# Eine Frau gegen Putins Hacker

**Natalia Oropeza verteidigt deutsche Unternehmen gegen Cyberangriffe. Bei Volkswagen hat sie damit angefangen, jetzt ist Siemens dran – und damit ist noch lange nicht Schluss.**

*Von Inge Kloepfer*

Natalia Oropeza, 57, Chefin der Abteilung Cybersicherheit bei Siemens und Vorsitzende der Unternehmensgruppe „Charter of Trust“

Foto Thomas Dashuber

Es gibt diesen einen Moment, den Natalia Oropeza nicht mehr vergisst. Einen, der nicht nur ihr die Augen geöffnet hat. Das war im Dezember 2021. Damals versetzte eine Entdeckung von Cybersicherheitsforschern des Tech-Giganten Alibaba die Welt in Angst und Schrecken. In der Java-Bibliothek Log4j machten sie eine gravierende Sicherheitslücke aus, die Hackern den Zugriff auf Milliarden Computer in aller Welt ermöglicht hätte.

Eine Zero-Day-Schwachstelle nennt man so etwas, wenn es zum Zeitpunkt ihrer Entdeckung keine Lösung gibt, ein Fukushima-Moment der weltweiten Software-Industrie, ein Desaster. Denn: Log4j, eine Art Türsteher-Software, ist weltweit verbreitet und wird von Systemadministratoren und Programmierern in Rechenzentren, Unternehmensservern, Netzwerktechnologien und Systemkomponenten eingebunden. Wären Hacker früher auf diese Lücke gestoßen als das Team von Alibaba, hätten sie Teile der Welt lahmlegen können. Ein schier unvorstellbares Szenario.

Natalia Oropeza, seit Anfang 2018 Cybersicherheitschefin von Siemens, und ihr 1300 Mann und Frau starkes Team waren seinerzeit mehr als alarmiert. Sie arbeiteten Tag und Nacht daran, die Lücke zu schließen. „Nach fünf oder sechs Tagen waren wir so weit“, erinnert sie sich. Sie hatten ein sogenanntes Tool entwickelt, ein entsprechendes Update und konnten für den Konzern Schlimmeres verhindern.

Der weltweite GAU blieb aus. Das lag nicht nur an Siemens. Auch andere hatten an dem Problem gearbeitet. Als sich Oropeza nach knapp einer Woche mit den Kolleginnen und Kollegen anderer Großkonzerne besprach, mussten sie feststellen, dass sie alle auf eine ähnliche Lösung gekommen waren. „Jeder hatte das Rad für sich erfunden, viel Zeit und Geld dafür aufgewendet“, sagt sie. „Unnötig viel. Das wird uns nicht noch einmal passieren.“

Die 57 Jahre alte Mexikanerin Natalia Oropeza, die fließend Deutsch spricht und viele Jahre für Volkswagen in ähnlicher Position tätig war, ist momentan eine der weltweit wichtigen Figuren für die digitalen Sicherheitsarchitektur. Denn die „ITlerin“, als die sie sich selbst bezeichnet, ist seit dem vorigen Jahr auch noch Vorsitzende eines Netzwerks von 14 global agierenden Großkonzernen, die in Sachen Cybersicherheit intensiver denn je zusammenarbeiten.

„Charter of Trust“ heißt die Gruppe. Genauer gesagt heißt so das Abkommen über zehn Grundsätze, auf die sich die beteiligten Konzerne 2018 geeinigt haben – darunter die Allianz, Microsoft oder auch Mitsubishi Heavy Industries und eben Siemens. Sie tauschen sich fortwährend aus, wehren Angriffe gemeinsam ab, arbeiten mit staatlichen Organisationen auf der ganzen Welt zusammen.

„Cyberangriffe hören ja nicht an den Toren von Siemens auf“, sagt Oropeza, „und auch nicht an den Landesgrenzen.“ Attacken können von der privaten Wirtschaft auf die öffentliche Hand und deren Systeme übergreifen, ganze Produktionsstätten lahmlegen, dazu die öffentliche Daseinsvorsorge mit ihren Wasserversorgungs-, Elektrizitäts- und Transportsystemen. Alles ist mit allem vernetzt, die öffentliche Hand nutzt schließlich Soft- und Hardware von privaten Unternehmen.

Auch Gesundheitssysteme und Krankenhäuser geraten immer wieder ins Visier von Hobby-Hackern, ganzer Cyberarmeen und von Geheimdiensten. Mancherorts hat es deshalb schon Todesfälle gegeben. Und es wird nicht besser. „Cybercrime ist ein hoch profitables Geschäft“, sagt die Ingenieurin, „deutlich profitabler noch als der Drogenhandel.“

Auf rund 200 Milliarden Euro wird der jährliche Schaden durch die Angriffe allein in Deutschland taxiert. Immer mehr solcher Attacken kommen aus China und Russland. Da geht es zunächst um Erpressung. Internetseiten oder auch ganze Systeme werden gesperrt und erst gegen die Zahlung von Lösegeld wieder freigeschaltet. Ferner kommt es zum Diebstahl von geistigem Eigentum, angefangen von Industriegeheimnissen bis hin zu medizinischen Entdeckungen. Und auch das Hacken von Kreditkarten ist hoch lukrativ.

„In geopolitisch konfliktreichen Zeiten mischen zudem einige Staaten ordentlich mit“, weiß Oropeza. „Sie bezahlen Hacker, um Systeme zum Absturz zu bringen.“ Das hat man im Fall der Ukraine beobachten können, wo gezielt kritische Infrastruktur angegriffen wurde. Oropezas Arbeit beginnt immer neu. Kaum ist ein Angriff abgewehrt, folgt schon die nächste raffiniertere Attacke.

„Die IT-Sicherheitslage ist besorgniserregend“, sagt Claudia Plattner, seit gut einem halben Jahr die Präsidentin des Bundesamts für Sicherheit in der Informationstechnik. „Für große Probleme braucht man große Lösungen. Und die können wir nur gemeinsam umsetzen. Dazu gehört eben auch der Schulterschluss mit Unternehmen, dazu gehören Formate wie die Allianz für Cybersicherheit oder die Charter of Trust.“ Plattner und Oropeza kennen sich, die beiden tauschen sich regelmäßig aus.

Längere Zeit blieb es um den Zusammenschluss der Großkonzerne eher ruhig. Es schien nicht recht nach vorn zu gehen, Gründungsmitglied Daimler stieg sogar aus, zu behäbig, zu wenig effizient war die Organisation offenbar. Jetzt aber, mit Oropeza an der Spitze, scheine die dringend notwendige Bewegung in die Sache zu kommen, heißt es beim Bundesamt. Zusammenarbeit fänden ja immer alle gut. Aber es brauche eben auch Leute, die dann auch die Dinge vorantrieben.

So wie Natalia Oropeza. Naturwissenschaften und Technologie haben sie von klein auf fasziniert, schon 35 Jahren, als noch niemand daran dachte, dass Tech-Jobs überhaupt etwas für Frauen sein könnten. Sie wuchs in einem Mittelklasse-Milieu in Puebla auf, einer Millionenstadt südöstlich von Mexiko-Stadt. Für die Ausbildung ihrer Tochter gaben die Eltern alles, ermöglichten ihr den Besuch der deutschen Schule, an der sie die Sprache büffelte, später studierte sie Elektroingenieurwesen an einer Privatuniversität.

Schon an der Hochschule fiel sie auf. Unter den hundert Studenten, die in ihrem Jahrgang Elektrotechnik studierten, gab es nur wenige Frauen. Und dann schaffte sie auch noch als Einzige von ihnen den Abschluss. Als Kind träumte sie eine Zeit lang davon, Tennisprofi zu werden, war aber nicht begabt genug, wie sie selbst sagt. Später schwärmte sie von der Physikerin Marie Curie. Dann wurde sie Ingenieurin.

Die Attacken sind auf der ganzen Welt so zahlreich wie nie zuvor, in diesem Jahr erreichten sie mit Hilfe der Künstlichen Intelligenz einen neuen Höhepunkt. „Allein bei Siemens haben wir rund tausend solcher Angriffsversuche im Monat“, sagt sie. Gegen alle könne man sich nicht schützen. „Wir müssen uns deshalb vor allem auf das Sensible und Schützenswerte konzentrieren.“ In geopolitisch derart schwierigen Zeiten allemal, wenn sich die Angriffe auf die komplette Zerstörung von Systemen richten.

Oropezas reagiert darauf mit einer Unaufgeregtheit, die vor diesem Hintergrund fast schon provokativ wirkt. Sie will sich nicht beirren oder gar einschüchtern lassen.

Jahrzehntelang hat sie als ITlerin gearbeitet, Teams in den IT-Abteilungen von Unternehmen geleitet. Der Schwerpunkt lag anfangs aber nicht auf der Cybersicherheit, im Gegenteil: Für die Aktivitäten der Abteilung Abwehr, deren Job sie heute macht, hatte sie damals nicht sonderlich viel Verständnis. „Für mich waren manche Leute in den Unternehmen eher Bremser, die meine Entwickler aus Angst vor neuen Angriffsflächen davon abhalten wollten, ganz neue Wege zu beschreiten“, erinnert sie sich.

Der Augenblick, in dem sich ihre Haltung änderte, war eines der Bewerbungsgespräche bei Volkswagen. Ihrem Gegenüber erklärte sie, warum sie gerade nicht für die Cybersecurity arbeiten wollte: Sie wisse so gut wie gar nichts über das Thema, und sie wolle nicht zu der Einheit im Konzern gehören, die im Ruf stand, Entwicklungen eher zu bremsen als voranzubringen. Da sagte ihr Gesprächspartner nur: Bei VW habe sie die Möglichkeit, genau das zu ändern.

Bei Volkswagen ging es für sie seinerzeit nicht allein darum, technisch versiert und organisatorisch beschlagen zu sein. Sie musste auch Menschen an einen Tisch bringen, die von ihrem Anliegen zunächst nicht begeistert waren. „Mit dem Argument habe ich die Herausforderung angenommen. Und dann habe ich mich in das Thema regelrecht verliebt. In seine Vielschichtigkeit. Denn es ist ja nicht nur ein technisches Thema, man muss auch die geopolitische Situation im Kopf haben und verstehen.“

Oropeza gibt ein Beispiel. Es führt in den Februar 2022 zurück, in die Tage nach dem russischen Angriff auf die Ukraine. „Die Mitglieder der Charter of Trust haben sich sofort getroffen.“ Jedes Mitgliedsunternehmen habe seine Risiken benannt. Am Ende einigten sich die Beteiligten auf das Kappen sämtlicher Netzwerke mit Russland – und auf den Abschied von einem Sicherheitstool, das sie alle benutzten. Es stammte vom weltweit größten Cybersecurity-Unternehmen Kaspersky mit Sitz in Moskau, das 1997 von dem Russen Eugen Kaspersky gegründet wurde. „Seine Produkte sind hervorragend. Aber es war politisch nicht darzustellen, solch ein hochwichtiges System weiterhin laufen zu lassen.“

In Sachen Cybersicherheit ist in der Bundesrepublik noch viel zu tun. Das hat inzwischen auch Bundesinnenministerin Nancy Faeser erkannt und kürzlich eine Wirtschaftsschutzstrategie vorgestellt. Großkonzerne wie Siemens oder die Allianz haben dabei allerdings nicht nur Deutschland im Blick, sondern den gesamten Globus. Regulierungen seien überall anders, sagt Oropeza.

Sie ist überzeugt davon, dass sich die Welt vor einem echten Daten-GAU auf Dauer so nicht wird schützen können, und da ist sie sich mit Bundesamts-Chefin Plattner einig. Plattner geht aber noch weiter. Zusammenarbeit in der Krise ist gut, sie setzt aber voraus, das sie vorher schon in internationalem Maßstab erprobt wurde. „Wir müssen den Krisenfall gemeinsam über Ländergrenzen hinweg üben können und kurze Wege etablieren. Auch deswegen wirbt das Bundesamt für die Einrichtung einer Zentralstelle, die uns eine verstetigte Zusammenarbeit mit den Ländern erst ermöglichen würde.“

In den Vereinigten Staaten funktioniert die Kooperation der Charter of Trust zwischen dem Weißen Haus, den Geheimdiensten und anderen Organisationen, die das Land schützen, sehr gut. Die Wege sind direkt und daher kurz. „Von diesem pragmatischen Ansatz können alles etwas lernen“, sagt Oropeza. Man ahnt, dass sie damit auch Deutschland meint.

Wenn die Lage so ernst ist, wie Oropeza sie schildert, dann verwundert es , warum ausgerechnet bei einem Technologie-Konzern wie Siemens Cybersicherheit nicht längst als eigenständiges Ressort im Vorstand des Unternehmens verankert ist. Immerhin: Cybersicherheit gehöre ganz grundsätzlich in die Chefetage der Unternehmen, fordert Bundesamts-Chefin Plattner. „Dort muss das Thema verstanden, angenommen und getrieben werden. Die handelnden Personen brauchen die Rückendeckung und die Ressourcen, um in den Unternehmen etwas bewegen zu können.“

Die hat Natalia Oropeza bei Siemens nach eigenen Worten auch ohne Vorstandsposten. Viel wichtiger ist für sie die grundsätzliche Akzeptanz des Themas in Politik und Wirtschaft. Nur dann kann Cyber auch wirklich sicher sein.