**Case Study: WannaCry Ransomware 2017**

**1. Introduction**

In May 2017, a major cyberattack called **WannaCry** affected many computer systems worldwide. It targeted computers running Microsoft Window OS by encrypting data and demanding bitcoin payment. This study explains the attack from a systems engineering point of view and how problems in system design and management helped the attack spread and what we can learn to prevent similar events in the future.

**2. Background**

**2.1. What Is Ransomware?**

Ransomware is a type of harmful software (malware) that locks users out of their files. It demands payment, usually in Bitcoin, to unlock the files. WannaCry is one of these ransomware attacks.

**2.2. The WannaCry Attack**

WannaCry started on May 12, 2017, and spread quickly by taking advantage of a known vulnerability in the Windows operating system. This vulnerability was in a tool called **EternalBlue**. The attack affected hospitals, businesses, and other organizations around the world, stopping many important services and causing significant problems.

**3. Systems Engineering Analysis**

Systems engineering is a way to design, manage, and keep systems working well over time. When we look at WannaCry using this method, we see several issues in the way computer systems were built and managed.

**3.1. Problems in System Design**

* **Outdated Systems and Patching:**  
  Many companies used old versions of Windows that were not updated. Without regular updates, these systems were easy targets for attackers. A strong patch management process (making sure systems are kept updated) is important to stop vulnerabilities like the one WannaCry used.
* **Interconnected Networks:**  
  Modern computer systems are networks of many parts that work together. WannaCry spread by moving through these connected systems. Systems engineers recommend designing networks with good security checks and clear boundaries between systems to slow the spread of such attacks.

**3.2. Handling Risks and Stopping the Attack**

* **Identifying Risks:**  
  Systems engineering involves constantly checking and fixing weak spots. Regular risk checks and computer tests (like vulnerability scans) could have found the problem before the attack happened.
* **Building System Redundancy:**  
  Systems should have backups and spare parts so that if one part fails, the system can still work. During the WannaCry attack, organizations with good backup plans and separate network parts were less affected.
* **Planning for Incidents:**  
  A big part of systems engineering is to plan for emergencies. Having a clear plan for responding to cyberattacks can reduce damage and help the system recover faster. Many organizations did not have clear plans when WannaCry attacked.

**3.3. Failures in System Architecture**

* **Centralized Systems:**  
  Many older computer networks have a single, central system. When this central part failed, the whole network was at risk. Decentralizing or splitting the network into smaller parts helps limit the damage from any one attack.
* **Lifecycle Management:**  
  Systems engineering involves knowing when to upgrade or replace hardware and software. Organizations using outdated systems were hit hardest by WannaCry. Regularly updating and retiring old systems is crucial.
* **Communication and Process Integration:**  
  Good design means that security should be considered from the start, not added later. Better communication between IT security teams and engineers can help build systems that are both efficient and secure.

**4. Impact and Lessons Learned**

**4.1. Operational Impacts**

WannaCry caused several serious problems:

* **Healthcare Disruptions:** Hospitals struggled to treat patients because their computer systems were affected.
* **Financial Losses:** Many companies lost money due to system downtime and the cost of fixing the problems.
* **Public Trust Issues:** The attack made people worry about the security of their digital information.

**4.2. Key Engineering Lessons**

This attack teaches important lessons for building and managing systems:

* **Keep Systems Updated:** Regular updates and automated patch systems are essential.
* **Improve Network Design:** Using smaller, separated networks can reduce the spread of attacks.
* **Include Security Early:** Security must be built into a system from the beginning.
* **Plan for Failures:** Backup plans and rapid response systems are needed in case of an attack.

**4.3. Recommendations for Future Safety**

To prevent similar attacks, organizations should:

* **Conduct Regular Security Checks:** Use vulnerability scans and risk assessments on a regular basis.
* **Design Modular Systems:** Create systems with independent parts to reduce overall risk.
* **Enhance Training:** Ensure that both IT security teams and systems engineers work together and understand each other’s roles.
* **Invest in Resilience:** Develop strong backup systems and automatic tools to detect and respond to attacks quickly.

**5. Conclusion**

The 2017 WannaCry ransomware attack shows the risks of relying on outdated systems and weak security practices. By using systems engineering principles—such as regular updates, better network design, and clear incident plans—organizations can build stronger and more secure systems. Learning from this event can help prevent future attacks and protect important data and services.