LARCEMENT
CONSULTING

Information Security Standards for Remote Network Access

Introduction

This document outlines the information security standards and practices followed by L Arcement Consulting to ensure secure access to remote networks. These standards are intended to safeguard client data, maintain the integrity of our network infrastructure, and protect sensitive systems from cyber threats.

1. Endpoint Protection and Detection Response (EPDR) - WatchGuard

L Arcement Consulting employs **WatchGuard EPDR** (Endpoint Protection and Detection Response) on all systems that access remote networks. This solution provides real-time protection and threat intelligence to detect and block potential security threats on endpoints. Key features include:

- **Real-time threat detection and prevention**: WatchGuard EPDR continuously monitors endpoints for malware, ransomware, and other types of cyber threats.
- **Automated response**: In case of suspicious activity or detected threats, WatchGuard EPDR can automatically isolate compromised systems to contain and prevent the spread of potential threats.
- **Comprehensive endpoint visibility**: Continuous monitoring provides detailed insights into endpoint activity, aiding in faster identification of threats and vulnerabilities.
- **Advanced analytics and reporting**: Detailed reports and logs are generated for security analysis and incident response.

2. Windows Update Requirements

To ensure that systems remain secure and up-to-date, **Windows updates** are mandatory for all machines accessing remote networks. The following standards are enforced for all systems:

- **Automatic Updates**: All Windows systems must be configured to automatically download and install updates to maintain the latest security patches.
- **Critical and Security Updates**: Only critical and security updates are required to be installed immediately, as these address known vulnerabilities and exploits.
- **Non-Critical Updates**: Non-critical updates may be installed during scheduled maintenance windows, but their installation should not interfere with system security.
- **Patch Management**: L Arcement Consulting follows a structured patch management process to ensure that updates are applied in a timely manner and tested for compatibility.

- **Verification of Compliance**: Systems are regularly checked for compliance with update requirements to ensure that no system is left outdated.

3. Multi-Factor Authentication (MFA) - WatchGuard AuthPoint VPN Access

All remote access to remote networks are secured using **Multi-Factor Authentication (MFA)** via WatchGuard **AuthPoint VPN**. The MFA protocol ensures that only authorized users can access the network, even in the event of a compromised password. The following standards apply to MFA for VPN access:

- **MFA Requirement**: Users must authenticate using at least two factors to access the network. This includes:
  - Something the user knows (username and password).
  - Something the user has (AuthPoint mobile app, token, or push notification).
- **Mobile App**: Users must install the WatchGuard AuthPoint app on their mobile devices to generate or receive time-sensitive authentication codes.
- **Push Notifications**: A push notification is sent to the user's mobile device upon login attempt, prompting them to approve or deny access. This is the preferred method of authentication.
- **Token-based Authentication**: In some cases, hardware or software tokens may be used as a second factor for authentication.
- **Fail-Safe Lockout**: If the user fails to provide valid authentication after a certain number of attempts, their account will be locked out and access will be temporarily suspended until further investigation.
- **VPN Access Logging**: All VPN login attempts are logged and monitored for suspicious activities. Alerts are generated in case of abnormal access attempts or other security concerns.

4. Remote Network Access Guidelines

To ensure the security of remote network access, the following guidelines must be followed:

- **Remote Access VPN**: All employees and authorized users accessing networks remotely must use the secure VPN connection with MFA enabled.
- **Strong Password Policy**: Users must adhere to strong password policies, including a minimum length of 12 characters, the use of upper and lowercase letters, numbers, and symbols, and regular password updates.

- **Role-based Access Control (RBAC)**: Access to sensitive data and resources is granted based on the user's role within the organization, ensuring the principle of least privilege is adhered to.
- **Session Timeout and Locking**: After a period of inactivity, VPN sessions will automatically log out, and systems will be locked to prevent unauthorized access.
- **End-user Training**: Regular training sessions are conducted to educate users on security best practices, phishing awareness, and secure use of remote systems.

5. Security Monitoring and Incident Response

L Arcement Consulting maintains a continuous monitoring framework to detect and respond to security incidents:

- **WatchGuard EPDR Monitoring**: WatchGuard's EPDR solution provides real-time alerts for any endpoint threats, and the security team is notified immediately to respond accordingly.
- **Incident Response Plan**: In case of a security breach, L Arcement Consulting follows a formal incident response plan to mitigate the impact, investigate the cause, and prevent future occurrences.
- **Security Audits**: Regular audits of the system and security infrastructure are conducted to ensure compliance with established security standards and identify areas for improvement.

6. Compliance and Best Practices

L Arcement Consulting adheres to industry-recognized security frameworks and best practices, including:

- **GDPR** (General Data Protection Regulation) for data protection.
- **NIST** (National Institute of Standards and Technology) Cybersecurity Framework for system and network security.
- **ISO/IEC 27001** for information security management.

Conclusion

L Arcement Consulting is committed to protecting sensitive information and ensuring secure remote access to remote systems. The standards outlined in this document represent our dedication to maintaining a secure working environment through the use of WatchGuard EPDR, Windows updates, MFA for VPN access, and other industry best practices.