Departamento de ENGENHARIA INFORMÁTICA
Instituto Superior de Engenharia do Porto

Systems and Information Security SEGSI

Topic 5

Supply chain Security

Pinto Leite, Jorge (jpl@isep.ipp.pt)

Supply chain Security

- What is a (the) supply chain?
- For an IT point of view, it can be assumed as a whole bunch of parts that are increasingly being connected to infrastructure
  - 3D printing
  - 5G
  - Augmented / Virtual reality
  - Autonomous vehicles
  - Big Data
  - Data & Analytics
  - Robotics Process Automation
  - IoT
  - Cloud Computing
  - Blockchain
  - AI & ML
- But also as all the interveners (from inside or outside) of the processes performed on a company

Supply chain Security

- 3D printing
  - They can or might pass information to the manufacturers
  - 3D printing devices by default insert a watermark on the devices produced
    - Analogue or digital? In the later case it can be traced revealing the location where it is
- 5G
  - By itself, he would probably not be considered as a threat, the problem arises due to the huge amount of different devices operating with 5G technology that can be appended to our infrastructure
- Augmented / Virtual reality
  - Eye-tracking can be performed leading to privacy issues
  - Biometric identifier
    - Is every user of this technology aware of that?

Supply chain Security

- Autonomous vehicles
  - Can they have a failure on their security controls?
  - Or be hacked?
- Big Data and Data & Analytics
  - Despite the benefits it provides, ethical, privacy and security vectors must / should be considered
  - T05 - Big Data Analytics - Manuscripts Final Version
- Robotics Process Automation (RPA)
  - Sensitive and confidential data treatment is being (or might be) transferred to RPA
  - However, nowadays the available RPA lacks security problems – like password management
  - However, they need to be connected to the infrastructure
  - Take a look into https://www.xenonstack.com/insights/rpa-security-risk-management

Supply chain Security

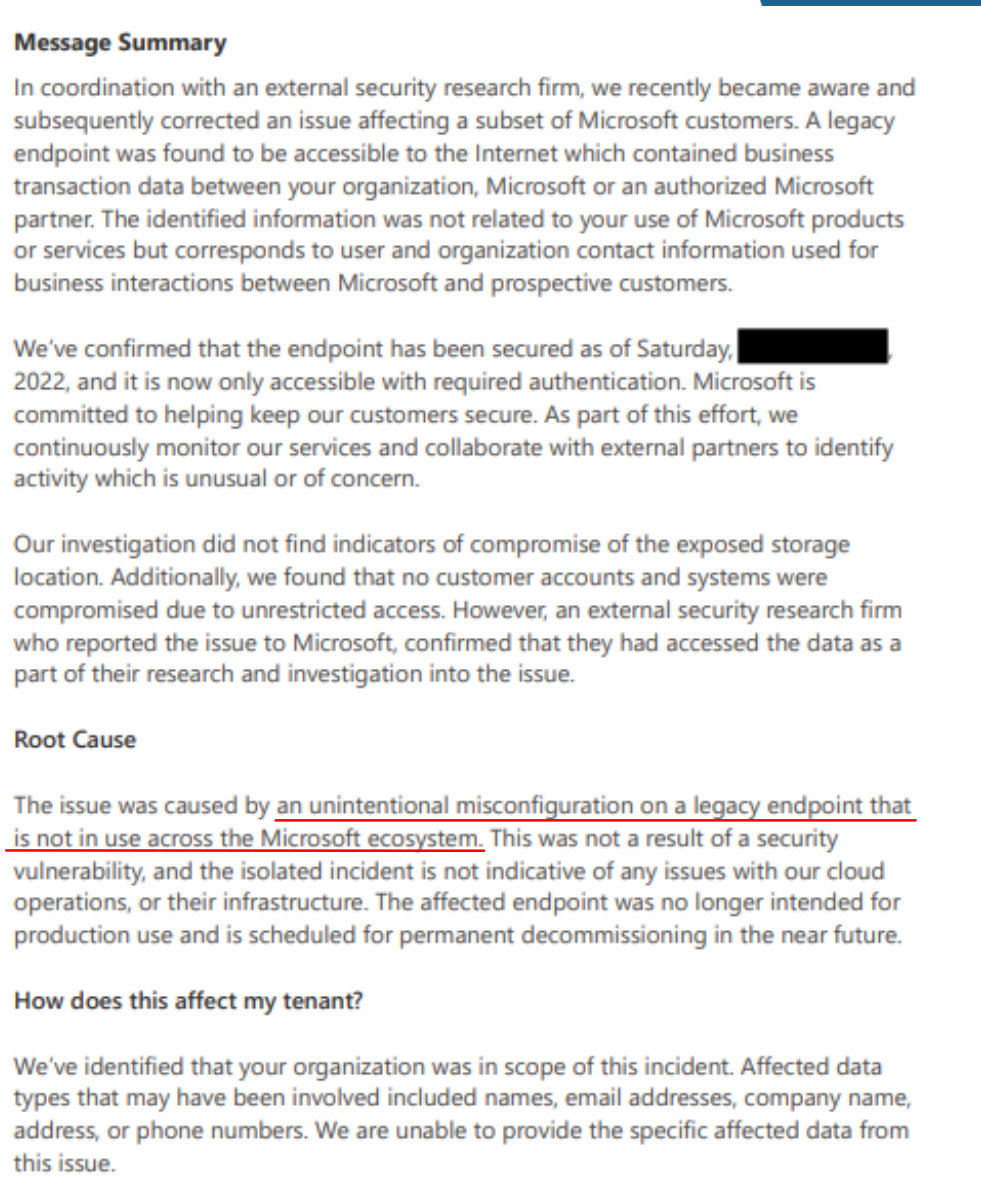
- IoT
  - IoT devices usually are weak in security terms
  - Guidelines have been produced (ENISA, 2020), yet there is no available data on the *de facto* implemented controls
- Cloud Computing
  - The cloud is just a computer on our neighbors basement
  - How clear are the applications and data stored there?
  - Secure design development practices and pipelines, and improve monitoring and observability should be employed

Supply chain Security

- Blockchain
  - Might be interconnected with IoT devices
  - Beyond the thoughts of IoT, immutability, transparency, and traceability should / must be implemented
- AI & ML
  - We all agree on the benefits it provides, however their security risks should also be thought
  - If it is implemented on autonomous processes, controls have to be implemented to mitigate the risks of incorrect assumptions

Supply Chain Security

- Interveners (from inside or outside) of the pr
- Internal systems, processes or people are cor reliable
- But are they?
- Decommission a system or process (which wil important as its entry on the supply chain
  - *Boarding-on* and *Boarding-off*
- An old system no longer updated and / or use infrastructure turns itself on the weakest link



Message Summary

In coordination with an external security research firm, we recently became aware and subsequently corrected an issue affecting a subset of Microsoft customers. A legacy endpoint was found to be accessible to the Internet which contained business transaction data between your organization, Microsoft or an authorized Microsoft partner. The identified information was not related to your use of Microsoft products or services but corresponds to user and organization contact information used for business interactions between Microsoft and prospective customers.

We've confirmed that the endpoint has been secured as of Saturday, [redacted] 2022, and it is now only accessible with required authentication. Microsoft is committed to helping keep our customers secure. As part of this effort, we continuously monitor our services and collaborate with external partners to identify activity which is unusual or of concern.

Our investigation did not find indicators of compromise of the exposed storage location. Additionally, we found that no customer accounts and systems were compromised due to unrestricted access. However, an external security research firm who reported the issue to Microsoft, confirmed that they had accessed the data as a part of their research and investigation into the issue.

Root Cause

The issue was caused by an unintentional misconfiguration on a legacy endpoint that is not in use across the Microsoft ecosystem. This was not a result of a security vulnerability, and the isolated incident is not indicative of any issues with our cloud operations, or their infrastructure. The affected endpoint was no longer intended for production use and is scheduled for permanent decommissioning in the near future.

How does this affect my tenant?

We've identified that your organization was in scope of this incident. Affected data types that may have been involved included names, email addresses, company name, address, or phone numbers. We are unable to provide the specific affected data from this issue.

Supply chain Security

- Some of the measure to improve the supply chain security has already been mentioned
  - Improve privacy
    - Cryptography and a careful analysis of the data that is *really* needed
  - Disable everything that is not absolutely needed
  - Segment the infrastructure so as the RPA and equivalents are not accessible from any system / process except from the ones that really needs to access
  - Implement controls (audit) to check the traffic from / to IoT devices
  - Apply cryptographic algorithms (two-way and one-way) on the data stored on the Cloud
  - Apply V&V when developing applications
  - Apply security on all sensitive data that cross pipelines

Supply chain Security

- Implement
  - Observability
    - The ability to measure a system's current state ba
      logs, metrics, and traces
  - Monitoring
  - Immutability
    - The state of not changing, or being unable to be c
  - Traceability
- Additional controls might be implemented to a
  assumptions by the hardware as well as / or by

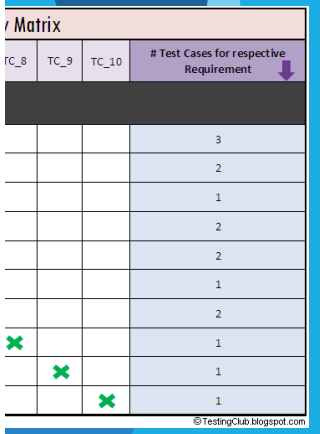
Definition 1: a dynamic system of the form $\dot{x}(t) = Ax(t) + Bu(t)$, $y(t) = Cx(t) + Du(t)$ where $n, B \in \mathbb{R}^{n \times 1}$, $A \in Mat_{n \times n}(\mathbb{R})$, $C \in \mathbb{R}^{1 \times n}$,and $y, u \in \mathbb{R}$ is said to be **Observable** if for any possible $x(t)$ state and $u(t)$ control vector, it is possible to determine the state $x(t)$ using only our ouputs $y(t)$ and control vector $u(t)$. In other words, a system is observable if given $y(t)$ output and $u(t)$ control, we can determine $x(t)$ (the state).

Definition 2:

Let $\Psi = \begin{pmatrix} C \\ CA \\ CA^2 \\ \vdots \\ CA^{n-1} \end{pmatrix}$

This is called **Kalman Observability Matrix**.
Theorem: The system $\dot{x}(t) = Ax(t) + Bu(t)$, $y(t) = Cx(t) + Du(t)$ with the dimensions mentioned above is **Observable if and only if** $rank(\Psi) = n$.

Source: oriamathematics



Source: blogspot.com

Supply chain Security

- Consider now incorrect assumptions by hardware or software
- Both can fail and that fail should be addressed
- To improve fault detection *redundancy* or *diversity* can be used (these will be seen in Topic 7)
- If a fault is detected – and let's assume that controls are implemented to detect it – two strategies can be put in place
  - Preventive fault detection
  - Retrospective fault detection

Supply chain Security

- Preventive fault detection
  - The fault detection mechanism is triggered before the change of state actually occurs
  - If an erroneous state is detected the change does not take place
- Retrospective fault detection
  - The fault detection mechanism is triggered after the system state change
  - This option is used when an incorrect sequence of correct actions leads to an erroneous state or when preventive detection requires unaffordable resources
- The recovery and fault repair can be *forward* (repair a corrupted system) or *backward* (restore to a previous known and safe state)

Supply chain Security

- Whatever method is choose, if diversity is (or must be) used there are some concerns that should be considered
  - Culturally similar teams tend to tackle problems in the same way
  - Programming errors
    - Different teams make the same mistakes - parts of the implementation are more difficult and teams tend to make mistakes in the same places
  - Specification errors
    - If there is a specification error it tends to arise in all implementations
    - This can be partially resolved by using various representations of the specifications

Supply chain Security

- Also, both approaches to redundancy in the software are susceptible to specification errors
  - If the specification is incorrect, the system may fail despite the great effort spent
- Although this problem also exists in the hardware, the software specifications are generally more complex and more difficult to validate
- A common partial solution is to develop different software specifications based on the problem specification

Supply chain Security

- On supply chain in hardware perspective, there might exist several controls to monitor activity and collect data to be inspected
  - Usually with sensors
- The way they exchange data varies
  - Periodic stimulus
    - Occurs at predictable time intervals
    - Example: a sensor can be interrogated 10 times per second
  - Aperiodic stimulus
    - Occurs in unpredictable moments
    - Example: a power failure can trigger an interruption, which must be processed quickly