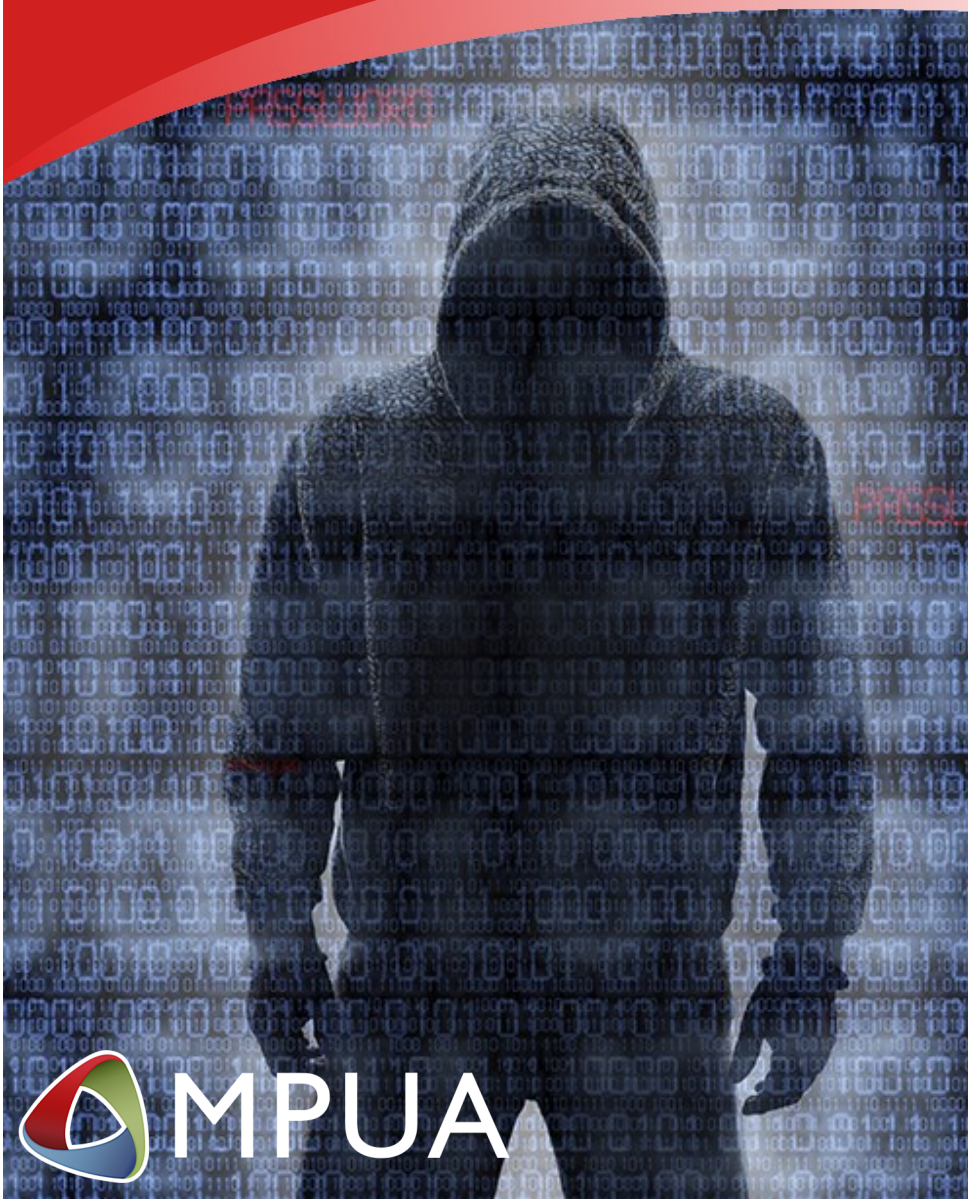
CYBERSECURITY PROGRAM



MPUA

THE MPUA CYBERSECURITY INITIATIVE

The utility industry has become increasingly aware of cybersecurity threats. In response, MPUA/MJMEUC launched a Cybersecurity Initiative to offer monitoring services that protect our utilities and show regulators, legislators, and the financial world that the group is doing its due diligence about these risks.

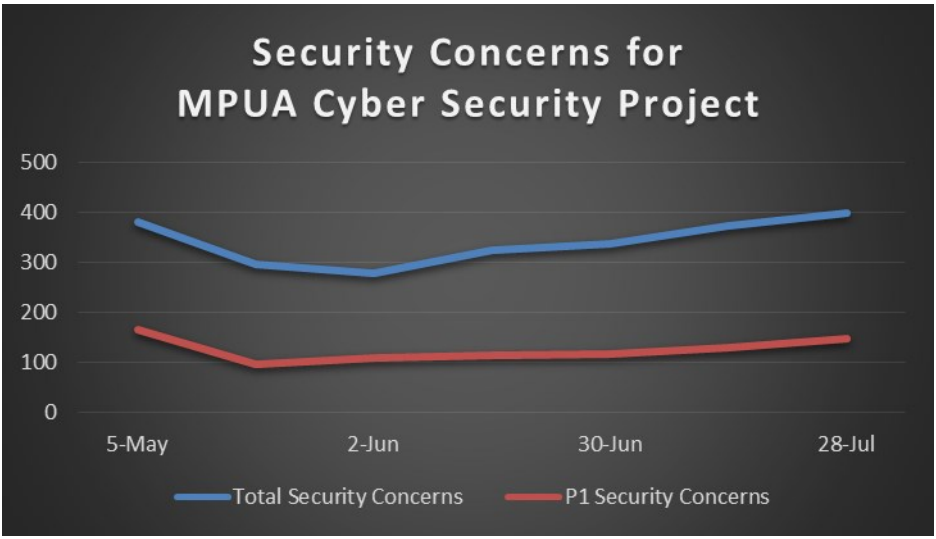
MPUA's selected service provider is **N-Dimension**, a market leading Managed Security Service Provider with innovative solutions to protect utility networks from cyber threats. N-Dimension was selected because of their special focus on utility systems and experience with municipal utilities and cooperatives. N-Dimension has the exclusive approval of APPA's Hometown Connections and the NRECA.

N-Dimension's monitoring service, N-Sentinel Monitoring, provides each city regular reports on breaches, hacking attempts, infections introduced internally, and other problems. The objective is to allow each city to evaluate its protections and vulnerabilities to support considerations of protective adequacy.

"We were unaware of some of the cybersecurity risks N-Sentinel Monitoring identified and guided us in fixing. We appreciate the initiative taken by MPUA in helping us reduce risk -- it is a real advantage for us."

- **Jason Peterson**
Director of IT and Broadband Services, Carthage Water & Electric Plant

The N-Sentinel secure portal provides access to your detailed threat reports along with aggregated utility community data so you can demonstrate threat reduction over time compared to other similar utilities. This service is not redundant of regular cyber protections provided by basic firewalls and antivirus programs.



RESULTS

- MPUA has deployed services to 36 utilities in our membership.
- Upon deployment of the program, Priority 1 alerts among participating utilities declined.
- About 6 percent of the alerts are of a critical nature and require timely attention.
- The program helps identify and prioritize cyber areas of concern.
- The program allows utilities to minimize alerts through work efficiency: Work smarter – not harder.

LESSONS LEARNED...

MPUA MEMBER UTILITY #1:

Issue Description: Monitoring detected unusual Internet Relay Chat (IRC) activities on a critical internal server. N-Dimension Security Analysts investigated to reveal constant SSH brute force attacks from China. The N-Sentinel security team brought the issue to the utility staff's for immediate attention. The SSH service was opened for the utility's third-party vendor remote access, but had been compromised.

Lessons learned: Allowing remote access from trusted sources is sometimes necessary but access must be closely monitored. Without N-Sentinel Monitoring, the hacker's activities would have gone undetected and led to stolen or corrupted utility data.

MPUA MEMBER UTILITY #2:

Issue Description: Monitoring detected and alerted on an executable file download activity from a source IP that belongs to Amazon. Even though the utility's cybersecurity policy allows executable file downloading and the source IP indicated a legitimate service provider, N-Sentinel's cloud-based analysis identified the source IP as servicing files related to adware / malware.

Lessons learned: Traditional network access control mechanisms (firewalls) will treat file downloading activities as normal. But monitoring validates the reputation and standing of the associated IP addresses. Since validation can change over time, monitoring is an important recurring activity.

LESSONS LEARNED...

MPUA MEMBER UTILITY #3:

Issue Description: An N-Sentinel Cybersecurity Monitoring device at an MPUA member utility detected a PDF file containing malware and also, communication to/from an external malware command and control center. These types of activities are an indication of the presence of malware on several internal hosts within the utility's internal network.

Lessons learned: Not all cybersecurity incidents can be detected by firewall and/or antivirus programs. Common system functions can be utilized by hackers, thus by-passing normal cybersecurity features. Cybersecurity monitoring helps detect and mitigate issues that by-pass standard tools faster, issues that go unnoticed without monitoring.

VARIOUS MPUA MEMBER UTILITIES:

Issue Description: N-Sentinel Monitoring at various MPUA member utilities detected and alerted on several cleartext passwords over both the internal network and to/from external networks. This means that anyone monitoring or capturing the network traffic could potentially obtain these critical login credentials and use them later for malicious intent.

Lessons learned: For organizations with websites that have login pages, it is recommended that TLS/SSL (Webserver Certificates) be implemented for securing sensitive data while in internet transit. Additionally, network to network traffic passing sensitive data should use encrypted information.

WHY DO OUR UTILITIES NEED IMPROVED CYBERSECURITY?

Today firewalls and malware/virus software are not enough to catch vulnerabilities and issues with networks and their protection. Firewalls do not protect the utilities interior and malware can embed itself easily and go undetected for over 6 months without proper monitoring. Hackers and evildoers are not concerned about how small or big your business but about getting financial data (utility's and customer information) to use for profiteering. By adding monitoring to your cyber defense plan, you get extra assurance that your firewalls, malware and virus protection are performing and updated. And as a service, there is little for you to do with the system except check reports and fix what the service finds. The service is designed to save you or your IT department time and money and provides you with cyber experts for additional support.

SUMMARY OF SERVICES

N-Sentinel Monitoring is a cloud-based managed security service for utilities. It delivers insights and guidance that protect networks, data and assets from cyber threats. Continuous threat monitoring and alerts provide 24/7 vigilance. Detailed insights about threats and systems compromised, along with specific guidance on remediation steps, enable timely action to be taken to shut down threats and minimize damages.

Key Features

- 24 x 7 intrusion detection monitoring and alerts
- Detection of general and utility-centric threats
- Intelligent cloud-based threat analysis and data aggregation
- Actionable steps to reduce risk and remediate threats
- Cloud-based customer reports
- Utility community cyber intelligence
- Access to cybersecurity experts

Benefits

- Comprehensive managed intrusion detection service for utilities
- Detection of both internal and external threats
- Utility community cyber intelligence
- Actionable threat data and reports
- Advanced threat alerts
- Hybrid service delivery combines cloud-based cybersecurity technology backed by cybersecurity experts
- Easy, fast deployment and hands-off management

CONTACT

Ewell Lawson
Manager of Member & Finance Services
elawson@mpua.org

MPUA
1808 I-70 Drive SW
Columbia MO 65203

MPUA

partnered with

n-dimension solutions