Risks to Connected Communities: Expanded and Interconnected Attack Surface

Integrating public services into a connected environment can increase the efficiency and resilience of the infrastructure that supports day-to-day life in our communities. However, municipalities considering becoming smart cities/connected communities should thoroughly assess and mitigate the cybersecurity risk that comes with this integration.

For more detailed information on this risk and others, scan the code here to access the Cybersecurity Best Practices for Smart Cities guide.

Integrating a greater number of previously separate infrastructure systems into a single network expands the digital attack surface for interconnected organizations. This expanded attack surface increases the opportunity for threat actors to exploit a vulnerability for initial access. After gaining access, the threat actor could then move laterally across networks to cause cascading, cross-sector disruptions of infrastructure operations or threaten confidentiality, integrity, and availability of the organization's data, systems, and networks.

Example: Malicious actors accessing a local government internet of things sensor network might be able to obtain lateral access into emergency alert systems if the systems are interconnected.

Integrating more systems diminishes the ability of network administrators and security personnel to understand and track collective system risks. The lack of visibility also extends to components that support integration and are owned and operated by vendors.

Mitigate the Risks

Communities implementing smart, emerging, and connected technologies should assess and manage risks associated with complex interconnected systems. To reduce risk, it is critical that system owners maintain awareness and control of the evolving network interconnectivity as well as the individuals/vendors responsible for the overall system and each segment. Jurisdictions should ensure secure planning and design through implementing the following best practices:

- Apply the Principle of Least Privilege
- Enforce Multifactor Authentication
- Implement Zero Trust Architecture
- Manage Changes to Internal Architecture Risks
- Securely Manage Smart City Assets
- Improve Security of Vulnerable Devices
- Protect Internet-Facing Services
- Timely Patch Systems and Applications
- Review the Legal, Security, and Privacy Risks Associated with Deployments

The Cybersecurity Best Practices for Smart Cities guide provides recommendations to balance efficiency and innovation with cybersecurity, privacy protections, and national security. Organizations should implement these best practices in alignment with their specific cybersecurity requirements to ensure the safe and secure operation of infrastructure systems, protection of citizens' private data, and security of sensitive government and business data.

Scan to read more about CISA's Cybersecurity Performance Goals:

cisa.gov
connected.communities@cisa.dhs.gov
linkedin.com/company/cisagov
@CISAgov
facebook.com/CISA