Viren für Auto keine Bedrohung

Beitrag von „owolter“ vom 9. Februar 2005 um 11:51

Nachdem vor einigen Wochen erstmals Eugene Kaspersky, Hersteller für Antivirensoftware, in seinem Weblog über Viren in Fahrzeugnavigationssystemen spekulierte, häuften sich Meldungen über angebliche Schädlinge für KFZ-Steuersysteme. So sollen unter Symbian/S60 laufende Handy-Viren bereits Modelle der Marke Lexus befallen haben, spann ein Sicherheits-Newsdienst die Spekulationen von Kapersky weiter, der auf eine Anfrage von Lexus-Fahrern reagiert hatte. Ein südafrikanischer Sicherheitsdienstleister ging sogar so weit, über Viren zu spekulieren, die sich für Autodiebstähle einsetzen lassen. Per Bluetooth an den Bordcomputer von Luxuslimousinen übertragen, würde er die Zentralverriegelung aktivieren. Ein Laborexemplar habe man bereits entwickelt. Jetzt warnt auch IBMs Security Intelligence Services in seinem "Security Threats and Attack Trends Report" vor kommenden Bedrohungen der Bordelektronik durch Schädlinge.
Tatsache ist, dass in modernen Fahrzeuge immens viel Computerhard- und -software verbaut wird. Im Schnitt sollen mittlerweile um die 20 Prozessoren mit ingesamt 60 MByte Software zur Steuerung des Fahrzeugs Einsatz finden. Hinzu kommen Systeme, die als Schnittstelle zwischen Fahrzeug sowie Fahrer fungieren und auch mobile Kommunikation respektive Navigation anbieten. Hier setzen die Hersteller natürlich auf bekannte Betriebssysteme wie beispielsweise Symbian OS oder Windows CE.
Allerdings sind in den letzten Monaten vermehrt Schädling für Symbian OS aufgetreten, die sich per Bluetooth auf in der Nähe befindliche Geräte übertragen. Ob das nun ein anderes Handy oder zufällig der Bordcomputer eines Autos ist, interessiert den Wurm dabei nicht. Zur Infektion mit den Handy-Würmern Lasco.A, Skull und Cabir ist bislang aber immer noch erhebliche Nutzerinterkation notwendig. So muss der Anwender mehrfach die Ausführung eines empfangenen Programms mit OK bestätigten. Allerdings zeigt sich schon bei Mail-Würmern, dass Anwender noch zu oft Objekte unbekannter Herkunft ungeprüft öffnen oder installieren. Zudem setzt ein Angriff voraus, dass das Zielsystem Bluetooth aktiviert hat.
Bislang sind Handy-Viren/Würmer noch kaum verbreitet, und die Infektion eines Automobils wurde noch nicht nachgewiesen. Allerdings ist schon jetzt abzusehen, dass auf die Hersteller und Kunden bei der weiter fortschreitenden Integration der Computertechnik in Fahrzeugen ein Problem zukommt. Zumindest für Symbian-Handys S60/S90 sind bereits Virenscanner verfügbar -- demnächst dann wohl auch für den Bordcomputer. (dab/c't)

Quelle

Beitrag von „Wolf“ vom 9. Februar 2005 um 13:36

http://oncomputer.t-online.de/c/33/43/51/3343516.html

Viren im Lexus
Die amerikanische Automarke Lexus hat offenbar bereits einen Virus in seinen Modellen Landcruiser LX470 und LS430 entdeckt. Der ungebetene Gast soll sich über Bluetooth-Handys in dem Wagen-Kommunikationssystem eingenistet haben. Eine entsprechende Anfrage von der Toyota-Tochter sei beim russischen Antiviren-Spezialist Kaspersky eingegangen, berichtet das US-Magazin für Sicherheitsfragen SC Magazine. Lexus weiß allerdings offiziell nichts davon.

Deutsche Hersteller betroffen?
Auch Audi soll bereits auf ein ähnliches Problem gestoßen sein, meldet das IT-Magazin Computer Partner. Demnach habe die VW-Tochter nach Aussagen eines Branchenkenners vor einiger Zeit das gesamte GPS-System nachträglich mit einem Virenschutz versehen müssen.

Windows in Flugzeugen und Schiffen
Nicht nur in Autos, auch in Schiffen und U-Booten übernehmen immer häufiger ähnliche Betriebssysteme wichtige Aufgaben. "Ich habe bereits Screenshots von Windows-2000-basierten Systemen in großen Verkehrsflugzeugen gesehen", sagte der Forschungsdirektor der Antiviren-Firma F-Secure, Mikko Hypponen.

Millionen Wegfahrsperren in Gefahr
Ähnlich beunruhigende Meldungen kommen von der Johns-Hopkins-Universität in Baltimore. Findige Forscher haben den Code-Chip geknackt, der weltweit in über 150 Millionen von modernen Autoschlüsseln zum Einsatz kommt. Wer den individuellen Schlüssel-Code seines Opfers kennt, kann die Wegfahrsperre seines Autos umgehen. In den USA ständen dem Dieb noch mehr Türen offen. An vielen Tankstellen funktioniert der Schlüssel praktisch als elektronische Kreditkarte.
Kinderspiel für Hacker
Der Code ließe sich mit "vergleichsweise günstigen elektronischen Geräten" knacken, sagte der Sicherheitsexperte Avi Rubin vom Information Security Institute. Das Prinzip: Der Angreifer spioniert zunächst aus einigen Metern Entfernung mit einem Lesegerät über Funk die Daten des Schlüssels seines Opfers aus. Anschließend ermittelt er daraus mit Hilfe eines oder mehrerer PC den Code. Einen wenig tröstenden Tipp, wie man sich vor den Schnüffel-Attacken schützen kann, haben die Wissenschaftler auch parat: Nach Gebrauch den Schlüssel in eine Metallfolie wickeln.

Gruss Wolf

Beitrag von „owolter“ vom 9. Februar 2005 um 13:50

nichts geht über anständige mechanik

Beitrag von „andreas“ vom 9. Februar 2005 um 13:54

> Zitat von owolter
>
> nichts geht über anständige mechanik

Das stimmt, wenn man so einen "altertümlichen"
Batterietrennschalter versteckt einbauen würde, schauten
die High-Tec-Diebe wohl dumm aus der Wäsche. 

Gruß
anderas

Beitrag von „agroetsch“ vom 9. Februar 2005 um 14:32

> Zitat von Wolf
>
> Nach Gebrauch den Schlüssel in eine Metallfolie wickeln.

Hallo,

heißt das der Schlüssel funkt permanent... Kann ich mir eigentlich nicht vorstellen.

Aber man könnte ja ein schönes Schlüssel-Etui aus Metall entwickeln, ist dann vielleicht auch billiger als der Leder-Überzieher vom/für den Phaeton.