Die Welt 8.10.2010
S. 2

„Eine große Cyber-Attacke ist für den Staat gefährlicher als ein Bombenanschlag“

Der Sicherheitsexperte Arne Schönbohm über gefährliche Computerviren, militärische Reaktionen auf Attacken mit Schadprogrammen und Versäumnisse in Deutschland

Der Computervirus Stuxnet ist erst der Anfang. Um für den Cyberkrieg gerüstet zu sein, benötigt die Bundeswehr mehr Kompetenzen und mehr Geld, sagt Sicherheitsexperte Arne Schönbohm, Autor des Buches „Deutschlands Sicherheit“ (Edition Octopus). Schönbohm war 13 Jahre in der Division Defence and Security beim Rüstungskonzern EADS tätig und ist jetzt Vorstand des Beratungsunternehmen BSSBuCet Secure Networks in München. Mit ihm sprach Peter Issig über die Gefahren aus dem Netz.

DIE WELT: *Der Computervirus Stuxnet hat nicht nur iranische Atomanlagen, sondern weltweit industrielle Objekte befallen. Ist es glaubhaft, dass der Computervirus unschädlich gemacht wurde?*

Arne Schönbohm: Der Spruch „Gefahr erkannt, Gefahr gebannt“ ist hier nicht zutreffend. Wenn man bedenkt, dass alle zwei Sekunden neue, meist maschinell gefertigte Schadprogramme entstehen, dann wird es immer wieder neue Abwandlungen von Stuxnet geben. Jetzt hat man eine temporäre Lösung gefunden, aber das Problem bleibt dauerhaft bestehen.

Wer fertigt diese Schadprogramme? Computerfreaks, Kriminelle oder staatliche Stellen?

Schönbohm: Da ist alles dabei. In der Regel dienen die Programme dazu, Daten abzufangen, die dann weiterverkauft werden. Die Entwicklung von Stuxnet hat aber nach Meinung von Experten einen siebenstelligen Betrag gekostet, und das Ziel war wohl nicht, Geld damit zu verdienen. Das könnte bedeuten, dass staatliche Stellen dahinterstecken, auch wenn es dafür keine Beweise gibt.

Sind die Energieunternehmen in Deutschland besser auf Angriffe aus dem Internet auf die Atomkraftwerke vorbereitet?

Schönbohm: Erinnern Sie sich an den Stapellauf eines Kreuzfahrtschiffs in Papenburg vor vier Jahren? E.on schaltete damals eine Starkstromleitung ab, damit das Schiff darunter durchfahren konnte, danach blieben Millionen Menschen in Westeuropa ohne Strom. Wenn so etwas passieren kann, wird klar, dass noch verschiedene Sicherheitsvorkehrungen getroffen werden müssen. Und zwar nicht irgendwelche Vernebelungsanlagen, um Atomkraftwerke vor Angriffen aus der Luft zu sichern. Die größere

Sicherheitsexperte und Buchautor Arne Schönbohm

Gefahr sind Schwachstellen bei der IT-Sicherheit oder Sabotage durch Mitarbeiter.

Fehlt es an der Sensibilität für das Thema oder am Geld?

Schönbohm: Jedes vierte deutsche Unternehmen ist in den vergangenen drei Jahren von Cybercrime betroffen gewesen. Die Ressourcen, die Bundes- und Landeregierungen zur Bekämpfung von Cybercrime zur Verfügung stellen, deuten darauf hin, dass man noch sehr dem traditionellen Denken verhaftet ist. Nach dem Motto: Wir schützen am besten, wenn wir einen Polizisten auf der Straße oder einen Eurofighter in der Luft haben. Gleichzeitig wächst der Sicherheitsmarkt für Dienstleistungen und Produkte überproportional stark. Das zeigt, dass die Wirtschaft hier großen Schutzbedarf für sich sieht, den der Staat nicht erfüllt.

Deutschland ist also nur bedingt abwehrbereit?

Schönbohm: Ja.

Das müssen sie jetzt aber belegen.

Schönbohm: Wenn ich mir die Vorlage für den Bundestag zum Haushaltsplan des Bundesverteidigungsministeriums anschaue, dann steht dort zum Thema IT-Sicherheit oder Cyberwar fast nichts drin. Es wird über Einsparungen von 455 Millionen Euro diskutiert, die die Wehrpflicht kostet. Aber über den Ernstfall eines Cyberangriffs wird nicht viel gesagt.

Es wird doch ständig über neue Sicherheitsgesetze diskutiert.

Schönbohm: Es wird aber nur begrenzt darüber diskutiert, wer zuständig ist, wenn wirklich ein Cyberangriff auf Deutschland stattfinden sollte, wie jetzt im Iran. Ist es Sache der Landespolizei, weil es eine „lokale“ Straftat ist? Ist es die Bundespolizei oder das Bundeskriminalamt? Oder sind es etwa die Streitkräfte? Diese Diskussion hat so nicht stattgefunden.

Wie sollten die Kompetenzen innerhalb der Sicherheitsorgane effektiv organisiert werden?

Schönbohm: Wenn es um Datendiebstahl bei einem mittelständischen Unternehmen geht, dann ist das mit Sicherheit eine Sache der Landespolizei. Wenn aber ein Unternehmen betroffen ist, das bundesweit oder europaweit Standorte hat und gezielt ausspioniert wird, dann müsste das BKA übernehmen.

Und wenn es zum Angriff auf zentrale Infrastruktureinrichtungen des Staates kommt?

Schönbohm: Die USA haben die Frage für sich so beantwortet, dass bei Attacken auf die Infrastruktur auch militärisch zurückgeschlagen werden kann. Auch die Nato scheint dies als Bündnisfall zu verstehen.

Halten sie den amerikanischen Weg für richtig?

Schönbohm: Er ist konsequenter. Mit einer großen Cyberattacke kann die Handlungsfähigkeit des Staates schwerer beeinträchtigt werden als durch einen Bombenanschlag oder Raketenangriff. Eine Cyberattacke wäre damit ein Angriff gegen den Staat und somit der Verteidigungsfall. Die Bundeswehr wäre sozusagen zuständig. Sie ist aber darauf nur begrenzt vorbereitet.

Wie sieht es im privatwirtschaftlichen Bereich aus?

Schönbohm: Der Mittelstand, das Rückgrat der deutschen Wirtschaft, bietet eine Vielzahl an möglichen Zielen für Cyberattacken, jedoch sind die Ressourcen zur Gefahrenabwehr auch hier begrenzt. In Bayern sollen beispielsweise zur Bekämpfung der Wirtschaftskriminalität zehn weitere Beamte mit wirtschaftswissenschaftlichem Hintergrund eingestellt werden. Ich denke, das ist ein bisschen wenig.

Tun sie dem Staat nicht unrecht? So behäbig, wie sie es darstellen, ist er doch auch wieder nicht.

Schönbohm: Nur ein Beispiel: 1996 begann die Diskussion über die Ausrüstung von Polizei, Feuerwehren und Rettungskräften mit Digitalfunk. Bis 2016 soll es wohl noch dauern, bis die Umsetzung erfolgt sein wird. Wenn die Beschaffung und der Know-how-Aufbau in anderen Bereichen, beispielsweise der Cybercrime-Abwehr, genauso laufen, dann könnte das für die Bundesrepublik Deutschland ein Problem werden.