La debolezza intrinseca dei protocolli Internet

Feb 19, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario, Tecnologia, Vulnerabilità 0

Le infrastrutture della Rete sono vulnerabili ad attacchi e abusi. Ma per cambiare le cose serve un intervento complessivo a tutti i livelli.

Buone pratiche, policies adeguate e controlli attraverso software di sicurezza sono elementi indispensabili per proteggere i dati ed evitare furti di informazioni. **In alcuni casi, però, tutti questi strumenti non sono sufficienti a evitare che dati e informazioni riservate finiscano sotto gli occhi di chi non dovrebbe metterci sopra le mani**.

Il problema è che, quando il dirottamento dei dati avviene a un livello più "alto", i singoli soggetti non possono fare nulla per impedire che questo avvenga. È il caso, per esempio, del **DNS poisoning**, cioè degli attacchi che prendono di mira i server DNS a cui è deputato il compito di indirizzare il traffico a livello di sistema.

La loro struttura, basata su un sistema "a piramide", non prevede alcun sistema di autenticazione sufficiente a impedire che un attacco a questo livello possa portare al dirottamento e la cronaca recente ha mostrato numerosi casi (principalmente legati al furto di cripto-valute) in cui i cyber-criminali sono riusciti a fare leva sull'architettura dei server DNS per mettere a segno colpi clamorosi.

Il mese scorso, come abbiamo raccontato su queste pagine, l'abuso dei sistemi DNS ha permesso a ignoti hacker (che secondo **FireEye** potrebbero avere legami con il governo

iraniano) di rubare le credenziali di numerosi account di posta elettronica collegati ad aziende ed enti pubblici.

Teoricamente, attacchi come questi potrebbero essere bloccati (o per lo meno mitigati) attraverso l'uso di tecniche come le **Domain Name System Security Extensions**, che prevedono l'uso di un sistema di signature crittografiche per verificare l'autenticità delle informazioni trasmesse. Sono ancora poche, però, le organizzazioni che si sono dotate di sistemi del genere.

Lo stesso ragionamento vale per quanto riguarda **BGP (Border Gateway Protocol)**, il sistema di smistamento dei dati che li indirizza tra le varie reti.

In questo caso il punto debole è rappresentato dal fatto che il routing dei dati è affidato a un sistema che si basa, essenzialmente, sulla fiducia reciproca tra gli operatori. In caso di anomalie (come accadde nel 2017 quando il traffico relativo a transazioni finanziare sono finite non si sa come in Russia) diventa addirittura estremamente difficile capire se si tratti di un errore tecnico o di un attacco vero e

proprio.

Anche in questo caso la soluzione potrebbe passare per un sistema di autenticazione applicato a ogni livello di Internet, ma la loro efficacia è legata al raggiungimento di una “massa critica” che consenta di avere continuità nella verifica della trasmissione dei dati.

Insomma: siamo di fronte alla classica situazione in cui la necessità di un intervento è evidente a tutti, ma nessuno vuole essere il primo a impegnarsi (e investire) in un’impresa che per i suo successo richiede un’ampia partecipazione.

Stiamo parlando infatti di modifiche architetturali che, in molti casi, richiederebbero la sostituzione di componenti hardware (i router utilizzati dai provider) e, di conseguenza, dei costi piuttosto elevati.

A muoversi, per il momento, sembrano essere più che altro i governi. Qualche esempio? Nel **Regno Unito** l’iniziativa è stata presa dal **National Cyber Security Center**, che ha recentemente annunciato di aver avviato una “interlocuzione” con i provider nazionali per irrobustire BGP.

In **Russia**, invece, stiamo assistendo a un tentativo di rendere indipendente il sistema dei server DNS per garantire **l’autonomia della rete sul territorio della Federazione**.

Il problema però rimane: fino a quando queste iniziative (con tutti i dubbi legati ai reali intenti che le muovono) rimarranno isolate e autonome, un vero cambio di passo a livello globale rimane lontano.

Please follow and like us:

Dostupno: l’app di messaggistica espone i dati degli utenti su Internet?

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/02/19/la-debolezza-intrinseca-dei-protocolli-internet/