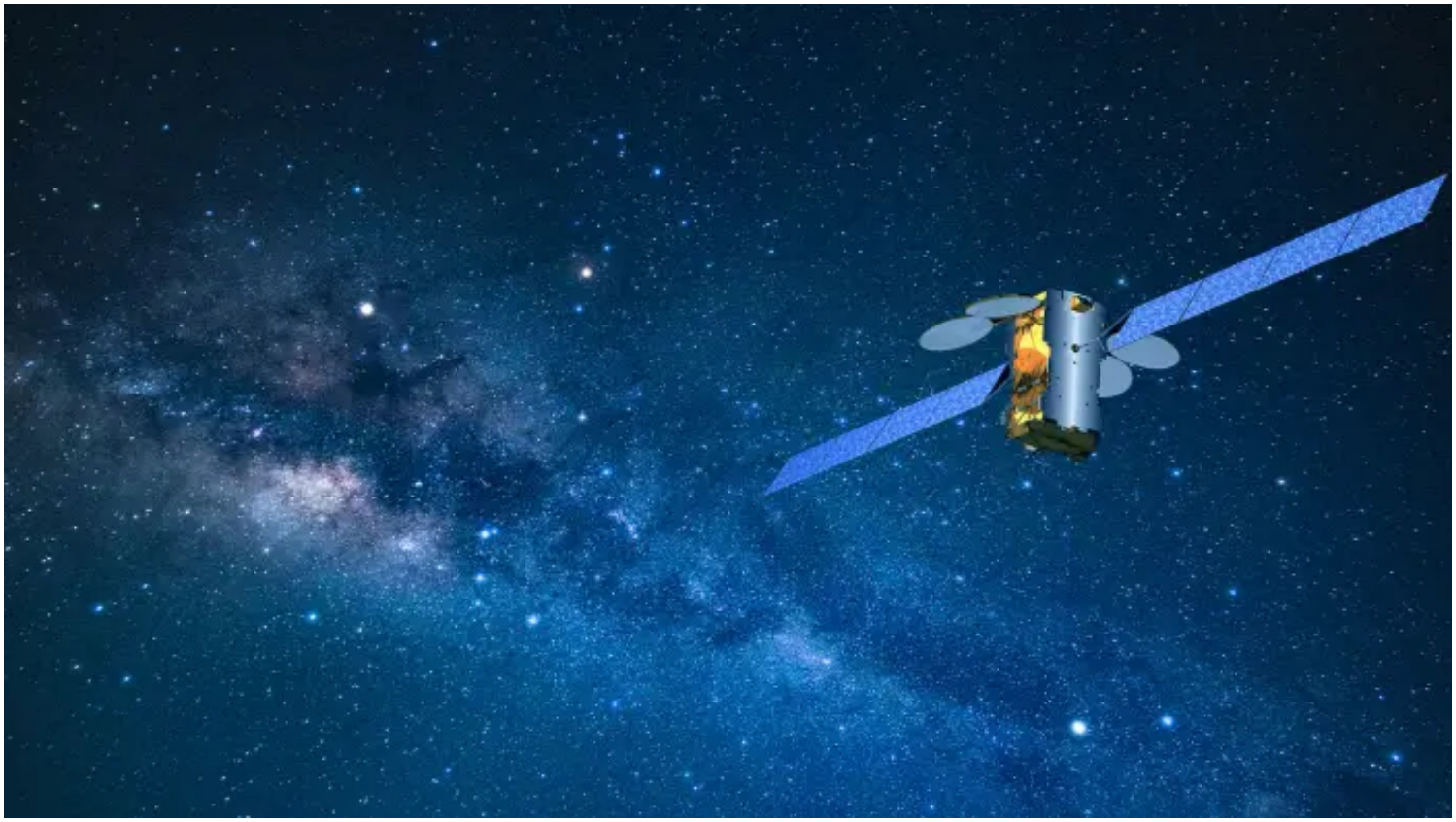
heise online

Angriff auf Satellitennetzwerk KA-Sat: Experten suchen nach dem Ursprung UPDATE

Stand: 09.03.2022 18:58 Uhr Monika Ermert



(Bild: Viasat, Symbolbild)

Mit Beginn der Invasion Russlands in die Ukraine kam es zu Störungen im KA-Sat-Netz. Wie genau der Angriff abgelaufen ist, versuchen Experten zu klären.

Die Störung von tausenden KA-Sat-9a-Terminals in mehreren europäischen Ländern ist laut Expertenmeinungen nur durch einen Angriff auf das zentrale Network Operation Center (NOC) zu erklären. Dass Terminals in verschiedenen Ländern betroffen sind, sei der Organisation des Netzwerkbetriebs zuzuschreiben. Unklar bleiben die unterschiedlichen Schadbilder an verschiedenen Modemklassen und die Ziele des Angriffs, der sich parallel zum Beginn der russischen Invasion in die Ukraine ereignete.

Update 10.3.21, 11.01: Viasat teilt mit, das Unternehmen habe die Untersuchung der Ursachen und Angriffsmethoden abgeschlossen. Seit dem heutigen 10. März könnten Terminals wieder in Betrieb genommen werden. Dabei müssen allerdings durch den Angriff in Mitleidenschaft

gezogene Modems ersetzt werden. Ein zunächst erhofftes Softwareupdate ist demnach nicht möglich, um die seit 24. Februar ausgefallenen Verbindungen wieder in Schwung zu bringen. Nicht abschließend geklärt ist vorerst offenbar, wer die Kosten für die kaputten Modems übernimmt.**]**

KA-Sat versorgt Europa und die Mittelmeerregion mit Satelliteninternet und wird wegen seiner Unabhängigkeit von terrestrischer Infrastruktur auch zur Anbindung von technischen Anlagen in abgelegenen Gebieten genutzt. So wurde **unter anderem der Betrieb tausender Windkraftanlagen eingeschränkt [1]**. Die Windkrafträder liefen zwar noch und erzeugten auch Strom, sie seien aber für eine Überwachung und Steuerung aus der Ferne nicht mehr erreichbar, hieß es Anfang dieses Monats.

Von Betreiber Viasat zunächst als "Cyberereignis" gemeldet, bestätigte das US-Unternehmen inzwischen gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI), dass es sich um einen Angriff gehandelt habe. **Andreas Knopp von der Universität der Bundeswehr München erläutert [2]**, die Unabhängigkeit von terrestrischer Infrastruktur mache das Satelliteninternet derzeit auch in der Ukraine zum wichtigsten Kommunikationsmittel. Einer der 82 "Spot-Beams" von KA-Sat liege über Kiew.

Bis heute gibt es von Viasat keine Entwarnung für Betreiber, die an das Netz angeschlossen sind, bestätigt Bernhard Neumeyer, Geschäftsführer von IPcopter. Das Unternehmen stattet Feuerwehren mit Satellitensystemen für die Notfallkommunikation aus. Sein eigenes Modem Spotbeam 2 Plus funktioniere bei routinemäßigen Tests, das Modem eines betroffenen Kunden zeige dagegen nur schwächelnde LED-Anzeigen.

Weder DDoS noch EM oder Terminal Zero Day

Der spanische Security-Forscher Ruben Santamarta legte als erster eine ausführlichere Hypothese [3] zur Erklärung des seit 24. Februar beobachten Angriffs vor. Er geht nach eigenen Recherchen davon aus, dass das KA-Sat-Netz für alle funktioniert, deren Modem während des Angriffs keinen Schaden genommen hat. Nutzer in Spanien und Portugal waren nach seinen Informationen ohnehin nicht betroffen. Erwischt habe es unter anderem Nutzer in der Ukraine, Deutschland, Griechenland, Ungarn und Italien.

In seiner Analyse kommt Santamarta zu dem Schluss, dass der Angriff auf das Satellitennetzwerk auf eine zentrale Stelle gezielt haben müsse. Letztlich sei nur so die zufällig wirkende Verteilung im Netz des US-Betreibers zu erklären. Eine DDoS-Attacke reiche dabei nicht aus, um tausende oder gar zehntausende defekte oder nur noch zuckende Modems zu erklären. Auch ein elektromagnetischer Impuls sei angesichts der Verteilung sehr

unwahrscheinlich, ebenso die direkte Übernahme der Satcom-Terminals etwa durch Zero-Day-Schwachstellen. Vielmehr bedürfe es der Kontrolle an einem zentralen Gateway oder NOC, um die angeschlossenen Geräte zu kompromittieren, etwa durch Schadcode oder ein manipuliertes Software-Update.

Angriff am zentralen NOC

Die Intelligenz im KA-Sat Netz-ist in einem zentralen NOC konzentriert, erklärt Thomas Lohrey, ehemaliger Mitentwickler des Satelliteninternetzugangs über KA-Sat bei Eutelsat. Über die in Europa verteilten Gateways werden die Terminals gemanagt, die aus Satellitenschüssel und Modem bestehen. Von dort werden regelmäßig Softwareupdates eingespielt. Die Terminals bekommen die Updates nur insoweit mit, als das Modem nach dem automatisch getriggerten Downloads neu bootet.

Ein Angriff über ein Software-Update, wie es Santamarta vermutet, würde bedeuten, dass die Angreifer ihren Schadcode über das NOC verbreitet hätten. Eine Anfrage von heise online an den zuständigen technischen Leiter von Eutelsat in Turin wurde bislang nicht beantwortet. Wie Viasat hält sich auch die fürs NOC zuständige Tochter Eutelsat dazu bedeckt.

Mit der Streubüchse

Dabei könnte letztlich nur der NOC-Betreiber klären, warum lediglich ein Teil des KA-Sat-Netzes betroffen war und welches genau. Wenig ist bekannt, welche Dienste in der Ukraine in Mitleidenschaft gezogen wurden.

Ein gezielter Angriff auf Terminals in nur einem Land ist durch die Struktur des KA-Sat-Netzes kaum möglich. Jedes Gateway ist für zehn Spotbeams zuständig, die Stellen in unterschiedlichen Ländern abdecken. Die Zuordnung der Beams zu den Gateways erfolgt praktisch mit der Streubüchse, heißt es in einer Expertendarstellung.

Die Terminals können ihrerseits auf jeden Fall zwei Gateways nutzen. Ist eines nicht erreichbar, ist ein zweites als Backup vorgesehen. Hätten die Angreifer also ein bestimmtes Gateway für die Zuspielung des bösartigen Softwareupdates ausgewählt, wären Terminals in verschiedenen Ländern betroffen, was sich beim Angriff auch gezeigt hat. Zugleich könnten Modems im "Zielgebiet" des Angriffs durch Zufall auch gerade ihr Backup-Gateway genutzt haben.

Knopp erläutert, "zwar sind die Beams untereinander relativ unabhängig, Störungen wirken sich wechselseitig nicht sofort aus, aber wenn ein Gateway durch einen Cyber-Angriff ausfällt, sind alle damit verbundenen Beams betroffen". So könne es sein, dass die Russen eigentlich die

Internetverbindungen in der Ukraine kappen wollten, aber damit auch die Windanlagen in Zentraleuropa vom Internet getrennt haben, mutmaßt Knopp.

Beschädigte Modems

Ein Angriff über das zentrale NOC wäre ein massiver Vorfall, sagt Lohrey und "dann sind viele Arten von Schäden in den Terminals denkbar". So könnte das Software-Update den Terminals die falsche Frequenzauswahl aufschreiben. Danach finden die Terminals den Satelliten nicht mehr und sind praktisch lahmgelegt.

Möglich wäre auch, dass die neue Software den Modems in die interne Spannungsverwaltung eingreift und etwa durch An- und Ausschalten die empfindlichen Hochfrequenz-Abläufe stören oder den "Alterungsprozess" beschleunigen, sodass die Hardware rasch den Geist aufgibt. Passen würde ein solcher Schaden zu Beobachtungen bei IPcopter, wo Experte Neumeyer von einem Modem spricht, dessen LEDs nur noch zucken.

Was sich aus einem der beschädigten Modems aus Deutschland herauslesen lässt, wird derzeit auch im Heise-Labor untersucht. Über das Schlupfloch, durch das die Angreifer ins NOC gekommen sein könnten, muss Viasat Rechenschaft ablegen. Über das Motiv und die politische Bedeutung dürfen sich Sicherheitspolitiker und Militärs den Kopf zerbrechen.

(**anw [4]**)

URL dieses Artikels:

https://www.heise.de/-6544706

Links in diesem Artikel:

[1] https://www.heise.de/news/Satelliten-Stoerung-Tausende-Windraeder-nicht-steuerbar-6529189.html

[2] https://idw-online.de/de/news789489

[3] https://www.reversemode.com/2022/03/satcom-terminals-under-attack-in-europe.html

[4] mailto:anw@heise.de