„IT-SYSTEME WERDEN IMMER KOMPLIZIERTER, UND ES IST KAUM NOCH MÖGLICH, SIE ZU VERSTEHEN, UND SEHR SCHWIERIG, SIE ZU SCHÜTZEN. BEVOR ABER DIE POLITIK HANDELT, KÖNNEN SIE SCHON ETWAS UNTERNEHMEN.“

Jörn Müller-Quade

Cybersicherheit in den Biowissenschaften – Was können wir tun?

DOI: 10.1007/s12268-017-0810-8
© Springer-Verlag 2017

■ Der Erpressungs-Trojaner WannaCry hat erheblichen Schaden angerichtet und sogar Krankenhäuser lahmgelegt. Dies ist besorgniserregend, da unsere Abhängigkeit von IT-Systemen immer größer wird. Das reicht vom Alltag, etwa der Hausautomation, über die Arbeitswelt, etwa die vernetzte Produktion, bis hin zum hochsensiblen Bereich der Bioinformatik, wo medizinische Studien mit Biochips automatisiert oder massenweise Gen-daten sequenziert und verarbeitet werden. IT-Systeme werden immer komplizierter, und es ist kaum noch möglich, sie zu verstehen, und sehr schwierig, sie zu schützen.

IT-Sicherheit ist so schwierig, weil wir es mit einem intelligenten Angreifer zu tun haben, der Schwachstellen, die wir vielleicht noch nicht kennen, gezielt nutzt. Inwieweit etwa automatisierte Studien in der Biomedizin gegen IT-Angriffe geschützt sind, die die Studie geschickt verfälschen, ist kaum erforscht. Zusätzlich wird es einem Angreifer häufig unnötig einfach gemacht. Es werden veraltete Betriebssysteme eingesetzt, oder es werden reihenweise netzwerkfähige Kameras ausgebracht, die alle dasselbe Passwort verwenden. An Sicherheit wird offensichtlich gespart! Häufig höre ich: „100-prozentige Sicherheit gibt es sowieso nicht!“, was stimmt, aber meist wird es mit Fatalismus im Ton vorgetragen und dient als Ausrede für laxen Sicherheitsmaßnahmen. In der Konsequenz ist die IT-Sicherheit häufig vernachlässigt.

Hackerangriffe und unsichere IT-Systeme sind eine zunehmende Bedrohung für Wirtschaft und Gesellschaft. Gute Ratschläge und freiwillige Maßnahmen haben bisher wenig genutzt. Dies ist auch deshalb verheerend, weil ungesicherte Rechner in Angriffswerkzeuge verwandelt werden können. Wer also seinen eigenen Rechner nicht schützt, schadet nicht nur sich selbst, sondern auch vielen anderen. IT-Sicherheit sollte daher eine nationale Aufgabe sein.

Was sollten wir also tun? Die drei Kompetenzzentren für IT-Sicherheit CISA (Saarbrücken), CRISP (Darmstadt) und KASTEL (Karlsruhe) haben der amtierenden Bundesministerin für Bildung und Forschung Johanna Wanka ein Positionspapier übergeben und konkrete Maßnahmen vorgeschlagen:

1. Wir müssen unsere digitale Souveränität zurückgewinnen: Jeder Nutzer sollte selbst festlegen können, was mit seinen Daten passiert. Unternehmen sollten ihren IT-Systemen nicht blind vertrauen müssen, und souveräne Staaten müssen auch in internationalen Krisensituationen geschützt und handlungsfähig bleiben. Um in Zukunft unabhängig und selbstbestimmt agieren zu können, sind Anstrengungen in der Größenordnung des europäischen Engagements im Flugzeugbau durchaus gerechtfertigt.
2. Wir brauchen vorgeschriebene Mindeststandards und Produkthaftung, denn wer nachlässig handelt, gefährdet nicht nur sich selbst. Gehackte Computer, die zu großen „Bot-Netzen“ zusammengeschlossen sind, können durch lawinenartige Anfragen Online-Shops und Internetinfrastrukturen lahmlegen oder Trojaner weiterverbreiten.
3. Der Staat sollte IT-Sicherheitsinfrastrukturen bereitstellen. Sichere digitale Identitäten und einfache Ende-zu-Ende-Verschlüsselung sollten staatlich gefördert werden, wie etwa Straßen, und auch die Beurteilung und Überprüfung von IT-Systemen und Internetdiensten muss staatlich unterstützt werden.
4. Unsere Grundrechte müssen gestärkt werden. Es darf nicht sein, dass große Internetkonzerne europäisches Datenschutzrecht missachten oder dass Sicherheitslücken geheim gehalten werden, um massenhaft Nutzer auszuspionieren. IT-Systeme verwundbar zu machen oder zu lassen, öffnet auch Türen für Verbrecher: Der Erpressungs-Trojaner WannaCry ist ein

Beispiel. Kryptografische Verfahren, etwa für die Verschlüsselung, können Grundrechte technisch unterstützen, und ihre Nutzung darf nicht eingeschränkt werden.

5. Wir brauchen mehr Aus- und Weiterbildung. Denn es gibt nicht nur einen großen Mangel an Fachkräften, sondern auch kein ausreichendes Mindestbewusstsein für die Problematik. Sehr viele erfolgreiche Angriffe nutzen „Social Engineering“, das heißt, sie nutzen gezielt menschliche Schwachstellen in Sicherheitsprozessen.
6. Wir brauchen mehr IT-Sicherheitsforschung. Vieles ist noch nicht verstanden. Etwa, wie man eine komplexe Infrastruktur, beispielsweise das Energienetz der Zukunft, absichert, selbst wenn einzelne IT-Komponenten gehackt werden könnten. Hier darf man nicht abwarten, bis es Vorfälle gibt.
7. Wir brauchen Forschungstransfer, um gute Lösungen in die Praxis umzusetzen, und einen offenen unbehinderten Wettbewerb, in dem sich die besten Sicherheitslösungen auch durchsetzen können.

Bevor aber die Politik handelt, können Sie schon etwas unternehmen. Beispielsweise beherzigen, was Sie auf www.bsi-fuer-buer.de finden.

Jörn Müller-Quade,
Professor für Kryptografie und Sicherheit,
Karlsruhe

Korrespondenzadresse:

Prof. Dr. Jörn Müller-Quade
Karlsruher Institut für Technologie (KIT)
Institut für Theoretische Informatik (ITI)
Am Fasanengarten 5, Geb. 50.34
D-76131 Karlsruhe
Tel.: 0721-608-44205
Fax: 0721-608-55022
crypto-info@iti.kit.edu