Extending Zero Trust to the End-User Ecosystem

Trust is at the heart of every relationship between an organization and its end users. Customers choose the organizations with which they do business based on their perception of an organization's trustworthiness. Regardless of whether business is conducted in person or digitally, trust is often measured by an organization's performance, history and reputation.

There are significant gaps in current approaches to achieving digital trust. To address these gaps, organizations need to ensure that security parameters align with a digital trust framework such as ISACA's Digital Trust Ecosystem Framework.[1]

What Is Digital Trust?

In the digital world, trust has become complex. Digital trust is defined as:

> *Digital trust is the confidence in the integrity of the relationships, interactions and transactions among providers and consumers within an associated digital ecosystem. This includes the ability of people, organizations, processes, information and technology to create and maintain a trustworthy digital world.*[2]

ISACA® notes that "The objective of establishing digital trust for an organization is to positively impact its relationship with its clients."[3] When measures that enhance digital trust are implemented, they help create a safe environment that protects the organization's digital assets and the users' data of the organization's digital ecosystem.

As opposed to taking place in writing, for example, digital online interactions occurs via emails, text messages and websites. Multiple industry studies conclude that whether it is via phishing, smishing, site impersonation or spoofing, the end user is the number one vulnerability and the initial attack surface for the majority of online fraud, malware insertion and ransomware attacks.[4, 5, 6] When an attack occurs, it decimates the attacked customers' trust, and the impact is amplified and spread to many other customers who hear about such attacks and fear they will be next.

Existing Approaches: How They Fall Short

With digital trust being a relatively new concept, existing enterprise-centric approaches are insufficient. Once trust has been established, it can easily be eroded by phishing and other impersonation attacks. While the concept of zero trust—never trust, always verify—is core to modern information security practices and technologies, it does not fully cover the multiple types of communications and transactions between customers and organizations that digital trust encompasses.

Specifically, end users have few effective ways of verifying whether they can trust the digital entity with which they are engaging, while organizations can verify customer identities by using passwords and multifactor authentication (MFA). Knowing this gap exists, organizations attempt to educate users on impersonation risk, sharing strategies for identifying phishing attacks. However, education is far from effective and might even result in the opposite of the desired outcome, as one study shows:

> *Students who identified themselves as understanding the definition of phishing had a higher susceptibility rate than did their peers who were merely aware of phishing attacks, with both groups having a higher susceptibility rate than those with no knowledge whatsoever. Approximately 70% of survey respondents who opened a phishing email clicked on it, with 60% of students having clicked overall.*[7]

Customers are already educated about the threats facing their online transactions but few implement the

GIDEON HAZAM

Is cofounder and chief operating officer (COO) of MEMCYCO. He has more than 30 years of experience in the cybersecurity and global high-tech industries. He has held senior positions in business and enterprise development, customer success, and global sales, mostly in emerging technology and solutions for Fortune 500 companies.

complex steps needed to stay safe online. They look to organizations to take proactive steps to protect their digital assets. Further, online fraud awareness can backfire on an organization as it can create phishing fear syndrome. This phenomenon occurs when consumers are fearful that their personal and financial information will be compromised, so they choose not to engage with digital communications and ecommerce.[8] This can negatively impact the effectiveness of digital advertising campaigns and online revenue.

When communicating with their users, many organizations embrace the zero-trust model for end-user access, often implementing MFA. Many have the false impression that when doing so they are also protecting themselves from impersonation because MFA does not work with an impersonation site. However, sophisticated cyberattackers have learned to bypass MFA with methods such as two-factor relay and short-lived domains, which are fake domains that stay live for no more than several hours.

Antiphishing software, also widely used, relies on blacklists that are not updated in real time, but rather when a new phishing source is discovered. These blacklists are not able to keep pace with ever emerging, evolving threats.

Smishing attacks leveraging text message communications are increasingly used to direct unsuspecting end users to fraudulent sites and log-in screens.

To combat these attacks, suspicious site identification and takedown also is commonly employed by threat intelligence enterprises. The issues with this method are time lag and completeness. This method cannot identify all fake sites as it relies mostly on finding similarly named domains, while attackers often use nondescript uniform resource locators (URLs). An attack can occur in the time between the organization requesting takedown of the fake site and it being taken down.

The Effect of Ineffective Approaches

Regardless of the method used, attacks succeed by misdirecting users to counterfeit, fraudulent websites where their personal and financial information and login credentials are stolen. This information is later used to steal money, execute fraud, steal identities and perpetrate many other types of scams. This results in harm to the consumers who were attacked and the organization with which they interacted. Organizations are often forced to spend time investigating reported attacks, verifying damages to customers, and reimbursing defrauded customers in increasing amounts and frequencies, either directly or indirectly via discounts.

Moreover, it has become popular for legislators to enact regulations that put the responsibility on the organizations to take proactive actions to protect their customers.[9] Cyberattacks erode the digital trust of the defrauded customers and those who hear about these attacks—including legislators—negatively impacting the essential trust relationship with the brand.

> Customers are already educated about the threats facing their online transactions but few implement the complex steps needed to stay safe online.

Existing security approaches have proven inadequate because by the time threats are discovered and mitigating actions are taken, the damage typically has already occurred. Customers who fall victim to phishing traps often blame the impersonated organization, which can be detrimental to maintaining digital trust. One study found that an average of 44 percent of customers have stopped transacting with an organization due to a lack of trust resulting from cyberattacks.[10]

Achieving Digital Trust

To achieve digital trust, any approach to security should include real-time capabilities, full visibility for the organization and its end users, and proactive damage prevention. Because threats continue to evolve in sophistication, solutions need to be equally sophisticated and adaptive, incorporating artificial intelligence (AI) when possible.

When an organization is attacked, it should ideally have a layer of security that warns its customers and prevents them from entering sites that are impersonating the brand. Assuming that not every attack can be stopped in real time, which depends on the specific techniques used by attackers, the organization's security team needs to quickly assess the nature of the attack, the target of the attack and the scope of the damage. This information enables the security team to implement a timely response to stop the attack before it can do further damage and to alert impacted end users of the threat.

To foster confidence in the legitimacy of an organization's online presence, there should be a method for the organization to provide clear proof to end users that the site they are visiting is indeed a brand-authentic digital presence. Such proof should be unforgeable, clearly visible and intuitive. It should allow end users to immediately differentiate fake sites from authentic ones. This extends the enterprise's zero trust concept model, which significantly enhances digital trust by showing customers that the organization is taking a proactive and personalized approach to securing the enterprise ecosystem.

Currently, the only ways for end users to know whether a website is legitimate are by inspecting the lock icon next to the browser's address bar and by visually comparing the displayed URL with the known legitimate URL of the organization. These methods are impractical and ineffective as they place the authentication burden on the end user.

To be effective, any security approach should be:

- Easily accessible and understandable to customers without requiring them to significantly change their behavior or invest time in education
- Affordable for organizations of any size
- Automatic and transparent to end users
- Easy to implement and manage
- Independent of but compatible with existing solutions, including security information and event management (SIEM) systems
- Include real-time identification and alerts
- Able to identify and stop existing, new and emerging threats (-1, 0, +1 day)
- Able to provide the end user with visual confirmation of website authentication

Solutions that meet these criteria would contribute significantly to achieving digital trust since end users could be confident that they are accessing a legitimate digital presence of the organization with which they intend to interact.

There should be a method for the organization to provide clear proof to end users that the site they are visiting is indeed a brand-authentic digital presence.

Practical Approaches to Achieving Digital Trust

Most impostor attacks direct end users to counterfeit websites and login and password reset pages. Effective approaches to limit this exposure include:

- Scanners and crawlers that constantly scan the web can be used to detect imposter sites. While these can be effective, they are not 100 percent accurate and can return false positives. When an impostor site is found, there is a takedown process. The impersonated organization needs to file a takedown request with the domain registrar and provide proof that the site is a phishing site. The domain registrar then informs the hosting organization that the site is indeed a fake. A response typically takes two to three weeks.
- Organizations and individuals buy website domains from providers. Domain Name System (DNS) providers use application programming interfaces, (APIs) to determine which domains are similar to authentic domains and may be attempting to impersonate them. This is a semimanual process. As soon as a pattern is detected, a manual takedown process is initiated.
- Instead of looking for DNS vulnerabilities or scanning for impostor sites, the Proof of Source Authenticity (PoSA)[11] approach is end user-centric. Since imposter attacks are continuously evolving and primarily target end users, this approach provides real-time automatic assurance of authenticity to all end users. This approach is agentless and implemented by the organization by installation on its website. It identifies when the site is being copied and launched from a domain that is not an authentic domain; presents users with a red alert on fake sites to warn users against accessing it; notifies the security team of the attack; and presents a digital watermark on the authentic site that proves to users that it is indeed the destination they desired to reach. With this approach, end

LOOKING FOR MORE?

- Read *Beating the Adversary at Their Own Game With Zero Trust. www.isaca.org/zero-trust*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

users can be sure they are always interacting with the authentic source and not a criminal impostor. Further, this approach provides real-time alerts to the organization as to the source, the nature of the attack, and which users have been targeted.

Conclusion

The digitization of the world has forced a fundamental shift in how organizations, their customers and other third-parties interact to ensure the essential trust relationship. When digital trust is not prioritized, an organization's brand and business health can be severely impacted. Without digital trust implementation, a single well-publicized attack could not only diminish the return on the organization's security investments but also damage its reputation, thus critically endangering customer relationships. Therefore, new methods are needed to address the complexity of the threats targeting digital interactions.

Organizations that hope to be at the forefront of the digital trust transformation should extend their enterprise zero trust models to include all members of their end-user ecosystem by implementing solutions that can provide real-time detection, protection and visibility.

Endnotes

1 ISACA®, *Digital Trust: A Modern-Day Imperative*, USA, 2022, *https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/white-papers/digital-trust-a-modern-day-imperative_whpdt_whp_eng_0322.pdf*

2 *Ibid*.

3 *Ibid*.

4 Singleton, C. *et al*.; *X-Force Threat Intelligence Index 2022*, IBM Security, February 2022, https://*www.ibm.com/downloads/cas/ADLMYLAZ*

5 *Help Net Security*, "Phishing Reaches All-Time High in Early 2022," 13 June 2022, *https://www.helpnetsecurity.com/2022/06/15/2022-total-phishing-attacks/*

6 AARP, "Half of U.S. Adults Have Been Targeted by Impostor Scams, Says AARP Survey," 19 February 2020, *press.aarp.org/2020-2-19-AARP-Survey-Shows-Half-of-US-Adults-Targeted-by-Impostor-Scams*

7 Diaz, A.; A. T. Sherman; A. Joshi; "Phishing in an Academic Community: A Study of User Susceptibility and Behavior," *Cryptologia*, vol. 44, iss. 1, August 2019, *https://www.researchgate.net/publication/335162516_Phishing_in_an_academic_community_A_study_of_user_susceptibility_and_behavior*

8 Hazam, G. *et al.; How to Protect Your Brand and Customers Against Impostors Using Proof of Source Authenticity (PoSA)*, MEMCYCO, Israel, 2022, *https://www.memcyco.com/home/wp-content/uploads/2022/10/Memcyco_White_Paper.pdf*

9 United Kingdom Parliament, Online Safety Bill, United Kingdom, 2 November 2022, *https://bills.parliament.uk/bills/3137*

10 PricewaterhouseCoopers (PwC), "The Complexity of Trust: PwC's Trust in US Business Survey," United Kingdom, 2021, *www.pwc.com/us/en/library/trust-in-business-survey.html*

11 *Op cit* Hazam *et al.*