Il Domain Name System: una infrastruttura da proteggere

>> L'importanza, lo stato di salute e le vulnerabilità del DNS

Andrea Rigoni
Igor Nai Fovino
Elena Agresti
Salvatore Di Blasi

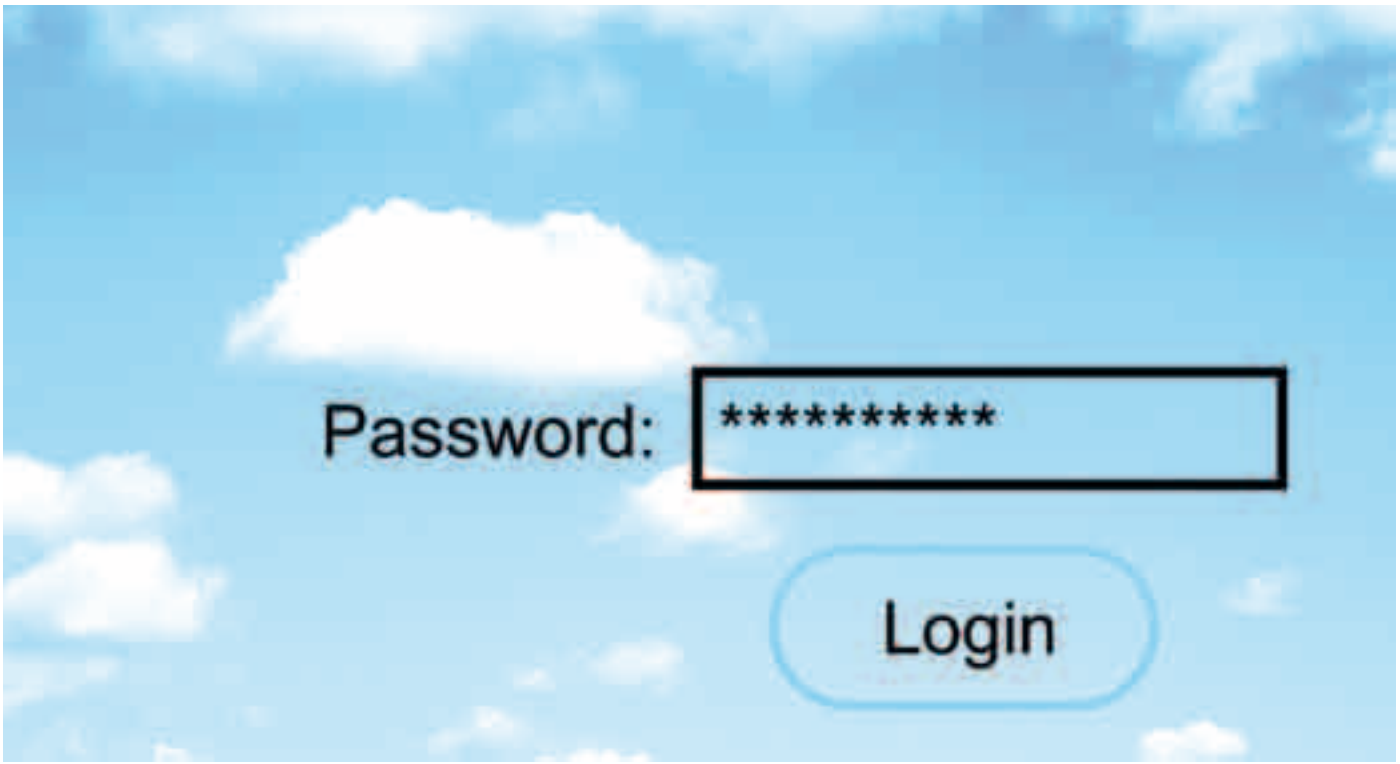
Global Cyber Security Center
GCSEC

Ci troviamo oggi di fronte ad una realtà in continuo divenire, in una società dinamica e digitalizzata, soggetta a nuove tipologie di minacce che insistono sulle infrastrutture del Paese.

La forte dipendenza delle infrastrutture critiche dalle tecnologie informatiche pone la Cyber Security al centro della protezione del Sistema Paese e dei cittadini.

In uno scenario di cyber-war, attacchi alle infrastrutture critiche, quali ad esempio i sistemi bancari e finanziari, potrebbero comportare notevoli impatti sul sistema economico del Paese stesso e di altri Paesi, causando interruzione dei servizi e perdite finanziarie dirette ed indirette.

Oggi infrastrutture critiche (CI) come i sistemi bancari e finanziari, non sono più esposti semplicemente a minacce di sicurezza tradizionali, ma anche a nuove minacce quali ad esempio quelle legate alle reti IP e al Domain Name System (DNS). Come diretta conseguenza, reti di telecomunicazione e DNS sono diventate a loro volta un bersaglio appetibile per la criminalità organizzata, che sfruttando la scarsa attenzione generalmente prestata per la sicurezza e la resilience dei DNS, può cercare di sfruttare questa "falla" nella >>



sicurezza delle infrastrutture critiche per minacciare o ricattare aziende.
Il DNS riveste oggi un ruolo importante e recentemente è stata riconosciuta come una infrastruttura di rilevanza internazionale.
Nel 2007 l'IETF DNS Extensions Working Group (dnsext), dopo un ampio dibattito, ha identificato il Domain Name System come "una infrastruttura Internet critica". Nonostante il DNS abbia operato globalmente in modo affidabile e robusto per decenni in tutto il mondo, la sua rilevanza nella moderna società digitale pone ora nuove sfide a livello operativo e di governance.
Recentemente il DNS ha guadagnato una grande popolarità mediatica proprio a causa di gravi vulnerabilità utilizzabili per perpetrare crimini informatici di rilievo.
La "falla" più evidente in termini di sicurezza del Domain Name System è sicuramente costituita dal fatto di essere sempre stato, sin dagli albori del suo concepimento, un protocollo privo di qualsiasi meccanismo atto a proteggere l'integrità delle informazioni distribuite (ad esempio l'associazione "indirizzo mnemonico di un server-indirizzo IP") e ad autenticarne la fonte (in altre parole a garantire che l'informazione richiesta sia stata veramente fornita dal server DNS preposto e non sia stata invece fornita da una terza parte non affidabile). Tale evidente mancanza, frutto ovviamente del fatto che ai tempi del concepimento del DNS, scenari di hacking, attacco informatico ecc. erano ben lungi dall'essere addirittura immaginati, è stata recentemente colmata con l'introduzione di una estensione di tale protocollo, DNSSEC, che mediante l'uso di meccanismi crittografici consente di garantire:

- l'effettiva origine dei dati DNS
- l'integrità dei dati ricevuti (ma non la riservatezza o la disponibilità)
- le asserzioni di non esistenza.

Parlando di impatto del DNS su infrastrutture critiche, nell'ambito bancario è divenuto ormai noto il fenomeno del pharming in cui l'attacco viene sferrato direttamente verso il server DNS inficiando la sua coerenza ed integrità. Gli utenti in questo caso, pur digitando la URL corretta del sito richiesto, ad esempio del proprio sito bancario, vengono indirizzati verso un sito illegittimo nel quale solitamente viene perpetrato il furto di identità e di dati bancari e finanziari. La complessità di questa minaccia è caratterizzata inoltre dal fatto che tali attacchi possono essere non solo effettuati in qualsiasi momento, ma soprattutto in qualsiasi punto delle catena di risoluzione del DNS.

Considerando che oggigiorno sono numerosi i servizi bancari che vengono erogati anche in modalità digitale,

e che in quanto "servizi online" essi devono appoggiarsi ai servizi del DNS (salvo rare eccezioni), risulta chiaro come non solo attacchi complessi che sfruttino bachi del sistema, ma anche brutali DOS contro nodi critici del DNS, possono avere un impatto rilevante sull'ecosistema economico. Basti pensare a cosa potrebbe accadere ai mercati finanziari a seguito di un attacco ai sistemi di trading.

Inoltre il coinvolgimento dei DNS nelle cyber-war e nella criminalità informatica è oggi uno scenario non più trascurabile, soprattutto se si considera che, mentre a livello globale il DNS appare abbastanza stabile ed elastico, localmente, a causa della sua intrinseca natura, non può essere considerato altrettanto robusto.

L'idiosincrasia tra livello globale e locale non è solo dovuta ad aspetti tecnici, ma anche ad una mancanza di politiche omogenee che regolino la governance e l'operatività del DNS.

Al momento non esiste una definizione standard di sicurezza e resilience del DNS, non è identificato un framework di metriche per la valutazione del livello di sicurezza e resilience, né sono definite delle best practice condivise per garantire una risposta efficace ed una governance in caso di scenari di crisi o di guerra cibernetica.

L'Internet Corporation for Assigned Names and Numbers (ICANN), che ha la responsabilità di gestire il sistema dei nomi a dominio generici di primo livello e dei country code Top Level Domain (ccTLD), che identificano uno specifico territorio, nonché i root server, ha organizzato due simposi sulla sicurezza, la stabilità e la resilienza del DNS.

In queste conferenze è stato introdotto il concetto di salute del DNS, è stata evidenziata la possibilità e la necessità di misurarne lo stato e tutti gli operatori e le parti coinvolte hanno manifestato un forte interesse alla problematica. I risultati dei due simposi sono stati

utilizzati anche come driver per la definizione del piano delle attività operative del 2011 dell'ICANN.
In particolare nel secondo simposio l'ICANN ha presentato i cinque indicatori vitali dello stato di salute del DNS:

- Coerenza
- Integrità
- Velocità
- Disponibilità
- Resiliency

Da un'analisi accurata del rapporto del secondo simposio emergono inoltre una serie di punti tutt'oggi da chiarire e di domande non risposte relative a:

- la necessità di metriche sullo stato di salute del DNS e sulla sicurezza dei diversi DNS (operatori dei root server, operatori del non root name server, recursive cache, open DNS resolver, gli utenti finali);
- la necessità di comprendere e definire metodi e tecniche per la misurazione della salute del DNS e degli indicatori di sicurezza;
- la necessità di definire livelli di soglia delle metriche che consentono alla comunità del DNS di capire quando la salute del DNS e/o gli aspetti di sicurezza a questo associati sono compromesse.

A tal proposito la fondazione Global Cyber Security Center (GCSEC) sta coordinando un'iniziativa a livello internazionale per lo sviluppo di un framework per la definizione del livello di salute del DNS. La fondazione GCSEC (www.gcsec.org) è un'organizzazione senza fini di lucro che vuole fungere da fulcro della conoscenza e della cultura sulla cyber-security a livello internazionale. Sta svolgendo diverse attività di ricerca, coinvolgendo esperti e ricercatori da tutto il mondo.
Il progetto di ricerca sul DNS consiste nella definizione di un quadro aperto di metriche, concepito per aiutare organismi nazionali, operativi e di regolamentazione, direttamente o indirettamente impattati dalla stato di funzionamento del DNS, a valutarne lo stato di salute, nell'ottica di supportare la definizione di più oculate politiche di gestione, piani di contingenza, modifiche architetturali delle proprie infrastrutture tenendo conto dell'impatto stesso del DNS.
Nella definizione del livello di salute del DNS è necessario tenere in considerazione le numerose vulnerabilità a cui il DNS è soggetto e che, in linea generale, possono essere classificate in tre macro categorie: *data corruption, attacchi DOS (Denial of Service) e perdita di confidenzialità.*
Per data corruption si intende qualsiasi modifica non autorizzata ai dati del DNS che potrebbe influenzare direttamente la coerenza e l'integrità di una parte o di tutto il DNS e, di conseguenza, influire sulla resilience

stessa del DNS, mentre per attacco Denial of Service si intende un attacco che rende inutilizzabile il servizio per gli utenti legittimi.
Entrambe le suddette tipologie di attacchi possono essere rivolte ad un servizio specifico, come nel caso del DNS, o a tutta una parte della rete.
Altre problematiche possono invece impattare sulla confidenzialità in quanto consentono agli aggressori l'accesso ai dati del DNS consentendo a questi di raccogliere informazioni sull'infrastruttura del DNS. Cache snooping e NSEC walk sono esempi di minacce di perdita di confidenzialità.
Nella tabella 1 è evidenziata la relazione esistente tra le minacce e gli indicatori del grado di salute del DNS. È stato aggiunto un ulteriore indicatore, "vulnerabilità", nell'ottica di utilizzarlo in fasi successive per valutare il livello di suscettibilità di particolari sistemi ad alcune vulnerabilità specifiche. È possibile osservare che la coerenza e l'integrità sono correlate alla data corruption, mentre la velocità e la disponibilità sono legate ad attacchi di tipo DDoS.
La resilience, correlata alla capacità DNS di mantenere un certo livello del servizio, è influenzata sia dal danneggiamento di dati e minacce DDoS. Anche la vulnerabilità, intesa come la probabilità che un problema nei DNS, produca una determinata vulnerabilità, è legata a tutte le categorie di minacce.
Attualmente la comunità scientifica sta iniziando a valutare le problematiche annesse alla confidenzialità del DNS come rilevanti per stabilire il grado di salute del DNS.
Nella definizione del framework sarebbe molto utile focalizzare l'attenzione sulla parte più debole del DNS, ovvero sugli elementi locali del DNS, per capire quale potrebbe essere l'effetto di un'estensione o del rafforzamento del DNS su infrastrutture critiche.
Il progetto della fondazione GCSEC sicuramente può rappresentare una risposta alle necessità di sicurezza del DNS e porre le basi per garantire un livello di governance e operatività sempre più elevato.

Categorie di minacce	Tipologie di minacce	Indicatori di Salute
Data corruption	Cache poisoning	Coerenza Integrità Resiliency Vulnerabilità
	Originating Modification	
	Response Modification	
DDoS	DNS server	Velocità Disponibilità Resiliency Vulnerabilità
	Network Infrastructure	
Perdita di confidenzialità	Cache Snooping	Vulnerabilità

Tabella 1: Esempi di minacce e di indicatori di salute