https://www.mcafee.com/blogs/other-blogs/executive-perspectives/trust-nobody-not-even-yourself-time-to-take-zero-trust-seriously/

By Adam Philpott on Apr 21, 2021

In the working world, there's a chance you've come across your fair share of team-building exercises and workshops. There's one exercise that comes to mind that often results in worried, and uneasy faces during these seminars: The Trust Fall. This is where you fall backward with the expectation that your colleague will catch you before you hit the ground.

Whether you have been with an organization for many years or just started, the same "pit in stomach" feeling reverberates across bellies as people exchange nervous glances and weigh their odds against whomever they may be paired up with when The Trust Fall is announced. That feeling is doubt, and it isn't fun. And the problem is, once doubt is introduced, it tends to stealthily expand in its always-on, silent, and transparent ways, either serving as an incessant top-of-mind presence or staying at bay only to rear its troubling head at an unexpected moment until it is addressed.

"I saw Chris drop his stapler once, will he drop me?" "I know Betsy is the Godmother to my children, but what if she sneezes as I'm falling?" "I just started at this company yesterday, I don't trust anybody I don't know!"

If you're wondering what Trust Falls have to do with cybersecurity, we just need to take a deeper look at the concept of trust in its simplest definition. Trust is a concrete concept: it is either there or it is not. Trusting your colleagues is based on multiple parameters; will they be strong enough to catch me, do they look mature enough to take this seriously, how did they behave when the game was announced – trust is not easily won and can also be quickly lost.

This is a necessity in today's enterprises as computing has moved from private data centers to most everything consumed as a service. There are endless choices to compare, contrast, and comprise a technology stack, but when organizations start leveraging outside infrastructure, tools, and solutions – the sense of trust in these solutions weakens, since integrity can be promised, but should never be assumed.

Examples of this are abundant. As we see organizations explore the concept of trust more and attempt to align practices with the reality of today's security circumstances, we are seeing an increasing number of trust models being exploited via poor management. Intent and implementation are not enough against today's threats.

So, my question to security operation center (SOC) staff, IT leaders, and the c-suite is: **Do you have complete trust in your current security infrastructure?**

In all honesty, can you with no doubt in your mind, say your organization's data and computing are secure? Is there any area you are unsure about?

If you hesitated when responding, even if for just a moment, keep reading.

Business as Usual is Not a Safe Space

Putting guards up, constantly looking over your shoulder, always expecting the worst or for the other shoe to drop – these are not desirable feelings. As a security professional, these are the feelings that cause them to stock up on antacids, with them knowing they are the front-line defense keeping an organization secure and in turn, revenue flowing. For the CIO and CISO, the onus is daunting as they face the challenge to piece together fragmented and disparate infrastructure from a strategic standpoint to best serve the business in an efficient, transparent manner all while simultaneously maintaining compliance and data integrity.

While we want to believe that trust is an intrinsic trait – that we're born bright-eyed and bushy-tailed ready to spout only the truth – we also unfortunately know the reality is not everybody has good intentions. We constantly see this unfold across the security industry where a company is breached, recognizing the flaw(s) that allowed the breach to occur, to then implement a solution to

fix the issue. This break-fix cycle can result in always looking backwards and rushing around to fix yesterday's problem to quickly get business functions up and running without looking at underlying problems or issues.

And no industry is immune. Hackers are coming after everything from Happy Hours and breakfast routines to our more personal and high-stakes data across the financial services and healthcare industries. They're more strategic too, and we can only expect them to continue to evolve. Adversaries today are looking for "low-hanging fruit" targets to take advantage of trust models and move laterally within an organization – first finding an avenue to exploit and enter to later gain access to higher-value targets, data, and assets.

The rush to get business–as–usual back on track is made doubly difficult as business momentum doesn't stop. Organizations are introducing new SaaS services, development teams are writing new code, and even software that you have already reviewed has new features rolled out. The wealth of personal and corporate cloud apps can lead to hasty decisions; increased sprawl of an organization's tech stack as new tools and solutions are introduced; as well as new policies, updates, and procedures for staff to learn and execute. This can all compound into more time spent addressing and fixing the past with blinders on to the future and other vulnerabilities that may exist.

From Zero to Hero

If this past pandemic-filled year has taught us anything, it is that plans do not always go according to plan.

Organizations that have traditionally leveraged a more piecemeal and solutions-based approach to security were blindsided as the work from home era was thrust upon them. From companies updating or adopting collaboration tools, sharing more data digitally, and opening access to external users to create greater efficiencies – the rule book was thrown out the window and malicious actors started looking at all the data being produced and shared like kids in a candy store.

The impact of these plans gone awry isn't pretty and perhaps risk could have been mitigated by using a least or earned trust model as a strategic framework to ensure sound security posture. The 'Zero Trust' concept coined more than a decade ago outlining a model of restricting access and control across an organization's infrastructure is only now getting increased attention.

The harsh reality is, cybercrime is up 300% since the pandemic began, according to the FBI's Internet Crime Complaint Center (IC3). At a time when bottom lines are more important than ever as businesses bounce back, our Hidden Cost of Cybercrime report adds that 35% of those surveyed said security incidents resulting in system downtime cost them between $100,000 and $500,000.

The correlation of a pandemic occurring and malicious actors taking advantage of weaknesses caused by it is crystal clear, leading to increased awareness. In its *Responding to COVID-19: What We are Hearing From Legal and Compliance Leaders* report, Gartner states that 52% of legal and compliance leaders are concerned about third-party cybersecurity risks since COVID-191. Knowing that the increased number of remote workers and their mobile (and potentially unmanaged) endpoints are leading to more breaches *and* that these breaches are increasingly costly, organizations need to get a handle on their existing architecture and shift from awareness to action, eliminating assumptions of who is safe or allowed access.

A Zero Trust mentality allows organizations to restrict and compartmentalize access and data manipulation while still maintaining optimal user experience and productivity levels. Guidelines such as those from the National Institute of Standards & Technology (NIST) can provide a practical framework to explore and implement Zero Trust.

With hackers getting more sophisticated to impersonate and infiltrate networks via verified users, it is time to go back to the drawing board – starting at zero and assuming everything is a threat until proven otherwise. This is a mindset shift and strategy, not another tool or solution to plug in. It involves a recognition of the importance of context and control over security posture, which can only be attained with continuous assessment. It is also about acknowledging trust is about risk – and that while risk is sometimes necessary for growth, it cannot outweigh the reward, so must be strategically managed. This line of thinking must be carefully

navigated as more and more enterprises seek to define and assign accountability and responsibility across infrastructure.

While the journey to Zero Trust isn't the same for every organization, the imperative to adopt Zero Trust is, given our collective experiences throughout the last year and cybercrime poised to keep increasing. It is time to stop looking over shoulders and anticipating the worst, acting only in a reactive manner, and instead feel empowered to erase doubt when maintaining security and compliance across an organization.

To learn more and start the journey toward implementing a Zero Trust strategy, I encourage you explore McAfee' Zero Trust Security hub.

Source: 1 Gartner Press Release, Gartner Says 52% of Legal & Compliance Leaders Are Concerned About Third-Party Cybersecurity Risk Since COVID-19, April 24, 2020. https://www.gartner.com/en/newsroom/press-releases/2020-04-24-gartner-says-52-percent-of-legal-and-compliance-leaders-are-concerned-about-third-party-cybersecurity-risk-rince-covid-19 (URL can be added as a hyperlink in source title)