Die dümmsten User und schlechte Software

Die meisten IT-Sicherheitssysteme funktionieren nicht wie gewünscht, weil Entwickler anders ticken als Anwender, meint der Verschlüsselungsexperte Peter Gutmann. Die Psychologie müsste beim Programmieren stärker berücksichtigt werden.

Robert Prazak

Wien – Phishing-Mails, Identitätsdiebstahl, falsche Shoppingportale, Malware, Spam, Viren: Im Internet lauern sowohl bei beruflicher als auch bei privater Verwendung vielfältige Gefahren. IT-Administratoren, Programmierer, Virenschutzverkäufer und andere Experten tun zwar einiges, um bei der Abwehr schädlicher Programme und bösartiger Geschäftemacher zu helfen, doch dabei sind sie sich manchmal selbst im Weg.

„Die Einstellung der Entwickler ist doch: User sind Idioten", sagt Peter Gutmann. Der Computerwissenschafter der Universität Auckland (Neuseeland) gilt als einer der weltweit profiliertesten Experten für Verschlüsselung; er hat unter anderem bei der Entwicklung der Verschlüsselungssoftware PGP 2.0 mitgearbeitet und eine nach ihm benannte Methode zur Löschung von Daten auf Speichermedien wie Festplatten entwickelt.

Nun hat sich Gutmann allerdings einer schwierigeren, weil unberechenbaren Seite der IT-Sicherheit zugewandt, nämlich dem Faktor Mensch. Im Rahmen der Campus Lectures des Fachhochschule Campus Wien erläuterte Gutmann auf Einladung des Kompetenzzentrums für IT-Security die Psychologie der IT-Unsicherheit. Bisher läuft es laut Gutmann nämlich so ab: Entwickler bauen Sicherheitsapplikationen, die Anwender verwenden sie nicht korrekt und daher sind die Anwender aus dem Blickwinkel der Experten unfähig. „Die User handeln irrational, zumindest nach Ansicht der Entwickler", sagt Gutmann.

Tatsächlich verhält sich nicht nur der vielzitierte „dümmste anzunehmende User" auf eine Art und Weise, die IT-Profis beunruhigt – gar die Mehrheit der Computernutzer klickt Warnfenster weg, lässt sich auf augenscheinlich gefälschte Sites locken und ignoriert Update-Aufforderungen. Und weshalb? Weil sie es nicht anders gewohnt sind und sich so verhalten, wie sie es sonst auch tun.

Studien zeigen, dass unter Druck nicht lange überlegt wird, sondern die erstbeste Möglichkeit gewählt wird. Gutmann nennt als Beispiel die Tierwelt: Wenn ein Affe von einem Löwen attackiert wird, überlegt er nicht lange, welcher Baum der höchste und stärkste ist, sondern klettert kurzentschlossen auf den erstbesten. Genauso handeln Menschen, selbst wenn es nur um Warnhinweise am Bildschirm geht, die ihnen zum Beispiel erklären wollen, dass diese Seite unsicher sein könnte. Sie wählen die erstbeste, von ihrer Intuition eingegebene Möglichkeit – also das Wegklicken lästiger Fenster .

Foto: EPA / Malte Christians

Die Mehrzahl der Computernutzer weiß nicht, welche Sicherheitsmängel bestehen, meint Peter Gutmann. Zudem gebe es falsche Vorstellungen von Internetbetrügern. Im Bild: ein Hackerkongress in Hamburg.

Lücken bleiben unbemerkt

Dazu kommt: Entscheidungen, die sofortiges Feedback bewirken, werden leichter getroffen als jene, deren Auswirkungen in zeitlicher Ferne liegen. Gerade bei Sicherheitsthemen gibt es laut Gutmann in den meisten Fällen aber keine unmittelbare Auswirkung einer Handlung: Wenn Kreditkartendaten gestohlen wurden, merkt man das oft erst nach einigen Wochen; in vielen Fällen bleiben Lücken im Sicherheitssystem gänzlich unbemerkt. Daher kann nicht beurteilt werden, wann und ob sich die Entscheidung überhaupt auswirken wird.

Dazu kommt: Offensichtlich irrelevante Dinge werden herausgefiltert – und dazu könnte die x-te Update-Aufforderung seitens des Computers zählen. Schließlich weiß die Mehrzahl der Computernutzer gar nicht, welche Sicherheitsmängel gerade vorhanden sind. Und wenn es um Internetbetrüger geht, denken die wenigsten an Programme, die selbstständig ihre Arbeit verrichten, sondern an zwielichtige Gestalten, die mit Panzerknackeroutfit in die Tastatur hämmern – gefördert werden solche Bilder nicht nur von Hollywood, sondern auch von den ewig gleichen Sujets in den Medien.

Die Psychologie liefere also Einsichten, wie Menschen denken und entscheiden. Wie kann das aber für die IT-Sicherheit genutzt werden? „Es gibt unzählige relevante Psychologiestudien, diese könnten bei der Entwicklung von Sicherheitssystemen verwendet werden", sagt Peter Gutmann dem STANDARD gegenüber.

Geeks denken anders

Ein Beispiel sei das Sicherheitsschloss in der Browser-Leiste: Fehlende Informationen werden Studien zufolge viel schwieriger verarbeitet als positive Informationen. Das bedeutet, dass das Fehlen dieses Browser-Symbols eine denkbar schlechte Möglichkeit sei, den Mangel an Sicherheit darzustellen, meint Gutmann: „Viel dümmer hätte man das nicht machen können."

Ein weiteres Beispiel: Bei Windows-Vista-Warnfenstern wurden in verschiedenen Situationen unterschiedliche Farben verwendet – nicht einmal erfahrenen Usern ist das aufgefallen. „Das Problem: Die Geeks, die Computersoftware entwerfen, denken nicht wie andere Menschen", meint Gutmann. „Weil diese beiden Gruppen auf unterschiedliche Weise Entscheidungen treffen, funktionieren viele Sicherheitssysteme nicht."

Wenn Sicherheitssysteme versagen, dann handelt es sich nach Ansicht von Gutmann um „schlecht designte Software, nicht um dumme User". Daher sollten beim Entwickeln öfters Menschen von außerhalb der Programmiersphäre herangezogen werden. „Die Entwickler sollten einfach die Leute machen lassen und nur zusehen, dann bemerken sie selbst, welche Fehler ihre Systeme haben." Die evolutionäre Konditionierung der User sollte nicht als Bug gesehen werden, sondern als Chance.

Sollte aber nicht gleichzeitig die Alarmbereitschaft bei den Anwendern erhöht werden, um sie zum längeren Nachdenken zu zwingen? Davon hält Gutmann nichts, denn „wenn es keine ausreichenden Antworten auf Bedrohungen gibt, ist das ohnehin sinnlos". Eine akute Bedrohung ist für ihn übrigens die aktuelle Entwicklung des Internets der Dinge, in dem smarte Gegenstände in einem Netzwerk zusammengeschlossen werden. Für Gutmann sollte dieses eher „Internet of Targets" heißen. Ebenso ist für ihn die steigende Verwendung von Mobilgeräten sicherheitstechnisch bedenklich: „Die Sicherheit bei Android-Geräten ist furchtbar."

Routinejobs für Roboter in der vernetzten Fabrik

In einer neuen Lern- und Forschungsfabrik an der FH Technikum Wien wird Industrie 4.0 erprobt

Wien – Der kleine Roboter bleibt stehen, als sich ihm plötzlich ein Hindernis in den Weg stellt. Nach kurzem Zögern umrundet er den menschlichen Kollegen aber und setzt seine Arbeit fort: Selbstständig holt er sich Teile von einer Werkbank und transportiert sie zu einer anderen. „Werden die Roboter so programmiert, dass sie den Weg finden, ist das Industrie 3.0. Wenn sie den Weg ganz von allein finden, ist es Industrie 4.0", sagt Corinna Engelhardt-Nowitzki vom Institut für Advanced Engineering Technologies der Fachhochschule Technikum Wien. Dort wurde kürzlich eine digitale Fabrik eröffnet, in der die theoretischen Möglichkeiten von Industrie 4.0 in die Forschungs- und Lehrpraxis übertragen werden sollen. Dabei werden Produktionsabläufe digital vernetzt, Maschinen kommunizieren selbstständig miteinander.

Ob menschliche Mitarbeiter in Zukunft nur noch eine Randerscheinung oder gar ein Hindernis sind, wird derzeit heftig diskutiert: Werden durch weitreichende Automatisierung Jobs wegfallen, ersetzt oder gar neue geschaffen? Bei der Eröffnung der digitalen Fabrik im Erdgeschoß eines Wohnturms auf dem Höchstädtplatz übte man sich in Zweckoptimismus. So betonte Lother Roitner, Geschäftsführer des Fachverbands der Elektro- und Elektronikindustrie und Obmann der FH Technikum, dass die neuen Möglichkeiten in Österreich 40.000 neue Jobs schaffen könnten. Es wird sich weisen, ob im Gegenzug nicht viele andere wegfallen.

Unumstritten ist, dass der Trend vor Österreich nicht haltmacht und entsprechend ausgebildete Fachkräfte mehr Chancen haben. In der neuen Minifabrik in Wien ist menschliches Zutun noch unverzichtbar, denn die Arbeit der Roboter leidet bisweilen an Kinderkrankheiten. Sind diese aber überwunden, sollen Roboter Routineaufgaben weitgehend selbstständig meistern. „Der Mensch bleibt allerdings dort unverzichtbar, wo Kreativität gefragt ist", sagt Engelhardt-Nowitzki.

Praxisnahe Ausbildung

Dieses Zusammenspiel von Mensch, Maschine und Software soll in der neuen Lehr- und Forschungsfabrik auf dem Höchstädtplatz erprobt werden. Unternehmen haben für deren Ausstattung insgesamt rund eine Million Euro ausgegeben; Firmen wie Siemens, ABB und Festo sind an einer Zusammenarbeit bei Ausbildung und Forschung interessiert. Die Verzahnung zwischen FH und Wirtschaft ist auch personeller Natur: Kurt Hofstädter ist Vorstandsmitglied von Siemens Österreich und sitzt sowohl im Vorstand der FH Technikum als auch in jenem der Plattform Industrie 4.0, bei der Verkehrsministerium, Industrieverbände und Arbeitnehmervertreter einen gemeinsamen Weg finden wollen. Für Hofstädter ist es wichtig, Studierenden gute Infrastruktur zu bieten, auch um Absolventen den raschen Einstieg ins Unternehmen zu ermöglichen.

Vergangenen Sommer wurde in der Seestadt Aspern eine Pilotfabrik für Industrie 4.0 eröffnet. Die Technische Uni Wien werkt dort in Kooperation mit Firmen wie Bosch, SAP und Siemens an entsprechenden Forschungsprojekten. Zwar sollen keine kommerziellen Produkte erzeugt werden, doch die rund 15 Wissenschafter untersuchen unter anderem, wie die Serienfertigung der Zukunft aussehen könnte – etwa maßgeschneiderte Prothesen. Die Kosten der Pilotfabrik von vier Millionen Euro werden zur Hälfte vom Verkehrsministerium getragen.

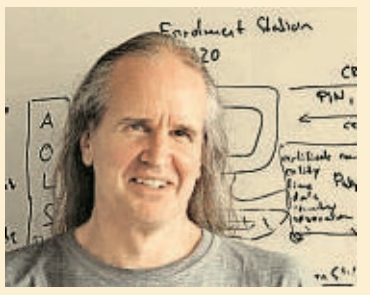
Erich Markl, dem Leiter des Instituts für Advanced Engineering Technologies der FH Technikum Wien, zufolge kommt man sich gegenseitig nicht ins Gehege: „Unsere digitale Fabrik ist industriefinanziert und daher stehen reine Industrieanwendungen im Vordergrund." Zudem würde man auch für Klein- und Mittelbetriebe passende Anwendungen probieren.

Eine Spezialität der digitalen Fabrik der FH Technikum Wien ist die Verbindung realer Produktionsabläufe mit deren digitaler Simulation. Dadurch sollen die einzelnen Produktionsschritte variabel bleiben: Wenn ein Fertigungsschritt wegen hoher Auslastung nicht möglich ist, könnte ein anderer vorgezogen werden.

Neue Sicherheitsstandards

Durch die Vernetzung der Maschinen über das Internet soll eine „technologische Austauschbarkeit" erreicht werden: Unternehmen können sich gegenseitig aushelfen, indem sie dringende Aufträge rasch übernehmen und beispielsweise bei Produktionsproblemen oder steigender Nachfrage Teile der Fertigung anderen übertragen. Bei dieser Vernetzung der Maschinen und in weiterer Folge der Endprodukte spielt die Sicherheit eine große Rolle – theoretisch könnte versucht werden, auf Teile der Produktion von außen zuzugreifen.

Laut TÜV Austria gibt es in dieser Hinsicht Aufholbedarf, nicht nur was die IT-Sicherheit betrifft: Auch die Sicherheit der Menschen in der Fabrik der Zukunft erfordert Forschungsarbeit. Die entsprechenden Normen und Standards müssen nach und nach adaptiert werden. In der digitalen Fabrik der FH Technikum soll auch das erprobt werden. Dass die Roboter den Menschen derzeit noch ausweichen, scheint ein gutes Zeichen zu sein. (rp)



Peter Gutmann ist Informatiker an der Universität Auckland.

Foto: privat