Lezione 11 modulo 2

Dopo aver visto i possibili attacchi che ci possono essere a un sistema, andremo adesso a considerare quali sono le proprietà che noi vogliamo avere da questi sistemi, in particolare per un sistema informativo. Quindi definiremo delle proprietà di sicurezza che saranno delle proprietà che potremo utilizzare per definire i requisiti di sicurezza che vogliamo avere per un certo sistema. Queste proprietà non necessariamente saranno richieste tutte nello stesso momento per lo stesso sistema; vediamo di definire adesso le proprietà che abbiamo e poi vedremo come possiamo usarle e successivamente vedremo quali sono le tecniche che potremo utilizzare per dare delle garanzie sul sistema. Innanzitutto cominciamo a elencare le proprietà: la 'integrità', la 'autenticità', la 'riservatezza', e, infine, la 'disponibilità'. Vediamo le loro definizioni e vediamo poi appunto quali sono le caratteristiche che vogliamo ottenere. Parliamo innanzitutto dell'integrità: abbiamo visto che all'interno di un documento che può essere trasmesso in rete, quello che può essere effettuato è una modifica non autorizzata di questo documento e quindi far arrivare il documento non integro al destinatario. C'è un aspetto che è importante in questa definizione che riguarda in particolare i sistemi informativi. In generale, i documenti saranno costituiti da un insieme di blocchi e quindi un documento arriva integro a destinazione se nessuno dei blocchi ha avuto una modifica, ma anche se arrivano a destinazione tutti i blocchi che compongono il documento originale e sono quelli originali. Quindi vedremo che questo sarà un aspetto importante quando andiamo a trasferire i documenti. Ovviamente quando noi stiamo parlando di integrità consideriamo dei documenti, ma possiamo anche considerare qualunque tipo di informazione all'interno di un sistema, quindi questa proprietà dovrà essere valida per qualunque sequenza di vita all'interno del sistema. Un aspetto particolare che sarà da considerare è l'integrità, ad esempio per quanto riguarda le configurazioni del sistema, che anch'esse possono essere alterate, quindi non parleremo solo di documenti a livello applicativo o di dati in una base di dati, ma anche di configurazioni del sistema, che anche esse possono essere attaccate. Passiamo alla seconda proprietà che vogliamo considerare: l'autenticità. Abbiamo detto che vogliamo, se stiamo trasmettendo dei documenti, trasmettere un documento da A a B e che questo documento deve essere integro. L'autenticità ha al suo interno l'integrità, quindi voglio che il documento sia integro, ma aggiungo un altro aspetto: voglio sapere chi ha creato il messaggio, quindi abbiamo l'autenticazione del soggetto creatore del messaggio, quindi sostanzialmente io voglio non solo che il mio documento arrivi a destinazione nella sua forma originale, ma voglio anche che B sappia che il documento proviene da A. Ovviamente questo vorrà dire che io sarò in grado di identificare gli agenti all'interno del mio sistema, quindi parleremo poi successivamente della necessità e delle varie modalità che potremmo avere per identificare chi scambia messaggi in rete. In questo modo io avrò un documento che arriva integro, quindi non è stato modificato, e so anche chi l'ha creato. Questa proprietà deve accompagnarsi anche a quella che viene chiamata 'Non ripudio', quindi non solo so che A ha creato effettivamente il documento, ma non potrà sostenere successivamente di non averlo fatto. Quindi effettivamente B sarà sicuro di avere un documento integro che arriva da A. Come abbiamo visto già per l'integrità, non necessariamente questo si applica a soli documenti o messaggi, ma possiamo applicarlo anche alla distribuzione del software, per cui voglio sapere perché effettivamente il software è quello che è stato generato da un certo produttore di questo software, non è stato alterato ad esempio inserendo delle parti malevole che l'autore non riconoscerebbe e quindi potremo anche in questo caso parlare di autenticità del software, quindi vogliamo avere queste garanzie relative all'autore del software e della sua integrità. Questo vale anche per dei dati che possono essere memorizzati all'interno di un archivio, quindi non sono nella trasmissione e così via... C'è una proprietà che naturalmente viene in mente quando si parla di sicurezza, che è la 'Riservatezza'. Quando voglio che un documento sia riservato, voglio che sia accessibile solo a agenti autorizzati. Abbiamo visto che molte forme di attacchi sono proprio attacchi che cercano di acquisire delle informazioni da parte di agenti non autorizzati. Ovviamente quello che abbiamo visto prima, l'autenticità, non comporta riservatezza. Io posso avere un documento che viene inviato, che è autentico, integro, ma non riservato, ovviamente. Quindi è una proprietà di natura diversa, quindi io tenderò in questo caso a creare delle

modalità di trasformazione dei documenti in modo che non siano leggibili da parte di chi non è autorizzato, oppure dovrò stabilire delle regole di accesso ai sistemi, in modo che un certo utente possa accedere solo alle parti di sistemi oppure ai dati che è autorizzato appunto a poter leggere. Ultima proprietà: la 'disponibilità'. Questa è una proprietà un po' diversa da quelle che abbiamo visto prima, che si concentravano sul fatto che ci sia una trasmissione oppure una memorizzazione di documenti, di dati, di configurazione di software. La disponibilità riguarda sostanzialmente un sistema a cui arrivano delle richieste e da cui ci si attende una risposta. La disponibilità definisce la capacità del sistema di poter fornire dei servizi, quindi delle richieste di servizi, in tempi ragionevoli rispetto alle caratteristiche definite per questi servizi. Quindi è la capacità di erogare il servizio da parte del sistema. Perché qua possiamo anche definire anche questo una proprietà di sicurezza? Perché il fatto che il sistema informativo sia in grado di fornire un servizio fa parte delle caratteristiche necessarie per il suo funzionamento e quindi è anche questa soggetta ad attacchi di sicurezza. Se voglio negare un servizio a qualcuno, cosa posso fare ad esempio? Inviare una quantità enorme di richieste in modo artificioso a questo sistema sovraccaricandolo in modo che quando arriva effettivamente la richiesta legittima, questa non possa essere servita secondo le modalità di fornitura dei servizi. Attacchi di questo tipo vengono chiamati di 'Denial of service', e in particolare quello che è caratteristico nei servizi forniti in rete è quello che viene chiamato il 'Distributed denial of service', in cui tanti sistemi appunto generano questi messaggi che vanno a sovraccaricare un certo sistema, un certo insieme di servizi che vengono forniti da un fornitore, in modo da impedirgli poi di funzionare correttamente. Questo è tipico di attacchi ad esempio a sistemi che erogano servizi ad esempio di posta elettronica oppure di distribuzione di documenti di tipo digitale, in cui sostanzialmente si rende il sistema non più in grado di fornire quel servizio. Questo avviene a causa di un sovraccarico artificioso da parte di altri sistemi che probabilmente saranno stati a loro volta attaccati, ad esempio tramite virus con un software malevolo che poi a un certo punto viene attivato, in modo da fare in modo che un certo sistema sovraccarichi un certo obiettivo. Ovviamente questo tipo di proprietà è una proprietà un po' diversa rispetto a quello che abbiamo visto nelle prime tre proprietà, perché non andiamo a vedere qual è l'oggetto informativo di cui ci stiamo occupando, ma stiamo andando a vedere un sistema che fornisce servizi e quindi anche il tipo di sistemi che dovremo adottare per prevenire attacchi di questo tipo o comunque per poterci difendere da attacchi di questo tipo avrà una natura diversa. Vedremo nei prossimi moduli vari aspetti di gestione di queste proprietà all'interno di un sistema informativo, ma esaminiamo quali sono le caratteristiche principali di questi sistemi che noi vorremmo andare a considerare. Innanzitutto, che obiettivi abbiamo? Abbiamo un obiettivo di evitare gli attacchi; ovviamente questo sarà un obiettivo che però non sarà sempre possibile raggiungere, quindi noi possiamo in realtà fare delle misure di prevenzione per rendere difficoltosi appunto questi attacchi. Ma molto importante non è solo evitare l'attacco ma soprattutto essere in grado di rilevare un attacco, ad esempio se un documento che è stato trasmesso in rete è stato modificato da un agente non autorizzato, io voglio essere in grado di dimostrare che non è un documento autentico, che quindi è stata violata la proprietà di autenticità e quindi essere in grado di rifiutare questo documento. Sarà invece molto più difficile e quasi impossibile in certe condizioni evitare che possano essere intervenute delle modifiche, però in questo caso diventa importante poter provare la proprietà: il documento è autentico oppure no? e quindi questo è un altro aspetto che noi andremo ad esaminare in dettaglio a seconda delle varie situazioni, delle varie tecniche che vogliamo andare ad utilizzare. Ultimo aspetto: abbiamo detto che non sempre possiamo evitare gli attacchi, ma possiamo limitare gli effetti degli attacchi. Quindi prendere delle contromisure che ci consentano appunto di continuare a fornire dei servizi anche quando si verifica un attacco e ci consentano appunto di continuare l'operatività del sistema informativo anche in questi casi.