Cybersicherheit

Alles andere als gute Nachrichten

Prof. Dr. Reiner Creutzburg, Informatikprofessor an der TH Brandenburg, referierte beim zweiten Cybersicherheitssymposium Nordwestbrandenburg im Resort Mark Brandenburg in Neuruppin über die Gefahren des Internets der Dinge. © Foto: Siegmar Trenkler

Siegmar Trenkler/ 12.06.2018, 06:00 Uhr

Neuruppin (MOZ) Hackerangriffe gab es in den 1990er-Jahren vor allem in Spionagefilmen. Mittlerweile sind diese Angriffe jedoch alltäglich geworden. Und ob unbedarfte Kinder, Hacker mit Ehrenkodex oder Spionage durch staatliche gestützte Gruppen – sie alle haben oft viel zu leichtes Spiel.

„Ich habe nichts Gutes zu berichten“, sagt Prof. Dr. Reiner Creutzburg. Er ist seit 1992 Informatikprofessor an der FH Brandenburg, der heutigen TH.

Creutzburg hat sich die Gefahren des Internets der Dinge vorgeknöpft – also der Vernetzung von Objekten: vom Garagentor über den Kühlschrank bis hin zur Alarmanlage. Bei aller Sicherheit, die die Smart-Home-Lösungen vorgaukeln, bei denen unzählige Funktionen auch vom Handy aus dem Urlaub überwacht und gesteuert werden können, kommen nach seiner Erfahrung viele Lücken hinzu.

So bleiben oft die Fabrikeinstellungen bei Passwörtern bestehen, was Dieben ungeahnte Möglichkeiten bietet. „Die können die Überwachung ausstellen, in Ruhe das Haus ausräumen und danach wieder anstellen“, berichtet er.

Es bedarf dafür nach seiner Erfahrung nicht einmal besonderen Fachwissens. Auf speziellen Internetseiten werden bekannte Sicherheitslücken aufgelistet. „Das ist gut, wenn man die Lücken beseitigen möchte. Aber alle anderen haben darauf auch Zugriff“, so Creutzburg. Wichtig wird das besonders, wenn es nicht mehr um das eigene Haus, sondern das Blockheizkraftwerk gehe, oder andere wichtige Anlagen. Dass es wirklich nur einige Klicks sein können, bis man beispielsweise im Menü für die Steuerung einer Industrieanlage in Deutschland oder eines Wassertanks in den USA ist, demonstriert er bei Seminaren auch den Teilnehmern. So legt er einfach mal den Hauptschalter im Menü einer Solaranlage irgendwo in Deutschland um, was ungläubiges Staunen beim Publikum provoziert. „Wir machen hier nicht einmal etwas Verbotenes, weil kein Zugangsschutz umgangen wurde“, erklärt er.

Glaubt man Creutzburg, so nehmen die Gefahren in den kommenden Jahren zu. „Wir werden bald bei neun Milliarden Menschen sein. Prognosen sagen 37 Milliarden vernetzte Geräte für 2020 voraus. Da der Markt das will, werden die kommen, weil dadurch ein Umsatz von 1,9 Billionen Dollar erwartet wird.“ Sollte später festgestellt werden, dass es dadurch eine größere Anfälligkeit und mehr Sicherheitslücken gebe, werde erst im Nachhinein nachgesteuert, ist sich Creutzburg sicher.

Schon jetzt gibt es Fälle, in denen durch Sicherheitslücken enorme Schäden entstanden sind. Der Professor verdeutlicht das mit einem Casino, dessen Geldströme umgelenkt wurden, weil der Hausmeister ein vernetztes Thermometer für das Aquarium im Lobbybereich genutzt hatte. Dadurch waren Hacker ins System eingedrungen und mussten dafür nicht einmal die Firewall knacken. In einem anderen Fall war nachgewiesen worden, dass sich Insulinpumpen von Hackern steuern lassen würden – mit möglicherweise tödlichen Folgen.

„Was lässt sich dagegen machen?“, fragt sich so mancher Zuhörer. Die Antwort, die Creutzburg parat hat, ist einfach, wenn sie auch keinen perfekten Schutz garantiert: Passwörter einsetzen, die nicht nur aus „1234“ bestehen und der firmeneigenen IT-Abteilung Bescheid geben über etwaige vernetzte Geräte. „Und wenn Sie einen Verdacht haben, weil ihr Mitbewerber immer ein Angebot macht, das fünf Euro unter ihrem liegt, kommen Sie zu uns und wir schauen, was gemacht werden kann“, erklärt er dann vor allem den Unternehmern im Publikum.