**Guide to Prioritizing Ransomware Defense for Critical Public Institutions based on 2021 attacks**

This document is intended underline security controls offering a high return on investment based on trends from 2021 ransomware attacks targeting U.S. utilities (Colonial Pipeline), municipalities (D.C. Metro Police), and public schools (Broward County, FL). Observations and TTPs were related to a subset of the CIS Controls v7.1 known to align with ransomware.

1. **Ensure All Backups Have at Least One Offline Backup (CIS Sub-Control 10.5)**

It’s not “if” you will need your backups, it’s “when.” Natural disasters and human error already work to ensure any digital data which is not backed-up has a finite life span. The importance of protecting data (backups) and ensuring they can be effectively restored to production when needed cannot be understated. Sub-control 10.5 is spotlighted given most modern ransomware variants are hardcoded to delete or encrypt any backup files they come across.

1. **Deploy Automated Operating System Patch Management Tools (CIS Sub-Control 3.4)**

Patch, patch, and keep patching. Automate where possible. Operating system vulnerabilities are commonly exploited by threat actors seeking to establish initial access, elevate their privileges, and move laterally throughout victim networks. Case studies illustrated Conti, Babuk, and DarskSide attacks were associated with several prominent OS vulnerabilities (e.g., CVE-2017-0143/0148, CVE-2021-26855, CVE-2021-27065, CVE-2020-1472, CVE-2021-1675, and CVE-2021-34527).

1. **Require All Remote Login to Use Multi-Factor Authentication (CIS Sub-Control 12.11)**

Nearly all ransomware attacks are predicated on some degree of remote access into or about victim environments; the attacks detailed in the case studies were no different. Secure MFA solutions add an additional layer of complexity (i.e., something you know + something you have) to the remote login authentication process that is extremely effective in reducing these types of attacks. All remote access solutions (e.g. VPN, RDP, SSH, TeamViewer, AnyDesk, etc.) are best protected when securely integrated with MFA. The DarkSide ransomware attack on the Colonial Pipeline System was reportedly enabled via leaked credentials used to access an internet-facing VPN system; MFA would have prevented the attack.

1. **Ensure Anti-Malware Software and Signatures Are Updated (CIS Sub-Control 8.2)**

Anti-Virus remains an important mitigation against ransomware attacks because endpoints have access to sensitive data and systems that must be safeguarded. The catalog of available anti-malware products are certainly not created equally nor are any of them 100% at defending against the gamut of ransomware. However, just the presence of AV software will cause even the most experienced hackers to tread lightly or hopefully consider moving on to easier targets to avoid detection. To perform at its very best AV software must regularly update their scanning engines and signature databases.

1. **Maintain and Enforce Network-Based URL Filters (CIS Sub-Control 7.4)**

The ransomware attack lifecycle includes several tactics and techniques that commonly leverage HTTP/S (e.g., C2 infrastructure, data exfiltration, and phishing campaigns). TTPs observed from all three case studies showed sensitive data was transferred out of internal networks using popular cloud-based websites (e.g., mega.io, mega.nz, pCloud, Google Drive, and GitHub).