.

Sono protocolli sicuri: HTTP abbinato ad SSL, POP + SSL, IMAP + SSL, SMTP + SSL.

La prima cosa da fare è quindi, ovviamente, capire quale protocollo è usato.

Il protocollo SMTP permette di trasferire la posta da un server ad un altro con una connessione point to point.

Il protocollo POP permette di recuperare la propria posta giacente su un server remoto ed è necessario a tutti gli utenti che non sono connessi in permanenza ad internet.

Il protocollo IMAP è un protocollo alternativo al protocollo POP (POP3 per la precisione) che consente la gestione di più accessi simultanei, di più caselle postali, di inviare la posta secondo più criteri, di criptare le password. Questo protocollo, impedendo il transito in chiaro delle password, rende inutile eventuali operazioni in corso di "Sniffing".

Tutto quanto sin qui detto è valido anche per applicazioni e servizi pubblicati in modalità non sicura ma spesso necessari alle aziende (portali WEB, scambi di informazioni via internet, accesso remoto ai sistemi, sistemi di messaggistica).

Anche per questi applicativi ci sono diversi protocolli alcuni sicuri, altri insicuri.

Protocolli insicuri: http, FTP, Telnet, PPTP, VPN, ICQ, SNMP.

Protocolli sicuri: HTTP abbinato ad SSL, FTPS o SFTP, SSH, PPTP su SSTP VPN, messaggistica istantanea con uso di SSL, PKI proprietario, SSL-VPN, L2TP, IPSEC, tunneling SSH VPN, SNMP.

L'uso di sistemi con protocolli sicuri può prevenire la perdita di username e password, che rappresenta la chiave di accesso a dati fondamentali e ben più complessi e importanti rispetto a una singola mail / utenza.

Molti, infatti, usano la stessa pw per tutti i servizi cui accedono.

Quindi, che fare?

Usare SSL per la ricezione e l'invio della posta elettronica o per l'accesso a portali sicuri è consigliabilissimo.

Così come impiegare in modo predefinito il protocollo https.

Mai trasmettere informazioni in chiaro!!!!

Negli ultimi anni c'è stato un vertiginoso aumento di pc compromessi, oggetto stesso di furti ovvero usati da remoto per altre più grandi truffe.

Il know how professionale e aziendale è ormaii tutto nei pc, oltre che nella testa delle persone che ci lavorano.

L'esposizione dei nostri sistemi a potenziali attacchi è una responsabilità personale gravosa, che può portare a danni potenzialmente incalcolabili, sia all'azienda che alle persone che, dipendenti di essa, vi lavorano.

Dunque, la gran parte degli attacchi informatici passa dall'interno della rete. Lo sviluppo di connessioni sempre più diffuse e sempre a minor costo, unite alla diffusione capillare di devices connessi, ha aumentato a dismisura le possibilità, le vie di accesso alle reti e da queste alle informazioni personale e aziendali.

Inoltre, proprio per ragioni di sicurezza le reti richiedono che alcuni dati siano in chiaro, accessibili, pena il mancato accesso ai servizi. Viceversa, ci sarebbe la tentazione di mettere tutto oscurato, proprio per proteggersi. Occorre trovare un bilanciamento.

Molto della sicurezza è demandato ai sistemisti e alle aziende che devono investire in sicurezza informatica, proporzionalmente al valore dei dati che vogliono proteggere.

Le persone, ciascun per sé e a seconda dei ruoli, devono usare un elevato livello di prudenza. Usare la rete è un po' come attraversare la strada nell'ora di punta: se sei giovane scatti, se sei anziano aspetti, se hai un bambino con te lo prendi in braccio.

In tal senso, occorre rispettare le regole per l'accesso e l'uso delle risorse (profili utenti e privilegi assegnati), adottare criteri di "robustezza password" (almeno 8 caratteri, alfanumerica, maiuscole e minuscole, di durata limitata, possibilmente dotarsi di Firewall.