Securing Government Networks – A Four-Pronged Approach

Security is broader than just an IT responsibility. All users and endpoints play a role in information security now. That's why adoption of zero trust is becoming more important in securing federal networks.

Have you started rethinking your assumptions about securing your agency's network yet? In an era of remote work, cloud computing and collaboration technologies, you can't always be sure that the only people on your network are trusted employees.

You can't assume that more access is better than less access. You can't even assume that all responsibility for security rests with your IT group.

Security is broader than just an IT responsibility. All users and endpoints play a role in information security now. That's why adoption of zero trust is becoming more important in securing federal networks.

Chris Roberts
Federal Technology Director
Quest Software

Zero trust addresses security at all levels of your agency by refusing access until anything attempting to use the network — APIs, nodes, people and devices — is fully authenticated. As you rethink your assumptions, keep in mind the following, four-pronged approach.

1. Know what data is in your network and who has permission to access it.

The first step in protecting your data is knowing what type of data you have, where it is located and who has access to it. That means good data governance — understanding exactly who has specific rights to view, access and manipulate the data based on their role, and whether the person is in a secure place to access the data.

Governance starts with structure: cataloging the data and applying metadata to it. With structure, it's much easier to classify data properly, determine where it is at all times and see who controls it. Then comes role-based access, where only users with the right roles are permitted to access the data. There should be no assumptions about users and their roles.

2. Know your nodes.

Unlike the past, nodes on your network now range from PCs, tablets and smartphones to internet-of-things (IoT) devices like smart thermostats, security systems, and intelligent heating-venting-air-conditioning (HVAC) systems. Your agency must be able to scan them, patch them and block ports on them.

Do you have a way of knowing every IP address and node on your network, and whether a given IP address goes to a port scanner? Not likely. You can't keep up with all the nodes on your network manually, but with automated tools, you can find and lock down any vulnerable ports.

3. Know your APIs.

Most on-premises networks are closed. Within their defined perimeters, ports cover all connectivity options. But modern architectures move data over open APIs rather than through ports, and the APIs are usually built into the applications and services.

Apply zero trust to APIs as you would to protect external services and SaaS-based applications. You may not even be aware of the APIs, but they are important entry points, and the vendors who supply technology to your agency should help you identify and secure them. Use automated tools for deep inspection of all your applications.

> “Privileged account management ensures that, if you have a domain administrator account, you know exactly who will be using it, what time they can use it and the machine they can use it on.

4. Know your users.

Remember when you could assume you knew your users if they were in Active Directory or LDAP? That was then. Now, Active Directory and LDAP are steps on the path to your domain controllers, the big prizes that hackers are after.

That's why it's necessary to know the authenticity of a user before allowing access. Now, knowing your users means building a profile based on details like their location, their devices, the IP addresses they use, how they connect and even how they use their mouse and keyboard. A profile makes it easier for you to spot unusual behavior and, when necessary, limit or deny access.

This is where privileged account management (PAM) comes in. It allows agencies to secure, control and audit privileged accounts by providing appropriate access. PAM ensures that, if you have a domain administrator account, you know exactly who will be using it, what time they can use it and the machine they can use it on.

Network security is non-negotiable.

Zero trust is a way of taking network security back to basics for everything from data, APIs, nodes and ports to users.

What's a good, first step toward zero trust? Start by avoiding superusers. In every organization, certain users want access to more resources than they'll ever use, but providing that much freedom is dangerous. In fact, it's the opposite of zero trust.

In both public and private sectors, the future of network security and zero trust lies in artificial intelligence. This is the perfect application for AI and machine learning. The more data we have, the better and faster our responsiveness to cyber incidents will become. ■