Vier Fragen an Linus Neumann

„IT-Sicherheit ist ein Prozess und kein Zustand, den man erreichen kann."

Linus Neumann, Keynote Speaker auf dem diesjährigen www.aareon-forum.de, ist Diplom-Psychologe und Hacker. Er berät Unternehmen und Betreiber kritischer Infrastrukturen rund um IT-Sicherheit. Im Chaos Computer Club engagiert er sich seit Jahren für netzpolitische Themen und ist mit seiner Expertise regelmäßig in Ausschüssen des Deutschen Bundestags gefragt. Auf dem Aareon Forum hält Linus Neumann den Vortrag: „Schöne neue Welt? Freiheit, Sicherheit und Recht in Zeiten der Digitalisierung"

Häuser aus dem 3D-Drucker, virtuelle Konferenzen und Datenmanagement per App: Die Digitalisierung hat unser Leben revolutioniert – und das in kürzester Zeit. Doch sie birgt Gefahren: Linus Neumann möchte für technische und gesellschaftliche Risiken sensibilisieren. Er spricht unter anderem über digitale Mündigkeit und Datensicherheit, vor allem aber über die Frage, in welcher Welt wir leben möchten. Dabei stellt er nicht nur Probleme vor, sondern zeigt auch mitreißende pragmatische Lösungsansätze auf.

Website: https://linus-neumann.de
Podcast: https://logbuch-netzpolitik.de
Youtube: https://www.youtube.com/channel/UCEvGxtMPQI8MsjyOwOUkGeQ

Wo liegen die Hemmnisse für mehr Sicherheit in der IT-Welt? Liegt es an mangelndem Bewusstsein der Nutzer? Oder ist es eher eine Systemfrage durch fehlende Regulierung?

Linus Neumann: Ich fürchte, dass es leider an mangelnder Kompetenz liegt. Wie ich darauf komme? Auch da, wo Sicherheit immerhin als unerlässlich anerkannt ist, wird sie oft nicht korrekt umgesetzt – wider besseres Wissen!
Das andere fundamentale Problem ist Komplexität. IT-Projekte werden oft mit der heißen Nadel gestrickt und haben schließlich einen viel größeren Umfang als ursprünglich geplant. Das gilt für einzelne Software-Projekte ebenso wie „die gesamte IT" von Organisationen. Diese Systeme versteht dann kein Mensch mehr und kann sie entsprechend auch nicht mehr sicher bedienen. Wenn das System selbst nicht intuitiv ist, dann ist es auch seine Sicherheit nicht.

Das wird leider auch so bleiben, bis wir eine IT-Basis-Kompetenz in der Gesellschaft haben. So ist es am Ende auch eine Frage der Bildungspolitik. Momentan basiert diese noch darauf, die Existenz von Computern und Internet so lange wie möglich vor Kindern geheim zu halten. Das wird katastrophale Folgen für die jungen Generationen haben, die Computer als geheimnisvolle Konsumgeräte mit sieben Siegeln kennenlernen, statt mächtiges alltägliches Werkzeug.

Jedes Jahr entstehen allein in Deutschland Milliardenschäden durch Cyberattacken, Phishing und Co. Wo sehen Sie Lösungen, die Privatpersonen wie Unternehmen für mehr Datensicherheit einfach anwenden können?

Linus Neumann: IT-Sicherheit ist ein Prozess und kein Zustand, den man erreichen kann. Natürlich wäre es schön und auch nach wie vor erstrebenswert, wenn Sicherheit einfach gekauft und angewendet werden könnte. Leider ist das nicht möglich, sonst gäbe es solche Produkte tatsächlich. Das ist aber leider nicht der Fall.
Ein einfaches Beispiel: Das technisch sicherste System bringt mir nichts, wenn ich überall das gleiche Passwort verwende. Eine Angreiferin knackt dann nur einen meiner Accounts und hat Zugriff auf alle. Die einzelnen Anbieterinnen können aber nicht sinnvoll prüfen, ob ich diesen Fehler mache oder nicht. Technisch lässt sich dieses Risiko kaum einfangen, außer mit einer 2-Faktor-Authentifizierung, die heute aber immer noch als zu umständlich empfunden wird.
Für die meisten Organisationen gibt es aber durchaus einen wichtigen Rat, den sie unbedingt befolgen sollten: Tägliche Back-ups von allen Systemen. Die Back-ups sollten so angefertigt werden, dass die gesicherten Systeme sie nicht löschen können, und der Back-up-Server darf nicht in die Domäne eingebunden sein. Dieser kleine Rat spart im Zweifelsfall Millionenschäden durch Ransomware.

Wie genau können Unternehmen von Ihrer Expertise profitieren? Hacken Sie sich auf Wunsch in deren Systeme oder geht es da eher um generelle IT-Schwachstellen?

Linus Neumann: Natürlich machen wir oft sogenannte „Penetration Tests", bei denen Sicherheitslücken gefunden und beseitigt werden. Das läuft aber etwas anders, als viele Leute es sich vorstellen: In der Regel sind der Untersuchungsgegenstand und das Angriffsziel klar vereinbart. Es geht also nicht darum, „das Unternehmen" „irgendwie" zu hacken, sondern Schwachstellen in einem konkreten Produkt oder System zu suchen – oft, bevor es in Betrieb genommen wird oder auf den Markt kommt. Notwendigerweise ist das dann eine Momentaufnahme eines kleinen Bereichs. Bei der strategischen IT-Sicherheitsberatung gehen wir über die konkrete Schwachstelle hinaus und blicken darauf, wie gut eine Organisation ihre IT im Griff hat und auf Angriffe vorbereitet ist. Das Ziel ist immer, sicherer gegen konkrete tatsächliche Bedrohungen zu sein, und zwar nicht nur präventiv, sondern beispielsweise auch im Bereich der Schadensminimierung.

Big Data, künstliche Intelligenz und Machine Learning – wo liegen die Chancen und wo fangen die Risiken an, zum Beispiel durch riskante Machtasymmetrie?

Linus Neumann: Das größte Risiko ist, dass wir Menschen Entscheidungen, Empfehlungen und Vorgaben des Computers nicht mehr infrage stellen. Und das sehen wir schon heute.

Herr Neumann, vielen Dank für den Einblick in die Welt der Datensicherheit.