This Data Security Consultant Explains Why Businesses Should Embrace Web3 — But Do It Cautiously

Opinions expressed by Entrepreneur contributors are their own.

After much initial skepticism and doubt, Web3 has emerged as a real source of value, paving the way for a new generation of decentralized applications (dApps) built on blockchain. These dApps provide fantastic opportunities for forward-thinking companies to transform their business operations and enhance their efficiency.

A 2023 survey of 600 enterprise decision-makers in the U.S., U.K. and China found that nearly 90% of them deploy blockchain technology in some capacity, with 87% saying they planned to invest in blockchain in the next year. This reflects businesses' fear of being left behind as blockchain developments accelerate globally. According to Deloitte, 73% of financial executives believe their organization will lose an opportunity for competitive advantage if they don't adopt blockchain and digital assets.

Advocates of Web3 laud the decentralized web's greater resilience and security compared to its predecessor, as blockchain ensures that every transaction is public and verifiable, improving record-keeping and data integrity.

However, despite the promise of blockchain's greater security, the increasing adoption of Web3 technologies has not eradicated security risks, merely changed them: The 2023 Web3

Security Landscape report by Salus shows that cyberattacks on the Web3 industry resulted in losses in excess of $1.7 billion last year, highlighting the extensive range of threats within the decentralized world.

Related: Confused About Web3? Steve Aoki Dissects His Business to Show How You Can Make Money.

New security challenges

Web3 avoids some of the security headaches of Web 2.0 but introduces several new ones, almost all unique to the industry.

Some of the biggest attacks of the year included the $200 million attack on the cloud-based blockchain services provider Mixin Network; the $197 million attack on Euler Finance; the North Korea-linked Lazarus Group attack on both the Poloniex cryptocurrency exchange and Atomic Waller, stealing more than $126 million from the former and more than $100 million from the latter.

The majority of Web2 attacks target users. Most threats faced by the Web3 industry, however, take advantage of code vulnerabilities of decentralized applications and protocols. Access control issues accounted for 39% of all Web3 attacks, whereas flash loan protocols, where flash loans are used to maximize the impact of another form of attack like the exploitation of smart contract bugs or the manipulation of cryptocurrency asset prices on an exchange, contributed to more than 16% of attacks.

User-targeted attacks, as mentioned, are “less popular” in Web3. Phishing attacks, which use social engineering tricks to manipulate unsuspecting users into exposing data, spreading malware infections or giving access to restricted systems accounted for a mere 4% of all attacks.

Besides software vulnerabilities, retail investors continue to fall for exit scams and “rugpulls:” fraudulent crypto projects that convince the community to back them before fleeing with the funds they’ve raised.

Mitigation is possible

Reassuringly, there are concrete steps that businesses can take to reduce the likelihood of falling victim to each of these threats. With appropriate caution and due diligence, there is no reason to pass up the many potential benefits of Web3.

Related: 5 Essential Tips for Starting a Successful Web 3.0 Venture

Enhance authentication

Introducing more robust authentication and authorization mechanisms, like decentralized identifiers (DIDs), access tokens or biometric and multi-factor authentication, will mitigate many security threats such as access control-based vulnerabilities and phishing attacks. Companies should make sure they always adhere to the principle of least privilege, a crucial step for remaining secure online across both Web2 and Web3.

Increase complexity

As in real life, cyber attackers like to get in and out quickly to avoid detection, so increasing the complexity of participation in Web3 projects will make attacks less likely. DeFi protocols offering flash loans can safeguard themselves against threats by introducing minimum borrowing amounts and time limits, as well as additional fees to raise the costs for attackers. In a similar vein, attacks on oracles can be reduced in a number of ways, such as by avoiding the use of markets with shallow liquidity for price predictions, and by

increasing manipulation costs for attackers through the use of TWAP (time-weighted average price) mechanisms.

Hardware wallets – the use of physical technology to store private cryptographic keys online until they are needed – can also help to avoid hacks. Short of physically stealing the hardware wallet itself, which resembles a USB drive, they are virtually impossible for cybercriminals to access.

Implement checks

As with Web2, businesses should regularly update their access permissions to avoid chinks in their security armor. In addition, they should conduct thorough audits of all smart contract code, as this often falls prey to re-entry vulnerabilities. They should also adhere to the check-effect-interaction model.

Perform due diligence

Organizations can employ penetration testing to find and exploit their own vulnerabilities before attackers do. Extensive employee education is also crucial to enable individuals to identify and avoid phishing attacks and other threats.

Finally, make sure to research new projects and their teams carefully to ensure that they have a reliable track record, thus avoiding falling victim to rugpull scams. Prioritize projects that have undergone transparent security assessments by reputable auditors.

Related: How to Own Your Online Narrative – Even When the Internet Owns You

Embrace Web3, but do it cautiously

The high exposure to scams in Web3 is one of the major

obstacles preventing mass adoption of decentralized technologies. However, though the amount of total losses in 2023 was very high, it was lower than the number for 2022. This suggests that the landscape’s overall safety is improving, as more companies adopt the necessary precautionary measures.

As Salus points out, $1.7 billion in losses is still an alarming number, and one that emphasizes the importance of improving security and educating users about the risks of Web3. The inherent vulnerabilities of the technology are distributed across multiple areas, demanding a multi-pronged approach to security, which can be enhanced by prioritizing those platforms and protocols that implement the strongest security measures.

My main takeaway from the report is that businesses need not shy away from embracing Web3 and all of the potential it offers. However, their adoption of the technology should be accompanied by extensive checks and research, and adherence to the same strict standards of security as they employ in their legacy technology systems.

https://www.entrepreneur.com/science-technology/businesses-should-embrace-web3-but-do-it-cautiously/469900