2017/21 Thema

https://shop.jungle.world/artikel/2017/21/die-monokultur-ist-schuld

Was lernen wir daraus? Über die Folgen des globalen Hacker-Angriffs

Die Monokultur ist schuld

Von **Enno Park**

Was bedeutet der Angriff mit Ransomeware für das digitale Verhalten der User? Wie viel Sicherheit ist im Netz überhaupt erreichbar? Antivirenprogramme allein können nicht die Lösung sein.

Nachdem die Schadsoftware einer kriminellen Hackergruppe mehr als 200 000 Rechner weltweit außer Gefecht gesetzt hatte, unter anderem Computersysteme von Krankenhäusern und Anzeigetafeln von Bahnen sowie Kassenautomaten, begann die Suche nach den Schuldigen – und das sind nicht nur die Hacker. In den vergangenen zwei Wochen wurden auch Microsoft und die NSA für den Angriff mitverantwortlich gemacht. Generell, da sind sich viele Kommentatoren und Experten sicher, seien aber ganz besonders die Nutzerinnen und Nutzer selbst schuld, wenn sie keine Sicherheitsupdates auf ihre Systeme einspielen. Dabei ist die Frage, wie die Wannacry-Attacke passieren konnte, und vor allem, wie sich ein solcher Angriff in Zukunft vereiteln ließe, komplexer, als die Schuldzuweisungen vermuten lassen.

> Antiviren-Software wird kritisiert, weil sie oft mehr Sicherheitslücken enthält, als das System, das sie schützen soll.

Ist ein Windows-PC mit einem Virus befallen, liegt nach gängiger Meinung die Verantwortung bei den Nutzerinnen und Nutzern selbst. Wer ist schließlich so dumm, auf Links in Spammails zu klicken? Diese aber kommen mittlerweile so echt daher, dass auch Profis leicht ein falscher Klick unterlaufen kann. Es gibt noch genug Menschen, die keine Ahnung von den Gefahren des Netzes haben und mit einem uralten PC arbeiten, auf dem Windows XP läuft. Woher sollen sie auch das nötige Fachwissen in Sachen digitaler Sicherheit nehmen? Das betrifft nicht nur Privatnutzer. Viele kleinere Firmen können sich oft nicht leisten, mit Rechnern neuester Generation zu arbeiten, und sind auf alte Kisten angewiesen, auf denen womöglich eigens entwickelte Spezialsoftware läuft. Diese funktioniert nur mit älterer Windows-Software oder benötigt Hardware, die nicht schnell genug ist für das neueste Windows ist. Krankenhäuser etwa benutzen ihre veralteten Rechner nicht aus Trantütigkeit, sondern weil ihnen schlicht die Mittel fehlen. Am Ende entscheiden die Controller, was weniger kostet. Der Virenbefall wird einfach in Kauf genommen und im Schadensfall wird ein Daten-Backup zurückgespielt.

Windows hat einen notorisch schlechten Ruf. Trotzdem läuft es auf etwa 90 Prozent aller PCs weltweit. Damit trägt Microsoft eine enorme Verantwortung und veröffentlicht deshalb

regelmäßig Sicherheitsupdates – so auch zum Schutz vor Wannacry. Vorwerfen kann man dem Konzern lediglich, dass es offenbar nicht zu dessen Prioritäten gehört, alte Versionen seiner Software zu pflegen. So brachte Microsoft den Patch für das 17 Jahre alte Windows XP viel zu spät heraus. Aber der nächste Schädling, der eine Lücke ausnutzt, die Microsoft noch gar nicht kennt, kommt bestimmt.

In dem Fall sollten eigentlich Antivirenprogramme helfen. Keines auf dem PC installiert zu haben, gilt zu Recht als grob fahrlässig. Allerdings konnte am 12. Mai, dem Tag, an dem der Angriff begann, kaum eines der einschlägigen Antivirenprogramme »Wannacry« entdecken. Nicht nur das: Die Epidemie konnte erst eingedämmt werden, nachdem bekannt geworden war, dass Wannacry sich nicht weiterverbreitet, sobald die Schadsoftware eine bestimmte Domain im Netz abfragen kann. Dies kam mehreren Antivirenprogrammen jedoch verdächtig vor. Sie unterbanden in vielen Fällen die Abfrage und ermöglichten damit erst, dass viele Rechner unbrauchbar wurden.
Tatsächlich wird Antivirensoftware mittlerweile kritisiert, weil sie oft mehr Sicherheitslücken enthält als das System, das sie schützen soll. Einige Experten empfehlen sogar, für Windows 10 auf ein zusätzliches Antivirenprogramm zu verzichten.

Dass Hacker Sicherheitslücken sammeln und verkaufen, wird sich nicht verhindern lassen. Allerdings spielen auch Geheimdienste auf diesem Markt eine große Rolle. Sie nutzen Sicherheitslücken, um in Computer einzudringen, die sie überwachen wollen, und sind deshalb gar nicht daran interessiert, dass diese Lücken geschlossen werden. Tatsächlich stammen wesentliche Teile von Wannacry von der NSA selbst, wo sie von Hackern erbeutet wurden. Regierungen verschlimmern die Situation zusätzlich: Mit immer neuen Überwachungsgesetzen sorgen sie dafür, dass IT-Riesen wie Apple und Microsoft immer mehr verschlüsseln. Beispielsweise findet die Kommunikation über Whatsapp mittlerweile verschlüsselt statt. Apple behauptet, seine iPhones so verschlüsselt zu haben, dass nicht einmal Apple selbst hinterher Daten herausholen kann. Das lässt staatlichen Ermittlungsbehörden, die jemanden überwachen wollen, nur einen Ausweg: sich in das Endgerät selbst zu hacken, um an der Quelle mitzuhören. Der Druck auf die Geheimdienste, Sicherheitslücken zu horten und ausnutzen, wächst also in den Maße, wie Überwachungsgesetze Leute dazu bringen, immer mehr zu verschlüsseln.

In Deutschland tut man so, als gäbe es in der IT-Welt nicht schon genug Sicherheitsprobleme: Die große Koalition plant für die kommenden Monate eine Verschärfung der Sicherheitsgesetze. Werden die Pläne umgesetzt, dürfen Ermittler den sogenannten Staatstrojaner zur Überwachung einsetzen und damit neue Sicherheitslücken schaffen.
Stark unterschätzt wird in der Debatte über die IT-Sicherheit die Rolle von Bitcoin. Die Digitalwährung erlaubt mit etwas Geschick anonyme Transaktionen rund um den Globus zu tätigen, ohne nennenswerte Kosten und in relativ kurzer Zeit. Ransomware wie Wannacry, die die Festplatten der angegriffenen Rechner verschlüsselt und dann ein Lösegeld verlangt, ist erst in großem Stil aufgekommen, seit es Bitcoin gibt. Vorher war Erpressung dieser Art wegen des Problems der Geldübergabe schlicht zu riskant und aufwendig.

Allerdings lässt sich Bitcoin nicht einfach so verbieten oder regulieren. Eine Nutzung im Untergrund wird immer möglich bleiben, genauso wie es immer Staaten geben wird, in denen sich Bitcoins ohne Kontrolle gegen andere Währungen eintauschen lassen.

Die Situation ist gründlich festgefahren. Bitcoins wieder verschwinden zu lassen, ist genauso unrealistisch wie die Hoffnung, Geheimdienste würden aufhören, Sicherheitslücken zu horten. Als naheliegende Lösung erscheint die Cloud. Wer keine Daten mehr auf dem eigenen PC hat, muss auch kein Lösegeld zahlen, wenn der PC von Ransomware verschlüsselt wird, sondern kann einfach von einem anderen Rechner auf die Cloud zugreifen. Die großen Cloud-Anbieter können große Sicherheitsteams unterhalten, die die Daten der Kunden vor Angriffen schützen. Dafür müssen die Anwender aber ein hohes Vertrauen in die Cloud-Anbieter aufbringen. Das haben alle schon einmal gemacht: Ihr Geld liegt auf einem Konto bei einer Bank, die als frühe Form der Cloud gesehen werden kann.

Selbst wenn Google & Co. das nötige Vertrauen entgegengebracht wird: Eine echte Lösung ist das nicht. So wie Banken zusammenbrechen können, ist es auch denkbar, dass ein großer Cloud-Anbieter eines Tages gehackt wird. Zudem verlagert sich die Gefahr: Statt in Rechner einzudringen, versuchen die Hacker dann eben, sich Login-Passwörter für die Cloud zu verschaffen.

Vielversprechender könnte daher ein anderer Weg sein: das Ende der Monokultur. Wer heute Linux oder Apple benutzt, ist vor Viren weitgehend sicher. Nicht, weil die Systeme überlegen sind, sondern weil sie wegen ihrer relativ geringen Verbreitung kein lohnendes Ziel für Hacker darstellen. Darin könnte der Schlüssel liegen: Würde das Quasimonopol von Microsoft durch eine Anzahl unterschiedlicher Systemen abgelöst, könnte ein Angriff nicht mehr dieselbe Wirkung erreichen. Dazu wäre es aber nötig, dass all diese Systeme gemeinsame Standards unterstützen, damit die Anwender zwischen ihnen wechseln und trotzdem ein und dieselbe Software nutzen können.