

„Das Internet ist offen – das ist seine größte Stärke und Schwäche“

TUD-Forscher Matthias Wählich über Gefahren im Netz und wie KI uns schützen soll.

Von Jana Mundus

Dresden. Wir alle nutzen das Internet wahrscheinlich täglich. Kommunizieren, einkaufen, informieren: Ohne Internet geht für viele von uns wohl kaum noch etwas. Doch es birgt Risiken. Und die Gefahren nehmen zu. Einer, der sich mit all dem bestens auskennt, ist Matthias Wählich von der TU Dresden.

„Professor Wählich, Sie leiten seit Mai 2023 den Lehrstuhl für Distributed and Networked Systems an der Fakultät Informatik der TU Dresden. Was reizt Sie persönlich an diesem Fachgebiet?“

Das Internet ist für mich das spannendste verteilte System, das es gibt. Es ist aus einem kleinen Experiment von Universitäten und Forschungsinstituten zu einer globalen Infrastruktur gewachsen, auf der heute fast alles aufbaut – Kommunikation, Handel, Transport, Energieversorgung, Gesundheitssysteme und mehr. Wenn wir das Internet abschalten würden, wäre es nicht nur still, vieles würde schlicht aufhören zu funktionieren. Mich reizt, dass dieses System trotz seiner Größe keine zentrale Steuerung hat und dennoch funktioniert. Es wächst mit der Zahl der Nutzer. Das ist beeindruckend, weil viele Grundprinzipien einfach und elegant sind.

Das Thema Sicherheit im Netz treibt heutzutage viele um. War es zur Geburtsstunde des Internets auch schon so?

Nein, überhaupt nicht. In den 1970er- und 80er-Jahren, als das Internet noch ein Zusammenschluss weniger Universitäten war, gab es zwar Fehler, aber kaum Angriffe. Die Teilnehmer kannten sich, man vertraute einander. Mit der Kommerzialisierung in den Neunzigern hat sich das verändert. Plötzlich gab es finanzielle Anreize für Kriminalität, später auch geopolitische Interessen. Heute ist das Internet selbst als kritische Infrastruktur eingestuft und damit leider auch ein attraktives Ziel für Angreifer aller Art.

Welche Angriffsarten sind aus Ihrer Sicht am gefährlichsten?

Manche sind sehr sichtbar, wie groß angelegte Denial-of-Service-Angriffe, bei denen Server durch massenhafte Anfragen überlastet werden. Das erleben beispielsweise regelmäßig auch Städte in Deutschland mit ihren Webseiten. Andere Angriffe laufen im Hintergrund und sind schwer zu erkennen. Zum Beispiel, wenn Angreifer die Wege manipulieren, über die Datenpakete durch das Netz reisen. Das kann dazu führen, dass der gesamte Verkehr für bestimmte Dienste umgeleitet wird, ohne dass Nutzer es bemerken. Auch Fehlkonfigurationen bei Netzbetreibern können gravierende Folgen haben, etwa wenn große Teile des Datenverkehrs unabsichtlich über fremde Netze geleitet werden.

Und dann gibt es noch die Klassiker wie Phishing ...



Matthias Wählich koordiniert an der TU Dresden ein großes Projekt zur Cybersicherheit. Die Forscher wollen KI einsetzen, um es Angreifern im Netz künftig schwerer zu machen.

FOTO: MATTHIAS RIETSCHEL

... ja, Phishing bleibt ein Dauerbrenner. Dabei geht es um den Missbrauch von Vertrauen – sei es über täuschend echt aussehende E-Mails, die zu gefälschten Login-Seiten führen, oder über Anrufe, die sensible Daten abfragen. Diese Methoden funktionieren deshalb so gut, weil die meisten Menschen keine natürliche Intuition für das Internet haben. Im Straßenverkehr sehen wir eine rote Ampel und wissen, was zu tun ist. Im Internet fehlen uns nicht nur solche klaren Warnsignale, sondern eben auch die Intuition.

In jüngster Zeit ist Künstliche Intelligenz auch bei Cyberangriffen ein Thema. Wie real ist diese Gefahr?

Sehr real. Wir wissen aus Beobachtungen und Berichten von Unternehmen, dass KI-gestützte Angriffe zunehmen. Besonders bei der Suche nach verwundbaren Systemen spielt KI ihre Stärken aus: Sie kann riesige Datenmengen analysieren und Muster erkennen, die einem Menschen entgehen würden. Angreifer können damit gezielter und effizienter vorgehen.

Die TU Dresden koordiniert nun das große Forschungsprojekt „AI.Auto-Immune“, in dem noch die HAW Hamburg und zwei Firmen, die Alpha Strike Labs und die Traversals, beteiligt sind. Sie und Ihre Projektpartner setzen dabei selbst auf KI – allerdings zur Verteidigung. Was genau machen Sie dort?

Unser Ziel ist zweigeteilt: Wir wollen, erstens verstehen, wie weit Angreifer KI tatsächlich nutzen können, und zweitens herausfinden, wie wir KI selbst wirksam einsetzen können. Dazu sammeln wir reale

”

Im Straßenverkehr sehen wir eine rote Ampel und wissen, was zu tun ist. Im Internet fehlen uns nicht nur solche klaren Warnsignale, sondern eben auch die Intuition.

Prof. Matthias Wählich,
TU Dresden

Messdaten aus dem Internet, unter anderem mit Netzwerkteleskopen. Das sind Rechner, die auf ungenutzten Adressen lauschen und so Angriffsversuche sichtbar machen, die ins Leere laufen. Unsere Partner aus dem Bereich Maschinelles Lernen entwickeln darauf basierende Mo-

Zur Person

Der Informatiker und Internetexperte Matthias Wählich ist Inhaber des Lehrstuhls für Distributed and Networked Systems an der Fakultät für Informatik an der TU Dresden. Er forscht zu Internetprotokollen, Netzsicherheit und verteilten Systemen und ist Mitgründer mehrerer Open-Source-Projekte. Zuvor war er Juniorprofessor an der FU Berlin, wo er auch promovierte.

delle, die verdächtigen Datenverkehr automatisch erkennen. Wir als Netzwerkspezialisten prüfen dann, ob diese Einschätzungen technisch stichhaltig sind.

Wie muss man sich die Arbeit im Projekt praktisch vorstellen?

Wir arbeiten in mehreren Phasen. Zuerst sammeln wir Daten aus verschiedenen Quellen, also bewusst verwundbaren Systemen, die quasi Angriffe anlocken oder einfach auf sie warten. Diese Daten sind riesig und oft unstrukturiert. Die größte Herausforderung ist, dass wir nur sehr wenige Informationen haben: Meist sehen wir nur den ersten Kontaktversuch eines Angreifers, nicht den gesamten Ablauf. Die KI muss also mit sehr fragmentarischen Hinweisen arbeiten und trotzdem lernen, Muster zu erkennen. Parallel dazu simulieren wir im Labor kontrollierte Angriffe, um die Modelle zu testen und besser zu verstehen, welche Signale wirklich auf bösartiges Verhalten hindeuten.

Wie nah dran ist diese Forschung an der Realität von Netzbetreibern?

Sehr nah. Wir sprechen regelmäßig mit Betreibern, stellen unsere Ergebnisse vor und erarbeiten gemeinsam Lösungen. Das ist nicht immer einfach. Niemand hört gern, dass die eigene Infrastruktur Schwachstellen hat. Aber wenn wir zeigen können, wie sich Angriffe vermeiden lassen, ist die Bereitschaft groß, etwas zu ändern. Einmal hat ein großer Anbieter nach unserer Analyse offene Server abgesichert, die vorher weltweit ungewollt erreichbar waren. Das hat die Angriffsfläche deutlich verringert.

Das Internet lebt von Offenheit. Ist das nicht ein unauflösbarer Widerspruch zur Sicherheit?

Das Internet ist offen – und das ist gleichzeitig seine größte Stärke und Schwäche. Es ist ein Spannungsfeld. Die Offenheit ist die Grundlage für Innovation, für freie Meinungsäußerung, für den schnellen Austausch von Wissen. Gleichzeitig erleichtert sie Angriffe. Wenn wir zu stark regulieren, riskieren wir, diese Offenheit zu zerstören. Beispiele wie China oder die Türkei zeigen, wohin das führen kann. Deshalb ist es so wichtig, Risiken zu minimieren, ohne die Grundprinzipien des Netzes aufzugeben.

Was raten Sie normalen Nutzerinnen und Nutzern im Alltag?

Das Wichtigste ist Aufmerksamkeit. Keine Links anklicken, die verdächtig wirken. Bei ungewöhnlichen Anrufen oder Mails nachhaken, ob der Kontakt echt ist. Manche Menschen vereinbaren sogar mit Angehörigen ein Codewort, um sich gegen KI-generierte Stimmfälschungen zu schützen. Außerdem sollte jeder Updates ernst nehmen. Sie schließen oft Sicherheitslücken, die sonst ausgenutzt werden könnten.

Was wäre Ihr Wunsch, wenn „AI.Auto-Immune“ in einigen Jahren abgeschlossen ist?

Ich wünsche mir, dass wir mit unserer Forschung dazu beitragen, Angriffe schneller und zuverlässiger zu erkennen – und zwar in einem Maßstab, der mit dem Internet mithalten kann. Wir werden nie alle Risiken ausschalten können, aber wir können das Spielfeld so gestalten, dass Angreifer es schwerer haben