trusted" – and that's where the principles of Zero Trust and Least Privilege come into play. "Organizations must discard the old model of 'trust but verify' which relied on ...

Feb. 06, 2019

Amid all the current talk of walls, let's spare a thought for firewalls. In the IT realm, firewalls have been pretty remarkable things – protecting accounting firms and their data through all manner of tech wizardry, as cyberthreats morph and malign actors proliferate. Still, as recent history demonstrates, firewalls are far from impenetrable

and, increasingly, are subject to workarounds that place CPAs and their

breaches are initiated using privileged credentials, and 66 percent of organizations still rely on manual methods to manage privileged accounts."

The newer, more enlightened paradigm for security is "more trusted" and "less trusted" – and that's where the principles of Zero Trust and Least Privilege come into play. "Organizations must discard the old model of 'trust but verify' which relied on well-defined boundaries," says Louis Columbus of the security firm Centrify. "Zero Trust mandates a 'never trust, always verify, enforce Least Privilege' approach to privileged access, from inside or outside the network."

Per Forrester, Zero Trust architecture abolishes the idea of a trusted network inside a defined company perimeter. Zero Trust mandates the creation of micro-perimeters of control around an accounting firm's sensitive data assets and provides visibility into how it uses data across its ecosystem to win, serve, and retain clients. Under a Zero Trust regime, all applications are configured to challenge and encrypt, enabling an accounting firm or department to build out its infrastructure around that concept. Zero Trust, paired with multifactor authentication, has become the industrial strength option in today's environment, which is why Zero Trust should be the linchpin of cloud accounting best practices.

In enlightened accounting firms, the notion of Least Privilege applies to every employee. Encryption is the rule internally, and multifactor authentication to log into every networking component and storage system is mandated; no one can delete a snapshot or burrow into the firewall. The upside is clear: since all user data is inside the network, there's no need to sweat issues like internal encryption – the hosting provider has already handled it. And that extends to the rights conferred on users, including, for example, their ability to use home equipment on an office network.

In theory, every hosting provider ought to embrace this essential principle. The fact

notion that is both unfamiliar and, at first blush, counter-intuitive – at least where the jargon is concerned. An implicit message of "trust no one" would appear to be something less than a confidence builder within the firm. It feels binary – our team, the other team. Or as Robert De Niro put it in "Meet the Parents," you're either inside the Circle of Trust or you're decidedly outside.

Except that in this case, there's nothing personal about Least Privilege and Zero Trust. Quite the contrary: those inside the firewall are infinitely better off for the presence of these policies and here's why: they're designed to protect everyone.

Auditors — who, as a group are notorious for erring on the side of caution — have long wanted to limit network privileges based on the roles of those within that circle. They're the ultimate enforcers of need-to-know. "What do you need to do your job?" is another way of saying that anyone can trip over gratuitous rights. Least Privilege principles keep people in their lane for their own good, no matter how patronizing that may sound.

As Gresham Harkless, Blogger-in-Chief for CBNation puts it, "the Zero Trust model of network security has been … spurred on by the constant barrage of cyber threats that seem to continually break through traditional security measures."

I'm with Russell Walker, CISO for Mississippi's Secretary of State, who recently told Cyber Security Hub that the game has changed, irrevocably. "The perimeter in the traditional sense has disappeared," he said. "The network itself is no longer a static environment we can put barriers around, have a guard at the gate and say, 'Now we are protected.'" He's also right to underscore that Zero Trust and Least Privilege aren't merely technologies and policies. They truly do involve "changing the way IT staff and end-users think and approach their environment."

And not a moment too soon.

==========

(NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.