# Post-Mortem-Report: Ransomware-Angriff

## 1. Zusammenfassung

Am [Datum] ereignete sich ein Ransomware-Angriff, der durch eine manipulierte Bewerbungs-E-Mail ausgelöst wurde. Diese E-Mail enthielt ein Office-Makro, das auf dem PC im Sekretariat ausgeführt wurde. Der Angriff breitete sich über ein File Share auf einen internen Server aus, wodurch ein Active Directory (AD)-Benutzeraccount mittels Ticket-Manipulation kompromittiert wurde. Anschließend übernahmen die Angreifer den Domänencontroller über eine Schwachstelle in Active Directory Certificate Services (ADCS). Der Angriff endete mit der Verschlüsselung des gesamten Netzwerks, wodurch wesentliche Geschäftsprozesse stark beeinträchtigt wurden.

## 2. Zeitlicher Ablauf

|  |  |
| --- | --- |
| **Zeitpunkt** | **Ereignis** |
| 08:30 Uhr | Empfang einer E-Mail mit einer gefälschten Bewerbung, die ein Office-Makro enthielt. |
| 08:45 Uhr | Ausführung des Makros auf dem Sekretariats-PC; erster Zugang des Angreifers. |
| 09:00 Uhr | Zugriff auf ein File Share, um Ransomware weiter zu verbreiten. |
| 10:30 Uhr | Kompromittierung eines AD-Benutzerkontos durch Pass-the-Ticket-Angriff. |
| 11:00 Uhr | Übernahme des Domänencontrollers durch eine Schwachstelle in ADCS. |
| 12:30 Uhr | Beginn der Netzwerkverschlüsselung durch die Ransomware. |
| 13:00 Uhr | Sicherheitsvorfall wurde durch die SOC-Überwachung erkannt und an das Incident Response Team gemeldet. |
| 13:30 Uhr | Netzwerksegmentierung und Isolierung betroffener Systeme zur Eindämmung des Schadens. |
| 14:00 Uhr | Incident Response Team beginnt mit der Untersuchung und ersten Eindämmungsmaßnahmen. |

## 3. Ursache

Die Ursache des Vorfalls war eine mangelnde Filterung von E-Mails und die Aktivierung von Office-Makros auf Endgeräten. Der Angriff wurde durch folgende Faktoren erleichtert:

• Fehlende Sandboxing-Funktionalität in der E-Mail-Sicherheitslösung.

• Ungeschützte File Shares, die den Zugriff und die Verbreitung von Malware ermöglichten.

• Schwache Sicherheitskonfigurationen in ADCS, die eine Privilegieneskalation erleichterten.

• Unzureichender Schutz der AD-Infrastruktur gegen Ticket-Manipulation-Angriffe.

## 4. Auswirkungen

**Finanzielle Auswirkungen:**

Der Angriff führte zu einer Schätzung von [Betrag] € durch Produktionsausfälle, Wiederherstellungskosten und potenziellen Bußgeldern für Compliance-Verstöße.

**Operative Auswirkungen:**

Die gesamte IT-Infrastruktur war für [Dauer] nicht verfügbar, was zu einem Stillstand der Geschäftsprozesse führte.

**Reputationsschaden:**

Der Vorfall beeinträchtigte das Vertrauen von Kunden und Partnern und führte zu erhöhter externer Aufmerksamkeit.

**Regulatorische Auswirkungen:**

Mögliche Verstöße gegen GDPR, NIS2 und andere Vorschriften aufgrund unzureichender Sicherheitsmaßnahmen.

## 5. Getroffene Maßnahmen

**Während des Vorfalls:**

• Isolierung des Netzwerks, um die Ausbreitung der Ransomware zu stoppen.

• Identifizierung und Deaktivierung des kompromittierten AD-Benutzerkontos.

• Sofortiges Abschalten und Trennen des Domänencontrollers.

• Einleitung der forensischen Analyse betroffener Systeme.

**Nach dem Vorfall:**

• Wiederherstellung des Netzwerks aus sauberen Backups.

• Implementierung vorläufiger Sicherheitsmaßnahmen, wie die Blockierung von Makros und striktere Firewall-Regeln.

• Schulung des Personals zur Erkennung von Phishing-Versuchen.

## 6. Lessons Learned

• **E-Mail-Sicherheit:** Einführung von Sandboxing für Anhänge und striktere Filterregeln für eingehende E-Mails.

• **Endpoint-Schutz:** Bereitstellung eines EDR/XDR-Systems zur Früherkennung und Eindämmung von Malware.

• **AD-Härtung:** Regelmäßige Überprüfung und Verbesserung der ADCS-Konfigurationen.

• **Awareness-Programme:** Regelmäßige Schulungen für alle Mitarbeiter, um Phishing-Angriffe zu erkennen und zu melden.

• **Incident Response Training:** Durchführung regelmäßiger Übungen, um die Effektivität des SOC und des Incident Response Teams zu testen.

## 7. Empfehlungen

• **Technische Maßnahmen:**

• Einführung von Multi-Factor Authentication (MFA) für alle Benutzer.

• Strikte Segmentierung von Netzwerken und File Shares.

• Aktualisierung und Härtung der ADCS-Konfigurationen.

• **Prozessoptimierung:**

• Einführung und Pflege detaillierter Playbooks für Incident Response.

• Implementierung eines Zero-Trust-Modells für den Zugriff auf kritische Systeme.

• **Schulungen:**

• Regelmäßige Anti-Phishing-Trainings für alle Mitarbeiter.

• Fortbildung des IT-Teams zu modernen Angriffsmethoden und Sicherheitsmaßnahmen.

## 8. Fazit

Der Vorfall zeigt, wie wichtig ein ganzheitlicher Sicherheitsansatz ist. Durch die Identifizierung der Schwachstellen und Umsetzung der empfohlenen Maßnahmen kann das Risiko zukünftiger Vorfälle minimiert werden. Ein strukturierter Incident Response Prozess, kombiniert mit proaktiven Sicherheitsmaßnahmen, wird dazu beitragen, die Resilienz des Unternehmens zu stärken.