

VORFALL - LAGEBILD

Tanker VL Prosperity: Zugriff auf Antriebssteuerung

Stand 19.10.2026 09:59 · Sendung: – · · Belegstärke: **bestätigt** · berichtet · **vermutet** · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

Wissensstand

■ Wissen 44 % ■ Wahrscheinlich 22 % ■ Nicht bekannt 34 %

Boarding, Untersuchung, Fund von Schadaktivität und das Fehlen von Schäden sind durch Küstenwache und FBI belegt (beide Recherchen übereinstimmend). Der Zugriff auf das Antriebssystem stützt sich nur auf anonyme Quellen bei Bloomberg. Für Weg, Täter und tatsächliche Eingriffe gibt es keinen öffentlichen Beleg; alle technischen Details zu Manipulationen stammen aus iranischen Staatsmedien.

1. Was ist passiert, und warum?

WISSEN

- Am 21.08.2026 ging ein Team an Bord: Law Enforcement der Küstenwache, Cyber Protection Team, ein Schiffsinspektor und das FBI Cyber Action Team. Es untersuchte OT- und IT-Systeme und arbeitete mit Crew und Reederei daran, „to eradicate the threat“. (100 %)

[<https://www.cbsnews.com/news/coast-guard-fbi-board-oil-tanker-texas/> ;

<https://www.dragos.com/blog/vl-prosperity-mtsa-maritime-cybersecurity>]

- Laut FBI gab es „indications that the networks of both vessels were compromised“. Die Küstenwache sprach von „foreign cyber actors“, nannte aber keinen Namen. (100 %) [<https://militarytimes.com/news/your-military/2026/09/17/coast-guard-boards-us-bound-vessels-apparently-compromised-by-hackers-officials-say/>]

- Rear Adm. Amy Grable (Coast Guard Cyber Command) sagte CBS, die Ermittler hätten „malicious cyber activity“ an Bord gefunden. Einen Täter nannte sie nicht. Die Angreifer seien „not necessarily that sophisticated“ gewesen, und „basic precautions“ würden die meisten solcher Vorfälle verhindern. (100 %)

[<https://www.cbsnews.com/news/coast-guard-fbi-boarded-energy-tankers-cyberattacks-amy-grable-iran/>]

- Bloomberg berichtete am 02.10.2026 unter Berufung auf US-Beamte, FBI und Küstenwache hätten Belege für einen vorübergehenden Zugriff von außen auf ein digitales System an Bord gefunden, das mit dem Antrieb verbunden ist. Der Text lief am 05.10.2026 bei Insurance Journal. (100 %) [<https://www.insurancejournal.com/news/national/2026/10/05/887853.htm>]

- Am 24.08.2026 wurde ein zweites Schiff im Golf von Mexiko geboardet (widersprüchlich: Dragos und Maritime Executive nennen den LPG-Tanker Kohaku, 227 m / andere Quellen sprechen von einem LNG-Schiff ohne Namen). (100 %)

[<https://www.dragos.com/blog/vl-prosperity-mtsa-maritime-cybersecurity> ;

<https://maritime-executive.com/article/the-vl-prosperity-breach-what-u-s-cybersecurity-rules-already-require> ;

<https://therecord.media/oil-tanker-cyberattack-coast-guard-fbi>]

- Die iranische Agentur Mehr meldete am 20.08. einen „major cyberattack“ beim Passieren der Straße von Gibraltar am 07.08. mit 30 Stunden Kommunikationsausfall. Einen Urheber nannte Mehr nicht. (100 %) [<https://militarytimes.com/news/your-military/2026/09/17/coast-guard-boards-us-bound-vessels-apparently-compromised-by-hackers-officials-say/> ; <https://www.cbsnews.com/news/coast-guard-fbi-board-oil-tanker-texas/>]

NICHT BEKANNT

- Wie die Angreifer ins Bordnetz kamen
- Wer dahintersteckt; es gibt keine offizielle Zuordnung und kein Bekennerschreiben
- Wie lange der Zugriff bestand und welche Funktionen tatsächlich steuerbar waren

- Ob die Vorfälle auf VL Prosperity, dem zweiten Schiff (Kohaku) und der gemeldeten Vivit Africa zusammenhängen oder vom selben Akteur stammen
- Ob es ein Erpressungs- oder ein Sabotagemotiv gab

WAHRSCHEINLICH (Einschätzung)

- Der Zugriff lief aus der Ferne über eine Kommunikationsverbindung des Schiffs (Satellit, Fernwartung, Landanbindung der Reederei) und nicht über eine Person an Bord. (55 %) – Auf See ist der Fernzugriff der typische Weg, und Grables Hinweis auf frei verfügbaren Schadcode und fehlende Grundvorkehrungen passt dazu. Ein vorher eingeschleppter Datenträger oder ein Laptop aus dem Hafen ist aber ebenso denkbar, und die Behörden sagen nichts zum Weg. (A 60 %, B 55 %)
- Hinter dem Angriff steckt ein staatlicher oder staatsnaher Threat Actor. (55 %) – Die Küstenwache spricht von „foreign cyber actors“, es gibt keine bekannte Lösegeldforderung, die USA beobachten fast 20 Schiffe, und der Fall fällt in den Konflikt zwischen den USA und dem Iran. Grable nennt die Angreifer aber nicht besonders ausgefeilt, Hacktivist*innen oder Kriminelle sind nicht ausgeschlossen. (A 55 %, B 60 %)
- Der Täter hat einen Bezug zum Iran. (45 %) – Laut WSJ prüfen die USA eine Verbindung zum Iran oder zu iranfreundlichen Akteuren, und iranische Staatsmedien haben den Fall zuerst gemeldet und propagandistisch genutzt. Offiziell zugeordnet ist nichts, und ehemalige Beamte warnen, dass solche Akteure ihre Fähigkeiten gern übertreiben.
- Die von Mehr gemeldeten Eingriffe (Kühlung gedrosselt, Drehzahl erhöht, Tanks abgeschaltet) haben so stattgefunden. (20 %) – Die einzige Quelle ist ein anonymes Crewmitglied in iranischen Staatsmedien. Bloomberg spricht nur von Zugriff, nicht von Steuerung, FBI und Küstenwache melden keine Betriebsstörung, und laut Grable war das Schiff nie unsicher. (A 25 %, B 20 %)

2. Was ist die Auswirkung?

WISSEN

- FBI: „Currently, there are no reports of operational disruptions, vessel instability, physical danger to crews, or environmental impacts.“ (100 %)

[<https://www.insurancejournal.com/news/national/2026/10/05/887853.htm> ;

<https://www.bairdmaritime.com/security/incidents/piracy/vl-prosperity-hackers-access-propulsion>]

- Laut Grable deutete bei der Inspektion nichts darauf hin, dass der Tanker unsicher zu betreiben war. (100 %) [<https://www.cbsnews.com/news/coast-guard-fbi-boarded-energy-tankers-cyberattacks-amy-grable-iran/> ; <https://www.securityweek.com/cyberattacks-on-two-oil-tankers-prompt-coast-guard-fbi-to-board-vessels/>]
- Laut Bloomberg-Schiffsdaten lag der voll beladene Tanker Anfang Oktober weiter vor Galveston vor Anker. (100 %) [<https://www.insurancejournal.com/news/national/2026/10/05/887853.htm>]
- Das Schiff ist 333 m lang, Baujahr 2015, 319.547 dwt, Flagge Liberia, IMO 9683697, und fasst rund 2,3 Mio. Barrel Rohöl. Gemanagt wird es von HMM Ocean Service (Südkorea). (100 %)

[<https://shipnext.com/vessel/9683697-vl-prosperity> ; <https://www.cbsnews.com/news/coast-guard-fbi-board-oil-tanker-texas/> ; <https://www.dragos.com/blog/vl-prosperity-mtsa-maritime-cybersecurity>]

- Laut Bloomberg (13.10.) war eine Raffinerie im Besitz Saudi-Arabiens Käuferin des Öls an Bord. (100 %)

[<https://bloomberg.com/news/articles/2026-10-13/saudi-owned-refinery-was-buyer-of-oil-on-cyberattacked-tanker>]

- Mehr und ein anonymes Crewmitglied behaupteten Eingriffe in Kühl-, Kraftstoff- und Schmierölsysteme sowie in die Drehzahl und 30 Stunden ohne Funkverbindung; die USA haben das nicht bestätigt. (100 %) [<https://militarytimes.com/news/your-military/2026/09/17/coast-guard-boards-us-bound-vessels-apparently-compromised-by-hackers-officials-say/> ;

<https://maritime-executive.com/article/uscg-and-fbi-investigate-cyberattacks-on-us-bound-tankers>]

NICHT BEKANNT

- Ob der Kommunikationsausfall von 30 Stunden in dieser Länge stattfand
- Warum das Schiff seit Wochen vor Anker liegt: Ermittlungen, Bereinigung oder kommerzielle Gründe
- Ob und wann die Ladung gelöscht wurde

- Wie hoch der wirtschaftliche Schaden für Reederei, Charterer und Käufer ist
- Ob Daten abgefließen sind

WAHRSCHEINLICH (Einschätzung)

- Am Schiff, an der Ladung oder in der Umwelt gab es keinen physischen Schaden. (85 %) – FBI, Küstenwache und Grable sagen das übereinstimmend. Es bleibt ein Restzweifel, weil die Untersuchung nicht abgeschlossen und kein Abschlussbericht veröffentlicht ist.
- Der Hauptschaden liegt bisher bei Liegezeit, Untersuchung und Bereinigung. (75 %) – Es gab ein viertägiges Boarding, das Schiff liegt seit Ende August vor Galveston, ohne dass ein technischer Schaden gemeldet ist, und HMM wartet auf den Abschlussbericht. Beifizierte Zahlen gibt es nicht. (A 75 %, B 80 %)
- Es gab tatsächlich eine längere Kommunikationsstörung an Bord. (75 %) – Neben Mehr berichten auch Bloomberg und Baird Maritime, das Schiff habe die Verbindung verloren. Die Dauer von 30 Stunden stammt nur von Mehr. (A 75 %, B 80 %)
- Der Vorfall verschärft Kontrollen für Schiffe auf dem Weg in die USA. (65 %) – Die Küstenwache verlangt für die fast 20 beobachteten Schiffe eine Vorabmeldung vor dem Einlaufen und hat verschärfte Port State Controls angekündigt. Über neue Versicherungsauflagen gibt es keine Belege.

3. Wie lange dauert es digital (Wiederherstellung IT)?

WISSEN

- Das Boarding-Team blieb ab dem 21.08. vier Tage an Bord, suchte nach Malware und untersuchte IT- und OT-Systeme. (100 %)

[<https://www.cbsnews.com/news/coast-guard-fbi-boarded-energy-tankers-cyberattacks-amy-grable-iran/>]

- Ziel war laut Behörden, „to ensure integrity of the vessel's operational and information technology systems“. Laut gemeinsamer Erklärung half die Crew, „to ensure the threats were mitigated“. (100 %) [<https://therecord.media/oil-tanker-cyberattack-coast-guard-fbi>]
- Der Schiffsmanager HMM Ocean Service bestätigte das Boarding und verwies auf „rigorous cyber protocols“. (100 %) [<https://www.cbsnews.com/news/coast-guard-fbi-board-oil-tanker-texas/>]
- HMM Ocean Service erklärte, die Küstenwache habe das Schiff für den Normalbetrieb freigegeben. Man warte auf einen Abschlussbericht der US-Behörden. (100 %)

[<https://gcaptain.com/us-coast-guard-and-fbi-conduct-cyberattack-probes-on-tankers/>]

NICHT BEKANNT

- Ob die Systeme vollständig bereinigt sind und der Angreifer vollständig entfernt ist; ein Abschlussbericht ist nicht veröffentlicht
- Ob Systeme neu aufgesetzt, Firmware geprüft oder Hardware getauscht wurde
- Warum das Schiff Anfang Oktober noch vor Anker lag und wann es wieder regulär eingesetzt wird

WAHRSCHEINLICH (Einschätzung)

- Die Bereinigung an Bord war nach Tagen bis wenigen Wochen abgeschlossen. Die forensische Aufarbeitung an Land dauert Monate, und die lange Liegezeit hat zusätzlich forensische, rechtliche oder kommerzielle Gründe. (55 %) – Das passt zu vier Tagen Boarding, einer überschaubaren Schiffs-IT und der von HMM gemeldeten Freigabe. Bei OT-Forensik mit Herstellerbeteiligung sind Monate üblich. Eine offizielle Erklärung für die Liegezeit gibt es nicht. (A 65 %, B 55 %)
- Auch Schwesterschiffe und die Landorganisation des Managers wurden überprüft. (50 %) – Das ist übliche Incident Response bei geteilten Zugängen und Fernwartung. Öffentlich gibt es dazu nichts.

4. Ist in der Anlage etwas kaputt, das lange dauert?

WISSEN

- FBI und Küstenwache melden keine Betriebsstörung und keine Instabilität des Schiffs. (100 %)

[<https://www.insurancejournal.com/news/national/2026/10/05/887853.htm> ;

<https://www.bairdmaritime.com/security/incidents/piracy/vl-prosperity-hackers-access-propulsion>

- Die Behauptungen über Eingriffe in Kühl-, Kraftstoff- und Schmierölsysteme stammen aus iranischen Staatsmedien und einem anonymen Crewmitglied. Bestätigt sind sie nicht. (100 %)

[<https://maritime-executive.com/article/uscg-and-fbi-investigate-cyberattacks-on-us-bound-tankers>]

- Der ehemalige Küstenwachen-Cyberexperte Quinton DuBose hält eine komplette Fernübernahme eines Supertankers für unwahrscheinlich, das Stören einzelner Teilsysteme aber für sicherheitsrelevant. (100 %)

[<https://www.cbsnews.com/news/coast-guard-fbi-boarded-energy-tankers-cyberattacks-amy-grable-iran/>]

NICHT BEKANNT

- Ob Steuerungen, Firmware oder Konfigurationen verändert wurden
- Ob mechanische Komponenten (Motor, Pumpen) belastet, geprüft oder getauscht wurden
- Welche Automationskomponenten an Bord verbaut sind

WAHRSCHEINLICH (Einschätzung)

- An der Hauptmaschine oder ihren Hilfssystemen ist kein Schaden entstanden, der eine lange Reparatur oder Werftzeit nötig macht. (75 %) – Es gibt eine Freigabe für den Normalbetrieb, keinen Hinweis der Behörden auf technische Schäden oder einen Werftaufenthalt, und laut Grable war das Schiff nie unsicher. Die gemeldeten Eingriffe in Motorparameter sind unbestätigt. (A 80 %, B 75 %)

- Steuerungskomponenten werden vorsorglich geprüft oder neu aufgespielt. (45 %) – Das ist bei OT-Kompromittierung üblich, über diesen Fall ist dazu nichts veröffentlicht.

5. Wie viele solcher Ziele gibt es?

WISSEN

- Laut Bloomberg beobachteten US-Behörden bis September Cyber-Bedrohungen gegen „nearly 20 shipping vessels around the world“. Die Küstenwache verlangt vor deren Einlaufen in US-Häfen eine Vorabmeldung. (100 %)

[<https://www.insurancejournal.com/news/national/2026/10/05/887853.htm>]

- Neben der VL Prosperity wurde am 24.08. ein zweites Schiff im Golf von Mexiko geboardet. (100 %) [<https://therecord.media/oil-tanker-cyberattack-coast-guard-fbi> ;

<https://maritime-executive.com/article/the-vl-prosperity-breach-what-u-s-cybersecurity-rules-already-require>]

- Das Cyber Protection Team der Küstenwache hatte laut Grable im vergangenen Jahr rund 40 bis 50 Einsätze. (100 %)

[<https://www.cbsnews.com/news/coast-guard-fbi-boarded-energy-tankers-cyberattacks-amy-grable-iran/>]

- Laut Grable laufen jährlich Waren im Wert von 5,4 Billionen US-Dollar durch US-Häfen. (100 %)

[<https://www.cbsnews.com/news/coast-guard-fbi-boarded-energy-tankers-cyberattacks-amy-grable-iran/>]

- Shodan (aggregiert): OT-Protokolle öffentlich erreichbar in Deutschland: 143472 gesamt (DNP3 33617, OMRON FINS 23242, ProConOS 16553, EtherNet/IP 15911, Siemens S7 8154, OPC UA 5644) (100 %)

NICHT BEKANNT

- Welche Schiffe auf der Liste mit fast 20 Schiffen stehen und warum
- Ob es weitere bestätigte Zugriffe auf Antriebs- oder Maschinensysteme gibt; der dritte gemeldete Fall (LNG-Tanker Vivit Africa) stützt sich bisher nur auf Crew-Aussagen ohne offizielle Bestätigung

WAHRSCHEINLICH (Einschätzung)

- Ein großer Teil der weltweiten Handelsflotte nutzt Satelliten-Internet, Fernwartung und vernetzte Maschinenraum-Technik, die zu einer vergleichbaren Angriffsfläche führen. (70 %) – Breitband auf See ist Standard. Laut Küstenwache-Alert von 2019 fuhr ein Frachter ohne wirksame Cybersecurity-Maßnahmen, und die IACS-Vorgaben E26/E27 gelten nur für Neubauten mit Vertrag ab Juli 2024, die Bestandsflotte ist älter. (A 75 %, B 70 %)

6. Kann das wieder passieren?

WISSEN

- Grable: „Just taking basic precautions would prevent most of these occurrences.“ Die Hürde, Maschinen an Bord zu manipulieren, sei niedriger als gedacht, Schadcode sei verfügbar und KI beschleunige die Bedrohung. Auf die Frage nach Hijacking sagte sie: „yes, it is a concern.“ (100 %) [<https://www.cbsnews.com/news/coast-guard-fbi-boarded-energy-tankers-cyberattacks-amy-grable-iran/>]

- Dryad-Global-CEO Corey Ranslem: „We are expecting these types of attacks to continue and will expand in the very near future.“ (100 %) [<https://militarytimes.com/news/your-military/2026/09/17/coast-guard-boards-us-bound-vessels-apparently-compromised-by-hackers-officials-say/>]

- Ausländische Schiffe müssen in den USA einen Cybervorfall als „hazardous condition“ melden (33 CFR 160.202). Die US-Cyberregel nach MTSA gilt seit 16.07.2025 (Meldepflicht); US-geflaggte Schiffe brauchen bis 16.07.2027 Cybersecurity Officer, Assessment und Plan. Bei ausländischen Schiffen will die Küstenwache laut Dragos die Port State Control zur Cybersecurity verschärfen. (100 %) [<https://maritime-executive.com/article/the-vl-prosperity-breach-what-u-s-cybersecurity-rules-already-require> ; <https://www.dragos.com/blog/vl-prosperity-mtsa-maritime-cybersecurity>]

NICHT BEKANNT

- Ob die Einfallstür bei VL Prosperity bekannt und geschlossen ist
- Ob der Angreifer weitere Zugänge in der Flotte oder an Land hat
- Ob dieselbe Lücke bei anderen Schiffen derselben Reederei oder Bauart besteht

WAHRSCHEINLICH (Einschätzung)

- In den nächsten Monaten werden weitere Cybervorfälle auf Handelsschiffen öffentlich. (75 %) – Die geopolitische Lage ist angespannt, der Konflikt dauert an, fast 20 Schiffe werden beobachtet, und durch die neuen Meldepflichten kommt mehr ans Licht.

Lage

Am 21.08.2026 ging ein Team aus US-Küstenwache und FBI an Bord des Rohöltankers VL Prosperity (VLCC, Liberia-Flagge, unterwegs von Sidi Kerir in Ägypten nach Galveston), weil es Hinweise auf kompromittierte Netze gab. Die Küstenwache bestätigt „malicious cyber activity“. Laut Bloomberg (02.10.2026, anonyme US-Beamte) hatten Unbefugte vorübergehend Zugriff auf ein digitales System, das mit dem Antrieb verbunden ist. Wie die Angreifer hineinkamen, was sie steuern konnten und wer dahintersteckt, ist offiziell weiter offen. Offiziell gibt es weder Betriebsstörungen noch Gefahr für die Crew oder Umweltschäden; die Angaben zu Eingriffen in Kühlung, Drehzahl und Treibstoff stammen nur aus iranischen Staatsmedien und sind nicht bestätigt.

Täter

unbekannt – unbekannt

Früherer Stand: Erstmeldung (05.10.2026 09:44)

Wissen 48 % · wahrscheinlich 20 % · nicht bekannt 32 %

US-Küstenwache und FBI sind am 21.08.2026 an Bord des Rohöltankers VL Prosperity gegangen, weil es Hinweise gab, dass „foreign cyber actors“ die Schiffsnetze kompromittiert hatten. Die Küstenwache bestätigt „malicious cyber activity“, aber keine Betriebsstörung. Laut Bloomberg (02.10.2026, anonyme US-Beamte; am 05.10. von heise, WinFuture und US-Fachmedien aufgegriffen) gibt es Belege für einen vorübergehenden Zugriff auf das Antriebssystem. Offen ist, wer dahintersteckt, wie der Zugang gelang und ob die Angreifer etwas gesteuert haben. Die drastischen Schilderungen (Kühlung gedrosselt, Drehzahl erhöht, 30 Stunden Funkausfall) stammen aus iranischen Staatsmedien und sind unbestätigt. Die kursierenden Bilder aus dem Maschinenraum sind laut Analysten Fälschungen.

Früherer Stand: Nach 24 Stunden (06.10.2026 09:54)

Wissen 47 % · wahrscheinlich 22 % · nicht bekannt 31 %

Laut Bloomberg, gestützt auf anonyme US-Beamte, fanden FBI und US-Küstenwache Hinweise darauf, dass Unbefugte im August 2026 vorübergehend auf ein digitales System zugreifen konnten, das mit dem Antrieb des voll beladenen Rohöltankers VL Prosperity verbunden ist. Offiziell bestätigt sind ein viertägiges Cyber-Boarding ab dem 21.08.2026, „malicious cyber activity“ an Bord und der Verdacht auf „foreign cyber actors“. Schäden für Betrieb, Besatzung

oder Umwelt sind nicht gemeldet. Offen sind der Einfallsweg, die Täter, die Dauer des Zugriffs und vor allem, ob die Angreifer den Antrieb tatsächlich steuern konnten.

Früherer Stand: Nach 72 Stunden (08.10.2026 10:11)

Wissen 48 % · wahrscheinlich 22 % · nicht bekannt 30 %

Küstenwache und FBI bestätigen, dass sie am 21. und 24.08.2026 an Bord von zwei Schiffen gegangen sind, weil es Hinweise auf kompromittierte Netze gab. Laut Küstenwache waren „foreign cyber actors“ beteiligt, und es gab nach offiziellen Angaben keine Betriebsstörung, keine Gefahr für die Crew und keine Umweltschäden. Neu ist ein Bloomberg-Bericht vom 02.10.2026, der sich auf anonyme US-Beamte stützt: Unbefugte hatten demnach vorübergehend Zugriff auf ein digitales System, das mit dem Antrieb verbunden ist. Wie die Angreifer hineinkamen und wer dahintersteckt, ist offen. Die iranischen Berichte über manipulierte Kühlung und Drehzahl sind nicht bestätigt.

Öffentliche Einschätzung von OT-Cyber auf Basis öffentlicher Quellen. Prozent = Einschätzung: 100 % bestätigt, 0 % sicher falsch. Fachliche Einschätzung, keine Schuldzuweisung.