EUROPEAN-NEWS-AGENCY.COM

EUROPEAN NEWS AGENCY

International Press Service

Ressort: Special interest

Weltweiter IT Ausfall ? Hintergründe Aufklärung 07/24

Welt, 20.07.2024 [ENA]

Wer bisher geglaubt hat, das IT – Computersysteme von Behörden, Wirtschaft und Infrastruktur voneinander unabhängig funktionieren und deshalb keine nationale oder gar globale Störung passieren kann, der wurde gestern eines besseren belehrt. Der große Stillstand der Welt - IT.

Ja was haben wir da vorgestern erlebt- im frühen Morgen fallen plötzlich erste Computer aus, bis sich in den folgenden Stunden wie ein Domino auf der ganzen Welt verbreitet. Computersysteme fallen eigentlich nicht aus, sondern es erscheint ein blauer Fehlerbildschirm, der einen erforderlichen Neustart ankündigt. Dieser entwickelt sich dann als Bootschleife und der Rechner kommt nicht wieder zu einem Ergebnis. Was viele zu diesem Zeitpunkt noch nicht wissen: Teilweise werden erhebliche Systemeingriffe erforderlich werden, um das System wieder funktionsfähig zu machen. Was auf den ersten Blick wie ein böser Virus, Trojaner oder womöglich ein Hacking aussieht, erweist sich erst einmal als ein Update.

Fehler einer Softwarefirma aus Texas mit Sitz in Austin. Die Firma Crowdstrike, die offensichtlich mit Ihrer Sicherheitssoftware Crowd Strike Falcon ein „ defektes „ Update weltweit gestreut hat, wurde 2011 gegründet, hat derzeit etwas über 7900 Mitarbeiter und macht einen Umsatz von über 3 Milliarden US – Dollar. Das Unternehmen ist börsennotiert und natürlich hat die Aktie deutlich reagiert und sauste von rund 315 Euro auf zwischenzeitlich 252 Euro in den Keller, inzwischen hat sie sich wieder bei 275 – 280 Euro stabilisiert.

Das mit der Aktie wird aber kaum jemanden in den betroffenen Institutionen interessieren, denn es traten daraufhin massive ernst zu nehmende Probleme auf: Krankenhäuser konnten keine OPs und wichtige Behandlungen nicht mehr durchführen, weil der Zugriff auf Patientendaten nicht mehr funktionierte. Tegut musste stundenlang wegen nicht funktionierender Kassen die Filialen schließen. Auf diversen Flughäfen wurde für Stunden der Flugbetrieb eingestellt, denn die Anmelde- und Boardingcomputer fielen mal eben aus. PC – Systeme von Privatpersonen waren eher nicht betroffen, denn diese Software richtet sich an Unternehmen, aber auch Privatpersonen wurden letztlich Opfer der IT – Abstürze.

Denn auch bei Geldautomaten gab es einige Zeit keine Kohle mehr, in Apotheken gab es Probleme bei der Ausgabe von Medikamenten, die auf E – Rezept verordnet wurden. Aber auch Stadtverwaltungen, Energieversorger, Betriebe, die sich um Trinkwasser, Abwasser und Telekommunikation kümmern, hatten ernsthafte Probleme. Und eines ist in dieser Situation doch immer klar: Viele Firmen melden sich nicht,

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

probieren, mit ihren Systemadministratoren oder einem Zentralserver die Probleme selbst zu beheben. Zumal ja erstmal gar keiner wußte zu Beginn, welche Problematik eigentlich den Rechnerabsturz verursacht haben könnte.

Dann meldete sich auch die BSI Präsidentin Plattner zu Wort und gab eine knapp 5 Minuten lange Pressemitteilung zu der Lage und dazu, was passiert sei. Und wieder die Rede von der Firma Crowdstrike. Aber längst hatte sich auch Microsoft zu Wort gemeldet und, Nanu, ein Problem mit der Cloud Azure gemeldet, die irgendwie auch in den Absturz diverser Rechner verstrickt sein sollte. Auf der Internetseite von Microsoft dann umfangreiche Lösungsvorschläge, die schon einige Kenntnisse im IT – Bereich erforderlich machten. Zwischenzeitlich meldete sich dann auch der Chef von Crowdstrike, es wäre ein neues korrigiertes Update verfügbar zum Download. Alles toll, aber wie ein Update runterladen wenn der Rechner nicht gestartet werden kann ?

Dafür gab es bei Microsoft den Hinweis, man solle doch den Windows – Rechner (MAC war nicht betroffen) im abgesicherten Modus aufrufen, eine bestimmte Datei im System suchen und die dann manuell löschen, dann würde beim nächsten Start sozusagen wieder aktualisiert. Aber was so leicht klang, erwies sich bei einigen Systemen als Problem. Diese Datei konnte nicht bei allen Systemen wegen Zugriffsverweigerung gelöscht werden, bei anderen war durch eine Bitlocker – Verschlüsselung der Recovery Key notwendig. Doch woher sollte man den bekommen, wenn man ihn Jahre nicht gebraucht hat, wo ist der abgeheftet oder wer in einer Firmenzentrale hat Zugriff darauf ?

Alles schwierig, so daß selbst am Abend nicht alles Systeme komplett nutzbar waren, jedoch ein Großteil. Wer noch Hilfe braucht, kann diese auf der Webseite von Crowdstrike bekommen: https://tinyurl.com/2994tcpc. Auch Microsoft bietet Lösungsmöglichkeiten in Sachen Azure hier an: https://azure.status.microsoft/en-gb/status. Die Webseite des BSI empfehle ich hier nicht, denn ich fand das Pressebriefing wenig informativ, abgelesen von der Präsidentin Plattner, allgemeine Infos, die schon längst in den Medien verbreitet waren. Auch der Hinweis, das das Problem nicht innerhalb von Stunden gelöst werden könnte, nanu, der Chef von Crowdstrike hatte doch längst das Update bereitgestellt.

Ich möchte an die Aktivitäten des BSI zu Beginn des Russlandkrieges 2022 erinnern, wo plötzlich ohne Belege und Hintergrundwissen einfach mal die am besten getestete Antiviren-/Antispam-/Antitrojaner-/Firewall Softwarepakete von Kaspersky als nicht mehr sicher eingestuft worden sind, einfach weil da russische Entwickler dahinter steckten. Wie gesagt, es gab nie Anhaltspunkte und Belege dafür, die Software ist natürlich weiterhin frei verkäuflich und nutzbar. Einzig und allein hatte sich damals wegen der Warnung z. B. Stiftung Warentest geweigert, die Software in einem Test zu bewerten. Das hatte hohe Wellen geschlagen und auch Kaspersky hatte sich dazu geäußert.

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

DESHALB halte ich persönlich nicht viel vom BSI. Und das ist freie Meinungsäusserung. Muß man ja heute immer wieder sagen. Komischerweise wird das Problem von Beginn an auf das Update von Crowdstrike zurückgeführt, die ja auch die Verantwortung dafür übernehmen. Welche Rolle dabei Microsoft mit der Cloud Entwicklung Azure hat, ist mir bis heute nicht klar geworden, komisch, das beide Firmen sozusagen gleichzeitig Probleme bekunden, oder greift die Software von Crowdstrike auf Azure zu ? Darüber keine Info. Aber alle 3, die beiden Unternehmen und auch das BSI, werden nicht schlapp immer wieder zu wiederholen: Nein, es gab keinen Cyber- oder Hackerangriff. Aber über das Mircosoft Problem keine Info beim BSI. Warum nicht ?

Ich bin da skeptisch: Wie kann es sein, das eine Software so massiv in das Windows – System eingreift, gleich den Rechner lahmzulegen. Und ich frage mich überhaupt, wie das passieren konnte. Wird ein Update nicht mehrfach geprüft und auch auf Windows – Rechnern installiert wegen der Lauffähigkeit ? Ist doch komisch das das keinem aufgefallen ist. Ein Update, was so massive Auswirkungen hat. Wie gesagt, auf der Microsoft – Seite kann man alle Länder sehen, die betroffen sind, das sind eine lange Liste. Und da frage ich mich, nirgends eine Nachricht, das ein AKW betroffen ist oder Waffensysteme.

Wenn das doch eine so tolle Sicherheitssoftware ist die weltweit auf Hunderten von Millionen Rechnern installiert ist, dann haben die ausgerechnet die wichtigsten System nicht ? Glaube das, wer will. Ich glaube eher, wir werden natürlich nicht komplett informiert, wie das inzwischen Gang und Gebe ist. Denn das sorgt ja für Beunruhigung unter den Bürgern und zeigt, wie anfällig wir sind. Und wenn das mit einem kleinen Update geht und das mal Hacker ausnutzen: Wie schnell kann die halbe Welt IT – technisch lahmgelegt werden ? Zu dem Thema kein Hacking, kein Cyberangriff habe ich noch eine interessante Info. Denn gerade in Sachen Azur Cloud hat letztes Jahr Microsoft einen herben Schlag erhalten.

Denn chinesische Hacker sollen einen Master Key der Azure Cloud in ihren Besitz gebracht haben und den gegen einige Regierungsbehörden eingesetzt haben. Der Angriff wurde dabei nicht etwa von Microsoft entdeckt, nein, ein Kunde, der die Cloud damals nutzte, entdeckte das. Inzwischen ist der Fall untersucht und von der CISA, der Cybersecurity and Infrastructure Security Agency in den USA ein abschliessender Bericht vorgelegt, bei dem Microsoft nicht besonders gut wegkommt. Zum einen haben Fehler in der Cloud Entwicklung diesen Angriff erst möglich gemacht, zudem bescheinigte die Firma hohe Defizite in der Cybersicherheit und mahnte vor einer Weiterentwicklung erst einmal deutliche Sicherheitsverbesserungen an.

Angeblich habe Microsoft nach dem Vorwurf aus dem September 2023 erst im März 2024 reagiert mit einer Verbesserung. Im übrigen haben sich natürlich schon einige IT – Experten zu dem Vorfall gemeldet und einige wundern sich doch darüber, das nicht nur die APP, sondern gleich der ganze Rechner lahmgelegt wird. Aber die Begründung liegt auf der Hand: Sicherheitssoftware greift immer mehr ins gesamte

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com

Windows – Kernsystem ein um umfassend zu schützen. Doch dadurch werden eben die Rechner anfälliger und schwerer geschädigt durch Manipulationen oder fehlerhaften Änderungen, wenn diese Apps betroffen sind.

Im übrigen habe ich auch keine Info gelesen und gehört, ob es irgendein Windows – System gibt, das nicht betroffen ist. Und wer für die entstandenen Schäden aufkommt, wird sich noch zeigen, denn der geht weltweit auf 9-stellig, also über 100 Millionen Euro.

Bericht online lesen:
https://www.european-news-agency.de/special_interest/weltweiter_it_ausfall__hintergruende_aufklaerung_07_24-89459/

Redaktion und Verantwortlichkeit:
V.i.S.d.P. und gem. § 6 MDStV: Uwe Hildebrandt

Redaktioneller Programmdienst:
European News Agency

Annette-Kolb-Str. 16
D-85055 Ingolstadt
Telefon: +49 (0) 841-951. 99.660
Telefax: +49 (0) 841-951. 99.661
Email: contact@european-news-agency.com
Internet: european-news-agency.com