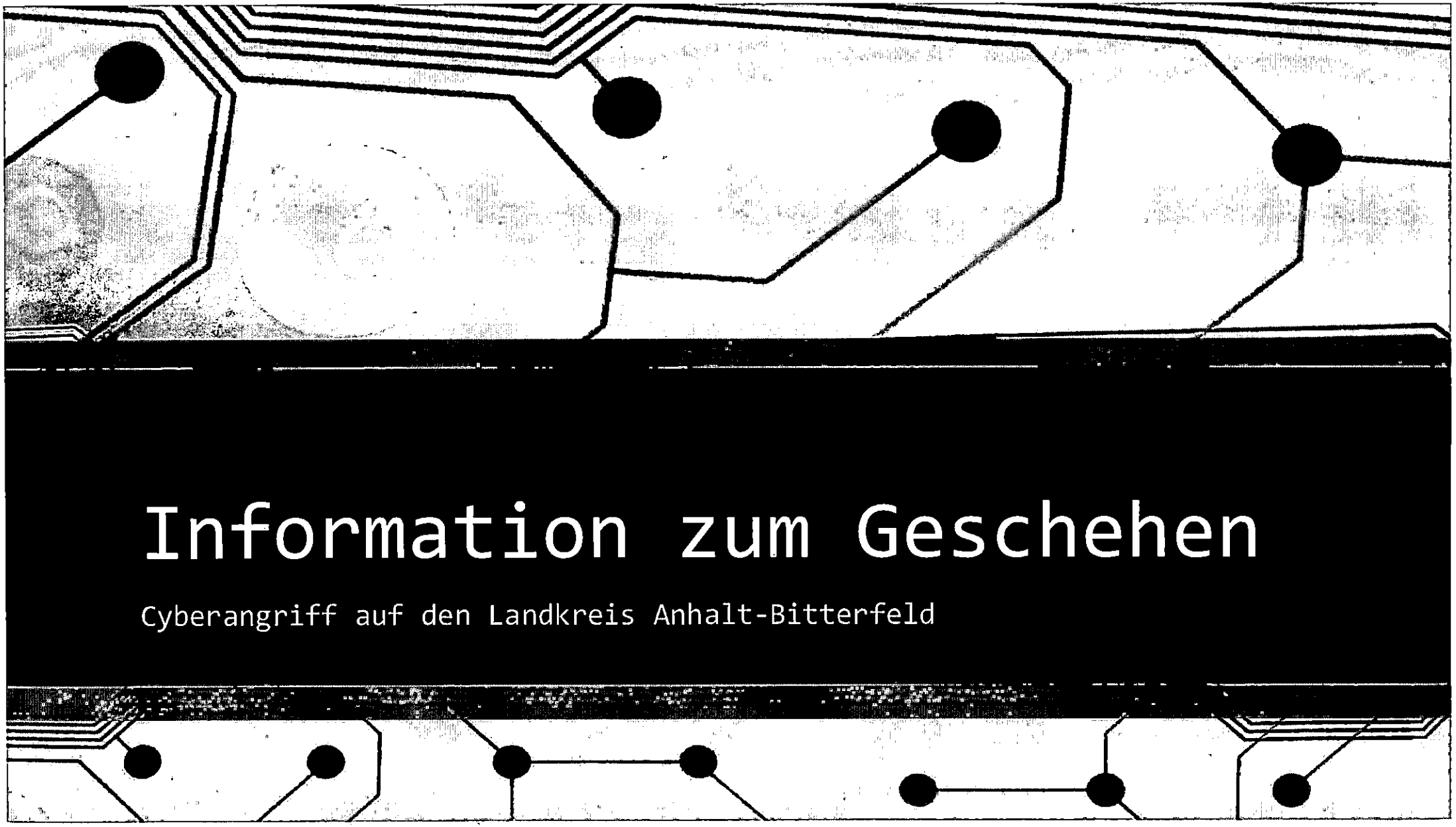

Information zum Geschehen

Cyberangriff auf den Landkreis Anhalt-Bitterfeld

Ablauf

- Nach erster Einschätzung der Lage und Sichtung der Backups wurden einzelne Systeme der virtuellen Umgebung mit getrennter Netzwerkverbindung hochgefahren und untersucht, dabei konnten Verschlüsselungen auf mehreren Servern festgestellt werden
- Ebenso wurden auf den betroffenen Servern die Systemdateien unserer Sicherheitssoftware gelöscht, sodass ein Start des Dienstes nicht mehr möglich war, die Systeme waren daher schutzlos
- Das CERT Nord und das BSI kontaktierten uns und versprachen schnelle Hilfe
- Auch Prof. Dr. Leich von der Hochschule Harz bot seine Hilfe an
- Der Landkreis stellte Strafanzeige gegen unbekannt bei der Polizei und der Stab außergewöhnliche Ereignisse wurde einberufen, hier nahmen bereits Vertreter der HS Harz, des Ministeriums für Finanzen, vom CERT Nord , vom Bundesamt für Sicherheit in der Informationstechnik und vom Landeskriminalamt (Zentrale Ansprechstelle Cybercrime) teil

Ablauf

- Das LKA entsandte ein Beweissicherungsteam der Polizei und diese stellten Logdateien und Festplatten zur weiteren Analyse sicher
- Aufgrund der Tragweite des Ereignisses und der nicht abschätzbaren Folgen für die Bevölkerung entschied sich der Landrat zur Feststellung des Katastrophenfalls und forderte weitere Unterstützung der anderen Institutionen an
- Daraufhin wurden sowohl vom BSI dem Ministerium der Finanzen, als auch vom CERT Nord Mitarbeiter entsandt
- Noch am Abend des 09.07. trafen die Experten Ortholf (IT-Sicherheitsbeauftragter, Ministerium der Finanzen LSA), Lobmeyer (BSI) und Prof. Dr. Leich (HS HARZ) ein
- Für den nächsten Morgen wurde auch ein Forensikerteam nach Köthen entsandt welches das Ausmaß des Befalls einschätzen sollte
- Nach den gewonnenen Erkenntnissen des LKA und den Technikern vor Ort musste nun von einem Angriff durch Cyberterroristen ausgegangen werden

Ablauf

- Am Abend des 10.07. wurde ein Plan der nächsten Schritte ausgearbeitet und dem Katastrophenstab am Folgetag vorgestellt
- Von CERT Nord wurde eine Fachfirma beauftragt den Neuaufbau der Infrastruktur zu koordinieren
- Am Montag nahm die Firma die Arbeit vor Ort auf und verschaffte sich zunächst einen Überblick
- Die Forensiker der Firma begannen mit der Analyse der Schadsoftware
- Durch den Incident Manager wurden erste Schritte zur Wiederherstellung vorgestellt

Ablauf

- Zunächst wurde eine Art Notnetz in Betrieb genommen, indem ca. 50 Arbeitsplätze mit einem Minimum an Anwendungen ausgestattet wurde und damit die Erreichbarkeit sichergestellt war (E-Mail, Office und Dokumentenaustausch)
- Die Fachfirma übergab den Staffelstab an das BSI, welches die weiteren Arbeiten begleitet
- Das Bundesamt für Sicherheit in der Informationstechnik erarbeitete zusammen mit der EDV und Hr. Ortholf vom Finanzministerium ein Konzept zur Netzwerkertüchtigung nach neuesten Sicherheitsstandards, welches aktuell abgearbeitet wird
- Ein Team von Forensikern des BSI begann mit der Analyse der Datensicherungen und erstellte Handouts zur Fortführung der Arbeiten durch die EDV des Landkreises
- In den letzten Tagen wurden einzelne Anwendungen (u.a. Bundeselterngeld, Vergaben, Wahlen) in den Notbetrieb überführt oder in andere Gebietskörperschaften ausgelagert, weitere werden noch folgen

Ablauf

- Aktuell wird an der Wiederinbetriebnahme der Kfz-Zulassung und des HKR Systems gearbeitet (Haushalts-, Kassen- und Rechnungswesen)
- Heute sind zwei Experten unseres Dienstleisters eingetroffen, die beim Aufbau des neuen Active Directory federführend unterstützen
- Ebenfalls sind heute zwei Vertreter der Bundeswehr des Kommandos Cyber- und Informationsraum zur weiteren Unterstützung eingetroffen
- Wir danken allen Beteiligten für die schnelle Hilfe

Ablauf

- Bereits am 05.07. wurden durch unser Sicherheitssystem mehrere Dateien mit dem Namen „spoolsv.exe“ als Malware identifiziert und in die Quarantäne verschoben
- Am nächsten Morgen wurden erste verschlüsselte Dateien auf den Netzlaufwerken der Landkreisverwaltung entdeckt
- Als Sofortmaßnahme wurden sämtliche Serversysteme heruntergefahren und die Verbindung zum Netz des Bundes sowie zum Internet getrennt
- Gleichzeitig wurden die Amtsleiterin der EDV und der Landrat über die Situation in Kenntnis gesetzt, das Herunterfahren der Clientsysteme wurde mittels Lautsprecherdurchsage veranlasst und alle Amtsleiter per Telefon informiert
- Die EDV meldete den Sicherheitsvorfall dem Bundesamt für Sicherheit in der Informationstechnik und dem Datenschutzbeauftragten des Landkreises