Hackt unsere Kampfjets!

Wie US-Militär und Unternehmen um Hacker buhlen

Die US-Luftwaffe karrte einen F35-Simulator zur DEF CON, BMW hielt gemeinsam mit chinesischen Security-Forschern einen Vortrag auf der Black Hat. Viele Organisationen und Unternehmen bemühten sich auf den IT-Sicherheitskonferenzen in Las Vegas aktiv um einen guten Draht zu Hackern. Andere fremdelten noch.

Von Uli Ries

Hi, ich bin Will. Ich arbeite für die US Air Force“. Der bebrillte Mann im 80er-Jahre-Star-Wars-T-Shirt stand inmitten einer Traube aus Hackern im erstmals auf der Hackerkonferenz DEF CON errichteten „Aviation Village“ und erklärte den hinter ihm aufgebauten Flugsimulator. „Mit diesem Simulator machen sich unsere Piloten fit für Einsätze mit der F35, unserem modernsten Kampfflugzeug“. Die F35 – und natürlich der Simulator – verlasse sich auf große Mengen Programmcodes, den es abzusichern gelte.

Bemerkenswert an diesem Auftritt war nicht nur der Aufwand, den die US-Luftwaffe mit dem Aufbau des Simulators betrieb. Sondern auch, dass „Will“ mit vollem Namen Dr. Will Roper heißt und als Assistant Secretary for Acquisition, Technology and Logistics den kompletten Einkauf der US Air Force verantwortet. Und dass er somit über ein Budget von rund 40 Milliarden US-Dollar gebietet. Jährlich.

Typischerweise buhlen daher Lieferanten um Ropers Gunst. Auf der DEF CON, die in diesem Jahr zum 27. Mal stattfand, war es genau umgekehrt: Das Militär buhlte um die Aufmerksamkeit von Hackern. Im Gespräch mit c’t erklärte Roper, warum er zusammen mit dem US-Heimatschutzministerium, einer europäischen Airline und anderen Unternehmen das Aviation Village unterstützt: „Wir haben natürlich auch Hacker in unseren Reihen. Aber nicht genug und wahrscheinlich auch nicht die besten Talente in ihrem jeweiligen Fachgebiet.“ Die Software sei es, die die F35 so überlegen mache. Und wenn man beim Thema Software-Sicherheit den Kopf in den Sand stecken würde, liefe etwas „ganz, ganz falsch“. Daher wollen die Air Force und auch zivile Luftfahrtorganisationen im Rahmen von IT-Sicherheits-Events talentierten Hackern Zugriff auf die relevante Avionik gewähren.

Konsequenterweise organisierte das US-Verteidigungsministerium parallel zur DEF CON in einem benachbarten Hotel auch einen Live-Hacking-Wettbewerb, bei dem es darum ging, Sicherheitslücken in der 20.000 US-Dollar teuren Trusted Aircraft Information Download Station (TADS) des F15-Kampfjets aufzudecken. Laut US-Luftwaffe sammelt und verarbeitet TADS während des Flugs Daten von Kameras und anderen im Jet verwendeten Sensoren.

Am Wettbewerb beteiligte Hacker kritisierten im Nachgang, dass sie zu wenig Zeit gehabt hätten, um sich mit den für sie völlig fremden Komponenten zu befassen. Denn Avionik ist für die meisten ein böhmisches Dorf. Umso bemerkenswerter, dass sie in weniger als zwei Tagen – teilweise unter Einsatz von Schraubenziehern, Zangen und Krokodilklemmen – diverse Bugs im TADS finden konnten. Patrick Kiley von der IT-Sicherheitsfirma Rapid7 (siehe Aufmacherbild) entdeckte bei dieser Gelegenheit einige üble Bugs in Bordsystemen von Kleinflugzeugen, über die sich unter anderem deren Autopilot ausschalten ließ. Weitere entdeckte Bugs hätten gar Systemausfälle verursachen können.

Die Vertreter der Luftfahrtindustrie, die im Aviation Village anzutreffen waren, sehen bis zur reibungslosen Zusammenarbeit aber noch einen weiten Weg. Denn die stark regulierte, von unzähligen Standards und Zertifizierungen geprägte Branche hat nach wie vor Berührungsängste mit den typischerweise unorthodox arbeitenden Hackern. Und die müssen sich ihrerseits erst an eben jene Standards und die bislang streng vor ihren Blicken abgeschirmten Technologien herantasten.

Hersteller und Hacker Hand in Hand

Die Automobilbranche ist da schon einen Schritt weiter. Tesla war schon 2015 als Unterstützer des ersten „Car Hacking Village“ auf der DEF CON, und im ver-

gangenen Jahr ließ es sich auch Unternehmensgründer Elon Musk nicht nehmen, einen Vortrag auf der Konferenz zu halten. Das Bug-Bounty-Programm seines Unternehmens zahlt bis zu 15.000 US-Dollar pro Schwachstelle.

Der Hauptpreis des diesjährigen Capture-the-Flag-(CTF)-Wettbewerbs im Car Hacking Village war zwar ein Tesla Model S, der Hersteller trat aber nicht als Sponsor auf. Nachvollziehbar, da die Sieger des Wettbewerbs das an sich brandneue Auto nicht ohne Gebrauchsspuren mitnehmen durften: Die Teams würfelten während des Wettstreits um Punkte. Würfelte ein Teilnehmer beispielsweise eine 3, durfte er dem Auto einen Schlag mit einem Hammer verpassen. Eine 6 bedeutete die Chance, eine Bowlingkugel auf die Motorhaube zu donnern.

Warum? Die CTF-Ausrichter erklärten es so: „Wenn man die Chance hat, etwas zu tun, das man sonst nie tun würde, dann muss man sie ergreifen“. Diese Aussage bezog sich offenbar sowohl auf die Chance, den Tesla zu hacken, als auch darauf, ihn zu demolieren, mit unzähligen Aufklebern zu verzieren oder mit Lippenstift-Abdrücken zu übersäen. Der Gewinner bekam letztlich die Schlüssel für ein, so die Veranstalter, „einzigartiges Fahrzeug mit Patina und Geschichte“ – und dem Wettbewerb war die Aufmerksamkeit von Besuchern und Presse sicher.

Ohne Auto im Gepäck, dafür aber mit Hackern auf der Bühne, präsentierte sich BMW. Offensichtlich fremdelt der Autobauer nicht, wenn es um Kontakte zur Hacker-Gemeinde geht: BMW-Vertreter hielten gemeinsam mit Sicherheitsexperten der Tencent Keen Labs einen Vortrag auf der Black Hat. Darin ging es um teils aus der Ferne ausnutzbare Lücken in BMWs „ConnectedDrive“-Software, die Tencent 2018 entdeckte. Das chinesische Unternehmen hatte BMW anschließend geholfen, sie zu beheben.

Auch in Sachen Bug Bountys gab es Neuigkeiten während der Black Hat und DEF CON: Apple zahlt Bugfindern jetzt bis zu eine Million US-Dollar für Sicherheitslücken, die das Ausführen von Kernel-Code aus der Ferne ohne Zutun des Nutzers erlauben und zusätzlich einen Neustart des verwundbaren Systems überstehen.

Microsoft nutzte die Black Hat, um Neuigkeiten rund um seine Bug-Bounty-Programme anzukündigen: Die Redmonder zahlen jetzt bis zu 300.000 US-Dollar für Schwachstelleninformationen, die die Cloud-Plattform Azure betreffen. Im eigens dafür eingerichteten Azure Security Lab können Hacker die produktiv eingesetzte Azure-Infrastruktur angreifen, ohne den Live-Betrieb und damit Kundendaten zu gefährden – online und zeitlich unabhängig von Events wie Black Hat oder DEF CON.

Kommunikation zum Kopfschütteln

Weniger offen für eine Zusammenarbeit zeigte sich ausgerechnet Flugzeughersteller Boeing, der seit Monaten wegen Sicherheitsmängeln an seinen Flugzeugen in der Kritik steht. Nachdem der Security-Fachmann Rubens Santamarta Boeing auf etliche Schwachstellen und schlampig programmierte Passagen in der Firmware einer wichtigen Netzwerkkomponente des Langstreckenfliegers 787 („Dreamliner“) aufmerksam gemacht hatte, nahm der Hersteller zwar den Dialog auf. Am Ende servierte er Santamarta aber mit dem Kommentar ab, die Lücken nicht reproduzieren zu können – ohne ihm die Gelegenheit zu bieten, seine Entdeckungen vor Ort mit Ingenieuren zu diskutieren.

Der Chief Information Security Officer einer europäischen Fluglinie sagte im Gespräch mit c’t, dass ihm dieses Verhalten unverständlich sei: „Wenn mir jemand einen Bug meldet und ich ihn nicht reproduzieren kann, dann tue ich doch alles, um die Schritte des Forschers nachvollziehen zu können“.

Gegenüber der US-Presse erklärte Boeing, dass die von Santamarta entdeckten Lücken zwar vorhanden, aber nicht ausnutzbar seien. Einen Beleg hierfür blieb das Unternehmen aber schuldig.

Problematisch gestaltete sich laut Daniel Romero und Mario Rivas von der Cyber-Security-Firma NCC Group auch die Kommunikation mit diversen Druckerherstellern. Die Hacker hatten sich mittels automatisierter Penetrationstests die Firmware von Brother-, HP-, Kyocera-, Lexmark-, Ricoh- und Xerox-Druckern vorgenommen und binnen kurzer Zeit 50 teils schwerwiegende Bugs gefunden.

Die Kommunikation im Rahmen des Responsible-Disclosure-Prozesses verlief größtenteils schleppend: Einige Hersteller reagierten erst nach Monaten auf die Kontaktaufnahme durch die Forscher. Kyocera und Ricoh haben auch ein halbes Jahr später noch keine Sicherheitsupdates veröffentlicht.

Air Force behält ihren Kurs bei

Für 2020 hat Will Roper von der Air Force noch größere Pläne, als er sie im Rahmen der DEF CON 27 umgesetzt hat: Während der nächsten Konferenz will er ausgewählte Hacker in einen Luftwaffenstützpunkt nahe Las Vegas bringen und sie dort auf alle digitalen Systeme eines echten Kampfjets loslassen. Wahlweise soll auch das Kontrollsystem von Militärsatelliten im Angebot sein.

„Mir ist es lieber, wenn Hacker die Bugs vorab finden, bevor wir die Systeme in eine Gefechtssituation bringen“, sagt Roper. Damit beweist er eine Einstellung gegenüber White-Hat-Hackern, die Organisationen und Unternehmen im Hinblick auf noch unentdeckte Bugs künftig eine Menge Zeit und Risiko sparen könnte – und die sich langsam, aber stetig durchzusetzen scheint. *(ovw@ct.de)* c't

Interessante Veröffentlichungen zu den Hacker-Konferenzen: ct.de/yvz8

„Hackt unsere Stadt“: Im ICS-Village konnten Besucher der DEF CON versuchen, eine simulierte, vernetzte Smart City zu kapern.