INFIZIERTES

NETZ

INFIZIERTES NETZ

VIRTUELLE KRANKMACHER

VINCENT HEUVELINE

Kennen Sie das auch? Der Computer wird immer langsamer, kryptische Fehlermeldungen tauchen auf, und mitten im Vorgang stürzt der Rechner ab. Schuld ist wahrscheinlich ein Virus. Wie sein biologisches Vorbild infiziert ein Computervirus seinen Wirt, benutzt dessen Ressourcen und schädigt ihn. Heidelberger Wissenschaftler untersuchen, wie weit die Analogie zur Biologie reicht und mit welchen Maßnahmen Rechner vor Viren geschützt werden können.

Wo hört Leben auf, wo fängt Leben an? Diese Frage beschäftigt die Menschheit seit jeher. Der französische Chemiker und Mikrobiologe Louis Pasteur (1822–1895) etwa war davon überzeugt, dass die molekulare Asymmetrie organischer Verbindungen in irgendeiner Weise mit dem Leben zusammenhängt. Auch zahlreiche weitere, nicht weniger bedeutende Wissenschaftler und Philosophen haben sich intensiv mit dieser Frage befasst. Ihre unterschiedlichen Thesen verweisen auf die Schwierigkeit, die Grenzen des Lebens zu definieren.

Vor diesem Hintergrund ist es nicht überraschend, dass auch Computern, die uns im tagtäglichen Handeln ständig begleiten, Eigenschaften lebender Organismen zugewiesen werden. Ist die Information, die in einem Silizium-Chip organisiert und gespeichert ist, weniger lebendig als die der DNA-Doppelhelix in unseren Genen? Ist das Virus, das sich nur innerhalb einer geeigneten Wirtszelle vermehren kann und weder über eine eigenständige Replikation noch über einen eigenen Stoffwechsel verfügt, lebendiger als ein Computer-Programm? Sowohl die Grauzonen, die mit diesen Fragen einhergehen, als auch die immer stärkere Durchdringung unseres Alltags durch den Computer führen zu einer Art Personifikation des Rechners. Vervollständigt wird dieses Bild durch die Entwicklung von Robotern mit künstlichen „Sinnesorganen“ und Gliedern, die in der letzten Dekade einen bemerkenswerten Sprung gemacht hat. Die semantische Übertragung des klassischen Virus-Begriffes aus der Biologie auf den Computervirus scheint in diesem Kontext nicht nur naheliegend – sie stellt auch einen weiteren Beleg dafür dar, wie sich die Rolle des Computers in unserem Leben und in unserer Gesellschaft gewandelt hat.

Der infizierte Computer

Ein Computervirus ist ein sich selbst verbreitendes Programm, das Veränderungen am Status der Hardware, am Betriebssystem oder an weiterer Anwendungssoftware vornehmen kann, ohne dass diese vom Anwender kontrollierbar sind. Wie sein biologisches Vorbild benutzt das Virus die Ressourcen seines Wirtes, des Computers. Es kann sich selbst reproduzieren, indem es Kopien von sich erzeugt, und es kann sich in bestehenden Programmen

PROF. DR. VINCENT HEUVELINE wurde im Jahr 2013 an das Interdisziplinäre Zentrum für Wissenschaftliches Rechnen (IWR) der Universität Heidelberg berufen, an dem er sich 2002 im Fach Informatik habilitiert hatte. Zeitgleich mit seinem Ruf an die Ruperto Carola übernahm er die Leitung des Universitätsrechenzentrums. Zuvor forschte und lehrte der gebürtige Franzose neun Jahre an der Universität Karlsruhe, wo er ebenfalls zunächst die Ko-Leitung, später die Leitung des dortigen Rechenzentrums innehatte. Zu seinen Forschungsschwerpunkten zählen wissenschaftliches Rechnen, insbesondere unter Verwendung von Hochleistungsrechnern mit Anwendungen in der Medizin, Uncertainty Quantification (UQ), Hardware-aware Computing, Energieeffizienz für IT-Infrastruktur, Cloud Computing und IT-Sicherheit.

Kontakt: vincent.heuveline@urz.uni-heidelberg.de

gleichsam einer biologischen Infektion einpflanzen. Dadurch werden Datenträger wie Festplatten und Wechselmedien wie USB-Sticks „infiziert". Durch das Handeln des Benutzers, zum Beispiel, indem er ein infiziertes Wechselmedium an ein anderes System anschließt, gelangt das Virus von einem Computer zum nächsten.

Es sind allerdings nicht nur Viren, die Rechner „befallen" – Schuld können auch sogenannte Computerwürmer und Trojanische Pferde sein. In der Umgangssprache wird der Ausdruck Computervirus für alle drei Formen der Schadsoftware verwendet, da sie in ihren Auswirkungen für den Anwender kaum zu unterscheiden sind. Viren, Würmer und Trojanische Pferde variieren jedoch wesentlich in ihrem Modus Operandi. Computerviren sind die älteste Art der Schadprogramme und lassen sich anhand der Methode kategorisieren, mit der sie einen Computer infizieren: Dateiviren, Bootsektorviren, Makroviren und Skriptviren. Computerwürmer dagegen sind in der Lage, sich ohne Wirtsprogramm, das heißt allein mit ihrem Maschinencode, auszuführen und zu verbreiten. Würmer können sich also direkt über das Internet verbreiten und entsprechend in andere Computer eindringen.

Das Universitätsrechenzentrum (URZ)
Das Universitätsrechenzentrum (URZ) ist der zentrale IT-Dienstleister der Universität Heidelberg in allen Belangen der Informations- und Kommunikationstechnik. Es bietet Zugriff auf ein breites Spektrum an IT-Serviceleistungen und betreut den Einsatz dieser Dienste. Zudem ist das URZ zuständig für die IT-Sicherheit an der Universität und gewährleistet die Verfügbarkeit von Daten, Diensten und Anwendungen sowie die Integrität und Vertraulichkeit der damit einhergehenden Daten. Unter der Leitung von Prof. Dr. Vincent Heuveline arbeiten im Rechenzentrum rund 90 Mitarbeiterinnen und Mitarbeiter.

Als IT-Innovationsträger setzt sich das URZ zudem für zukunftsweisende Technologien ein und unterstützt damit die Forschung der Heidelberger Wissenschaftler. Eckpfeiler dieser Aktivitäten sind unter anderem Projekte, in deren Mittelpunkt die Energieeffizienz der IT-Infrastruktur und das Cloud Computing stehen, mit dem flächendeckend ein virtualisiertes Serverkonzept für Institute ausgebaut wird. In Kooperation mit Forschungseinrichtungen und mit der Industrie sowohl auf Landesebene als auch auf nationaler und internationaler Ebene trägt das Rechenzentrum dazu bei, die Rahmenbedingungen im IT-Bereich für Forschung und Lehre fortwährend zu verbessern.

www.urz.uni-heidelberg.de

„Ist die Information, die in einem Silizium-Chip organisiert und gespeichert ist, weniger lebendig als die der DNA-Doppelhelix in unseren Genen?"

Ein Trojanisches Pferd – umgangssprachlich auch Trojaner genannt – kombiniert stets ein nützliches Wirtsprogramm mit einem bösartigen Code, zum Beispiel einem angehängten Virus. Vom klassischen Computervirus unterscheidet sich ein Trojanisches Pferd, indem es nicht die Eigenschaft besitzt, sich selbstständig zu reproduzieren und zu verbreiten. Durch die Infektion des Wirtsprogramms lädt es beim Programmstart unbemerkt den dort versteckten Virus in das System. Somit werden Trojanische Pferde allgemein als Mittel zur Verbreitung von Viren eingesetzt. Trojaner nehmen inzwischen den größten Teil der Schadprogramme – auch Malware genannt – ein. Schätzungen gehen von folgender Verteilung aus: Trojanische Pferde 70 Prozent, Computerviren 16 Prozent und Computerwürmer acht Prozent.

Das Spektrum an Manipulationsmöglichkeiten durch Schadprogramme ist quasi unbegrenzt – ebenso die damit einhergehenden Bedrohungsszenarien:
- Ausspähen von sensiblen Daten wie Passwörtern, Kreditkartennummern und Kontonummern
- Überwachung aller Benutzeraktivitäten mithilfe von sogenannten Sniffern und/oder von Keyloggern, die die Eingaben des Benutzers an der Tastatur aufzeichnen
- Fernsteuerung des Rechners, um Werbe-E-Mails und Spams zu versenden, aber auch zur Bildung von Botnetzen, das heißt einer großen Anzahl infizierter Rechner, die gemeinsam konzertierte Angriffe im Internet ausführen können
- Deaktivierung der Schutzmechanismen des Computers wie zum Beispiel des Antivirenprogramms oder der Firewalls
- Umleiten des Benutzers auf gefälschte Webseiten, um mit erhaltenen Daten eine Kontoplünderung zu begehen – das sogenannte Phishing
- Benutzung der eigenen Speicherressourcen zur Ablage von illegalen Dateien, die dann für andere Internet-Nutzer zur Verfügung gestellt werden
- Verschlüsselung der lokalen Benutzerdaten und Erpressung der Benutzer, den unbekannten Schlüssel nur gegen ein „Lösegeld" mitzuteilen; normalerweise kommt trotz Zahlung kein Schlüssel, und wertvolle Daten sind dann unwiederbringlich verloren

Exponentielles Wachstum
Viren aller Couleur verbreiten sich vorwiegend über E-Mails oder über getarnte Programme auf Internetseiten. Verlässliche Zahlen zu Risiken und Angriffen durch Computerviren sind leider Mangelware. Man nimmt jedoch an, dass die Infektion durch Schadprogramme inzwischen die größte Gefahr für die IT-Infrastruktur von Unternehmen darstellt. Der Faktor „Irrtum und Nachlässigkeit des Nutzers" wurde damit auf Platz zwei verdrängt. An der Spitze der Infektionswege scheint derzeit die E-Mail noch vor entsprechend präparierten Internetseiten zu stehen. Auch wenn ihre genaue Zahl nicht belastbar ermittelt werden kann, geht man davon aus, dass weltweit über 20 Millionen Schadprogramme existieren. Das exponentielle Wachstum dieser Zahl ist unter anderem auf sogenannte polymorphe Viren zurückzuführen. Diese Art von Computerviren ändert automatisch ihre Gestalt von Generation zu Generation, sodass zahlreiche, teilweise vollkommen verschiedene Varianten entstehen. Schon heute ist es praktisch unmöglich, die große Zahl der sich schnell ändernden Schadprogramme durch Antiviren-Software in vollem Umfang zu erkennen.

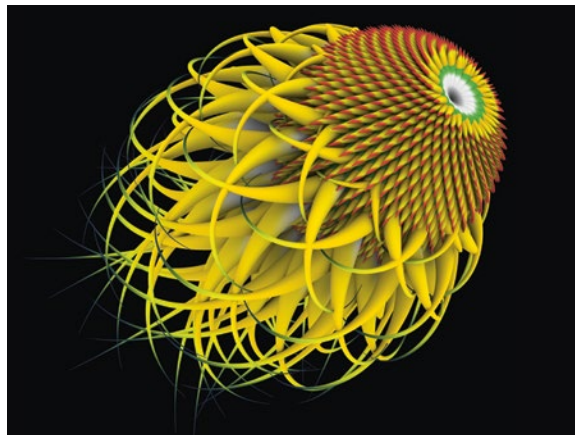
„Ein Computervirus kann sich selbst reproduzieren, indem es Kopien von sich erzeugt, und es kann sich in bestehenden Programmen gleichsam einer biologischen Infektion einpflanzen."

Das hohe Ausmaß der Gefährdung, die von Computerviren ausgeht, legt die Frage nahe, aus welcher Motivation heraus Entwickler diese Art von Schadprogrammen implementieren. Folgende Klassifizierung hat sich hierfür bewährt, die auch bei der kriminalistischen Verfolgung sogenannter Hacker-Angriffe verwendet wird:
- Soziale Motivation: Der Betroffene möchte zu einer bestimmten Hacker-Gruppierung gehören und durch mehr oder weniger spektakuläre Entwicklungen Aufmerksamkeit erregen.
- Technische Motivation: Durch entsprechende Hacks sollen Fachwelt und Öffentlichkeit auf Sicherheitslücken aufmerksam gemacht werden.
- Politische Motivation: Hier wird aus politischen Motiven agiert, auch um Aufmerksamkeit in den Medien zu bekommen.
- Finanzielle Motivation: Entwickler dieser Gruppe möchten sich persönlich bereichern, zum Beispiel über Wirtschaftsspionage oder Finanzbetrug.
- Staatlich-politische Motivation: Entwickler handeln im Auftrag einer Regierung oder staatlicher Institutionen. Typischerweise stehen dann andere Regierungen aber auch Unternehmen anderer Länder im Fokus.

Schutzmaßnahmen gegen Viren
Neben der Verwendung von Antiviren-Software, die Schadprogramme aufspüren, blockieren und beseitigen soll, gibt es zahlreiche weitere Maßnahmen, die vor derartigen Angriffen schützen können. Ihr vorrangiges Ziel ist es, die Datenintegrität, die Vertraulichkeit und die Verfügbarkeit der Daten zu gewährleisten.

Für den sicheren und rechtskonformen Betrieb der IT-Dienste an der Universität Heidelberg arbeitet am Universitätsrechenzentrum (URZ) eine Arbeitsgruppe von EDV-Sicherheitsfachleuten, die bei unmittelbaren Sicherheitsvorfällen die nötigen Schritte – einen sogenannten Incident Response – einleiten kann. Darüber hinaus implementieren wir proaktiv einen Katalog spezifischer Maßnahmen, um vor Missbrauchsfällen der Rechnersysteme und des Datennetzes zu schützen. Akute Bedrohungen sollen zeitnah erkannt und eingeordnet werden können. Neben dem klassischen und sehr aufwendigen Betrieb von Spamfiltern setzen wir unter anderem ausgefeilte Konzepte für Netzsicherheitssysteme ein, die verschiedene Schutzstufen entsprechend dem benötigten Sicherheitslevel vorsehen. Eine Überwachung des Verkehrsdatenstroms auf Angriffsmuster ermöglicht es uns zudem, schadhafte Datenpakete rechtzeitig zu identifizieren und zu entfernen.

Insgesamt verfolgt das Universitätsrechenzentrum die Entwicklung eines ganzheitlichen und fächerübergreifenden Ansatzes für die IT-Sicherheit. Unsere Forschung adressiert dabei nicht nur technische, sondern auch gesellschaftliche Fragestellungen. In einem interdisziplinären



Visualisierung eines MSNthreat-Trojaners auf Basis seines informatischen Codes, © Alex Dragulescu, www.sq.ro

„Die größte Gefahr für die IT-Infrastruktur von Unternehmen geht inzwischen von Schadprogrammen aus – nach dem Faktor ‚Irrtum und Nachlässigkeit des Nutzers‘.“

Netzwerk, dem neben Informatikern und Mathematikern auch Wissenschaftler der Juristischen Fakultät und des Instituts für politische Wissenschaft angehören, untersuchen wir Strategien und Politiken der Cybersicherheit aus rollentheoretischen Perspektiven sowie das Verhältnis von Internettechnologie und Grundrechten. Dabei wird insbesondere die Interaktion der derzeit vorhandenen technischen Möglichkeiten mit den rechtlichen Rahmenbedingungen erörtert.

Das Ende einer Ära

Die Analogie der Computerviren zu biologischen Viren kommt bis dato nur teilweise zum Tragen. Ein Hauptgrund liegt darin, dass Computerviren fast durchweg absichtsvoll von menschlicher Hand erzeugt werden und nicht in der Lage sind, zu „mutieren“. Die derzeitigen technologischen Entwicklungen im IT-Bereich könnten jedoch zu einem Paradigmenwechsel führen. Allgemein werden Computer als deterministische Maschinen vorausgesetzt: Zu jedem Zeitpunkt ergibt sich der Folgeschritt des ausgeführten Programms eindeutig aus den Eingabedaten und dem zugrunde liegenden Algorithmus. Der Computer, der nur 0 und 1 „versteht“, hat keinen freien Willen, mit dem er einen Flüchtigkeits- oder Denkfehler begehen könnte. Was aber passiert, wenn der Rechner aufgrund externer Bedingungen, zum Beispiel der kosmischen Strahlung, immer wieder zufällig von 0 nach 1 oder von 1 nach 0 schaltet?

„Schon heute ist es praktisch unmöglich, die große Zahl der sich ständig ändernden Schadprogramme in vollem Umfang durch Antiviren-Software zu erkennen.“

Die zunehmende Dichte der integrierten Schaltkreise, auf denen Computer basieren, macht solche Fehler – „Bit Flips“ genannt – immer wahrscheinlicher. Auch wenn Maßnahmen getroffen werden können, die bis zu einem gewissen Grad eine Fehlertoleranz ermöglichen, scheint die Ära des Rechners als deterministische Instanz Schritt für Schritt zu Ende zu gehen. Zwar sind solche Überlegungen noch sehr spekulativ, dennoch ist vorstellbar, welche Auswirkungen Computer mit stochastischen Eigenschaften auf die Entstehung und mögliche Zerstörung von Viren haben könnten. Insbesondere angesichts der ungeheuren Rechenleistung heutiger Supercomputer rückt die Vision näher, dass sich Computerviren durch Mutationen, die das zufällige Verhalten des Rechners hervorruft, „evolutionär“ entwickeln werden.

THE INFECTED NETWORK

VIRTUAL GERMS

VINCENT HEUVELINE

We're all familiar with this scenario: The computer grows increasingly sluggish, displays cryptic error messages, and finally crashes mid-process. The culprit is probably a virus that has infected the computer. A computer virus is a self-propagating programme that, like its biological counterpart, uses the resources of its host and damages the host in the process. It changes the status of the hardware, operating system or other application software in ways that cannot be controlled by the user. The virus can reproduce by making copies of itself, and it can embed itself in existing software in a manner similar to a biological infection. It is assumed that there are more than 20 million malware programmes worldwide. Already it is impossible to detect every one with antivirus software in real time.

Experts at the Heidelberg University Computing Centre implement numerous proactive measures to protect their systems against malware. Their primary goal is to ensure the integrity, privacy and availability of the data. Acute threats must be identified and analysed quickly. In their research, the scientists address social as well as technical issues. An interdisciplinary network of computer scientists, legal experts and political scientists investigates cyber security strategies and policies from a role theory perspective and the relationship between internet technology and fundamental rights. ●

PROF. DR VINCENT HEUVELINE accepted a chair at Heidelberg University's Interdisciplinary Center for Scientific Computing (IWR) in 2013, the same institute where he completed his habilitation in computer science in 2002. Also in 2013, he became director of the university's Computing Centre. Heuveline, who is French by birth, previously held a teaching and research position at Karlsruhe University for nine years, where he was also co-director, and later sole director, of the computing centre. His research interests include scientific computing, particularly using supercomputers for medical applications, uncertainty quantification (UQ), hardware-aware computing, energy-efficient IT infrastructures, cloud computing and IT security.

Contact: vincent.heuveline@urz.uni-heidelberg.de

"A computer virus can reproduce, i.e. make copies of itself, and it can embed itself in existing software in a manner similar to a biological infection."

„Die Ära des Rechners als deterministische Instanz scheint Schritt für Schritt zu Ende zu gehen. Fehler werden immer wahrscheinlicher.“

Computerviren – und allgemeiner Schadprogramme – tragen wie biologische Viren Namen, die gleichermaßen bedrohlich wie faszinierend anmuten: Blaster, Code Red, Conficker, ILoveYou, Melissa, MyDoom, Sasser, Slammer, Stuxnet. Weniger bekannt für Computerviren ist ihre mögliche Visualisierung, die sich an biologische Abbildungen wie die weltberühmte Darstellung des Influenzavirus anlehnt. Künstler und Wissenschaftler haben hierzu Verfahren entwickelt, die Viren, Trojanern und Würmern auf Basis ihres informatischen Codes und mithilfe statistischer Auswertung der generierten Daten Gestalt verleihen (siehe Abbildung Seite 103). Die resultierenden 3D-Bilder wirken wie künstliche Organismen, die in ihrer Schönheit ihren biologischen Pendants in nichts nachstehen. ●

Herausgeber
Universität Heidelberg
Der Rektor
Kommunikation und Marketing

Wissenschaftlicher Beirat
Prof. Dr. Peter Comba (Vorsitz)
Prof. Dr. Beatrix Busse
Prof. Dr. Markus Hilgert
Prof. Dr. Marcus A. Koch
Prof. Dr. Carsten Könneker
Prof. Dr. Alexander Marx
Prof. Dr. Manfred G. Schmidt
Prof. Dr. Joachim Wambsganß

Redaktion
Marietta Fuhrmann-Koch
(verantwortlich)
Ute von Figura (Leitung)
Claudia Eberhard-Metzger

Gestaltung und Reinzeichnung
KMS TEAM GmbH, München

Druck
ColorDruck Solutions GmbH, Leimen

Auflage
6.000 Exemplare

ISSN
0035-998 X

Vertrieb
Universität Heidelberg
Kommunikation und Marketing
Grabengasse 1, 69117 Heidelberg

Tel.: +49 6221 54-19026
kum@uni-heidelberg.de

Das Magazin kann kostenlos unter oben genannter Adresse abonniert werden.

Im Internet ist es verfügbar unter www.uni-heidelberg.de/rupertocarola.