

# IT Cybersecurity Presentation

Manhasset Board of Education  
January 19, 2022

# **Overview of Presentation**

**Prior to the Attack**

**Lessons Learned**

**Cybersecurity Enhancements**

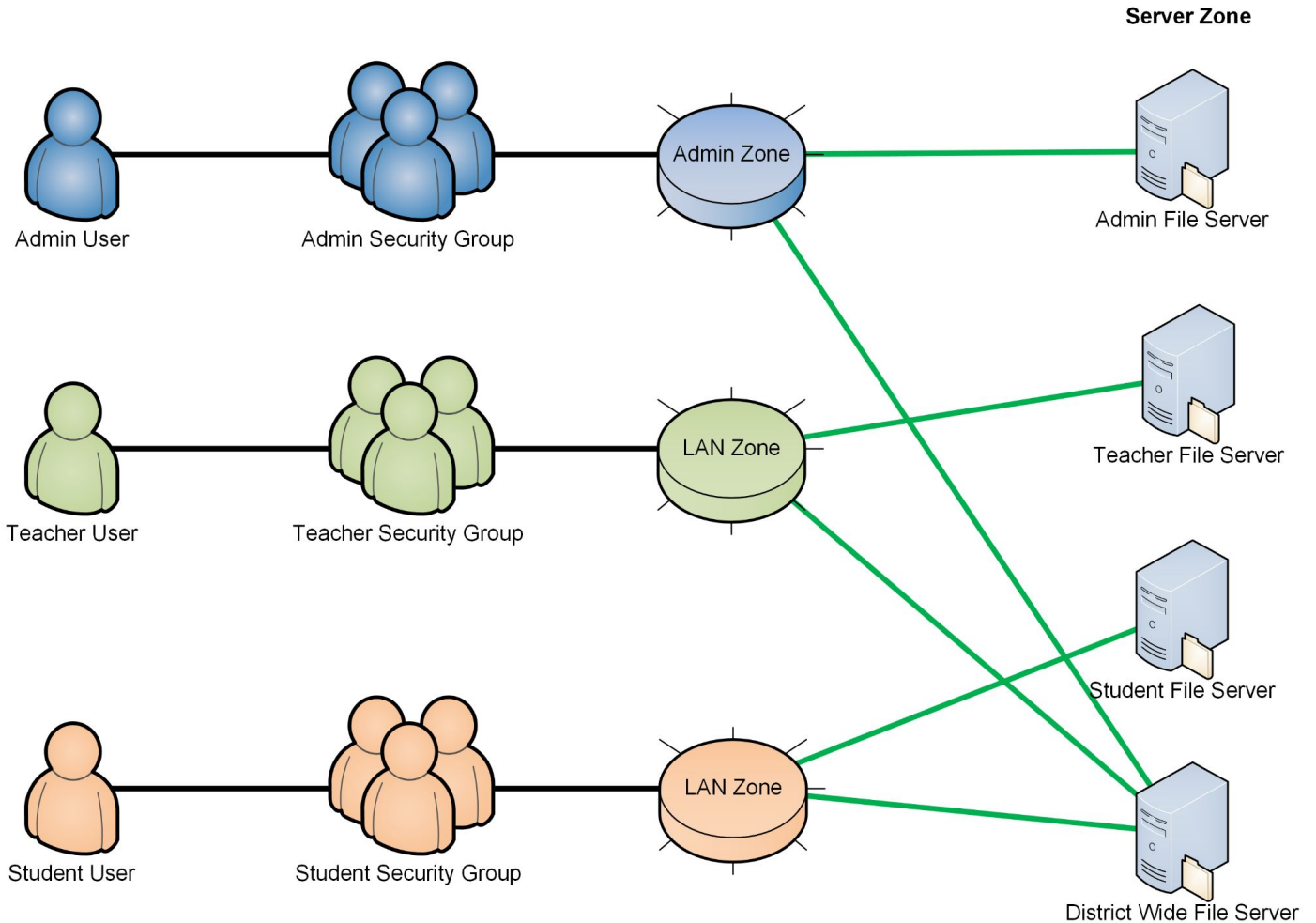
**Budgetary Implications**

Prior to the Attack

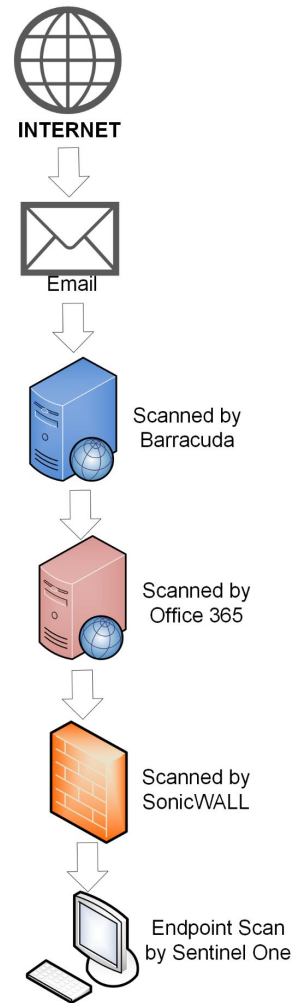
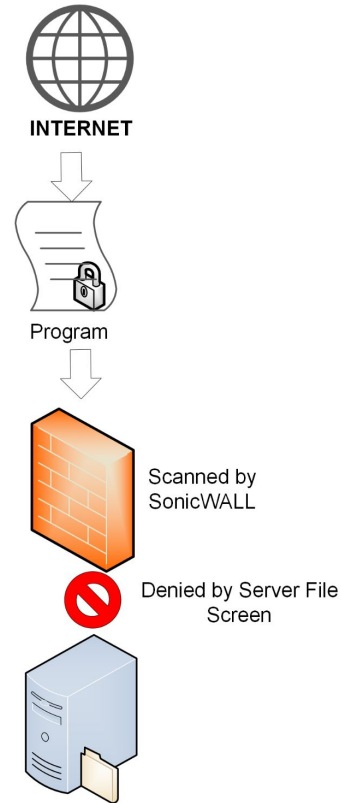
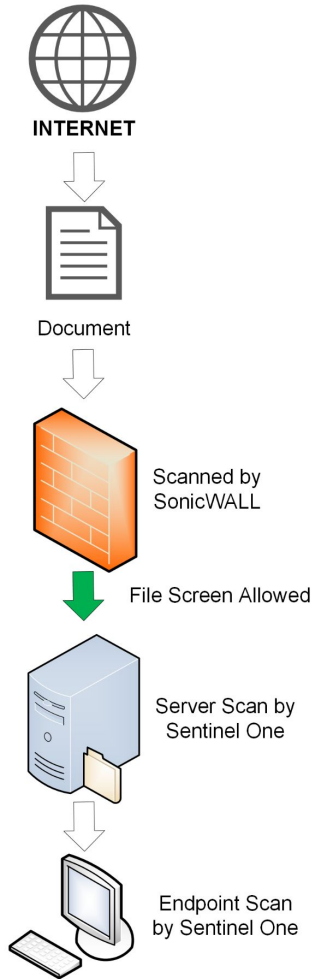
# Prior to Attack

- **Added Capture Client Endpoint Detection & Response (EDR) to specific endpoints**
- **CyberInsurance Coverage**
- **Added Secondary Cyberinsurance Policy**
- **Implemented mandatory password changes twice annually (Spring 2019)**
- **Network Segmentation put in place (Fall 2019)**
- **Contracted with Bonadio Associates for IT Audit (Winter 2020)**
- **Increased coverage levels on Cyberinsurance Policies (Summer 2021)**
- **Added Unitrends backup solution (Spring 2021)**
- **Began Multifactor Authentication rollout (July 2021)**

**Separate User Types & Network Zones** ensure that end users can only reach data to which they should have access.



# Layered Internet Protection by data type



# Unitrends Backup Solution

Hardened backup appliance was installed in the spring of 2021

Its location is obfuscated to end users; it is not browsable from the network; has unique username and passwords; not part of AD; pw is stored in a secure password vault

Reporting; sandbox capabilities for testing backup restores; Cloud base backup portion;

The device is pointed to our virtual structure and anything that is added to our structure is automatically backed up

“Synthetic full backups” allowed us to look back as far as two months to pull our systems back.

Closest to an air gapped back up

Service level accounts now have separate complex passwords maintained in password locker; none are domain level accounts;

# Lessons Learned

# Lessons Learned

Since the attack, discussions have been held with multiple cyber security experts from industry, state and federal agencies.

These resources have helped us to plan our approach for increased cyber security which will be outlined.

One key point that has been echoed by many is that staying abreast of rapidly evolving cyber security threats requires a high level of expertise and large amounts of time.

This consideration has led us to include a Managed Detection and Response (MDR) solution as one of the key components.

# Lessons Learned

- **LIMIT remote network access to those users with MFA**
- **MFA for on site server access**
- **EDR should be installed on all endpoints**
- **An MDR solution should be added**
- **Add length, complexity & lookbacks to all staff passwords**
- **Add complexity & lookbacks to student passwords grades 4-12**
- **Add electronic records management tools & procedures**
- **Increase Granularity of Network Segmentation (Microsegmentation)**

# Network Micro Segmentation

No Micro Segmentation

From	To	Priority	Source	Destination	Service	Action
LAN	VRF-Server	4  (Auto)	Any	LAN_FILE_SERVERS	Any	Allow

With Microsegmentation

From	To	Priority	Source	Destination	Service	Action
LAN	VRF-Server	111  (Auto)	LAN_AD_ALLOWED	LAN_FILE_SERVERS	SMB	Allow

# CyberSecurity Threat Surface

## **After Rebuilding our Network**

Remote access ONLY provided to those using MFA

MFA - all key IT & School Administrative Staff

MFA - internal access to network servers

Inbound traffic only from US IP addresses

Password complexity - 14 characters with password history ( cannot use last 5 passwords)

Network MicroSegmentation

Encrypted Password locker for IT workers & Key Staff

**EDR on all devices**

**MDR w/Security Operation Center (SOC) 24/7 monitoring**

# What Helped to Mitigate the Attack

Sophisticated Backup Solution

Network Segmentation

Paessler Alerts - pw change alerts, account lockout alerts, change in group member alert, access level changes;

Security event and management solution (Elastic Search Kibana and Log stache)

Monthly Nessus Scan meetings

IT Risk Assessment & Penetration Testing

Cybersecurity Awareness Training

# Security Enhancements

# Security Changes

## **NO remote access without MFA**

MFA needed to access all servers

Micro-segmentation - granular rules between zones further restrictive data movement

Wifi network segmentation

Guest network sits outside so that it physically doesn't touch any other network

Four wifi zones - Guest, Student, Teacher, Admin,

# Ongoing Actions & Considerations

Continue to utilize a multi-tiered approach to network monitoring:

- CSDNET Cybersecurity Team (weekly network scans; quarterly network enumerations deep dives)
- Bonadio Associates - external IT audit with penetration testing
- Reports from MDR from active threat hunting including dark web monitoring

Electronic Records Management (ERM)

- Review procedures for managing electronic records
- Explore tools to enhance ERM
- More sophisticated ERM solution

# Budgetary Implications

# Budgetary Impact of Added Critical CyberSecurity Tools

## Annual Cost Additions to the 2022-23 Budget and Beyond

Endpoint Detection and Response (EDR) - \$72,000

Managed Detection and Response (MDR) - \$54,000

Multi-factor authentication (MFA) - \$7,500

Password Locker - \$5,800

MS A5 Security - \$14,180

**Total Costs - \$153,480**