Week 09

Microsoft Exchange Server Hack (2021)

**Step 2: Research the Attack**

**How did the attack happen?**

* The attack exploited four zero-day vulnerabilities in Microsoft Exchange Server:
  + **CVE-2021-26855** (Server-side request forgery),
  + **CVE-2021-26857** (Insecure deserialization),
  + **CVE-2021-26858** (Post-authentication arbitrary file write),
  + **CVE-2021-27065** (Post-authentication arbitrary file write).

Attackers first exploited **CVE-2021-26855** to gain unauthorized access, then chained it with the other vulnerabilities to execute code and drop web shells, which allowed persistent backdoor access to the compromised servers.

**Who were the attackers?**

* The attack was attributed to a **state-sponsored group** called **HAFNIUM**, believed to be operating out of China.

**What was the impact?**

* Tens of thousands of organizations globally were affected, including government agencies, think tanks, universities, and private companies.
* The breach allowed attackers to exfiltrate sensitive data and maintain long-term access to systems.
* **Financial Impact**: Costs were incurred for incident response, system patching, legal consequences, and reputational damage.
* **Operational Impact**: Many organizations had to take down servers temporarily for investigation and remediation.
* **Reputational Impact**: The trust in Microsoft Exchange Server security was severely affected.

**How was it discovered?**

* The attack was initially identified by **Volexity**, a cybersecurity firm, which detected suspicious activities on Exchange servers in early January 2021.
* Microsoft later confirmed the attack in **March 2021**, releasing security updates to patch the vulnerabilities.

**Step 3: Determine the Cause and Mitigation**

**Why did the attack succeed?**

* **Zero-day vulnerabilities** were exploited, meaning they were unknown to Microsoft before the attack.
* **Delayed patching**: Many organizations were slow to apply available patches after the vulnerabilities were disclosed.
* **Lack of network segmentation** and **insufficient monitoring** allowed attackers to maintain access without detection.

**How could it have been prevented?**

* Faster adoption of **security patches** and updates.
* Enhanced **threat detection and monitoring** for unusual activities on critical infrastructure.
* **Zero Trust architecture** to limit lateral movement inside networks.

**What mitigation strategies should be in place to prevent future attacks?**

1. **Regular patch management**: Apply updates as soon as they're released, especially for critical infrastructure.
2. **Network segmentation**: Isolate critical systems to reduce lateral movement.
3. **Endpoint Detection and Response (EDR)**: Monitor for abnormal behaviors like web shell deployment or unusual file writes.
4. **Threat hunting**: Proactively search for indicators of compromise (IOCs).
5. **Incident response plan**: Have a tested playbook ready for high-profile vulnerabilities.
6. **User awareness training**: Ensure IT teams are alert to emerging threats and zero-day exploits.

**Step 4: Peer Collaboration**

* Work with a peer and share your findings.

**Lab Logbook Requirement**

* **Attack Chosen**: Microsoft Exchange Server Hack (2021)
* **Useful Source**:
  + Microsoft Security Response Center: <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855>
  + Volexity’s analysis: https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/