IT-Defense 2022 – von Blockchain, Bugs und Angst

Verarscht!

Jörg Riether

Nachdem man im Jahr 2021 COVID-bedingt auf den bekannten IT-Sicherheitskongress verzichtet hatte, fand er in diesem Jahr wieder statt – hybrid und mit überraschenden Erkenntnissen.

Mit seinem Vortrag „Blockchain! – So sicher wurden Sie noch nie verarscht" traf CCC-Sprecher und Sicherheitsexperte Linus Neumann bei der diesjährigen IT-Defense einen Nerv. Denn wohin man auch schaut, die Blockchain-Technik wird derart inflationär eingebracht, dass man sich zuweilen nur noch verwundert die Augen reiben kann.

Bei Kryptowährungen, so Neumann, gebe es genau zwei Anwendungsfälle. Der erste umfasse Kriminalität, Drogen, Lösegeld und Geldwäsche und der zweite Spekulation. Bemerkenswert war seine Prognose, wo das alles einmal hinführen solle, im schlimmsten Fall zum Nachteil der Gesellschaft. Dies war dann auch der hässliche Teil, wie Neumann es beschrieb, denn es könne einfach nicht gut enden.

Linus Neumann sieht kein gutes Ende für die Blockchain.

Zum Stichwort Web3 erklärte er, vollkommen egal, wie es mit dem Blockchain-basierten Webableger ausgehe, die Nutzer werden keine Autonomie gewinnen und das Web werde nicht dezentraler. Bei den Kryptowährungen sieht Neumann zwei mögliche Szenarien in der Zukunft und beide seien nicht schön. Das erste und wahrscheinliche Szenario bedeute das Platzen der Blase. Und zwar spät, ganz ähnlich wie es bei der Tulpenblase in den Niederlanden oder der Subprime-Mortgage-Krise in den USA passierte.

Nachteilig fürs Gemeinwesen

Das zweite Szenario würde bedeuten, dass sich die Krypto-Utopie tatsächlich durchsetzt. Somit würde es dann aber auch schwierig, Steuern zu erheben, Geldwäsche zu unterbinden oder Korruption zu kontrollieren. Also nichts, wovon die Gesellschaft profitieren würde. Neumann ergänzte im Lichte dieses Szenarios, dass er sich ja schon ein wenig schmutzig dabei fühle, zuzugeben, dass es nicht verkehrt sei, wenn ein Staat Kriminalität bekämpft und Geldwäsche oder Korruption zumindest auf dem Papier unter Strafe stellt und theoretisch verfolgen könnte.

Wenn wir also jetzt weltweites anonymes Geld machen würden, dann habe er nicht den Eindruck, dass wir als Gesellschaft auf der Gewinnerseite stehen werden. Sein Fazit: Wenn man glaubt, eine Blockchain zu brauchen, habe man das Problem nicht verstanden. Insofern sei die Antwort: Nein, man braucht keine Blockchain. Man sollte sich lieber auf Lösungen für Probleme konzentrieren und nicht umgekehrt.

Warum fassen Staaten und Unternehmen das Thema aber immer wieder ins Auge? Beide haben doch eigentlich gar kein Interesse an der Grundidee einer öffentlichen dezentralen Blockchain, denn diese stellt einen fundamentalen Angriff auf zentrale Machtstrukturen dar. Der eigentliche Grund, warum sie dennoch Blockchain bewerben, liege darin, dass man versuche, die gesamte Idee durch die Nutzung einer privat kontrollierten Blockchain ad absurdum zu führen. Nur brauche man dann keine Blockchain.

Bugs und Exploits

Felix von Leitner (Fefe) berichtete in seinem Vortrag vom Umgang der Hersteller mit Softwarefehlern. So habe es die Industrie im Wesentlichen aufgegeben, Bugs zu finden und zu beheben. Man beschäftige sich eher mit Mitigationen, das bedeutet, man verhindert nicht die Ausnutzung, sondern macht sie lediglich schwieriger und teurer. Die Bugs seien also oft immer noch da. Irgendwann würden sie zwar dann beseitigt, allerdings ohne Nachweis der Sicherheitsimplikationen, weil es schlicht zu teuer wäre, echte Exploits zu bauen. Man brauche auch nicht davon auszugehen, dass Hobbyisten dies tun werden. Nur Geheimdienste und Mafia hätten das Geld, Exploits zu bauen.

Eine kleine Ausnahme gebe es, nämlich die Idealisten. Als Beispiel nannte Fefe Googles Project Zero. Nun würden aber Sicherheits-Bugs nur als solche akzeptiert, wenn es einen echten Nachweis gibt. Hat also ein Hersteller einen Bug behoben, ohne dass es einen Nachweis gab, dann war es offiziell auch keine Sicherheitslücke. Ergo müsse man dann auch nicht in die Hinweise schreiben, dass es ein Sicherheitsproblem gab, man kann es also einfach unter der Haube beheben. Somit seien Patch-Hinweise heutzutage weitgehend wertlos. Zusammenfassend könne er daher nur dringend empfehlen, alle Patches sofort zu installieren. Und zwar überall und ohne Nachfragen. 24 Stunden zu warten sei schon zu lange.

Niemals Awareness durch Angst

Der Sicherheitsexperte und Hacker Jayson E. Street berichtete im Gespräch mit dem Autor von einer bemerkenswerten Beobachtung. So würden einige Red Teams heute oft derart aggressiv und selbstgerecht in Unternehmen auftreten, dass sie damit letztlich die Sicherheit des Unternehmens gefährden, statt sie zu stärken. Dies nicht, wie man vielleicht glauben würde, durch die eigentliche Kompromittierung, sondern durch die negativen Auswirkungen des Verhaltens, insbesondere durch das Arbeiten mit Angst. So würden nämlich in direkter Konsequenz manche Blue Teams diese Haltung spiegeln, anstatt sie zu verurteilen. Es entstehe eine angstgetriebene toxische und feindliche Haltung innerhalb der Belegschaft, die bei einer Eskalation eine ganze Reihe potenzieller Insider-Bedrohungen auslösen könnte.

Dies müsse man im Auge haben und rechtzeitig gegensteuern. Man müsse verstehen, dass man mit Angst keine nachhaltigen Resultate erzielen könne, sondern lediglich ganz kurzlebige – wenn überhaupt. Es mache einen gravierenden Unterschied, ob man als Red Teamer nach einem erfolgreichen Angriff einfach wegspaziert und sein „Opfer" links liegen lässt, vielleicht sogar mit der unterschwelligen Andeutung von Konsequenzen, oder ob man danach zur betroffenen Person geht, ihre Bemühungen wertschätzt und erklärt, was besser laufen könnte. (ur@ix.de)