CROWDSTRIKE E CRASH INFORMATICO: SECONDO GLI INGEGNERI SI POTEVA EVITARE

Da **Massimiliano Cassinelli** - 23/07/2024

Il caso Crowdstrike evidenzia la fragilità dei sistemi informativi e la necessità di affidare la progettazione ad autentici esperti di settore

Anche il Comitato Italiano Ingegneria dell'Informazione (C3i) del Consiglio Nazionale degli Ingegneri prende posizione sul caso Crowdstrike e lo fa

attraverso un comunicato, pubblicato sul proprio sito, il cui si chiede, in modo provocatorio: “Il malfunzionamento globale dei sistemi informativi verificatosi a partire da venerdì 19 luglio, con le gravi ripercussioni registrate a livello mondiale, pone una domanda: l’evento era evitabile?”

La scelta degli ingegneri, anche alla luce delle numerose inesattezze diffuse nei giorni scorsi, parte da un approfondito esame dei fatti. Questo perché “In contesti complessi come quelli dei sistemi informativi, le conclusioni superficiali sono frequenti, dato che si basano sulle dichiarazioni delle aziende coinvolte, le uniche a possedere una conoscenza dettagliata degli eventi”.

Crowdstrike non è un evento isolato

Un evento come quello legato a Crowdstrike è però un segnale d’allarme da considerare con estrema attenzione. Non dobbiamo infatti dimenticare, come evidenziano gli esperti dell’Ordine degli Ingegneri, che “dal punto di vista dell’Ingegneria del Software, si può certamente dire che esistono procedure consolidate per mitigare questi rischi. Pertanto, le domande fondamentali da porsi sono: “Sono state seguite le procedure adeguate?”, “Le persone chiave nelle aziende interessate possiedono le competenze necessarie?”, “Chi garantisce queste competenze?”.

La risposta è arrivata dalle parole di Gennaro Annunziata, Coordinatore del C3i, organismo compostodai delegati dei 106 Ordini territoriali e istituito dal Consiglio Nazionale degli Ingegneri (CNI). Su questi temi, infatti, da anni il C3i evidenzia l’importanza delle competenze specifiche dell’Ingegnere dell’Informazione, in quanto la tutela della qualità e della sicurezza dei sistemi informativi è cruciale in un mondo sempre più digitale e interconnesso. La definizione di standard professionali rigorosi e la certificazione delle competenze sono necessarie per prevenire il ripetersi di eventi di tale portata e garantire la fiducia degli utenti nei sistemi tecnologici: “Solo così sarà possibile garantire che coloro che progettano, implementano e gestiscono i sistemi informativi siano adeguatamente preparati per affrontare le sfide attuali e future, proteggendo la sicurezza e l’affidabilità delle infrastrutture digitali essenziali per la collettività”

Chi possiede le competenze per prevenire un crash informatico?

Proprio nella gestione della cybersecurity (come ci insegna Crowdstrike) e dell’intelligenza artificiale, continua la nota, “il ruolo degli ingegneri dell’informazione è fondamentale anche nella due ambiti di crescente importanza. La cybersecurity è essenziale per proteggere le infrastrutture digitali da attacchi esterni, intrusioni e altre minacce che possono compromettere la funzionalità e la sicurezza dei dati. Incidenti come quello del 19 luglio evidenziano la necessità di competenze avanzate in materia di protezione dei dati e delle reti. L’intelligenza artificiale offre enormi potenzialità per migliorare

l'efficienza e l'affidabilità dei sistemi informativi, ma introduce nuove sfide e rischi. Gli algoritmi di AI devono essere progettati, testati e monitorati con estrema attenzione per evitare errori e bias che potrebbero avere conseguenze gravi. Inoltre, l'AI deve essere integrata nei sistemi informativi in modo sicuro, garantendo che non diventi un ulteriore vettore di attacco per cybercriminali.
L'integrazione di cybersecurity e AI nella progettazione dei sistemi informativi richiede
competenze specialistiche e un approccio multidisciplinare. Per questo, gli ingegneri
dell'informazione devono essere formati non solo nelle tecniche tradizionali di sviluppo
software, ma anche nelle pratiche di sicurezza informatica e nei principi dell'intelligenza
artificiale. Questo comporta un impegno continuo e costante nell'aggiornamento professionale, che il sistema ordinistico è in grado di supportare".

Come superare Crowdstrike?

Per risolvere le problematiche legate a Crowdstrike, consigliamo di seguire quanto prescritto da CSIRT – istituito presso l'Agenzia per la cybersicurezza nazionale (ACN).

Un recente aggiornamento di CrowdStrike Falcon Sensor ha causato gravi problematiche, su sistemi Windows, di tipo "Denial of Service".

Tipologia

- Denial of Service

Descrizione

Sono state riscontrate problematiche con un aggiornamento di CrowdStrike Falcon Sensor rilasciato il 18 luglio 2024 che causa errori BSOD (Blue Screen Of Death) su sistemi Windows con conseguente interruzione della normale operatività. In particolare la problematica sarebbe causata da un file (C-00000291*.sys) il quale ha causato il blocco degli endpoint che hanno ricevuto l'aggiornamento.

Il vendor ha fornito maggiori dettagli in merito all'aggiornamento rilasciato, dichiarando che:

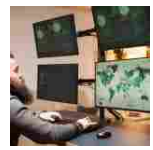
- la problematica non impatta sistemi Mac o Linux;
- gli host Windows che non sono stati impattati non richiedono alcuna azione in quanto il file problematico è stato ripristinato all'ultima versione funzionante.

Azioni di mitigazione

Nomina di Francisco Mateo-Sidron Senior Vice President Sales EMEA di Cloudera
Redazione BitMAT - 05/07/2024

Cyber Security Culture

Intelligenza artificiale amica dei cyber criminali
Redazione BitMAT - 28/05/2024



Università di Siena: ACN annuncia il ripristino dei servizi
Redazione BitMAT - 21/05/2024

Synlab: allarme Data Breach
Redazione BitMAT - 14/05/2024

PuntoFisco: nuova ondata di false comunicazioni
Redazione BitMAT - 07/05/2024

Tutte le tipologie di attacchi informatici: a cosa le aziende devono porre attenzione?
Redazione BitMAT - 30/04/2024

App & Device

Arriva anche in Italia l'app Gemini per un'AI sempre con sé!
Redazione BitMAT - 05/06/2024

Sicurezza stradale: arriva l'App che salva la vita dei motociclisti
Redazione BitMAT - 04/06/2024

LG CineBeam Q Projector: il proiettore che trasforma la parete di casa in uno...
Redazione BitMAT - 24/04/2024

CrowdStrike Engineering ha provveduto a effettuare il downgrade del file che causa la problematica e reso disponibile al download la precedente versione dello stesso.

Per gli host in stato di blocco e/o non in grado di accedere alla versione precedente del file, è possibile seguire le seguenti procedure:

Per i singoli host:

- Riavviare l'host per consentire il download della precedente versione del file. Ove l'host presenti nuovamente crash:

1. avviare Windows in modalità provvisoria o in Ambiente di Ripristino Windows;
2. andare nella cartella %WINDIR%\System32\drivers\CrowdStrike;
3. individuare il file "C-00000291*.sys" ed eliminarlo;
4. riavviare l'host normalmente.

Nota: gli host criptati da Bitlocker potrebbero necessitare di una chiave di ripristino.

Per ambienti cloud o simili (inclusi ambienti virtuali):

Opzione 1:

- scollegare il volume del disco del sistema operativo dal server virtuale impattato;
- creare uno snapshot o un backup del volume del disco in via precauzionale prima di proseguire;
- collegare/montare il volume ad un nuovo server virtuale;
- andare nella cartella %WINDIR%\\System32\drivers\CrowdStrike;
- individuare il file "C-00000291*.sys" ed eliminarlo;
- scollegare il volume dal nuovo server virtuale;
- ricollegare il volume al server impattato.

Opzione 2:

- Ripristinare da uno snapshot precedente alle ore 06:09 del 19 luglio 2024.

Per console seriale di Azure:

- effettuare il login alla console di Azure;
- andare alle macchine virtuali > selezionare la VM;
- in alto a sinistra sulla console: cliccare su "Connetti" > cliccare su "Altri metodi di connessione" > cliccare su "Serial Console";
- una volta che la console si è avviata, digitare "cmd" e premere invio > digitare "ch -si 1" e premere invio;
- premere un tasto qualsiasi. Inserire le credenziali di Amministratore;
- digitare:

1. bcedit /set {current} safeboot minimal
2. bcedit /set {current} safeboot network

- riavviare la VM;
- opzionale: eseguire il comando “wmic COMPUTERSYSTEM GET BootupState”.

Aggiornamento del 22/07/2024:

Microsoft ha recentemente pubblicato un tool per agevolare il personale IT nella risoluzione della problematica in oggetto.

Il tool fornisce 2 modalità di riparazione:

- **“Recover from WinPE”** (Raccomandata): permette di avviare il recupero del sistema senza necessità di privilegi di amministrazione (nei dispositivi cifrati con tecnologia BitLocker è necessario inserire la *recovery key*).
- **“Recover from safe mode”**: permette di effettuare il recupero di sistemi cifrati con BitLocker senza la necessità della *recovery key*. Questa soluzione è da utilizzarsi nei sistemi configurati come “*TPM-only*” o dove la recovery key BitLocker risulti indisponibile. Per questa opzione è necessario avere accesso ad un account utente con i privilegi di aministratore locale nel dispositivo impattato.

In base all’opzione scelta verrà creato un supporto d’avvio da eseguirsi nei dispositivi interessati.

Nota: Ove vengano utilizzati sistemi di cifratura di terze parti, è necessario rivolgersi ai rispettivi fornitori per assistenza sulle opzioni di recupero dei dispositivi.

Riferimenti

https://supportportal.crowdstrike.com/s/login/?ec=302&startURL=%2Fs%2Farticle%2FTech-Alert-Windows-crashes-related-to-Falcon-Sensor-2024-07-19

https://azure.status.microsoft/en-gb/status

https://techcommunity.microsoft.com/t5/intune-customer-success/new-recovery-tool-to-help-with-crowdstrike-issue-impacting/ba-p/4196959

C3i Comitato Italiano degli Ingegneri dell'Informazione CrowdStrike Ingegneri