Kai Schwardt
Sicherheitsbeauftragter der Kreisstadt Erbach

Michelstadt, 30.04.2023

Lage der IT-Sicherheit – Kreisstadt Erbach

Rahmenbedingungen - aktuelle Bedrohungslage/Internetkriminalität

- Die Bedrohungslage durch externe Angriffe/Ransomware Attacken von Internetkriminellen ist in den vergangenen Wochen und Monaten erneut erheblich gestiegen
- Angriffe durch Internetkriminelle erfolgen weiterhin bevorzugt über Mailanhänge, in Teilen jedoch ebenso über infizierte Downloads aus dem Internet
- Identitätsdiebstahl, d.h. der Diebstahl von Anmeldedaten in Internetsystemen und „lokalen" IT Systemen nimmt an Verbreitung zu. Identitäten werden durch entsprechende Mails von Internetkriminellen eingeholt, jedoch auch durch „Hacks" von Internetdatenbanken erworben
- Durch Identitätsdiebstahl in Besitz genommene Anmeldeidentitäten werden von Internetkriminellen genutzt, um sich Zugang zu Internetportalen aber auch lokalen IT-Systemen zu verschaffen
- Attacken/Zugriffe auf Internetsysteme bzw. lokale IT-Systeme der Kreisstadt Erbach können nicht final ausgeschlossen werden. Daher wurden/werden Maßnahmen ergriffen um die Eintrittswahrscheinlichkeit zu reduzieren sowie mögliche Auswirkungen zu mildern bzw. abzusichern.

Bereits ergriffene und umgesetzte Maßnahmen

- Regelmäßiges Updating der eingesetzten IT-Systeme um Sicherheitslücken der eingesetzten Betriebssysteme zu schließen und zu beseitigen
    - Serversysteme
    - Clients
    - ***Ergebnis: Reduzierung der Eintrittswahrscheinlichkeit von Hackerattacken***
- Regelmäßige Datensicherung und Auslagerung der Datensicherungsmedien
    - Serversysteme
    - ***Ergebnis: Milderung der Auswirkungen bei Hackerattacken***
- Regelmäßige Sensibilisierung und Schulung der Anwender
    - Handhabung von Mail und Internet, Vorsicht bei der IT-Nutzung
    - zuletzt Ende 2022
    - ***Ergebnis: Reduzierung der Eintrittswahrscheinlichkeit von Hackerattacken***
- Einführung einer Dienstanweisung zur IT-Nutzung/IT-Benutzerrichtlinie
    - mit konkreten Vorgaben zur IT-Nutzung
    - ***Ergebnis: Reduzierung der Eintrittswahrscheinlichkeit von Hackerattacken***
- Einführung einer Dienstvereinbarung „Telearbeit" (nicht durch den IT-Sicherheitsbeauftragten)
    - mit konkreten Vorgaben zur IT-Nutzung im mobilen Arbeiten
    - ***Ergebnis: Reduzierung der Eintrittswahrscheinlichkeit von Hackerattacken***
- Verbot der Privatnutzung der IT-Systeme der Kreisstadt Erbach
    - Im Rahmen einer Dienstanweisung/IT-Benutzerrichtline
    - ***Ergebnis: Reduzierung der Eintrittswahrscheinlichkeit von Hackerattacken***
- Verbot der Nutzung privater Endgeräte für die Tätigkeiten im Rahmen des Beschäftigtenverhältnisses mit der Kreisstadt Erbach
    - Im Rahmen einer Dienstanweisung/IT-Benutzerrichtline
    - ***Ergebnis: Reduzierung der Eintrittswahrscheinlichkeit von Hackerattacken***
- Weitestgehende technische Deaktivierung von USB-Medien für Speichernutzung
    - Im Rahmen einer Dienstanweisung/IT-Benutzerrichtline
    - ***Ergebnis: Reduzierung der Eintrittswahrscheinlichkeit von Hackerattacken***

- Kontrolle und Überarbeitung und Reduzierung der Anzahl von Nutzerkonten mit administrativen Berechtigungen
    - ***Ergebnis: Reduzierung der Eintrittswahrscheinlichkeit von Hackerattacken***
- Wiederholte Änderung zentraler administrativer Kennworte
    - ***Ergebnis: Reduzierung der Eintrittswahrscheinlichkeit von Hackerattacken t***
- Einführung verbesserter Kennwortqualität und Nutzungsdauer
    - regelmäßiger Änderungsintervall der zu verwendenden Kennworte
    - Vorgabe bezüglich Kennwortkomplexität
    - ***Ergebnis: Reduzierung der Eintrittswahrscheinlichkeit von Hackerattacken***
- Verbesserung der Zutrittssicherheit zu IT Systemen
    - durch neue Schließanlage
    - durch Reduzierung der Nutzung des Serverraums für „andere Zwecke“
    - ***Ergebnis: Reduzierung der Eintrittswahrscheinlichkeit von Hackerattacken***
- Qualifizierung und Sensibilisierung der Anwender im Rahmen von Ortsbegehungen im Verwaltungsgebäude
    - Sichtung der Arbeitsumgebung und Empfehlungen zur Anpassung bezüglich Informationssicherheit
    - Verbesserung der Situation bezüglich Vernichtung „analoger“ Datenbestände (Shredder)
    - ***Ergebnis: Reduzierung der Eintrittswahrscheinlichkeit von Hackerattacken***
- Einführung eines zentral verwalteten Virenschutz incl. Personal FireWall zum Schutz der Client Systeme
    - ***Ergebnis: Reduzierung der Eintrittswahrscheinlichkeit von Hackerattacken***
- Einführung eines lokalen Mailsystems mit Spam und Virenschutz an Stelle des zentralen (und in 2022 ausgefallenen) Mailsystems der Odinet
    - ***Ergebnis: Reduzierung der Eintrittswahrscheinlichkeit von Hackerattacken***
    - ***Ergebnis: Milderung der Auswirkungen bei Hackerattacken***

<u>Kurzfristig geplante Maßnahmen</u>

- Einführung einer 2-Faktor-Authentifizierung (Anmeldung) bei remote-Zugriffen auf das Netzwerk der Kreisstadt Erbach (für Home Office und Travelling-User)
    - ***geplant bis Ende zweites Quartal 2023***

<u>Weitere mittelfristig zu diskutierende und ggf. umzusetzende Maßnahmen</u>

- Einführung Festplattenverschlüsselung
    - für mobile IT Systeme
    - für „feste“ IT Systeme
- Fortsetzen der Ortsbegehungen und Überprüfung und Sensibilisierung hinsichtlich Informationssicherheit
    - in der Stadtverwaltung
    - im Bauhof
    - in Kitas
    - in der Feuerwehr
- Schulung / Sensibilisierung neuer Beschäftigte
- Verbesserung der IT-Betriebssicherheit der Serversysteme im Rahmen der nächsten Aktualisierung der Systeme

Kai Schwardt, 30.04.2023