Demystifying Cybersecurity: It’s About Trust, Visibility, and Resilience

By Chris Coleman, Director of Cybersecurity for U.S Public Sector, Cisco

What used to be called information security is now commonly called cybersecurity. The new term reflects the reality that more than information is now at stake. Governments also need to protect the vast array of vital services that operate over networks, from energy and transportation to world financial engines and intelligence operations.

Recently Cisco convened a team of experts to define cybersecurity in terms of the capabilities that public– and private–sector organizations need to protect the mission and keep vital services up and running. At the highest level, the answers are trust, visibility, and resilience.

Trust: Scope Out the Challenge

Before you can protect a connection or device, you need to know it exists. This is harder than it sounds in state and local governments with steadily growing numbers of servers, services, end-user devices, and users. Therefore, the first tenet of a cybersecurity plan is knowing:

- Who is on the network
- What devices are on the network
- When access occurred
- Where access occurred
- How the device is connected

Visibility: See Risk to Stop It

Visibility requires tools that constantly scan to identify and manage risk. Examples include malicious code that infiltrates the network, unpatched operating systems, and misconfigured applications that enable policy violations, such as copying files to removable media.

A certain type of malware stealthily moves from host to host, enabling someone outside the network to collect passwords and exfiltrate information. Depending on the specifics of the attack, the clue might be movement within the network, command-and-control actions initiated from outside the network, or large volumes of data leaving the network using nonstandard protocols. To give government IT teams visibility into the threat, the network needs the intelligence to detect these clues and more.
Resilience: Continue Supporting the Mission When Under Attack

Threats can slip through even the most advanced cybersecurity programs, and the reality is that successful cyberattacks against government networks are inevitable. Therefore, the third tenet of cybersecurity programs is to give them the resilience to continue delivering citizen and workforce services when the IT infrastructure is under duress due to a cyberattack, environmental disaster, or even a human error such as switch misconfiguration.

To build resilience, first determine which network-based resources are most critical to allowing personnel to continue communicating and accessing information they need to do their jobs. Then implement the technology and resources to safeguard those resources.

Make Adversaries Work Harder

By applying the three principles of cybersecurity—trust, visibility, and resilience—state and local governments can formulate a strategy to mitigate risk and recover quickly when attacks do occur. The network is a critical piece of the strategy, and a well-executed refresh and upgrade plan continually strengthens government’s cybersecurity posture to make adversaries to work harder.

Finally, remember that cybersecurity programs also require proper staffing to gain the full value of technology investments. Within the IT organization, network, application, and security teams need to collaborate on an effective defense, because threats don’t pay attention to organizational boundaries.

To learn more about Cisco® cybersecurity solutions and services for government, visit: