WHAT SUNBURST CAN TEACH GOVERNMENT ABOUT ZERO TRUST

In this Q and A, Andrew Harris, senior director of public sector technology strategy for CrowdStrike, explains what the 2020 SUNBURST cybersecurity attack can teach government about how it should authenticate identities and protect both cloud-based and on-premises environments.

What was the 2020 SUNBURST cyberattack, and how did it impact state and local government?

The SUNBURST attack occurred when nation-state actors inserted themselves into a widely used supply chain. Because the supply chain was tainted, the adversary could then enter numerous customers' environments, including state and local government.

This attack showed government that if your on-premises environment is compromised, an adversary can then jump onto your cloud, bypassing any multi-factor authentication (MFA) you have. Before, many people thought that if you applied MFA in the cloud, no one could move from your on-premises resources to the cloud. This attack showed this was not the case.

What did SUNBURST demonstrate about the importance of Zero Trust within the public sector?

There are three important tenets to Zero Trust: trust nothing, verify everything and anticipate breach. If you are anticipating an attack, and you are continuously evaluating users, then you can react quickly to contain a breach.

Zero Trust is important for state and local government because it allows them to maintain mission resilience. Government needs to be able to face a capable adversary while still supporting their constituents.

Along with SUNBURST, the COVID-19 pandemic also heightened government focus on Zero Trust. In this environment of remote government workers, network boundaries are no longer the penicillin to protect against cyberattacks.

What are some challenges state and local governments face when trying to secure identities?

Some governments say they want to move all their identities onto the cloud to be secure. However, this can lead to operational risks. If you are dependent on one cloud service provider and that service goes down, then you face mission resiliency issues. If the service goes down, employees won't be able to authenticate as users or access any resources on that service.

Everyone thinks they have to move fully onto the cloud to apply Zero Trust concepts. But you can achieve Zero Trust in a true hybrid environment that includes on-premises and cloud services.

What should state and local governments look for in an identity protection solution to defend themselves against attacks?

You want a tool that will provide you with full visibility into what is happening in your on-premises, cloud and hybrid environments. Your tool should look holistically at your environment.

You want a solution that can identify all security dependencies, measure them continuously, and let you know if something changes or if you need to respond to a breach.

Also think about how to utilize your existing vendors so you don't have to acquire all brand-new technologies or go all in with one vendor. You want to hold your vendors accountable so you have the right integrations to enable you to react to any attack.

A recent executive order to improve the nation's cybersecurity shows an increased understanding within federal government of the need for Zero Trust Architecture. This is a moment of tremendous opportunity for state and local governments to inspect their own cybersecurity and make the move toward Zero Trust.