Microsoft-CrowdStrike outage

làm thế nào một bản cập nhật phần mềm duy nhất có thể gây ra sự hỗn loạn CNTT trên toàn cầu (19/7)

Phùng Lí Trưởng khoa Quản lý thông tin, Phó khoa Nghiên cứu và Đổi mới, Trường Kinh doanh Bayes, Thành phố, Đại học London

The Conversation (22/07/24)

Multiple blue screens of death, caused by an update pushed by CrowdStrike, on airport luggage conveyer belts at LaGuardia Airport, New York City

Thế giới như chúng ta biết ngày càng phụ thuộc vào kết nối kỹ thuật số, phần lớn, hoạt động lặng lẽ và vô hình trong nền. Vậy làm thế nào mà một bản cập nhật phần mềm duy nhất lại làm sập một nửa internet?

Sự cố ngừng hoạt động CNTT toàn cầu vào ngày 19 tháng 7 là lời nhắc nhở nghiêm khắc về sự dễ bị tổn thương của chúng ta trước các lỗi công nghệ. Được kích hoạt bởi một bản cập nhật phần mềm lỗi duy nhất do công ty an ninh mạng CrowdStrike cung cấp, điều này đã có tác động tai hại đến với các hãng hàng không, phương tiện truyền thông, ngân hàng và nhà bán lẻ trên toàn thế giới, đặc biệt là các doanh nghiệp sử dụng hệ điều hành Microsoft Windows.

Sự cố này, được mô tả là "sự cố CNTT lớn nhất trong lịch sử" , nhắc nhở chúng ta về mạng lưới kết nối CNTT rộng lớn duy trì cơ sở hạ tầng kỹ thuật số của chúng ta - và về khả năng gây ra hậu quả sâu rộng khi nó xảy ra.

Những gì bắt đầu với sự chậm trễ tại các sân bay đã làm các chuyến bay bị hủy trên diện rộng. Sự gián đoạn trong hệ thống hàng không không chỉ làm gián đoạn lịch trình chuyến bay mà còn ảnh hưởng đến chuỗi cung ứng toàn cầu phụ thuộc vào vận chuyển hàng không, thể hiện bản chất đa diện của hệ sinh thái CNTT hiện đại. Trong khi đó, các chương trình phát sóng bị gián đoạn tại nhiều đài truyền hình, đài phát thanh, ngân hàng và hoạt động tại các siêu thị bị đình trệ.

Phân tích sơ bộ cho thấy sự hỗn loạn bắt nguồn từ bản cập nhật phần mềm từ phần mềm bảo mật Falcon Sensor của CrowdStrike được áp dụng cho hệ điều hành Microsoft Windows. Nhân viên tại các công ty sử dụng CrowdStrike đã gặp phải "màn hình xanh chết chóc" (“blue screen of death - a screen with an error message indicating a systems crash. Màn hình có thông báo lỗi cho biết hệ thống bị sập) khi họ cố gắng đăng nhập.

Ngoài việc phơi bày mạng lưới phụ thuộc ẩn duy trì xã hội và nền kinh tế kỹ thuật số của chúng ta, sự cố ngừng hoạt động cũng làm nổi bật các chiều hướng địa chính trị của những sự phụ thuộc này. Các quốc gia có mối quan hệ chặt chẽ với Microsoft và CrowdStrike cảm thấy gánh nặng của tác động, nhưng các doanh nghiệp ở các quốc gia như Trung Quốc, với cơ sở hạ tầng CNTT được kiểm soát và tương đối biệt lập, dường như ít bị ảnh hưởng hơn.

Với căng thẳng địa chính trị gia tăng trong những năm gần đây, Trung Quốc và ngày càng nhiều quốc gia khác đã tích cực phát triển các biện pháp an ninh mạng và cơ sở hạ tầng kỹ thuật số của riêng mình, điều này có thể đã giảm thiểu tác động của sự cố này.

Việc Trung Quốc tập trung vào việc sử dụng công nghệ bản địa và giảm sự phụ thuộc vào công nghệ nước ngoài cũng có thể góp phần làm giảm tác động đến hệ thống của họ. Sự cố này là lời nhắc nhở nghiêm khắc rằng sự phụ thuộc vào công nghệ có thể chuyển thành lỗ hổng địa chính trị, với các cơ quan nhà nước ngày càng cần phải xem xét không chỉ các tác động kinh tế mà còn cả các tác động chiến lược và địa chính trị của các liên minh CNTT của họ.

Phục hồi và ý nghĩa

Cách các ngành bị ảnh hưởng đã quản lý cuộc khủng hoảng này phản ánh cả sức mạnh và điểm yếu của các chiến lược bảo mật và phục hồi sau thảm họa của riêng họ. Vấn đề chính đã được xác định và báo cáo là đã được khắc phục. Quá trình phục hồi chậm chạp sắp tới sẽ cho thấy những thách thức đáng kể trong việc khôi phục tính liên tục của dịch vụ trong các hệ sinh thái kỹ thuật số phức tạp, được kết nối sâu với nhau của chúng ta.

Điều đặc biệt đáng ngạc nhiên là mặc dù đã có nhiều bài học trong quá khứ, như thảm họa di chuyển CNTT TSB năm 2018 ảnh hưởng đến hàng triệu khách hàng của ngân hàng Anh, nhưng việc triển khai phần mềm theo từng giai đoạn lại không được áp dụng.

Việc thiếu bước này, một chiến lược cơ bản nhưng quan trọng trong quản lý CNTT, đã phơi bày sự mong manh của các hệ thống mà nhiều người cho là mạnh mẽ. Nó cũng đặt ra những câu hỏi nghiêm túc về khả năng phục hồi của cả hệ điều hành Windows và các biện pháp an ninh mạng của CrowdStrike được cho là để bảo vệ chúng.

Ngoài ra, tập phim còn nêu bật những rủi ro chiến lược khi dựa vào một nguồn công nghệ duy nhất. Sự cố ngừng hoạt động cầu này cho thấy tầm quan trọng của việc có nhiều liên minh công nghệ khác nhau để tăng cường an ninh quốc gia và ổn định kinh tế, đồng thời làm dấy lên mối lo ngại về khả năng các quốc gia thù địch khai thác những lỗ hổng như vậy. Vụ việc này sẽ bổ sung thêm một lớp cấp bách mới vào các hoạt động hợp tác an ninh mạng quốc tế và các can thiệp chính sách.

Khi các dịch vụ bắt đầu ổn định và hoạt động trở lại, sự cố ngừng hoạt động này sẽ là lời cảnh tỉnh cho các chuyên gia CNTT, lãnh đạo doanh nghiệp và các nhà hoạch định chính sách. Nhu cầu cấp thiết phải đánh giá lại và thậm chí là đại tu các chiến lược an ninh

mạng hiện có và các hoạt động quản lý CNTT là rõ ràng. Cải thiện khả năng phục hồi của hệ thống để chống lại sự gián đoạn quy mô lớn phải là ưu tiên hàng đầu.

Sự cố ngừng hoạt động CNTT toàn cầu là lời nhắc nhở kịp thời và là thời điểm quan trọng cho các cuộc thảo luận về khả năng phục hồi kỹ thuật số và tương lai của quản trị công nghệ ở cấp độ doanh nghiệp, cơ sở hạ tầng và chính sách.

Còn AI thì sao?

Một điều khác mà chúng ta vẫn chưa biết câu trả lời là: nếu một lỗi phần mềm duy nhất có thể đánh sập các hãng hàng không, ngân hàng, nhà bán lẻ, cơ quan truyền thông và nhiều đơn vị khác trên toàn thế giới, thì liệu hệ thống của chúng ta đã sẵn sàng cho AI chưa?

Có lẽ chúng ta cần đầu tư nhiều hơn vào việc cải thiện độ tin cậy và phương pháp luận của phần mềm, thay vì vội vã tung ra các chatbot. Một ngành công nghiệp AI không được quản lý sẽ là công thức cho thảm họa, đặc biệt là trong một thế giới có căng thẳng địa chính trị ngày càng gia tăng.

Mặc dù việc áp dụng các công nghệ mới nổi như AI hoặc blockchain là điều cần thiết, chúng ta cũng phải nắm vững những điều cơ bản. Các nhà điều hành an ninh mạng cần đảm bảo rằng các hoạt động quản lý và bảo trì CNTT cơ bản là mạnh mẽ và đáng tin cậy, đồng thời có thể xử lý mọi thứ từ cuộc tấn công an ninh mạng đến bản cập nhật phần mềm đơn giản.

Những bài học rút ra từ sự cố này chắc chắn sẽ ảnh hưởng đến các chiến lược tương lai trong phát triển cơ sở hạ tầng CNTT và quản lý khủng hoảng.

Related Subjects:

- CrowdStrike Holdings, Inc. is an American cybersecurity technology company based in Austin, Texas. It provides cloud workload protection and endpoint security, threat intelligence, and cyberattack response services.

- On July 19, 2024, CrowdStrike released a software update to the vulnerability scanner Falcon Sensor. Flaws in the update caused blue screens of death on Microsoft Windows machines, disrupting millions of Windows computers worldwide. Affected machines were forced into a bootloop, making them unusable. This was caused by an update to a configuration file, Channel File 291, which CrowdStrike says triggered a logic error and caused the operating system to crash. The downtime caused a widespread global impact, grounding commercial airline flights, temporarily taking Sky News and other broadcasters offline, and disrupting banking and healthcare services as well as 911 emergency call centres (Vào ngày 19 tháng 7 năm 2024, CrowdStrike đã phát hành bản cập nhật phần mềm cho máy quét lỗ hổng Falcon Sensor. Các lỗi trong bản cập nhật đã gây ra 'blue screen of death' trên các máy tính Microsoft Windows , làm gián đoạn hàng triệu máy tính Windows trên toàn thế giới).

> A bootloop is a problem that occurs on computing devices when they repeatedly fail to complete the booting process and restart before the sequence is finished, preventing the user from accessing the regular interface.