Schadprogramme als Steuermann

Schifffahrt in der IoT-Falle

09.04.18 | Autor / Redakteur: Bernd Schöne / Peter Schmitz

Moderne Schiffe sind in vielen Fällen schwimmende Computernetzwerke und dementsprechend ähnlich anfällig für Cyber-Angriffe, die Gefahr wird aber von den Reedereien noch immer unterschätzt. (© donvictori0 - stock.adobe.com)

Schiffe sind die größten Komponenten des Internets der Dings (IoT), und sie sind oft nicht besser geschützt als eine Webcam für 20 Euro. Ein deutscher Sicherheitsexperte knackte die IT einer Millionen-Euro Jacht binnen kürzester Zeit.

Supertanker und Luxusjachten haben eines gemeinsam, sie sind schwimmende Computernetzwerke. Den Kontakt zum Internet hält, wie in jedem Büro, ein Router. Der ist allerdings auf See etwas Besonderes, arbeitet via Satellit, ist fit für Sturm und Regen und auch etwas teurer als der typische Edge-Router. Dafür erhält der Eigner Zugang zum Internet auf hoher See. Zum Beispiel um zu surfen, über Voice-over-IP zu telefonieren, oder mit dem Smartphone die Kajütenbeleuchtung stimmungsvoll gestalten. Der deutsche Sicherheitsspezialist Stephan Gerling brachte für einen Bekannten dessen Luxusjacht IT-mäßig auf den neuesten Stand und erkannte die Gefahren der umfangreichen Vernetzung. Alle wichtigen Komponenten des Schiffes sind über ein Bussystem untereinander verbunden, und dieses über ein Gateway über den Router mit dem Internet. Das bietet viel Komfort, aber eben auch Risiken.

Heute lächelt niemand mehr über den James Bond Thriller "Der Morgen stirbt nie" von 1997. Damals jagte Bond einem heimtückischen GPS-Sender hinterher, der Schiffe durch falsche Angaben ins Verderben manövrierte. Aber warum das GPS-Signal mit viel Aufwand fälschen und dann den Störsender auch noch in die Nähe des fremden Schiffes bringen, wenn es doch viel direkter geht. Denn Supertanker und Luxusjachten haben eine weitere Gemeinsamkeit: Nur

selten steht der Steuermann selbst am Ruder. Die langweilige Routinenavigation auf dem weiten Meer überlässt man dem Autopiloten. Das ist eigentlich nicht erlaubt, aber auf See schwer zu kontrollieren.

Angriffe nicht nur theoretisch möglich

Es wäre fatal, wenn man über das Internet auf diese Steuerkomponente zugreifen könnte. Stephan Gerling erläuterte auf der Konferenz IT-Defense 2018 erstmals, dass ein solcher Hack konkret umsetzbar ist. Möglich wurde der Angriff durch einen Router mit etlichen Sicherheitslücken. Gerling fand ein Generalpasswort, welches den Zugang zu allen Geräten dieses Typs ermöglichte. Die Idee dazu entstand, als er seine IT-Installation mit dem branchenüblichen Tool Wireshark überprüfte. Der unverschlüsselte Datenverkehr über das FTP-Protokoll zeigte erste Angriffspunkte. Anschließend war es ihm möglich, den Source Code des verwendeten Routers auszulesen und zu decompilieren. Im Source Code waren die Zugangkennungen fest verankert.

"Das Hauptproblem des Jacht-Routers war, dass in der Konfiguration Username und Passwort im Source Code fest verankert waren und nicht durch den Betreiber geändert werden konnten", sagt Stephan Gerling.

Startet der Nutzer zum Beispiel seinen Browser, um auf das Internet zuzugreifen, ruft die Software per FTP den Router auf, benutzt den Username und Passwort aus dem Source Code und loggt sich ein. "Als nächstes wird eine XML Datei vom Router zur Software, also etwa iOS, Android oder Windows übertragen. In dieser XML-Datei steht im Klartext die Konfiguration, inklusive Zugangsdaten für WLAN und WAN"; "Das ist purer Leichtsinn", meint Stephan Gerling.

Eine zusätzliche Gefahrenquelle ist der Management Port Routers für die Fernwartung des Routers. Auch auf ihn konnte man aus dem Internet mit den gleichen Zugangsdaten zugreifen. "Dieses Passwort ist für alle Router, die mit dieser Software ausgestattet sind, das Gleiche. Wer also den Source Code ausließt und sich näher ansieht, erhält Zugriff auf alle Schiffe, die mit diesem System ausgestattet sind, sofern sie mit dem Internet verbunden sind. IoT Suchmaschinen wie Shodan helfen bei der Suche nach geeigneten Zielen", so Gerling.

Um die Herrschaft über ein Schiff zu übernehmen, ist es dann nur noch ein kleiner Schritt. Alle wichtigen Sensoren und Aggregate des Schiffes hängen an einem zentralen Bussystem, dem NMEA 2000 Bus. Spritzwassergeschützte Stecksysteme verbinden GPS, Tiefenmesser, Windmesser, Kompass und Autopilot. Mit dem Bus sind aber auch der Schiffsmotor, das Ruder, der Feueralarm und der Stromerzeuger verbunden. Wer den Bus beherrscht, der beherrscht das Schiff! Technisch baut NMEA 2000 auf dem aus der Autoindustrie bekannten CAN Bus auf. Was geschieht, wenn Hacker diesen Bus übernehmen zeigten, 2013 und 2014 Hacker Charlie Miller und Chris Valasek. Sie drangen über den Entertainmentzugang in den CAN Bus eines Autos ein schließlich übernahmen sie die Herrschaft, konnten Licht ein und ausschalten, aber auch die Lenkung übernehmen und Gas geben, alles zu Demonstrationszwecken auf einem Testgelände.

Um nun auf das interne Steuerungsnetz, den NMEA 2000 Bus zugreifen zu können, muss ein TCP/IP Gateway ins Bordnetz erreichbar sein. „Ist dies der Fall, lassen sich gefälschte NMEA Datagramme in das Steuerungsnetz absetzen“, warnt Stephan Gerling, „Inwieweit das Auswirkungen hat, ist noch Teil der Forschung.“ Forschung ist in diesem Fall ein problematisches Wort. Welcher Eigner riskiert schon eine Millionen Euro teure Jacht für ein Experiment?

Ein weiteres Einfallstor ist das WLAN, das der Mannschaft zur privaten Kommunikation zur Verfügung gestellt wird. Auf vielen Schiffen verzichtet man auf Zugangsbeschränkungen und Passwörter. Auf dem Pazifik kein Problem, in Küstengewässern aber eine enorme Gefahrenquelle. Aufgrund der hohen Reichweite auf See könnten Hacker schon bei der Einfahrt in den Hafen in das Bordnetz eindringen, erst recht aber im Hafen. Die maritime IT-Security steht noch ganz am Anfang.

Unfälle oder Cyber-Angriffe?

Gerling wies in seinem Vortrag auf der IT-Defense 2018 München auf eine ganze Reihe von Vorfällen mit Schiffen hin, die ihn motivierten, die IT auf See einmal näher zu betrachten. Im Februar 2017 konnte ein Containerschiff nach einem IT-Problem 10 Stunden nicht auf die eigene Navigation zugreifen. Im selben Monat lief der Lenkwaffenkreuzer USS Antietam vor Tokio auf Grund, drei Monate später kollidierte der Lenkwaffenkreuzer USS Lake Champlain mit einem Fischerboot. Die US-Navy geht in einem Untersuchungsbericht von „vermeidbare Fehler“ von Kapitän und Crew aus. Aber spielte die IT vielleicht auch eine Rolle? Die Pechsträhne der Navy geht 2017 immer weiter. Am 17. Juni 2017 kollidierte der Zerstörer "USS Fitzgerald" südwestlich von Yokosuka mit dem unter philippinischer Flagge fahrenden Containerschiff "ACX Crystal". Es wird gemutmaßt, dass das der digitale Autopilot des Containerschiffs gehackt worden sein könnte. Die USS John S. McCain traf es am 21.8.2017, sie wurde von dem Tanker "Alnic MC" getroffen. Die US-Schiffe blieben mit knapper Not schwimmfähig. Infolge der Vorfälle starben insgesamt 17 Crewmitglieder, die Schäden an den Schiffen werden mit über 700 Millionen Dollar angegeben. Besonders auffällig sind die Schadensverläufe. Die Schiffe rammten einander wie zu Zeiten der antiken Seekriege. Haben Schadprogramme am Ruder gestanden?

Reeder bewerten Cybersicherheit neu

Die Cyber Defence Conference 2017 der Deutsche Gesellschaft für Wehrtechnik (DWT) thematisierte die Vorfälle aus Sicht der deutschen Marine. Brigadegeneral Christian Leitges wies im Dezember 2017 in Bonn auf die Notwendigkeit hin, sich gegen die Gefahren aus dem Cyberraum zu schützen. Die Marine versucht, künftige Mehrzweckkampfschiffe wie (MKS) 180 auch gegen die Gefahren der Computertechnik zu schützen. Schadprogramme, so der General, können sogar über das Radar in die Schiffsnetzwerke eindringen.

„Die Reeder sind inzwischen auf das Thema aufmerksam geworden“, erläutert der Sprecher des Bundesverbandes Christof Schwaner. Ganz allgemein ist allen Beteiligten klar, das massiver Nachholbedarf besteht.

Auslöser des Umdenkens ist der IT-Gau der größten Containerreederei der Welt. Über die Niederlassung in der Ukraine, wo ein infiziertes Update einer staatlichen Steuersoftware in das Netz gelangte, drang der Kryptotrojaner NotPetya in der Maersk Netz ein und legte weltweit die Riesenschiffe der Reederei lahm. 15 Prozent des Welthandels froren quasi ein, weil niemand mehr wusste, welcher Container wo ausgeladen werden sollte. Teilweise kehrte man zu Papier und Bleistift zurück. Für mehrere Wochen im Juli, so der Geschäftsbericht der Firma, sank das Handelsvolumen der Firma deutlich. Betroffen waren auch der Logistikdienstleister Damco und die Firma APM Terminals. Sie betreibt Containerhäfen und Verladestationen weltweit. Der Schaden wird auf minimal 300 Millionen Dollar geschätzt.

Seit Juli 2017 verteilen die Reeder eine Kurzeinführung in die IT-Sicherheit für den Seemann. Auf 47 Seiten geben die „Guidelines On Cyber Security Onboard Ships“ einen theoretischen Abriss der Gefahren des Internets. Die praktische Umsetzung obliegt dann den Mannschaften und Offizieren.