CYBER SECURITY, FRAUD AND PHISHING – LESSONS LEARNED AND BEST PRACTICES

Peggy Halik – Village of Woodridge

Chris Conrad – Village of Highland

Jerry Irvine

Moderator – Jigar Desai

FEBRUARY 10, 2023

CYBER SECURITY: A LOCAL GOVERNMENT PERSPECTIVE

Village of Woodridge

Established 1959

FEBRUARY 10, 2023

PEGGY HALIK

Assistant Village Manager – Village of Woodridge

Peggy has served as the Assistant Village Administrator for the Village of Woodridge, IL since 2003. She has over 30 years of municipal experience and is the current ILCMA President-Elect. Previously, she was with the City of Naperville for ten years in a number of operating departments and the City Manager's Office. She received both her BA and MPA from Northern Illinois University. For the past 20 years she has overseen Woodridge's IT division. Her team has successfully navigated through a data breach, coming out with lessons learned and improved security practices.

Village of Woodridge

Established 1959

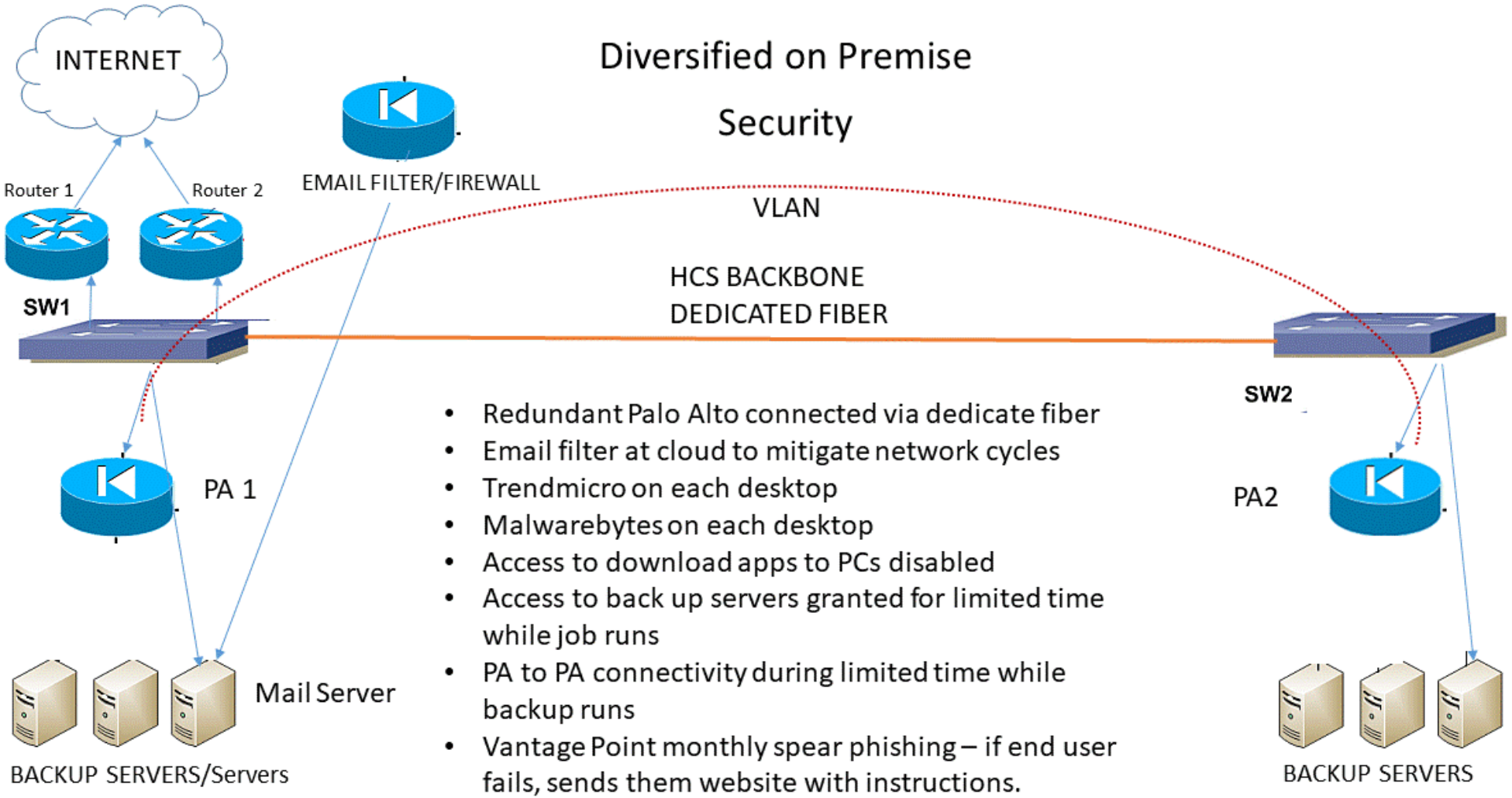
FEBRUARY 10, 2023

CHRIS CONRAD

City Manager – Village of Highland

Chris Conrad served 12 years in the US Army Reserves, 21 years as a police officer retiring as a chief of police in May 2021 and currently serves as the city manager for the City of Highland, IL. Chris graduated from Saint Louis University Law School in 2014 and the Southern Police Institute at the University of Louisville in 2018. Chris has been a licensed attorney in IL since November of 2014 and is a member of the Illinois State Bar Association, IL City Managers Association and past member of the IL Chiefs of Police, Southern IL Police Chiefs and International Chiefs of Police Associations. He has served on the Illinois Municipal League 2021 and 2022 Resolutions committees and currently serves on the Governor's Task Force on Constitutional Rights and Remedies.

Diversified on Premise Security



- Redundant Palo Alto connected via dedicate fiber
- Email filter at cloud to mitigate network cycles
- Trendmicro on each desktop
- Malwarebytes on each desktop
- Access to download apps to PCs disabled
- Access to back up servers granted for limited time while job runs
- PA to PA connectivity during limited time while backup runs
- Vantage Point monthly spear phishing – if end user fails, sends them website with instructions.

JERRY IRVINE

Assistant Village Manager – Village of Woodridge

Jerry Irvine has been deeply involved with the IT industry since 1987. As a result of his early experience, he became an expert in network communications and protocols when others in the industry were just learning how to use their first computer. Armed with this expertise, Irvine entered the consulting world working for companies like Network General and Advantis, performing detailed network analysis, design and troubleshooting. Since then, Irvine has filled MIS and CIO positions at multiple facilities and has managed more than 100 technicians and thousands of devices. He has led multiple project teams, such as the largest Microsoft Directory migration project ever. In 2008, Irvine was selected to join the National Cyber Security Task Force, a joint operation between the Department of Homeland Security and the U.S. Chamber of Commerce. This task force is responsible for advising federal decision-makers on cyber security policy and sharing best practices related to this urgent and ongoing need. His expertise on cyber security has been featured in a number of national and industry publications, including The New York Times, WGN Radio and Wired magazine.

Seven Effective Defense Strategies

1. IMPLEMENT APPLICATION
   - WHITELISTING
2. ENSURE PROPER CONFIGURATION /
   - PATCH MANAGEMENT
3. REDUCE YOUR ATTACK SURFACE AREA
   - (Segmentation)
4. BUILD A DEFENDABLE ENVIRONMENT
5. MANAGE AUTHENTICATION
6. IMPLEMENT SECURE REMOTE ACCESS
7. MONITOR AND RESPOND

•(NCCIC, 2016).

Seven Effective Defense Strategies

1. IMPLEMENT NEXT GENERATION ENDPOINT SECURITY SOLUTIONS
    - John McAfee: **"Antivirus is dead"**
        - May only detect 30% of known viruses
        - ***Antivirus cannot keep up. AV-test estimates a whopping 12 million new malware variants a month***
    - New technology is required
        - Major Characteristics of Next Gen Endpoint Protection (EPP)

            - Prevention
            - Detection
            - Mitigation
            - Remediation
            - Forensics

CARBON BLACK
ARM YOUR ENDPOINTS

CROWDSTRIKE

SentinelOne®

Seven Effective Defense Strategies

2. ENSURE PROPER CONFIGURATION & PATCH MANAGEMENT
   - Implement Automated Patch Management Solutions

   - Utilize configuration management tools and perform best practice analysis

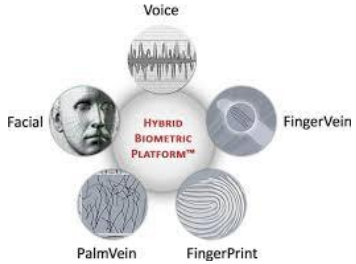
   - Perform periodic Application and Vulnerability Assessment Scans

Seven Effective Defense Strategies

3. REDUCE YOUR ATTACK SURFACE AREA
4. BUILD A DEFENDABLE ENVIRONMENT
   - Segmentation (Application, Communications, Network, Systems)
     - Create separate physical and logical networks to maintain secure environments (i.e. public Wi-Fi, PLC/SCADA/IoT, Client networks, VoIP)
     - Air Gap segments requiring legacy protocols and devices (i.e. PLC/SCADA/IoT)
   - Use Secure Protocols
     - Encryption, VPN
   - Protect Your Infrastructure
     - IIoT/IoT Aware Devices

Seven Effective Defense Strategies

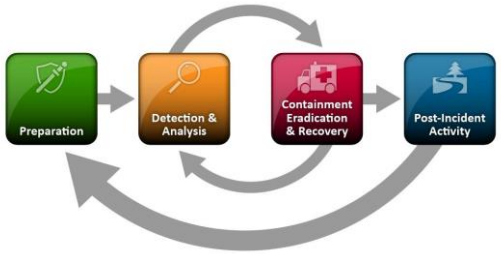
5. MANAGE AUTHENTICATION & ACCESS
   - Authentication
     - Unique and complex IDs and Passwords
     - Multi form factor authentication
     - Follow the principals of least privilege,
     - Disable Unused Accounts, Connectivity, Ports, Switches, etc.
   - Logical and Physical Access Controls / Rights Management
     - Follow the principals of least privilege



Seven Effective Defense Strategies

6. IMPLEMENT SECURE REMOTE ACCESS
   - Use Secure Protocols
   - Classify Users for access requirements and permissions
     - Limiting who has remote access and their user access controls
     - [conn

     - Define Incident Response Pla ch *.



* Source: NIST Incident Response Life Cycle

Seven Effective Defense Strategies

7. MONITOR AND RESPOND
   - Implement Automated Real-time Monitoring and Alerting tool to proactively analyze and report on systems and network communications, status, and utilizations
     - Define all missions critical devices to be monitored
     - Define who is alerted and escalation procedure

     - Implement Filtering and Logging

Questions?

Thank you for attending the Session.

Peggy Halik

Chris Conrad

Jerry Irvine

Jigar Desai