Current State of Cybersecurity

November 3, 2022

VERMONT
AGENCY OF DIGITAL SERVICES

Cybersecurity Trends from Other States

- Talent Gap
  - Salary pressures
    - ADS-Security suffers from this trend. Salary studies show the gap between open market and State salaries.
  - Contractor support
    - ADS-Security has relied on contractors increasingly to meet operational requirements (SOC, firewalls, networks).
  - Remote work
    - ADS-Security does well with our remote work policies. Staff cite the hybrid model as a plus for flexibility and productivity.

Cybersecurity Trends from Other States

- Whole of State Approach
  - Tighter ties between branches
    - Three-party discussions between ADS, LEG, and JUD
    - Support for election security with SOS
  - Local and municipal governments receiving services from the State
    - SLCGP as part of IIJA will drive closer ties with L/M and create an environment where we can offer State administered services related to cybersecurity
  - Critical Infrastructure reporting and regulations at the State level
    - Exploring steps to create a framework for CI in Vermont. Ties into Emergency Management and critical services

Cybersecurity Trends from Other States

- Cyber Maturity
  - Refining cybersecurity plans
    - ADS-Security refining plans to address trending initiatives and take advantage of momentum of other states
    - Documenting current practices and process as part of consolidating efforts
  - Multifactor authentication
    - Vermont has had MFA for 4+ years, enhancing MFA to adaptive system is on the roadmap
  - Risk assessment and remediation
    - Cornerstone of our cybersecurity program (next slide)

Risk Maturity Journey

- Improvement in platform updates
  - Marked reduction in old operating system platforms
  - Pre-set configuration standards for new systems
- Software patching cadence
  - Weekly scans and reporting
  - Tracking vulnerability loads and trending over time
- Intrusion prevention and endpoint detection
  - Continued refinement of sensors
  - Tie-ins to threat intelligence feeds

VERMONT
AGENCY OF DIGITAL SERVICES

Cybersecurity Projects In-progress

- Security Information and Events Manager (SIEM)
  - Eliminates fractured approach to log collection and aggregation
  - Allows for enterprise-wide identification of attack and infection patterns
  - Includes vendor supported response
  - Incorporates playbooks for automated response

- Firewall and Security Architecture
  - Addresses network challenges brought about by remote work (statewide)
  - Re-allocation of resources to areas of high traffic
  - One core data center complete
  - Second scheduled for December 2022

Overarching Threat Trends

- System and network vulnerabilities are trending down through risk management efforts
  - Bucking the trend
- Attacks on our internet edge are up sharply
  - Geopolitical pressures
- Increase in incidents
  - Phishing
  - Browser plug-ins
  - Watering hole attacks
- No ransomware attacks in State government
  - We are not immune, just spared

VERMONT
AGENCY OF DIGITAL SERVICES

VERMONT
AGENCY OF DIGITAL SERVICES