Buchrezension

Nicole Perlroth, This Is How They Tell Me The World Ends

Rezension von Prof. Dr. Antje von Ungern-Sternberg

IT-Sicherheit war lange eine Materie, mit der sich nur Eingeweihte beschäftigten. Erst in jüngerer Zeit wird auch der breiteren Öffentlichkeit klar, dass Sicherheitslücken in Software und IT-Infrastruktur in großem Stil für kriminelle Aktivitäten genutzt werden, etwa um Lösegeld für die Freigabe von Daten zu erpressen. Zugleich ermöglichen Sicherheitslücken aber auch Spionage oder Cyberangriffe zu politischen Zwecken – mit potentiell verheerenden Folgen, etwa wenn Cyberaktivitäten die kritische Infrastruktur eines Landes lahmlegen oder wenn sie Wahlkämpfe und Wahlen manipulieren.

Das Buch „This Is How They Tell Me The World Ends" der US-amerikanischen Journalistin Nicole Perlroth wirft einen Blick auf die Hintergründe dieser Entwicklung. Ihre zentrale These lautet, dass die US-Behörden die Gefahren für Cyberaktivitäten, die sich gegen die USA richten, selbst heraufbeschworen haben. Denn heutzutage hat sich, wie Perlroth beschreibt, der Handel mit Sicherheitslücken („Zero Days") und ihren Nutzungsmöglichkeiten („Zero Day Exploits") zu einem lukrativen Geschäft entwickelt. Dies ist auch auf die US-Sicherheitsdienste zurückzuführen, die seit langem Sicherheitslücken erforschen, erwerben und für eigene Zwecke nutzen. Allerdings sind inzwischen – so Perlroth – nicht mehr nur die USA, sondern eben auch andere Staaten und Organisationen willens und in der Lage, Sicherheitslücken selbst zu entdecken oder anzukaufen, für ihre eigenen Zwecke einzusetzen und hiermit den USA oder anderen westlichen Staaten zu schaden.

Perlroth schildert den Umgang mit Zero Days und Zero Day Exploits auf packende und für technische Laien gut verständliche Art und Weise. Ihre Geschichte über die Verbreitung von Stuxnet etwa liest sich spannend wie ein Spionageroman. Das Buch strukturiert sie anhand der unterschiedlichen Akteure, die bei der Entdeckung und Nutzung von Sicherheitslücken eine Rolle spielen. Sie behandelt Hacker (ob angestellt oder unabhängig, an Werten oder Geld interessiert), private Sicherheitsunternehmen, staatliche Nachrichtendienste (westlicher und gegnerischer Staaten wie China, Russland, Nordkorea, dem Iran oder Syrien), Organisationen wie Al-Kaida, sowie – nicht zuletzt – die IT-Firmen selbst.

Perlroth versteht ihr Buch als Weckruf, das der Öffentlichkeit die große Bedrohung einer digital weltweit vernetzten und daher höchst verwundbaren Gesellschaft angesichts schädlicher Cyberaktivitäten vor Augen führen will. Ihr Buch schließt mit konkreten Handlungsempfehlungen, die Resilienz gegen diese Aktivitäten schaffen sollen: für eine Wirtschaft, in der sich die Schaffung sicherer (nicht schnell entwickelter) Software lohnt, für einen Staat, der vor allem die kritische Infrastruktur effektiv schützt, und für Menschen, die ihr Verhalten auf digitale Sicherheit ausrichten. Auch wenn das Buch aus einer dezidiert US-amerikanischen Perspektive geschrieben ist, lohnt sich die Lektüre gerade auch andernorts: Denn das Buch liest sich fesselnd – und klärt hierbei umfassend über die weltweite Problematik der IT-Sicherheit auf.