SCOTT MACLEAN

DECEMBER 2024

POLICIES FOR TESLA INC.

TABLE OF CONTENTS

SOFTWARE UPDATE AND PATCHING POLICY

1.1 Purpose

The purpose of this policy is to ensure that all Tesla systems and devices are updated and patched regularly to protect against ransomware attacks that exploit known vulnerabilities in software, firmware, and operating systems. This aligns with the Canadian Centre for Cyber Security's (Canada, C. S. E. (2024, April 18). Ransomware: How to prevent and recover (ITSAP.00.099). Canadian Centre for Cyber Security) recommendation to "check for updates and patches to repair known bugs and vulnerabilities in your software, firmware, and operating systems" to prevent exploitation by threat actors.

1.2 Scope

This policy applies to all Tesla systems and devices, including:

- Operating systems (e.g., Windows, Linux, macOS)
- Applications (e.g., web browsers, productivity software, manufacturing control systems)
- Firmware (e.g., network devices, embedded systems)
- Vehicles and in-car systems

1.3 Policy

- All systems and devices must have the latest security updates and patches installed.
- Critical security updates must be applied within 48 hours of release, in line with industry best practices for timely patching.
- Non-critical updates will be applied within a defined maintenance window.
- Automated patching mechanisms will be implemented wherever possible.
- A vulnerability scanning program will regularly identify and prioritize patching needs.
- Exception requests for delaying patching require approval from IT Security and a documented risk assessment.

SOFTWARE UPDATE AND PATCHING POLICY

1.4 Responsibilities

- Director of IT Operations: Oversees the patching process, ensuring adherence to the policy and timely implementation of updates.
- System Administrators: Execute the technical aspects of patching, including deploying updates, testing systems, and troubleshooting issues.
- Security Operations Center (SOC) Manager: Supervises vulnerability scanning and risk assessment activities, ensuring timely identification and prioritization of critical patches.
- CISO: Provides final approval for any exceptions to the patching policy.

1.5 Playbook

The Ransomware Playbook - Preparation section provides detailed procedures for:

- Identifying and prioritizing software updates and patches.
- Testing updates and patches in a non-production environment.
- Deploying updates and patches to production systems.
- Monitoring systems for successful update and patch implementation.
- Troubleshooting any issues that arise during the patching process.

1.6 Non-Compliance Consequences

Failure to adhere to this policy may result in:

- Disciplinary action, up to and including termination of employment.
- System vulnerabilities that could be exploited by ransomware attacks.
- Data loss or corruption.
- Disruption of business operations.
- Reputational damage to Tesla.
- Legal or regulatory fines.

DATA BACKUP POLICY

2.1 Purpose

The purpose of this policy is to ensure that Tesla has a comprehensive data backup plan in place to enable the recovery of critical systems and data in the event of a ransomware attack or other data loss incident. This aligns with the Canadian Centre for Cyber Security's recommendation to "implement a backup plan for your organization" and maintain offline backups to prevent ransomware infection.

2.2 Scope

This policy applies to all Tesla data, including:

- Critical business data (e.g., financial records, customer data, intellectual property)
- System configurations and settings
- Applications and software

2.3 Policy

- Daily backups of all critical data must be performed, consistent with NIST's guidance on data backup and recovery. (National Institute of Standards and Technology. (n.d.). PROTECTING DATA FROM RANSOMWARE AND OTHER DATA LOSS EVENTS)
- Backups must be stored in a secure, off-site location.
- Backups must be encrypted using AES-256 (xopero_blogger. (2023, December 7). AES encryption 101 - why you should use encrypted backup. Xopero Blog) to protect confidentiality.
- Backup processes will be tested weekly to ensure they function correctly.

DATA BACKUP POLICY

2.4 Responsibilities

- Data Center Manager: Oversees the implementation and maintenance of the backup infrastructure, ensuring its security and reliability.
- Backup Administrators: Execute the technical aspects of data backups, including scheduling backups, verifying their integrity, and managing backup storage.
- IT Operations Team: Collaborates with backup administrators to ensure that all critical systems and data are included in the backup plan.
- Individual employees: Responsible for backing up their own critical data, such as project files, research data, and sensitive documents.

2.5 Playbook

The Ransomware Playbook - Preparation section provides detailed procedures for:

- Selecting appropriate backup solutions and technologies.
- Defining backup schedules and retention policies.
- Performing backups and verifying their integrity.
- Restoring data from backups in the event of a data loss incident.

2.6 Non-Compliance Consequences

Failure to adhere to this policy may result in:

- Disciplinary action, up to and including termination of employment.
- Inability to recover critical data in the event of a ransomware attack or other data loss incident.
- Significant downtime and disruption of business operations.
- Financial losses due to data loss and recovery efforts.
- Reputational damage to Tesla.

STRONG AUTHENTICATION POLICY

3.1 Purpose

The purpose of this policy is to enforce strong authentication methods to prevent unauthorized access to Tesla systems and data, reducing the risk of ransomware attacks. This aligns with the Canadian Centre for Cyber Security's recommendation to "enforce strong authentication methods".

3.2 Scope

- This policy applies to all employees, contractors, and third-party vendors accessing Tesla systems and data.

3.3 Policy

- Multi-factor authentication (MFA) is mandatory for all user accounts (Multi-factor authentication. NIST)
- Passwords with 8 characters, one captial letter, one digit and one special character are required.
- Passwords must be changed monthly.
- Users must using remote services must use a second piece of authentication such as a cell phone verification code or authenticator.

3.4 Responsibilities

- Chief Information Security Officer (CISO): Oversees the implementation and enforcement of the strong authentication policy.
- Identity and Access Management (IAM) Team: Manages user accounts, implements MFA solutions, and enforces password policies.
- Security Awareness Training Team: Educates employees about strong authentication best practices and the importance of adhering to the policy.
- All users: Responsible for enabling MFA on their accounts, creating strong passwords, and complying with password management guidelines.

STRONG AUTHENTICATION POLICY

3.5 Playbook

The Ransomware Playbook - Preparation Section provides detailed procedures for:

- Implementing MFA across different systems and applications.
- Enforcing password complexity requirements.
- Educating users about strong authentication best practices.
- Monitoring authentication logs for suspicious activity.

3.6 Non-Compliance Consequences

Failure to adhere to this policy may result in:

- Disciplinary action, up to and including termination of employment.
- Unauthorized access to Tesla systems and data.
- Increased risk of ransomware attacks and other security breaches.
- Data loss or corruption.
- Disruption of business operations.
- Reputational damage to Tesla.
- Legal or regulatory fines.

CITATIONS AND REFERENCES

Canada, C. S. E. (2024, April 18). Ransomware: How to prevent and recover (ITSAP.00.099). Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/ransomware-how-prevent-and-recover-itsap00099#protect

National Institute of Standards and Technology. (n.d.). PROTECTING DATA FROM RANSOMWARE AND OTHER DATA LOSS EVENTS. https://www.nccoe.nist.gov/sites/default/files/legacy-files/msp-protecting-data-extended.pdf

xopero_blogger. (2023, December 7). AES encryption 101 - why you should use encrypted backup. Xopero Blog. https://xopero.com/blog/en/aes-encryption-101-why-you-should-use-encrypted-backup/

Multi-factor authentication. NIST. (2024, March 12). https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication