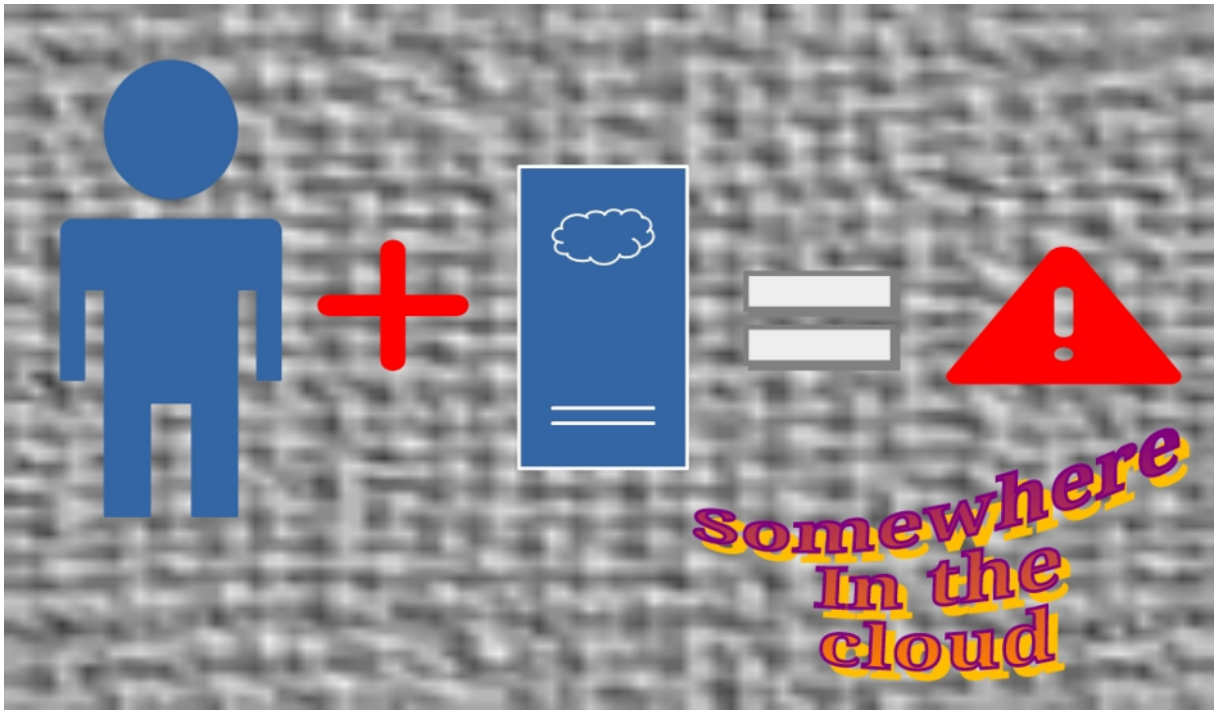
Für mehr Bürgerbeteiligung!
human-dignity

Was geschah am 19. Juli 2024 mit CrowdStrike?

Köln, 28.07.2024



Ganz bestimmt hast du Wind über eine unter der größten IT-Panne weltweit aller Zeiten bekommen. Am 19. Juli wurden Millionen von EDV-Systemen wegen eines Aktualisierungsfehlers in einer Anwendung namens CrowdStrike (Cybersicherheit) lahmgelegt wurden.

Die bekannte und sehr unangenehme Überraschung machte sich mit einem Bluescreen (BSOD) bemerkbar, und zwar als Endlosschleife. Selbst mittels eines Neustarts eines Rechners blieb der Bildschirm blau. Dieser Ausfall traf nur dem Betriebssystem Windows aus dem Haus Microsoft zu. Andere Betriebssysteme wie iOS, Android und Linux blieben verschont.

Microsoft 365 (1) wurde ebenfalls von dieser Panne betroffen. Zahlreiche Flughäfen, Kassensysteme, Tankstellen, Züge und weitere Infrastrukturen streikten. Ein Schaden in Milliardenhöhe ist entstanden. Die Ursachen hängen mit einer fehlerhaften Aktualisierung Cloud-Sicherheitsdaten zusammen, die zu einer Konfigurationsänderung in einem Teil des Azure-Back-End-Workloads (2) führte und auf dieser Weise die Systeme lahmlegte.

Auch im KRITIS-Bereich sind die Systeme ausgefallen. Es sind zwei unterschiedliche Ereignisse, die zufällig bzw. sich überlappend abspielten. Zuerst wurde eine fehlerhafte Aktualisierung der CrowdStrike Anwendung

Verantwortlicher Herausgeber: © Human-dignity - Thierry Vandries
T.: +49 (0) 221 – 550 87 12
Email: info@human-dignity.org
https://www.human-dignity.org

zugespielt, und zweitens eine Konfigurationsänderung von Microsoft in Azure-Systemen führte zu Problemen mit der Cloud (3).

Sofort wurden ebenfalls Verschwörungstheoretiker aktiv und behaupteten, dass dieser Ausfall wohl vorgeplant gewesen sein könnte (4). Als Leiter der Informationssicherheit u.a. bei der Metro Bank meint Ehden Biber, dass eine normale Anwendung – was versteht er bitte unter normal? – so einen Absturz nicht verursachen kann.

Dar bin ich ganz anderer Meinung, denn er vergisst zu erwähnen, dass ein Betriebssystem wie Windows aus 40 Millionen Programmierzeilen besteht. Google Chrome beispielsweise besteht aus 100 Millionen Programmierzeilen. Versuche mal bei solch einem Digitalbauwerk stets eine fehlerfreie Aktualisierung aufzuspielen.

Als EDV-Fachmann kann ich bestätigen, dass jede Anwendung eine Lücke hat. Sonst würden alle Dienstleister aus dem Bereich Cybersicherheit sofort Konkurs anmelden können. Das ist klar, dass wir hier mit einem anderen Fall als mit einer Sicherheitslücke zu tun haben.

Das, was Ehden Biber mit DevOps und SecOps schildert, stimmt mit der Realität überein. Aber, jetzt komme ich zu den ungeprüften „Unterlagen“ bzw. Links im Artikel von TKP. Auf der Website des World Economic Forum wurde ein Artikel über das Unternehmen CrowdStrike aus dem Jahr 2015 veröffentlicht. Inzwischen hat der ehemalige Geschäftsführer Dmitri Alperovitch das Unternehmen verlassen. Er wurde durch George Kurtz ersetzt. Diese Daten wurden auf der Website des World Economic Forum nicht aktualisiert.

Ebenfalls betreibt Ehden Biber einen Blog und die veröffentlichen Artikel kommen mir vor, wie aus dem Kopf eines improvisierten Wissenschaftlers verfasst. Deshalb ist Vorsicht bei diesem Verfasser geboten.

Es kann zwar die Rede eines großen Ausfalls sein, jedoch aber nicht von einem unter den größten EDV-Pannen aller Zeiten, weil „nur“ 8,5 Millionen Windows-Systeme von diesem Ausfall weltweit betroffen wurden. Das entspricht weniger als ein Prozent aller laufenden Windows-Geräte (5). Deshalb bleibt die Spekulation mit einem geplanten Ausfall, eine Spekulation und nichts anderes.

Erinnerst du dich noch als die Schadanwendung Sasser (6)
Rechner automatisch herunter- und hochfahren ließ? Weltweit wurden Millionen Rechner von dieser Schadanwendung betroffen. Mein Rechner war auch betroffen, konnte aber unmittelbar wieder einwandfrei am Laufen gebracht werden, als ich im Pfad Windows\System32 die *.exe-Datei entfernt hatte.

Im Fall CrowdStrike sind alle möglichen Spekulationen über einen geplanten Ausfall unwahr, solang dieser sich nicht eindeutig mit einem manipulierten Programmiercode belegen lässt. Und das genau liefert uns Ehden Biber nicht.

Wachsam sollte man stets bleiben, aber in diesem Fall handelt es sich eindeutig um einen menschlichen Fehler. Daraus lernt man, und findet Lösung, die diesen Fehler beseitigt. Immerhin der durch CrowdStrike verursachte Ausfall von Windows-Systemen kostet allein den US Fortune 500-Unternehmen 5,4 Milliarden US-Dollar. Laut der Versicherer Parametrix sind die größten Geschädigten: Fluggesellschaften, Banken und Gesundheitsunternehmen. Der Schaden für weitere Opfer, die nicht zu Windows-Systemen gehören, werden zwischen 540 Millionen und 1,08 Milliarden Dollar geschätzt (7). Beispielsweise in Deutschland sind beim Uniklinikum Schleswig-Holstein aufgrund des CrowdStrike-Ausfalles 9.000 Systemen betroffen gewesen.

Bis die Schuldzuweisung geklärt sein wird, kann das noch Jahre dauern. In diesem Fall könnte dieser Ausfall für kleine und mittelständische Unternehmen die Konkursanmeldung bedeuten.

Quellen

(1) Günter Born, Ausfall von Microsoft 365 und weltweite Störungen – wegen CrowdStrike-Update, was zum BSOD führt? https://www.borncity.com/blog/2024/07/19/ausfall-von-microsoft-365-und-weltweite-strungen/

(2) Günter Born, Weltweiter Ausfall von Microsoft 365 (19. Juli 2024) https://www.borncity.com/blog/2024/07/19/weltweiter-ausfall-von-microsoft-365-19-juli-2024/

(3) Güter Born, Wieso weltweit zahlreiche IT-Systeme durch zwei Fehler am 19. Juli 2024 ausfielen https://www.borncity.com/blog/2024/07/19/wieso-weltweit-zahlreiche-it-systeme-durch-zwei-fehler-am-19-juli-2024-ausfielen/

(4) Dr. Peter F. Mayer Wurde der CrowdStrike Windows-Computer-Crash absichtlich verursacht? https://tkp.at/2024/07/21/wurde-der-crowdstrike-windows-computer-crash-absichtlich-verursacht/

(5) Andreas Frischholz, Microsoft-Schätzung: 8,5 Millionen Windows-Systeme von Crowdstrike betroffen https://www.computerbase.de/2024-07/microsoft-schaetzung-rund-8-5-millionen-windows-systeme-von-crowdstrike-betroffen/

(6) Microsoft, Win32/Sasser https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=Win32/Sasser

(7) Günter Born, CrowdStrike: Untersuchungsbericht; Schadenssumme und Entschädigungen; Schuldzuweisungen https://www.borncity.com/blog/2024/07/25/crowdstrike-untersuchungsbericht-schadenssumme-und-entschdigungen-schuldzuweisungen-und-mehr/