COVER PAGE

TITLE: Titan Industries - 2021 Risk Analysis & Mitigation Strategy

NAME: Mark Darling

POSITION: Information Security Manager, Titan Industries

DATE: November 26, 2021

TITAN

INDUSTRIES

TABLE OF CONTENTS

INTRODUCTION

Titan Industries' upper management have seen the headlines filled with American companies/organizations large and small lately as various news outlets reveal the security incidents, network breaches, and ransomware attacks being launched against our own peers and customers. These disasters have upper management concerned about Titan Industries' current state of security within the company and management has requested a full investigation and review of Titan Industries' current server and network hardware and infrastructure out of fears of vulnerabilities that may be present within currently deployed/implemented company-wide infrastructure. This white paper seeks to clarify currently deployed hardware/software configurations within the company's control and identify inside and outside attack vectors that these configurations may be vulnerable to that can be patched. By finding the weak links within Titan Industries' currently deployed infrastructure the risks will be able to be mitigated as quickly as possible, reducing liability to future data leaks or network breaches while simultaneously maintaining and bolstering customers' hard-earned trust.

SYSTEM DESCRITPION

- **Operating System:**
  - Windows Server 2016 Standard // Version 1803 // 64 bit
- **Processor:**
  - Intel Xeon E5 2680V3 // 12 cores, 24 threads // 120W TDP
- **Motherboard:**
  - ASRock Rack EPC612D8A (ATX)
    - Intel C612 chipset // BIOS Version 2.30
- **Memory:**
  - Crucial 32GB 288-Pin DDR4 2133MHz SDRAM ECC (PC4 17000) SMM
    - ECC load reduced // CAS latency 15
    - 4 x 32GB DIMMs // 128 GB total
- **Storage:**
  - Seagate IronWolf Pro 10TB Helium 7200RPM 256MB Cache SATA 6.0Gb/s 3.5” HDD
    - Model: ST10000NE0004 // 300TB/year // 1.2M hours MTBF
    - 4 x 10TB HDDs // 40TB total raw // RAID 10 // 10TB VDD
- **Network:**
  - Intel Ethernet Controller I210-AT // 1GbE
  - Intel Ethernet Controller I217-LM // 1GbE
- **Management:**
  - Realtek TRL8211E IPMI LAN port
    - ASPEED AST2400 BMC Controller
      - 16MB DDR3 VRAM

SYSTEM STRENGTHS & WEAKNESSES

- **Strengths**
  - ECC memory protects against bit flips
    - ensures system integrity
      - essential for certain types of rendering/simulations, CAD, or high-precision computing applications involving real-world applications of math and science
  - Intel Hyper-Threading improves single-threaded performance
    - improves system responsiveness
    - improves performance further for highly-threaded applications
  - Intel AES New Instructions
    - provide robust hardware-based encryption, RNG, & authorization functionalities
    - minimizes software-based attack vectors that are likely to result in compromised keys
  - AVX 2.0 256-bit integer instructions
    - includes new FMA (Fused-Multiply-Add) instruction
      - improves performance for math and science algorithms
        - better performance for machine learning and AI applications
  - Long service and support life from Intel
    - microcode updates and patches
  - Supports up to 768GB RAM
    - pairs well with Intel HPC Xeon server CPUs
      - virtually unlimited virtualization possibilities
  - 40 PCIe lanes at PCIe 3.0 speeds

    - allow graphics cards or other computing peripherals to utilize system specs and hardware to their fullest possible extents
  - Intel SpeedStep & Idle (C-State) Technologies
    - increased operating efficiency during times of low demand

- **Weaknesses**
  - Scalability is limited in 2021
    - maximum of 2 CPUs per motherboard
    - QPI link 9.6GT/s interconnect speeds will bottleneck in large-scaled configurations
  - Susceptible to Meltdown race condition vulnerabilities
    - attackers may be able to access higher-privilege data stored in memory
  - Susceptible to Spectre speculative execution vulnerabilities
    - attackers may be able to access memory arbitrarily, regardless of privilege levels
  - Susceptible to Zombieload Intel CPU vulnerabilities
    - may permit attackers remote monitoring
  - Physical access to server room is not monitored, logged, or controlled
    - increased risks of inside attacks by disgruntled employees
  - BIOS password not configured
    - rootkits and/or firmware attacks possible
  - entire-disk encryption not implemented
    - vulnerable if file system is bypassed
  - software-based firewall
    - faults elsewhere in the operating system could yield a software-based firewall inoperable with no indication of malfunction

SYSTEM PROTECTION OPTIONS

To better protect Titan Industries' primary server, we suggest starting with integrating hardware-based access control and biometrics logging to limit and control physical access to the main server room itself. This ensures disgruntled employees and/or covert attackers cannot plant viruses, malware, or backdoors on the server itself via untraceable attacks or vulnerabilities nor exfiltrate data they are otherwise entitled to access during normal business use. If such an incident were to occur, there would be objective proof in the form of biometrics logs, proving presence at a minimum. Additionally, the main server's BIOS should have a password configured and enforced in order to avoid various types of downgrade or local access attacks (should somebody gain physical access to the server room after fortifying physical access constraints). Additional low-level protections that should be leveraged include implementing hardware-level disk-level encryption as a safeguard in the event an active server storage disk were to be exfiltrated from the premises such that its contents would remain encrypted regardless of operating system or file system protections being compromised.

Since receiving the Windows emergency update in early 2018, the server's comprehensive security and monitoring suite from a smaller third-party vendor has been unable to perform regular antivirus and malware scans as it uses unsupported kernel calls that were eliminated by the emergency patch as an immediate stop-gap security measure. This has left the main server out of date and out of compliance since 2018 and no longer protected against significant new classes of attacks such as ZombieLoad as well as numerous variants of known ransomwares, and more. It is recommended to update the BIOS of main server to newest version provided by the OEM of the motherboard and to re-install the newest OEM operating system release with valid microcode updates so that the main server may continue to receive regular service and security updates from Microsoft via the operating system's software-based update mechanisms. Additionally, moving to a larger, more recognized, and compliant comprehensive security suite is recommended to help avoid any future lapses in regular security upkeep practices.

Finally, introducing employee training involving security best practices, password improvement and enforcement programs, forcing employees to rotate to a new, never-used-before password every 30-90 days, and where applicable, allowing for single sign on authentication will help increase employee adoption and utilization of security industry best practices and common-sense computing security improvements.

RISK MITIGATION STRATEGIES

To reduce risk, it has been determined that all employees shall be forced to utilize multi-factor-authentication based on their personal phone number. This will help to reduce/eliminate potential incidents of unauthorized users accessing privileged materials outside of their authorization level while inadvertently using a higher-privilege account than their own. Beyond that scope, it will also help eliminate risks of social engineering and infiltration. In addition to requiring MFA on a per-account, per-sign-in bases, a strict single-instance policy shall be adopted to prevent co-workers from leaving a single worker's credentials signed in at a workstation and rotating their credentials at the software level as they use the software on the workstation. This will ensure integrity and help keep cleaner, more consistent and accurate logs, that are easier to review and spot questionable instances of potential internal abuse.

Adding a hardware-based firewall at the front of the network will serve to improve overall network security and performance while still complimenting/maintaining the software firewall as a fallback alternative in the event of a hardware fault or failure on the physical firewall's part. Physically locking the rack area containing the server using a padlock with a controlled access system of its own will ensure only verified service technicians are able to access the main server once issued the access keys/token from their higher-up.

A comprehensive backup and restoration plan needs to be drafted and tested to ensure the process is feasible and within practice in the event it shall ever be required in the future due to an attack or breakdown. Additionally, a regularly-scheduled local and regularly-scheduled offsite backup regime shall be determined to recur indefinitely and help avoid potential data losses whether due to a malicious attack or unfortunate hardware failure.

CONCLUSIONS

In conclusion, while a review of Titan Industries' security and compliance practices does not reveal an ideal environment for security to propagate, we have encountered far worse realities. By all accounts, there have not been any detectable breaches or loss of data despite not following industry best practices which seemed to have fallen out of compliance shortly after 2018, during the transition to a new CEO, CFO, and CTO. If the suggested improvements are made, we expect overall security and integrity to fall in line with industry standards and best practices.

In order to avoid future deterioration in security structure, it is critical that such processes for updating, setting, and maintaining software and hardware security keys, passwords, software updates, etc. be codified into explicit checklists and to-do lists based on their importance to overall security architecture and around respective product's typical update cycles.

Equally important is restricting and logging physical access to all aspects of the premises on which Titan Industries is housed. Requiring multi-factor authentication including biometrics will significantly reduce local and physical attack vectors as well as potential incidents of social engineering, which are on the rise these days.

REFERENCES

https://en.wikipedia.org/wiki/Windows_Server_2016

https://www.techrepublic.com/article/windows-server-2016-the-smart-persons-guide/

https://www.intel.com/content/www/us/en/products/sku/81908/intel-xeon-processor-e52680-v3-30m-cache-2-50-ghz/specifications.html

https://www.newegg.com/crucial-32gb-288-pin-ddr4-sdram/p/N82E16820148900

https://www.asrockrack.com/general/productdetail.asp?Model=EPC612D8A#Specifications

https://download.asrock.com/Manual/EPC612D8A.pdf

https://www.newegg.com/seagate-ironwolf-pro-st10000ne0004-10tb/p/N82E16822179103

https://www.hostdime.com/blog/best-raid-configuration/

https://ark.intel.com/content/www/us/en/ark/products/64400/intel-ethernet-controller-i210at.html

https://ark.intel.com/content/www/us/en/ark/products/60019/intel-ethernet-connection-i217lm.html

https://www.microway.com/hpc-tech-tips/intel-xeon-e5-2600-v3-haswell-processor-review/

https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability)#Affected_hardware

https://meltdownattack.com/

https://meltdownattack.com/meltdown.pdf

https://spectreattack.com/spectre.pdf

https://zombieloadattack.com/zombieload.pdf