WHITE PAPER

REGOLAMENTO DI ESECUZIONE NIS2 E BEST PRACTICE PER DNS

Autore: Craig Sanderson,
Principal Cyber Security Strategist
presso Infoblox

INDICE DEI CONTENUTI

La direttiva sulle reti e sui sistemi informativi dell'UE ("**NIS2**"), che mira a migliorare la resilienza alla sicurezza informatica in tutta l'UE, dovrebbe essere recepita nel diritto nazionale degli Stati membri dell'UE il 17 ottobre 2024. Per una panoramica completa dei requisiti NIS2, consulta il nostro blog precedente.

In vista di tale data, la Commissione europea ha adottato il Regolamento di esecuzione NIS2, che stabilisce in modo più dettagliato alcuni dei requisiti tecnologici che le entità soggette a NIS2 sono tenute a rispettare. I requisiti del regolamento di esecuzione costituiranno la base di conformità in tutta l'UE e ci aspettiamo che siano integrati con ulteriori dettagli tecnici e linee guida nei prossimi mesi.

Di particolare rilevanza per i professionisti legali, della conformità e della sicurezza informatica che lavorano per le entità soggette a NIS2 sono i requisiti del regolamento di esecuzione sulla sicurezza DNS. La Commissione europea ha da tempo riconosciuto la criticità del DNS come controllo di sicurezza. La direttiva NIS2 afferma che: "Il mantenimento e la conservazione di un sistema di nomi di dominio (DNS) affidabile, resiliente e sicuro sono fattori chiave per mantenere l'integrità di Internet e sono essenziali per il suo funzionamento continuo e stabile, da cui dipendono l'economia e la società digitali".

Passando dal riconoscimento delle politiche all'applicazione pratica, l'articolo 6, paragrafo 7, del regolamento di esecuzione NIS2 richiede che "le entità pertinenti devono... applicare le migliori pratiche per la sicurezza del DNS". L'Agenzia dell'Unione europea per la cybersicurezza (ENISA) contribuirà a definire ciò che costituisce la "best practice per la sicurezza del DNS".

In questo whitepaper, esaminiamo e raccomandiamo regolari valutazioni dello stato e della sicurezza del DNS ed evidenziamo alcuni elementi chiave delle best practice di sicurezza DNS che dovrebbero essere considerati:

- Proteggere la piattaforma DNS;
- Proteggere il protocollo DNS; e
- Implementare il DNS come misura di sicurezza informatica.

1. ESECUZIONE DI VALUTAZIONI REGOLARI DELL'INTEGRITÀ E DELLA SICUREZZA DEL DNS

L'infrastruttura DNS è mission-critical. In caso di guasto, intere reti, con le relative applicazioni e i relativi utenti, potrebbero essere bloccate. Pertanto, il DNS è un elemento critico per la resilienza digitale di un'organizzazione. Purtroppo, in molte organizzazioni, l'infrastruttura DNS non viene valutata regolarmente.

Le organizzazioni devono condurre valutazioni periodiche dell'integrità e della sicurezza dell'infrastruttura DNS per garantire la sicurezza e la resilienza. Tali valutazioni dovrebbero includere una verifica della capacità dei server DNS di soddisfare le esigenze dell'organizzazione, soprattutto quando si adottano protocolli DNS crittografati. Le valutazioni devono includere anche una revisione dell'integrità e della configurazione dei server per garantire che l'infrastruttura DNS sia ottimizzata come parte di un'architettura altamente resiliente e ridondante.

Infoblox esegue regolarmente valutazioni dell'integrità e della sicurezza del DNS per organizzazioni globali di tutte le dimensioni. Rivolgiti al tuo account team Infoblox locale o registrati per partecipare a un seminario sulla sicurezza Infoblox utilizzando il link qui.

2. PROTEZIONE DELLA PIATTAFORMA DNS: USARE SERVER DNS DEDICATI E SICURI

Le appliance DNS, come altre appliance di rete, sono progettate appositamente per garantire facilità di gestione, sicurezza e prestazioni. I server generici non possono eguagliare l'ottimizzazione offerta da queste appliance e, di conseguenza, espongono le organizzazioni a rischi significativi data la criticità del DNS come servizio di rete.

Tuttavia, le organizzazioni usano in genere server Windows che ospitano DNS e DHCP insieme ad Active Directory (AD), un'altra infrastruttura di identità mission-critical. AD gestisce l'accesso e le autorizzazioni degli utenti e archivia le informazioni critiche, creando un'ampia superficie di attacco vulnerabile agli attacchi informatici.

Senza questa separazione dei compiti, se un utente malintenzionato segue un percorso di escalation comune e prende di mira Active Directory, il servizio DNS e la rete su cui si basa sono a rischio. Poiché il DNS assume un ruolo più significativo nella strategia di sicurezza informatica di un'organizzazione, un server DNS dedicato sarà essenziale per mitigare questi rischi.

Allo stesso modo, gli attori di minacce cercano spesso di sfruttare le vulnerabilità scoperte nel DNS, che possono avere un impatto sull'integrità del sistema DNS o provocare un denial of service. È fondamentale che le organizzazioni mantengano il loro software DNS aggiornato. Infoblox collabora con ISC (Internet Systems Consortium) per fornire patch tempestive alle vulnerabilità di BIND. Le organizzazioni devono disporre di processi per garantire che la loro infrastruttura DNS mitighi il rischio che gli attori di minacce sfruttino le vulnerabilità della piattaforma e del software DNS.

3. PROTEZIONE DEL PROTOCOLLO DNS: L'ABUSO DEL DNS – ESFILTRAZIONE DEI DATI DNS

Il protocollo DNS è essenziale per la localizzazione dei servizi per consentire la navigazione web, la posta elettronica e altre applicazioni mission-critical. Di conseguenza, le piattaforme di sicurezza tradizionali, come i firewall di nuova generazione, spesso passano il traffico DNS senza ostacoli e senza controlli. Gli attori di minacce si sono sempre più rivolti al DNS come vettore di esfiltrazione. Secondo la Cybersecurity and Infrastructure Security Agency (CISA) degli Stati Uniti, "l'infrastruttura DNS è un vettore di minaccia comune per le campagne di attacco".[1] Gli attori di minacce spesso incorporano dati rubati in pacchetti DNS, affidandosi all'infrastruttura DNS per inoltrare i dati rubati ai server DNS controllati dagli attori di minacce. Le piattaforme DNS sono posizionate in modo ideale per valutare le richieste DNS ricorsive che ricevono per i tentativi di esfiltrazione dei dati.

Ulteriori informazioni sul vettore di minaccia dell'esfiltrazione dei dati DNS sono disponibili qui: Centro risorse sull'esfiltrazione dei dati DNS.

Infoblox ha sviluppato un'analisi delle minacce sia per le appliance on-premise che per la piattaforma cloud Threat Defense, per mitigare in modo specifico questa minaccia. Maggiori dettagli sono disponibili su: Threat Insight.

a) Protezione del protocollo DNS: limitare l'uso di servizi DNS pubblici non autorizzati basati su Internet

Le organizzazioni devono assicurarsi che gli utenti non utilizzino deliberatamente o inavvertitamente servizi DNS pubblici non autorizzati, basati su Internet. Questa best practice è stata specificamente richiamata dalla CISA, che ha notato come i servizi DNS pubblici crittografati forniscano agli attori di minacce un modo efficace per eludere le difese di sicurezza informatica della rete. In linea con la sua guida, le organizzazioni dovrebbero:

- Bloccare il DNS dalla rete interna a Internet, ad eccezione dei name server autorizzati a comunicare direttamente con i name server su Internet, come i forwarder.
- Bloccare il traffico DNS su TLS (DoT) dalla rete interna a Internet utilizzando il firewall o ACL del router.
- Bloccare il traffico DNS su HTTP-S (DoH) dalla rete interna a Internet utilizzando RPZ e ACL firewall.
- Utilizzare la gestione dei dispositivi mobili (MDM) o altre soluzioni di gestione centralizzata per impedire agli utenti di configurare server DNS crittografati esterni.

1 https://cyberscoop.com/nsa-secure-dns-service-pilot-defense-industrial-base/

Infoblox Threat Defense dispone di un feed di politiche che tiene traccia dei server DoT e DoH pubblici, che può essere applicato alle piattaforme dell'infrastruttura di controllo degli accessi di sicurezza di rete come i firewall di nuova generazione.

b) Protezione del protocollo DNS: protezione dello spazio dei nomi DNS

Gli attori di minacce hanno dimostrato che gli attacchi come il phishing hanno molte più probabilità di successo se sono collegati a domini di proprietà di organizzazioni fidate. Di conseguenza, spesso registrano domini "lookalike" che sembrano simili ma non sono di proprietà dell'organizzazione target. Ancora più preoccupante, una scarsa igiene dei domini autorevoli può consentire agli attori di minacce di prendere il controllo dei domini di proprietà di un'organizzazione fidata. Come dimostrato dai recenti documenti di ricerca di Infoblox, molte organizzazioni sono esposte a questo rischio fondamentale, ma questo può essere facilmente mitigato e dovrebbe essere implementato come best practice standard.

Le organizzazioni dovrebbero mettere in atto un processo per valutare in modo proattivo le configurazioni e verificare i dati nei file di zona dei loro domini DNS autorevoli, assicurandosi di mantenere il controllo su tali registrazioni di dominio e sulle relative deleghe dei name server. Allo stesso modo, il monitoraggio proattivo dei tentativi da parte degli attori di minacce di registrare domini simili o "lookalike" è fondamentale per garantire che gli attori di minacce non li utilizzino per colpire dipendenti o consumatori.

Infoblox Threat Defense ha un servizio in abbonamento che consente alle organizzazioni di cercare in modo proattivo i lookalike dei loro domini DNS esterni, nonché a quelli di importanti partner della supply-chain e altri obiettivi di alto profilo.

4. IMPLEMENTAZIONE DEL DNS COME CONTROLLO DI SICUREZZA INFORMATICA

Oltre a proteggere i server DNS, esiste un motivo convincente per implementare controlli all'interno della piattaforma DNS per sfruttare l'enorme potenziale del DNS come livello fondativo di un'architettura di sicurezza informatica.

La piattaforma DNS è già utilizzata da tutti i tipi di client sulla rete, inclusi quelli locali, nel cloud e in tutti i tipi di dispositivi IoT. Pertanto, qualsiasi protezione fornita dall'infrastruttura DNS avvantaggia tutti i client che utilizzano tale infrastruttura per la risoluzione dei nomi, indipendentemente dal tipo di dispositivo. È per questo motivo che le organizzazioni e i governi dovrebbero adottare il DNS come componente fondamentale nella loro strategia di sicurezza informatica.

a) Implementazione del DNS come controllo di sicurezza informatica: servizi di DNS protettivi

DNS protettivo ("PDNS") è un termine generico utilizzato per riferirsi all'infrastruttura DNS che applica criteri alla risoluzione DNS. Un'implementazione PDNS può rifiutarsi di risolvere un insieme di nomi di dominio noti per essere utilizzati per scopi dannosi, come campagne di phishing o infrastrutture di command-and-control malware. Le implementazioni PDNS registrano (logs) anche le query per i nomi di dominio che attivano i criteri di filtraggio, perché tali query possono indicare un'infezione da malware o altre attività dannose.

Come dimostra la distribuzione di piattaforme PDNS da parte dei governi di tutto il mondo e l'iniziativa DNS4EU nell'Unione Europea, l'uso di PDNS è diventato una best practice DNS. Secondo la funzionaria statunitense per la sicurezza informatica Anne Neuberger, "l'utilizzo di un DNS sicuro ridurrebbe la capacità del 92% degli attacchi di malware... dal punto di vista del command-and-control, con la distribuzione di malware su una determinata rete". Le organizzazioni dovrebbero approfittare dell'efficacia, del basso sovraccarico e della facilità di configurazione dei PDNS, sia configurando le RPZ (Response Policy Zone), sia inoltrando ai servizi DNS ricorsivi sicuri, o tramite una combinazione di queste due soluzioni.

Durante l'implementazione di PDNS, le organizzazioni devono comprendere le funzionalità di sicurezza in diverse soluzioni PDNS. Se utilizzano le RPZ, le organizzazioni dovrebbero configurare le RPZ sui name server ricorsivi locali, interrogati direttamente dai client, ove possibile. Questo semplifica notevolmente l'attribuzione, ossia la possibilità di identificare quale dispositivo ha inviato la query. Allo stesso modo, se si utilizza un servizio DNS ricorsivo sicuro, le organizzazioni dovrebbero assicurarsi che supporti un meccanismo per l'attribuzione.

Le piattaforme PDNS devono essere arricchite con una threat intelligence che protegga sia dai domini dannosi sia dai domini che si sospetta con un alto grado di certezza che saranno utilizzati per lanciare un attacco in futuro. Le funzionalità allo stato dell'arte di rilevamento precoce su DNS cercano di analizzare questi domini e classificarli come "sospetti" ben prima che i domini vengano utilizzati per scopi dannosi. In questo modo, con un tasso di falsi positivi trascurabile, le organizzazioni possono avere la certezza di bloccare automaticamente i domini sospetti senza interrompere l'accesso a Internet legittimo.

b) Implementazione del DNS come controllo di sicurezza informatica: mantenere i log di sicurezza DNS per supportare la risposta agli incidenti

Le organizzazioni devono conservare i dati dei log DNS e DHCP per supportare le attività di risposta agli incidenti. Durante la risposta a un incidente, il team delle operazioni di sicurezza di un'organizzazione sarà spesso tenuto a coordinarsi con il team dei servizi di rete per ricercare la cronologia degli indirizzi IP, la posizione della rete, i registri di accesso, gli utenti assegnati e altri metadati necessari per indagare e mitigare l'incidente. Questa procedura manuale può richiedere diversi giorni e richiedere a chi risponde all'incidente del tempo che altrimenti potrebbe essere impiegato per valutare l'incidente. I logs DNS e DHCP possono aiutare il team SOC di un'organizzazione a identificare rapidamente chi, cosa e quando: quale dispositivo è stato compromesso, chi lo possedeva, quale minaccia è stata coinvolta, quali attività si sono verificate sul dispositivo, quali dati sono stati archiviati o sono accessibili dal dispositivo, quando l'attacco ha raggiunto il dispositivo compromesso e, ultimo ma non meno importante, quali azioni correttive devono avere la priorità. Automatizzare l'allocazione dei metadati chiave attribuibili in tempo reale e renderli accessibili sia al team SOC che al team dei servizi di rete può accelerare gli sforzi di ricerca e risoluzione.

Per garantire una notifica rapida delle query che potrebbero indicare un'infezione o un'attività dannosa o sospetta, le organizzazioni devono integrare i log di sicurezza DNS dai name server o dal servizio DNS ricorsivo sicuro con il SIEM o la piattaforma di analisi dei log.

Se la tua organizzazione desidera sfruttare queste funzionalità, Infoblox Cloud Data Connector offre un mezzo semplificato per esportare il contesto di rete e i dati pertinenti alle piattaforme operative di sicurezza, come i sistemi SIEM.

In qualità di azienda leader nel settore della sicurezza informatica e del networking e leader di mercato nelle soluzioni DNS gestite in cloud, Infoblox è in grado di assistere le organizzazioni di tutta l'UE nella valutazione e nel rispetto dei requisiti NIS2 attraverso le valutazioni dell'integrità e della sicurezza del DNS di Infoblox. Se ritieni che la tua organizzazione possa trarne beneficio, contatta il tuo account team Infoblox locale o registrati per partecipare a un seminario sulla sicurezza Infoblox utilizzando il link qui.

Per ulteriori informazioni, contatta ga@infoblox.com.

Sede centrale
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Versione: 20241014v1