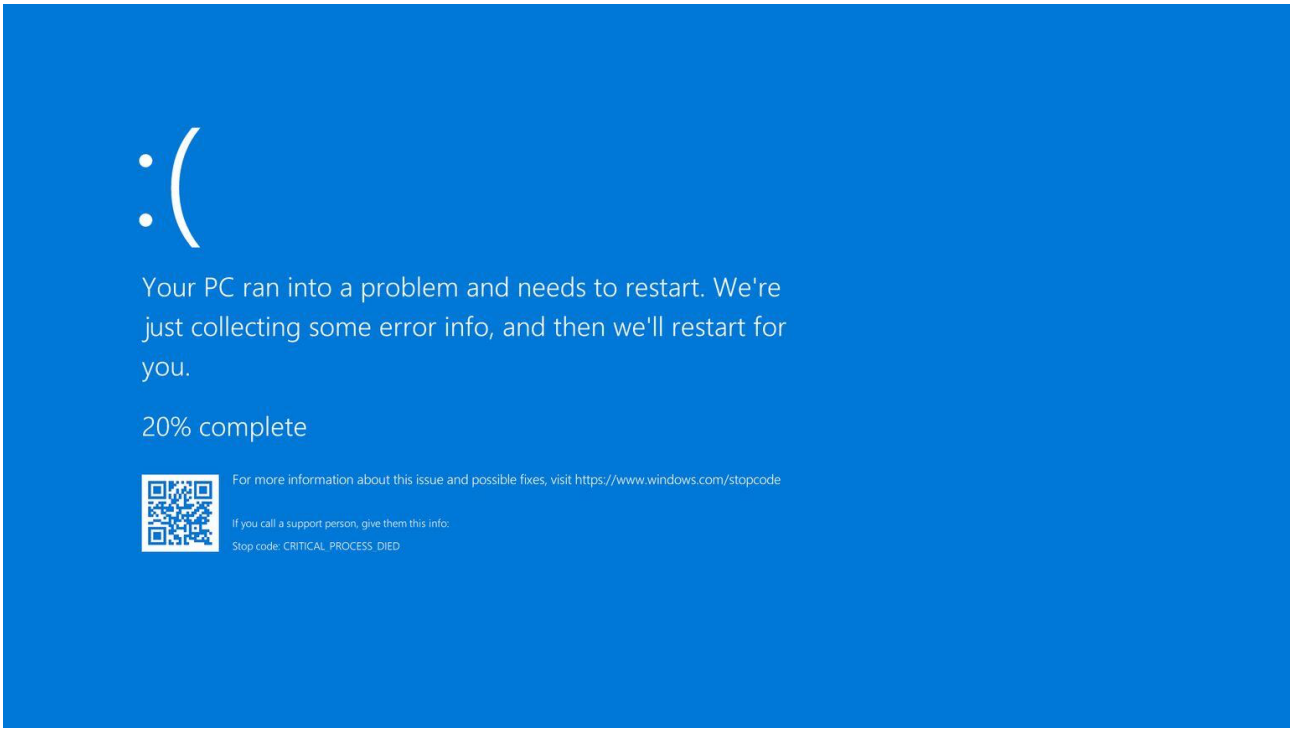
DETTAGLI TECNICI

Il 19 luglio 2024, CrowdStrike ha rilasciato un aggiornamento di configurazione per il sensore Falcon destinato ai sistemi Windows. Questo aggiornamento ha innescato un errore logico che ha causato crash del sistema e schermate blu (BSOD) su molti dispositivi.



Il problema si è verificato tra le 04:09 e le 05:27 UTC di quella giornata, e ha coinvolto i sistemi con la versione del sensore Falcon 7.11 e successive che erano online durante quel periodo.
L'aggiornamento difettoso era relativo ai "**Channel Files,"** specificamente il file di configurazione denominato "C-00000291-.sys," che controlla l'esecuzione dei named pipe in Windows. Questo file è fondamentale per la protezione comportamentale del sensore Falcon contro nuovi metodi di attacco cibernetico. Il problema è stato risolto entro le 05:27 UTC dello stesso giorno, ma ha causato significativi disagi globali, compreso l'arresto di sistemi aziendali critici e la cancellazione di migliaia di voli.
Il processo di riparazione richiedeva l'intervento manuale su ogni sistema colpito, complicando ulteriormente la situazione, specialmente per i dispositivi protetti con BitLocker. In alcuni casi, era necessario riavviare le macchine fino a 15 volte o ripristinare un backup precedente al 18 luglio.

SPECIFICHE TECNICHE

1. **Channel Files e Named Pipes**:
    - **Channel Files**: Questi file sono parte della protezione comportamentale del sensore Falcon e sono aggiornati regolarmente per rispondere a nuove tattiche, tecniche e procedure di attacco cibernetico.
    - **Named Pipes**: Sono utilizzati per la comunicazione interprocesso in Windows. Channel File 291 specificamente gestisce come Falcon valuta l'esecuzione dei named pipe.
2. **Errore Logico**:
    - **Causa dell'Errore**: L'aggiornamento del Channel File 291 includeva una nuova logica per affrontare named pipe malevoli usati da comuni framework di

Comando e Controllo (C2) nelle cyberattacchi. Tuttavia, questa nuova logica conteneva un errore che causava un crash del sistema operativo.

- **Effetto dell'Errore**: Quando il sistema tentava di processare named pipe secondo la nuova logica difettosa, questo causava un crash del sistema, risultando in una schermata blu (BSOD).

3. **Remediation**:
    - **Correzione**: CrowdStrike ha aggiornato il contenuto del Channel File 291 per correggere l'errore logico. Non sono state fatte altre modifiche, oltre a questa correzione.
    - **Recupero dei Sistemi**: I sistemi colpiti potevano essere ripristinati avviandosi in modalità provvisoria o nell'ambiente di ripristino di Windows e cancellando manualmente il file "C-00000291-.sys" dalla directory C:\Windows\System32\drivers\CrowdStrike\.

Processo di Recupero

- **Manuale**: Gli operatori dovevano intervenire manualmente su ogni sistema colpito, rendendo il processo laborioso, soprattutto per grandi organizzazioni con molti dispositivi.
- **Complicazioni con BitLocker**: Per i sistemi con BitLocker attivo, era necessario disporre della chiave di recupero, complicando ulteriormente il processo se il server che la ospitava era anch'esso colpito.

CROWDSTRIKE NON È STATO IL "PRIMO CASO"
Il caso CrowdStrike non è isolato. Numerosi altri episodi hanno visto aggiornamenti antivirus provocare instabilità nei sistemi operativi. Ad esempio, Windows Defender ha causato crash nel 2020 a causa di un errore nel trattamento dei file con nomi contenenti due punti. Allo stesso modo, un aggiornamento di Sophos nel 2022 ha portato a BSOD su Windows 11, mentre McAfee Livesafe ha causato problemi simili nel 2020. Anche ProtonVPN ha visto i suoi clienti affrontare schermate blu a causa di conflitti con alcuni software antivirus nel 2021.

Questi incidenti sottolineano l'importanza critica di test approfonditi e di una rigorosa verifica degli aggiornamenti prima del loro rilascio. Evidenziano anche la necessità di una comunicazione chiara e tempestiva con gli utenti per mitigare rapidamente i problemi quando si verificano. La gestione dei software di sicurezza richiede un approccio olistico e collaborativo per prevenire disagi significativi e mantenere l'integrità e la sicurezza dei sistemi informatici.

Windows Defender:

- **Data dell'incidente**: Aprile 2020.
- **Descrizione**: Un aggiornamento delle definizioni di Windows Defender ha causato crash del sistema quando il software tentava di scansionare file con nomi contenenti due punti. Questo problema è stato risolto con un aggiornamento delle definizioni antivirus.
- **Fonte**: BleepingComputer, 16 aprile 2020.

Sophos Antivirus:

- **Data dell'incidente**: Maggio 2022.
- **Descrizione**: Dopo l'installazione dell'aggiornamento KB5013943 di Windows, molti utenti di Windows 11 che utilizzavano Sophos Home hanno riscontrato BSOD. Il

problema era causato dal driver hmpalert.sys. Sophos ha rilasciato una patch automatica per risolvere il problema.

- **Fonte**: BleepingComputer, 16 maggio 2022.

McAfee Livesafe:

- **Data dell'incidente**: Dicembre 2020.
- **Descrizione**: Un aggiornamento automatico di McAfee Livesafe ha causato crash su molti laptop, costringendo gli utenti a disinstallare il software antivirus per risolvere il problema.
- **Fonte**: HP Support Community, 21 dicembre 2020.

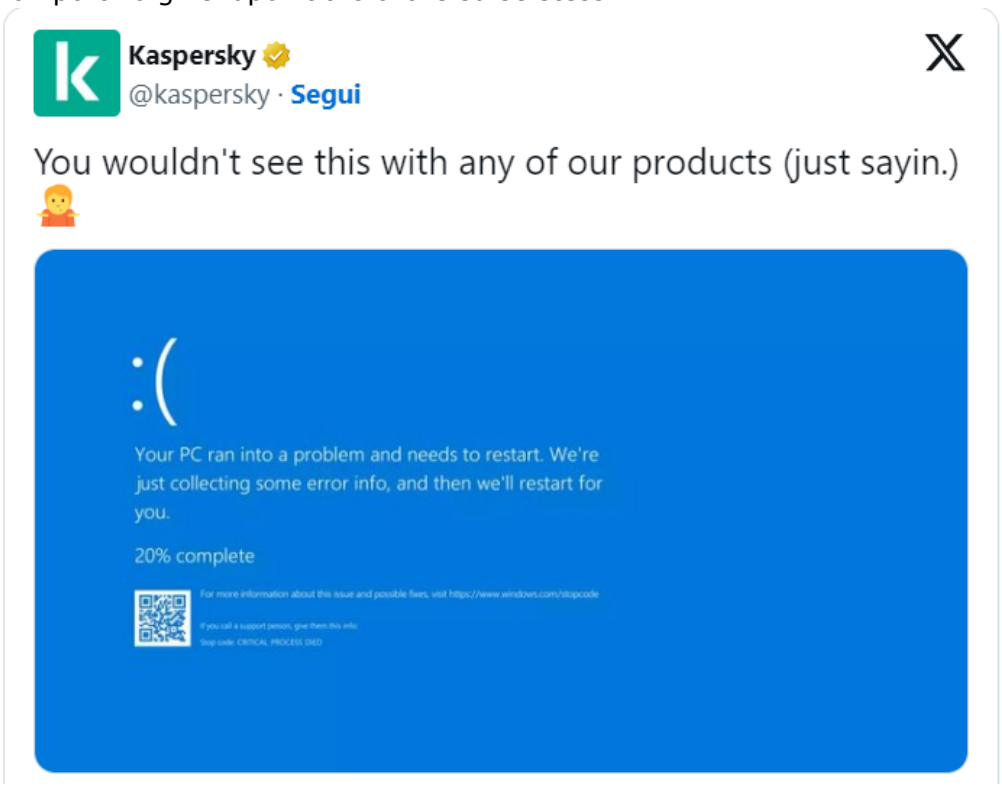
ProtonVPN:

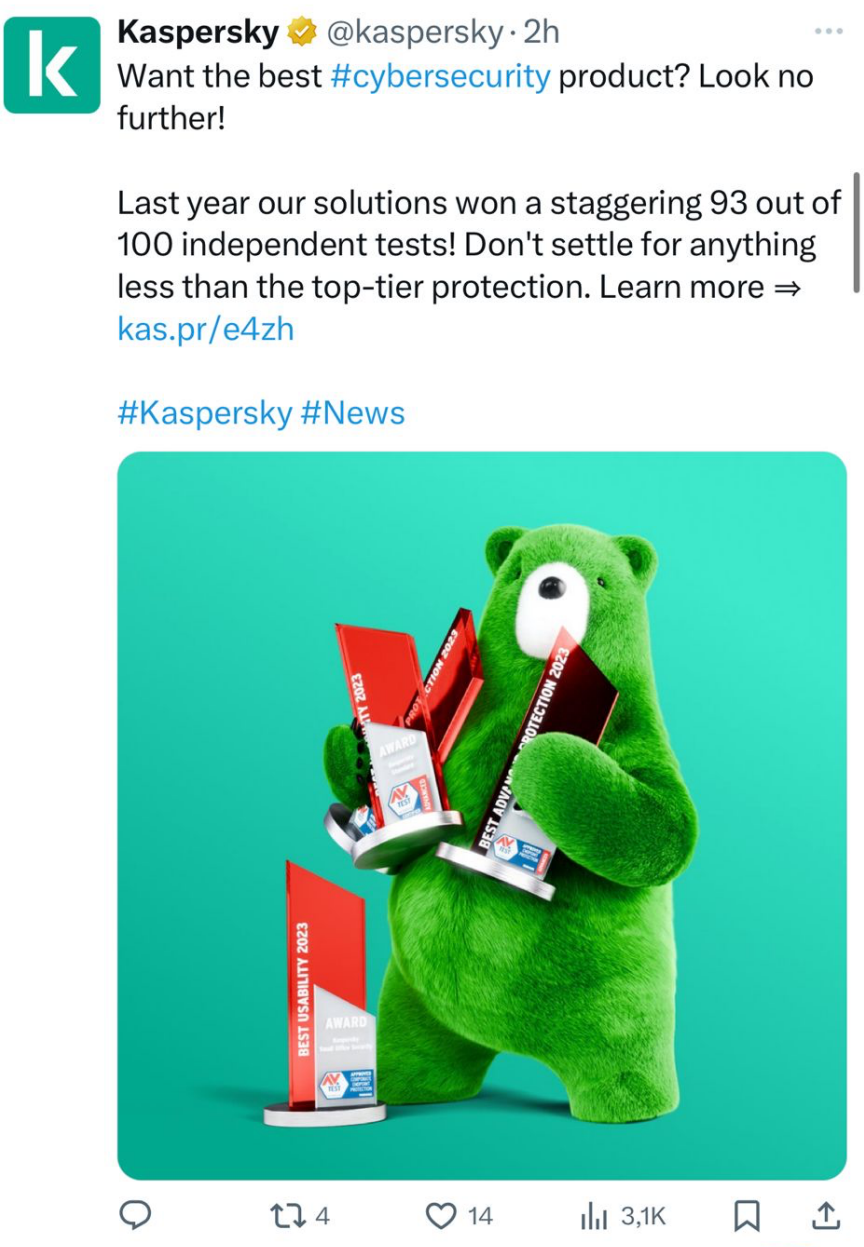
- **Data dell'incidente**: Gennaio 2021.
- **Descrizione**: ProtonVPN ha causato BSOD su Windows a causa di conflitti con alcuni software antivirus. Gli utenti hanno segnalato crash subito dopo il lancio del client VPN. ProtonVPN ha rilasciato una versione beta per risolvere il problema.
- **Fonte**: BleepingComputer, 25 gennaio 2021.

ANALISI COSTRUTTIVA DEGLI ERRORI NELLA COMMUNITY INFOSEC

È inevitabile che, nel corso delle attività, tutti possano commettere errori. Pertanto, è cruciale focalizzarsi sull'analisi approfondita degli errori piuttosto che indulgere in recriminazioni. Tuttavia, non sempre la calma e la lucidità caratterizzano l'intera comunità della sicurezza informatica. Questo spesso distoglie l'attenzione da riflessioni costruttive e favorisce la nascita di divisioni interne.

Kaspersky, dopo il ban dei suoi prodotti negli USA, ha voluto precisare come i loro prodotti non portino gli endpoint a crollare su se stessi.





CONCLUSIONI E RIFLESSIONI

L'insuccesso può spesso fungere da catalizzatore per lo sviluppo di nuove opportunità, offrendo la possibilità di affinare le soluzioni esistenti e di rafforzare ulteriormente le misure di sicurezza, in particolare in contesti caratterizzati da equilibri delicati come quelli delle infrastrutture digitali moderne. Questo principio assume una rilevanza ancora maggiore quando si considerano gli incidenti recenti che hanno messo in luce vulnerabilità specifiche all'interno delle catene di approvvigionamento tecnologico del software.

Pur non essendo direttamente responsabile, il caso di Microsoft Windows ha svelato debolezze insite nelle catene di approvvigionamento del software che erano note in teoria, ma che non erano mai state esposte con tale chiarezza pratica. Questo incidente evidenzia la necessità di una gestione più proattiva dei rischi associati alle dipendenze tecnologiche, soprattutto in un'epoca in cui le infrastrutture digitali sono interconnesse e interdipendenti.

È imperativo riconoscere che il concetto di "rischio zero" è un'utopia; le aziende devono quindi implementare strategie preventive più rigorose, garantire una vigilanza costante e promuovere una comunicazione efficace e tempestiva con i loro fornitori. La mitigazione dei rischi richiede un approccio olistico e collaborativo che coinvolga tutte le parti interessate, dalle imprese tecnologiche ai fornitori, fino agli utenti finali.

La collaborazione si rivela particolarmente preziosa durante le crisi, consentendo di affrontare le sfide in modo più efficace e coordinato. In parallelo, è cruciale adottare un approccio critico e riflessivo agli incidenti, andando oltre il giudizio immediato per comprendere le cause profonde e sviluppare soluzioni sostenibili a lungo termine. Questa riflessione deve includere una valutazione approfondita delle politiche di gestione dei rischi, delle procedure di risposta agli incidenti e delle strategie di resilienza organizzativa.

In sintesi, gli insuccessi non devono essere visti come semplici battute d'arresto, ma come opportunità per rafforzare le difese e migliorare la sicurezza complessiva delle infrastrutture digitali. Un'analisi critica e una collaborazione efficace tra tutte le parti coinvolte sono fondamentali per costruire un ecosistema digitale più robusto e sicuro.

Fonti

https://www.fiercehealthcare.com/health-tech/global-it-outage-takes-down-health-system-ehrs-forces-hospitals-cancel-non-emergency

https://www.euronews.com/travel/2024/07/23/crowdstrike-chaos-why-did-the-global-it-outage-ground-so-many-planes-last-week

https://www.bbc.com/news/articles/c725knvnk5zo

https://www.bloomberg.com/opinion/articles/2024-07-23/crowdstrike-outage-is-another-sharp-warning-for-banks