PUBLICATION

Lessons From the Suffolk County Ransomware Attack That Apply to All Businesses

Authors: Justin S. Daniels
October 21, 2024

In December 2021, Suffolk County, New York, experienced a significant cybersecurity breach that culminated in a ransomware attack in September 2022. The attack went undetected for months, allowing the attackers to install remote-access tools and steal sensitive files before encrypting the county's data. This incident, which cost taxpayers $25 million, serves as another data point about the vulnerability of IT systems, especially public ones.

Governmental agencies are particularly vulnerable to ransomware attacks due to budget challenges and the high cost of downtime. However, governments are no different from other organizations in balancing the tension between the allocation of scarce budget resources to projects that drive revenue and profitability, as opposed to managing risk.

The key lesson for any organization from the Suffolk County experience is clear: spend your budget to focus on the basics. Here are some important steps that organizations, especially municipal governments, can take to bolster their cybersecurity defenses:

1. **Keep Systems Up to Date**: Ensure that all systems including firmware, operating systems, and applications, are regularly updated to protect against known vulnerabilities;
2. **Strong Password Policies**: Require long (16+ character), complex passwords, and encourage the use of password managers to enhance password security;
3. **Multifactor Authentication (MFA)**: Implement MFA company-wide for all remote access methods and internal privilege elevations to add an extra layer of security;
4. **Use of VPNs**: Require employees to use a VPN when connecting to remote wireless networks to protect data in transit; and
5. **Incident Response Plan and Tabletop Exercises**: Your organization should have a written incident response plan you practice at least annually.

As we observe Cybersecurity Awareness Month, it's important to reinforce the basics of cybersecurity hygiene, especially as we are asked to use new and nascent technologies like generative artificial intelligence.

If you have any questions or would like assistance in reviewing your cybersecurity policies and procedures, contact Justin S. Daniels or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity team.