VULNERABILITY MANAGEMENT PROGRAM (VMP)

City of Waukesha

INTERNAL USE
Access Limited to Internal Use Only

Table of Contents

Executive Summary

Vulnerabilities pose a significant risk to the confidentiality, integrity, and availability of City of Waukesha resources, as well as those who access City systems. These vulnerabilities have the potential to impose significant negative consequences, including, but not limited to, identity theft, reputational damage, compromise of confidential data and could result in legal ramifications. To reduce this risk, requires a team effort to identify and remediate vulnerabilities in a timely manner.

What a Vulnerability Management Program (VMP) is and Why the City of Waukesha Needs One

Vulnerability management is a continuous, proactive, and often automated process that keeps the City of Waukesha computer systems, networks, and enterprise applications safe from cyberattacks and data breaches. As such, it is an important part of an overall security program. By identifying, assessing, and addressing potential security weaknesses, we can help prevent attacks and minimize damage if one does occur.

Document Contents

This document contains the components and solutions to prevent and mitigate threats. Documented below we will address the different phases of the VMP.

Target Audience

The target audience for this document includes both business process owners and IT personnel responsible for maintaining the networks, systems, databases, and applications that allow City of Waukesha to function.

The vulnerability management program document is for IT and cybersecurity personnel as well as those responsible for important business processes. Anyone responsible for the safe operation of applications in the business should understand the concepts explained here. Everyone obligated to safeguard employee and client information benefits from understanding this vulnerability management program.

Vulnerability Management Overview

The goal of vulnerability management is to reduce the City of Waukesha's overall risk exposure by mitigating as many vulnerabilities as possible. This can be a challenging task, given the number of potential vulnerabilities and the limited resources available for remediation. Vulnerability management should be a continuous process to keep up with new and emerging threats and changing environments.

Before we begin, we need to understand what vulnerability, threat and risk. We have each defined as the following:

Vulnerability – A weakness of an asset or group of assets that can be exploited by one or more threats, where an asset is anything that has value to the organization, its business operations, and their continuity, including information resources that support the organization's mission.

Threat – Is something or someone that can exploit a vulnerability.

Risk – Is what happens when a threat exploits a vulnerability. It's the damage that could be caused by the open vulnerability being exploited by a threat.

Vulnerabilities are assigned a business criticality rating based on Common Vulnerability Exposure Database. When a vulnerability is discovered, the vulnerability needs a risk rating assigned to it, and remediation efforts are subsequently prioritized on a risk basis.

Based on the degree of exposure, these risk categories help enable City of Waukesha's leadership to make informed decisions at the appropriate level of management oversight.

Critical Risk Vulnerabilities: Critical CVSS Base Score 9.0-10.0.

Loss of system or data [Confidentiality I Integrity I Availability) is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization, e.g., students, faculty, and staff. Exploit development has reached the level of reliable, widely available, easy to-use automated tools. Flaws could be easily exploited by an unauthenticated (or authenticated) remote attacker and lead to system compromise (arbitrary code execution) without requiring user interaction.

High Risk Vulnerabilities: CVSS Base Score 7.0-8.9.
Loss of system or data [Confidentiality I Integrity I Availability] is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization (e.g., employees, customers). Functional exploit code is available. The exploit code works in most situations where the vulnerability exists. These types of vulnerabilities allow local users to gain privileges, allow unauthenticated, remote users to view resources that should otherwise be protected by authentication, allow authenticated remote users to execute arbitrary code, or allow remote users to cause a denial of service.

Moderate Risk Vulnerabilities: CVSS Base Score 4.0-6.9.
Loss of system or data [Confidentiality Integrity I Availability) is likely to have a serious adverse effect on the organization or individuals associated with the organization (e.g., employees, customers). This rating is given to flaws that may be more difficult to exploit but could still lead to compromise under certain circumstances. These are the types of vulnerabilities that could have a critical or important impact but are less easily exploited based on a technical evaluation of the flaw, or affect or require an unlikely configuration.

Low Risk Vulnerabilities: CVSS Base Score 0.1-3.9
Loss of system or data [Confidentiality I Integrity I Availability) is likely to have only a very limited adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).These are the types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would cause either no adverse effects, or, result in only very minimal adverse consequences..

WHAT ARE COMMON VULNERABILITIES?

Vulnerabilities exist beyond unpatched software. Vulnerabilities can also take the form of:

- Technical Vulnerabilities
  - Open ports;
  - Incorrectly configured software (e.g., access permissions, password policy, user rights, encryption, etc.); and
  - Unnecessary services or unnecessarily installed software.
  - Outdated Devices (Printers, legacy devices) that use software that is no longer supported like Java and Flash
- Non-Technical Vulnerabilities
  - Weak physical access control to buildings or areas housing key IT infrastructure;
  - Untrained or poorly trained non-technical staff / end users;
  - Untrained or poorly trained IT / cybersecurity personnel; and
  - Lack of formalized program documentation:
    - Enterprise security policies & standards;
    - Disaster recovery plans;
    - Business Continuity / Disaster recovery (BCDR) plans;
    - Data backup & recovery procedures;
    - Acceptable use standards;
    - Configuration management standards; and
    - Hardware and software inventories.

RISK TREATMENT OPTIONS FOR VULNERABILITY MANAGEMENT

Essentially, there are only four (4) options for managing risk, and it is management's responsibility to analyze available information and decide upon one of the following options:

- Reduce the risk to an acceptable level;
- Avoid the risk;
- Transfer the risk to another party; or
- Accept the risk.

Reduce Risk

When a risk is reduced, a strategy is implemented that is designed to remediate the risk to an acceptable level.

Risk reduction can be achieved through management controls or other arrangements which reduce the frequency of, or opportunity for, error – such as alternative procedures, quality assurance, testing, training, education, supervision, review, documented policy, and procedures.

Examples of reducing risk include, but are not limited to:

- *Apply compensating controls.*
- *Remediate vulnerabilities to correct identified deficiencies.*

Avoid Risk

When a risk is avoided, a decision is made not to proceed with the activity.

Wherever possible, risk avoidance measures should be designed to be embedded in normal business processes, activities, and systems. They should not impede the logical and natural flow of processes and should be easy to understand and appreciate.

Examples of avoiding risk include, but are not limited to:

- *Terminate the project.*
- *Select a different solution that does not have the same risk.*

Transfer Risk

When risk is transferred, a strategy is implemented that shares or transfers the risk away from City of Waukesha.

Risk can be transferred by shifting the responsibility for a risk to another party. Risks may be transferred in full, or they may be shared with another party. Risks should be allocated to the party that can exercise the most effective control over those risks.

Examples of transferring risk include, but are not limited to:

- *Purchase additional cybersecurity insurance.*
- *Select a vendor that will accept indemnification for the risk associated with providing the service (e.g., PCI DSS payment processing).*
- *Move to a hosted solution.*

Accept Risk

While accepting risk is an option for management, the decision needs to be reasonably justified and documented using the Risk Acceptance Form.

Examples of reducing risk include, but are not limited to:

- *Continue with the project, being fully aware of the risks.*
- *Choosing not to remediate vulnerabilities, based on untenable remediation costs.*

Accepting and retaining the risk is the least desirable option for City of Waukesha. However, after careful analysis of the cost of risk treatments, management may determine that risk cannot be avoided, reduced or transferred, or where the cost to do so is not justified (usually, because the likelihood and consequences are low). These retained risks should be monitored, and it must always be remembered that all unidentified risks are retained risks.

Vulnerability Management Components

Threat and vulnerability management uses a variety of tools and solutions to prevent and address cyberthreats. An effective vulnerability management program typically includes the following components, Asset discovery, Vulnerability Scanning, Patch Management, Configuration Management, SIEM, Pen Testing, Threat Intelligence and Remediating Vulnerabilities.

This section will provide information on each of the components listed above and what the City of Waukesha uses to manage vulnerabilities and risks.

ASSET DISCOVERY

Discovering assets enables a holistic approach to cyber security and allows you to identify and prioritize assets that may be at risk. Knowing this information can help the City of Waukesha take remedial action before an incident occurs. for tracking and maintaining records of all devices, software, servers, and more across the City's digital environment.

Control Objective:
Utilizing an asset management software solution, the City can identify quantitatively measure risk impacts of an organization's specific IT assets and to propose a proper mitigation strategy.

Standard:
Microsoft Intune helps the City of Waukesha comply with The National Institute of Standards and Technology (NIST) Special Publication 1800-5.

Procedure:
On a regular basis, the Cities asset management software, Microsoft Intune, will scan the network and identify newly discovered assets. This tool will actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise.

VULNERABILITY SCANNING

Is the process of detecting and classifying potential points of exploitation in network devices, computer systems, and applications. This is done by inspecting the same attack areas used by both internal and external threat actors across the City's networks and assets.

Control Objective:
Utilizing an asset management software solution, the City can identify quantitatively measure risk impacts of an organization's specific IT assets and to propose a proper mitigation strategy.

Standard:
SP 800-115, Technical Guide to Information Security Testing and Assessment | CSRC (nist.gov)

Procedure:
The City works with Netrix, who we is a strategic partner, who monitors our Tenable Nessus product to actively detect and alert on vulnerabilities across the digital footprint. Netrix actively looks at the logs and helps the City understand what is affecting the network at every moment. They enable us to be proactive and help make strategic decisions that maximize our efficiency and effectiveness.

PATCH MANAGEMENT

Patch management software is a tool that helps organizations keep their computer systems up to date with the latest security patches. Most patch management solutions will automatically check for updates and prompt the user when new ones are available. Some patch management systems also allow for deployment of patches across multiple computers in an organization, making it easier to keep large fleets of machines secure.

Control Objective:
The process of controlling the deployment and maintenance of interim software releases into production environments. It helps you maintain operational efficiency, overcome security vulnerabilities, and maintain the stability of your production environment.

Standard:
Patch Manager Plus helps the City comply with the ISO 27001:2013 controls, and The National Institute of Standards and Technology (NIST) Special Publication 800-171

Procedure:
The City follows a phased approach to patching its servers. As vulnerabilities to the Windows OS are found they are downloaded to the patching repository. From there, each scan will determine what patches are needed for that specific asset. Once a new patch is

identified as being needed, it will get deployed to a test server. Once that server is successfully patched and has no errors it will get deployed to our Pilot group of servers. Once the patch is successfully installed then it will get released to the rest of the environment based on their patch schedule.

CONFIGURATION MANAGEMENT

Configuration Management (CM) software helps to ensure that devices are configured in a secure manner, that changes to device security settings are tracked and approved, and that systems are compliant with security policies. Many CM tools include features that allow organizations to scan devices and networks for vulnerabilities, track remediation actions, and generate reports on security policy compliance.

Control Objective:
Configuration Management software helps build robust and stable systems using tools that automatically manage and monitor updates to configuration data.

Standard:
NIST SP 800-128 assumes that information security is an integral part of an organization's overall configuration management.

Procedure:
Using guidelines and procedures gathered from both CIS (Center for Internet Security) and NIST SP 800-128, the City has established benchmarks and controls for implementing and controlling baseline configurations across all endpoints. The endpoints consist of Desktop and Server operating systems, network device, mobile devices and multifunction printing devices, to name a few.

SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM)

SIEM is a tool set that gives visibility into the City's digital footprint to help detect, analyze and respond to security threats before they cause critical issues. The SIEM collects logs from a variant of sources, analyzes these logs real-time and helps City staff take appropriate action.

Control Objective:
SIEM tools use predetermined rules to help the City define threats and generate alerts.

Standard:
Using the guidance of NIST SP 800-92, the City of Waukesha can establish, develop, and perform a robust log management process.

Procedure:
The Cities leverages Microsoft Sentinel as its log collector and partners with a strategic partner, Netrix, to actively alert and investigate incidents. As part of this partnership, logs and alerts are reviewed on a bi-weekly basis.

PENETRATION TESTING

Penetration testing is an authorized cyber-attack designed to help IT staff identify vulnerabilities across computer systems.
Goals of penetration testing vary, with the primary goal focused on finding vulnerabilities that could be exploited and inform the client of those vulnerabilities along with recommended mitigation strategies.

Control Objective:
The selected security vendor will utilize their own hardware and software tools which are specialized for penetration testing.

Standard:
SP 800-115, Technical Guide to Information Security Testing and Assessment | CSRC (nist.gov), PCI DSS (Payment Card Industry Data Security Standard)

Procedure:
Every two years the City partners with different security firms to complete a penetration test. During the engagements, the City will determine how much information is given to the security firm. Primary focus of these tests are external attacks on our firewall, internal attacks on our files and servers, and attacks on our wireless networks.

Threat Intelligence
Software that provides the City with the ability to track, monitor, analyze, and prioritize potential threats to better protect themselves. By collecting data from a variety of sources it helps identify trends and patterns that could indicate a future security breach or attack.

Control Objective:
In conjunction with Microsoft's Sentinel product, the City uses Microsoft's Defender solution to gather logs and alert on suspicious activities in our network and at the borders.

Standard:
NIST Special Publication (SP) 800-150, introduces cyber threat intelligence and information sharing concepts, describes the benefits and challenges of sharing, clarifies the importance of trust, and introduces specific data handling considerations.

Procedure:
The City uses several different products such as Microsoft Sentinel, Microsoft Defender, Microsoft Intune and Nessus Tenable to gather information in a real time dashboard. This dashboard contains information on threats, incidents, and alerts. On a weekly basis the City along with its security partner Netrix meet and discuss the threats and how to remediate them.

Remediating Vulnerabilities (Currently Working on this section)
Remediation involves prioritizing vulnerabilities, identifying appropriate next steps, and generating remediation tickets. Tracking is an important tool for ensuring that the vulnerability or misconfiguration is properly addressed.

Control Objective:
See Threat Intelligence

Standard:
SP 800-115, Technical Guide to Information Security Testing and Assessment | CSRC (nist.gov)

Procedure:
See Threat Intelligence

Appendices

Appendix A – VPMP Roles & Responsibilities

Chief Risk Officer (CRO) – The Technical Operations Manager performs the role of the CRO
The Chief Risk Officer (CRO) is accountable to City of Waukesha's executive management for the development and implementation of the risk management program.

The CRO's responsibilities include, but are not limited to:
- Protecting City of Waukesha from unacceptable risk or losses associated with operations; and
- Developing and implementing mechanisms for effectively managing the risks that may affect the achievement of City of Waukesha objectives and operational outcomes.

Chief Information Security Officer (CISO) – The IT Director performs the role of the CISO
The CISO is accountable to City of Waukesha's executive management for the development and implementation of the cybersecurity program. The CISO will be the central point of contact for setting the day-to-day direction of the cybersecurity program and its overall goals, objectives, responsibilities, and priorities

The CISO's responsibilities include, but are not limited to:
- Oversee and approve the company's cybersecurity program, including the employees, contractors, and vendors who safeguard the company's systems and data, as well as the physical security precautions for employees and visitors;
- Ensure an appropriate level of protection for the company's information resources, whether retained in-house or under the control of outsourced contractors;

- Issue cybersecurity policies, standards, and guidance that establish a framework for an Information Security Management System (ISMS);
- Identify protection goals, objectives, and metrics consistent with corporate strategic plan;
- Ensure appropriate procedures are in place for Security Testing & Evaluation (ST&E) for all systems; and
- Monitor, evaluate, and report to company management on the status of cybersecurity within the organization.

Executive and Senior Management

The effectiveness of risk management is unavoidably linked to management competence, commitment, and integrity, all of which forms the basis of sound corporate governance. Corporate governance provides a systematic framework within which the executive management group can discharge their duties in managing City of Waukesha.

Executive and Senior Management responsibilities include, but are not limited to:

- Considering and documenting new and existing risks and their impact on proposed plans as part of the annual planning cycle.
  - Risk records must be maintained up-to-date on an on-going basis to reflect any changes which may occur;
- Providing direction and guidance within their areas of accountability so that staff best utilize their abilities in the preservation of City of Waukesha's resources;
- Successfully promoting, sponsoring and coordinating the development of a risk management culture throughout City of Waukesha;
- Guiding the inclusion of risk management in all strategic and operational decision making;
- Possessing a clear profile of major risks within their area of control, incorporating both opportunity and negative risks;
- Maintaining a framework to manage, monitor and report risk;
- Managing risks to meet City of Waukesha objectives, goals, and vision; and
- Improving corporate governance.

Management

Managers at all levels are responsible for the adoption of risk management practices and are directly responsible for the results of risk management activities, relevant to their area of responsibility.

All Employees

All employees are responsible for:

- Acting at all times in a manner which does not place at risk the health and safety of themselves or any other person in the workplace;
- Identifying areas where risk management practices should be adopted and advising their supervisors accordingly;
- Meeting their obligations under relevant statutory, regulatory and contractual requirements; and
- Taking all practical steps to minimize City of Waukesha's exposure to contractual, tortuous and professional liability.

Asset Owner

The asset owner "owns" the process, application, service or asset in question.

Risk/asset owner responsibilities include, but are not limited to:

- Ensuring that the risks they are assigned are managed appropriately;
  - Management of individual risks may be delegated to a person with relevant expertise to undertake the task of managing the risk on behalf of the risk owner.
  - The risk owner retains ultimate responsibility
- Monitoring progress against treatment plans;
- Ensuring that the risk review process is carried out in a timely fashion, within their areas of responsibility; and
- Ensuring the currency of the risk register and responding to any risk register actions that have been assigned to them.

Internal Audit

The internal audit function supports City of Waukesha risk management by providing advice and support on risk management, and through an annual independent review of risk management practices and procedures to provide assurance on their efficiency and relevance to the Audit Committee.

Vulnerability Management Personnel

The internal vulnerability management function supports City of Waukesha vulnerability management by implementing and executing the controls associated with a Vulnerability & Patch Management Program (VPMP).

Vulnerability management responsibilities include, but are not limited to:

- Conducting vulnerability assessment scans;
- Conducting penetration tests;
- Maintaining vulnerability management tools;
- Generating metrics to report on the status of vulnerability management and remediation operations; and
- Consulting with asset owners and custodians on remediation activities.

ASSET CUSTODIANS

Asset custodians maintain assets for asset owners.

Asset custodian responsibilities include, but are not limited to:

- Implementing assets according to secure configuration standards;
- Performing proactive, recurring maintenance activities;
- Maintaining situational awareness on evolving threats; and
- Collaborating with asset owners and vulnerability management personnel for remediation actions.