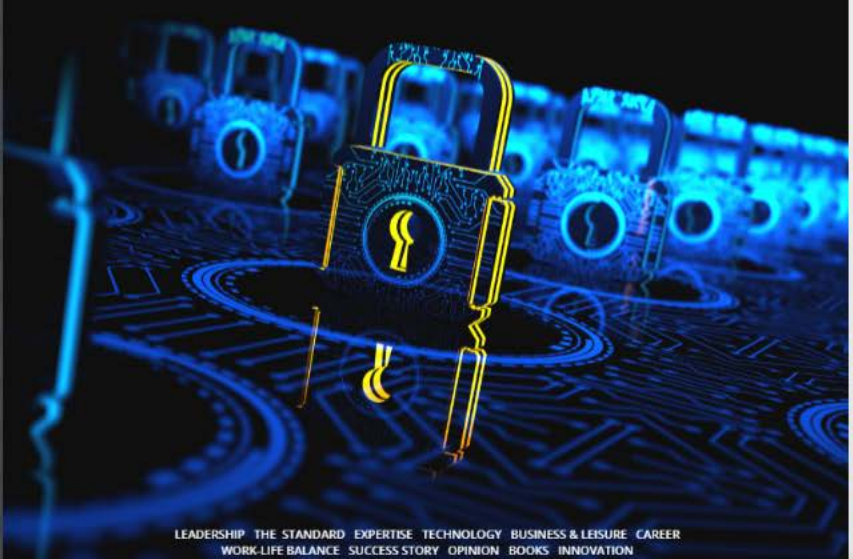
PECB Insights

ISSUE 39 ISO STANDARDS AND BEYOND JULY-AUGUST 2022

NETWORK SECURITY, ETHICAL HACKING, AND CYBERSECURITY

PROTECT YOUR ONLINE PRESENCE



LEADERSHIP THE STANDARD EXPERTISE TECHNOLOGY BUSINESS & LEISURE CAREER
WORK-LIFE BALANCE SUCCESS STORY OPINION BOOKS INNOVATION

In This Issue

38

26

62

The views and opinions expressed in the PECB Insights Magazine do not necessarily reflect the views of PECB Group.

The Use of Blockchain in Cybersecurity

BY RUDY SHOUSHANY

These days cyber-attack trends are increasing in magnitude, frequency, and sophistication constantly. In recent years, we have witnessed escalated cyber-attacks, such as distributed denial of service (DDoS) attacks, phishing, ransomware attacks, man-in-a-middle (MiTM) attacks, SQL injection, and much more, aimed at major networks like Mailchimp, LinkedIn, Canva, Google, Amazon, CNA, WHO, etc. It is safe to say that as technology evolves, so do the bad guys.

The most recent cyber-attacks were launched by nation-states, hacktivist groups, and lone-wolf hackers. Cyber-attacks render a significant threat to government agencies, businesses regardless of size, and all internet users.

Hence, birthing the need for tight cybersecurity to protect online networks from digital attacks on sensitive data, information, and transactions.

In April 2022, email marketing company, Mailchimp revealed that its system was hacked and information was exported from the platform's accounts. This affected users such as Trezor and Bitcoin's wallet, whose newsletter database is hosted on Mailchimp.

In March 2021, insurance firm, CNA experienced a ransomware attack where the company had to pay a settlement fee of $40 million to retrieve their stolen data. The attack also logged employees out of their systems and blocked access to corporate resources.

In October 2020, Google announced the details of a major cyber-attack against its servers in September 2017, to the public. According to the report, the incidence was a distributed denial-of-service (DDoS) attack that lasted for over six months.

Thus, topping the record as the biggest attack of its kind. Undoubtedly, hackers hide behind the decentralized nature of the internet to keep their anonymity and overcome any opposition to their attack.

For instance, a DDoS attack will first, infect multiple nodes across different domains to produce a semi-coordinated network called a “botnet.” Hackers then hijack each bot and launch them against centralized targets.

Meanwhile, other ways to make centralized targets less vulnerable include database management, increased software deployment, security protocols, and depending less on central "trust."

The decentralized solution relies on blockchain technology to increase the resilience of cybersecurity.

Blockchain technology is equipped with multiple features, configurations, and applications specific to improve security. Configurations including public and private cryptographic keys, contracts, and identity control ensure data protection through verification and authentication of transaction records, privacy, and traceability maintenance.

Blockchain technology is trustless and consensus-focused, which distributes transaction records across a network of computers.

Thus, shifting record-keeping and transaction verification processes from a central authority to a decentralized network. Thereby, removing the single point of failure, thus, enhancing resilience to attack and security.

5 Uses of Blockchain in Cybersecurity and Privacy

1. Decentralization of Data

Due to blockchain's consensus nature, data stored on-chain are tamper-proof, blockchain-based storage solutions will help achieve decentralized storage that will secure digital data.

2. IoT Security

Blockchain technology can be used to maintain cybersecurity in the IoT system by apportioning operation and administrative controls away from central authority, enhancing device-to-device encryption, and key management techniques to secure data. Distributing information redirects users when a centralized database is hijacked.

3. Software Authentication

Blockchain is perfect for verifying updates to detect and stop malicious software from sabotaging the devices. Companies can use blockchain hashing to verify patches, updates, and downloads to prevent chain attacks.

4. DDoS Attacks Resistance

The most common and potent cyber-attack is the DDoS attacks, which hit Google and Amazon. Distributed denial of service (DdoS) attacks are launched to hijack the traffic on a targeted network or service by spamming it with false requests from different infected bots. These attacks are decentralized in nature.

However, blockchain's decentralization and immutability solution will be 'beating the hackers on their game' as it efficiently bypasses these attacks.

5. DNS Security

Like a public directory, the Domain Name Server (DNS) connects domain names to their IP addresses. Decentralizing DNS Security can ensure the domain names are tightly secured and beyond reach during a DDoS attack.

The Benefits of Blockchain in Cybersecurity

1. Eradicates single-point failures

Unlike centralized structures, data is decentralized on the blockchain, thus, one node failure can hardly disrupt the system. Therefore, not even DDoS attacks (which are unlikely to happen to a decentralized structure because of insane computational cost) can compromise the system.

2. Transparent and traceable

Blockchain's transactions are trackable due to its accurate record-keeping. Each transaction is verified, recorded, and digitized across the network for transparency.

3. Reliable transfers

Blockchain is ideal for authenticating data transfers. Here, smart contracts play a vital role since they execute instructions (in this case, transfer) once pre-set agreements are met.

4. Efficient storage

Once records are verified and stored on the blocks, they become unchangeable. This blockchain's immutability keeps the data entries safe in a manner never seen before.

5. User confidentiality

Blockchain's built-in cryptographic key features ensure user confidentiality across all networks.

Drawbacks of Blockchain in Cybersecurity

1. No governance

Even though blockchain is bubbling with use cases virtually in all industries, it lacks global regulations.

2. Irrecoverable keys

Keys (private and public) are to blockchain what keys are to cars. These private keys enable device-to-device data encryption. But what happens when a driver loses his car keys? The car becomes inaccessible.

However, in blockchain, once these keys are lost, they are irrecoverable, meaning that encrypted data could be lost forever.

3. Blockchain literacy

Although blockchain technology has been around for over a decade, understanding its concept requires deep knowledge of some tools and programming languages. As a result, few blockchain developers are readily available.

4. Complexity and costs

As expected, blockchain technology is very complex and comprises of many nodes and computers actively working. This inadvertently requires high computing power and storage capacities, which in turn causes high transaction fees.

5. Satellite development ecosystem

Though blockchain is secure, more and more security efforts and focus should be put on satellite development around the blockchain, which we are seeing being compromised more and more.

Final Thoughts

Cyberattacks like data breaches, DDoS attacks, phishing, ransomware attacks, etc are cause for alarm especially as the attack keeps evolving with technology, growing in volume and frequency.

The financial impact cost thousands of victims millions of dollars yearly. We are seeing more and more utilization of Blockchain use cases, government agencies and companies must join hands in cyber warfare by looking out for ways to counter or prevent these attacks.

Employing Blockchain's decentralization feature will not only prevent these attacks but pay the bad guys in their coins.

Rudy Shoushany
Founder of CryptoTaks
and DxTalks

Rudy has a wide experience in the Information Technology field in the financial sector with over 20 years of experience, which gives him the ability to aid organizations. His specialty is ICT Governance, Compliance, Strategies, and CyberSecurity in the Digital Transformation of fintech.

Rudy is a Certified professional with many achievements and awards, skilled in executive leadership. He has been an active speaker, Board Member, coach, and mentor for startups. He is the Host and Moderator of the DXTalk Series, a Digital Transformation talk show. Which has lately been selected as top 50 Global Thought leaders and Influencers.