Zero Trust Architecture Made Simple for Lawyers

by Sharon D. Nelson, Esq. and John W. Simek

We are still unconvinced that we will ever know the full extent of the damage from what is perhaps classified as the worst data breach ever. The compromise of the SolarWinds Orion platform has impacted approximately 18,000 public and private sector customers according to Cyber Unified Coordination Group (UCG). The UCG also said that the Russian-backed Advanced Persistent Threat (APT) group is most likely responsible for the SolarWinds hack. As the investigation continues, we are learning more and more details about the attack and those impacted.

What we do know is that the attackers spent many, many patient months learning about the SolarWinds environment and determining the best and most effective way to insert backdoor access into the Orion product. The supply chain attack was extremely sophisticated and a real wake-up call for cybersecurity professionals.

It is now painfully obvious that the traditional castle and moat designs for security don't work in these modern computing days. We can't just create perimeter security by walling off our resources and controlling access through a firewall. We are very much a mobile workforce and many of the services we utilize in our law practices are cloud based. We need a new approach to secure access to the confidential data law firms possess.

The National Institute of Standards and Technology (NIST) released the final version of its Zero Trust Architecture (ZTA) publication (NIST Special Publication 800-207) in August 2020, which will help organizations deploy a security model for the future. The National Security Agency (NSA) and Microsoft are also advocating for Zero Trust Architecture to help combat sophisticated cyber-attacks such as SolarWinds.

The obvious question is…what is zero trust? The concept of zero trust networks has been around for at least a decade, but cybersecurity events such as SolarWinds and attacks on Microsoft on-premise Exchange servers has brought renewed focus to the Zero Trust discussion.

The NSA stated, "The Zero Trust security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting critical assets (data) in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, allowing or denying access to resources based on the combination of several contextual factors."

In other words, trust nothing and constantly verify. It gives new meaning to Ronald Reagan's words, "Trust, but verify."

The current security perimeter model is one and done. Once a device or person is trusted, that trust is not re-verified. This means if someone gains access to a user's credentials, they will be allowed to access the network and data no matter who they really are. Since users and devices regularly move from inside

the network to outside, the ZTA approach means that a once-safe device cannot be assumed to still be safe.

We won't drill down into the intimate details of ZTA since it will probably make your head hurt. Instead, we'll describe some general concepts and techniques for moving forward with ZTA. As previously stated, our approach is to trust nothing and to constantly verify.

The 'trust nothing and constantly verify' means that every device, user, application, network traffic, etc. is untrusted. Every attempted access needs to be authenticated and explicitly authorized with the least amount of privilege. Multi-factor authentication is a good first step to authenticate a user. MFA was very influential in helping to uncover the initial SolarWinds compromise of FireEye. A second MFA device (a phone) was registered to a user using valid credentials. The second registration was an unusual event and required verification. When queried, the authorized user verified that they did not register a second device, hence an impersonator was accessing the network.

Our network designs will also need to be changed. Instead of a single "flat" network, we'll need to segment the network into much smaller pieces that can be monitored and controlled. A user could be authorized for access to resources on one segment but denied access to resources on a different segment.

It's not just users either. Application access also needs to be authorized. In other words, if a piece of software wants to access data in a database, the application needs to be authenticated for access. The type of access is also verified and granted. Just because an application can access data in a database doesn't mean it can actually change the data. Perhaps only read or view access is granted. Next generation firewalls will monitor and control traffic between the various segments.

Another baseline principle is always to assume a breach. The assumption is that an attacker has already compromised your network and is present within the environment. The assumption is further justification for segmentation of the network. Compromising one segment won't allow complete access to all of the firm's data. Assuming a breach means all access should be denied by default. It also means that we need to have a way to continuously monitor access to all resources, monitor any configuration changes and certainly monitor all network traffic for suspicious activity.

ZTA will not happen overnight and is a long-term project. TechRepublic published a very good "cheat sheet" for implementing ZTA and boiled the project down to five steps.

1. Segment the network
2. Implement access management and identity verification
3. Extend the principle of least privilege to the firewall
4. Firewalls should be contextually aware of traffic
5. Gather, and actually analyze, security event logs

These five steps will allow for a controlled implementation in a gradual fashion. As we move our computing environment to a Zero Trust Architecture, we must be cognizant of the user experience. Any restrictions or access to resources cannot be difficult or time consuming for the user. It needs to be a "frictionless" rollout. If it isn't already obvious, there is a lot of data to analyze in order to make the necessary decisions to allow whether to grant access and the type of access that should be allowed.

Firms will ultimately need to implement a SIEM (Security Information and Event Management) solution to analyze all of the collected data in order to make those access decisions.

Zero Trust Architecture is the future of our computing environment. COVID-19 has certainly accelerated the need to change the way we authorize and verify people, devices and application access. We are already seeing ZTA being adopted, mostly in the corporate world. Law firms will have a slower adoption rate, but we expect ZTA to be widely embraced by law firms in 2022.

Sharon D. Nelson, Esq. is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA. snelson@senseient.com.

John W. Simek is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional, Certified Ethical Hacker and a nationally known expert in the area of digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm. jsimek@senseient.com.