LANDRATSAMT
ERZGEBIRGSKREIS

Landratsamt Erzgebirgskreis · Paulus-Jenisius-Str. 24 · 09456 Annaberg-Buchholz
02000

Fraktion GRÜNE
Herrn Kreisrat
Heiko Reinhold

ausschließlich per E-Mail

DER LANDRAT

Bearbeiter/in: Frau Milazeck
Dienstgebäude: Paulus-Jenisius-Str. 24
09456 Annaberg-Buchholz
Zimmer-Nr.: A0.07
Telefon: 03733 831-1015
Telefax: 03733 831-1028
E-Mail: christel.milazeck@kreis-erz.de
Ihre Zeichen:
Ihre Nachricht:
Unsere Zeichen:
Datum: 30.08.2021

nachrichtlich: Fraktionsvorsitzende, fraktionslose Kreisräte

IT-Sicherheit

Sehr geehrter Herr Kreisrat Reinhold,

Ihre per E-Mail am 08.08.2021 eingegangenen Anfragen beantworte ich wie folgt:

Ihren Anfragen stellen Sie Folgendes voran:

Im Juli wurde das Landratsamt Anhalt-Bitterfeld das Opfer einer Cyber-Attacke, die die interne und externe Kommunikation weitgehend verhinderte und zu massivem Datenverlust führte.
Obwohl eine hundertprozentige Sicherheit nicht zu gewährleisten ist, gibt es doch bewährte Konzepte, die auf verschiedenen Mitteln und Methoden basieren, um zumindest die Auswirkungen solcher Hackerangriffe zu minimieren. Besondere Aufmerksamkeit erlangte das Thema auch im Zuge der verstärkten Arbeit im Home-Office.

1. Gibt es ein IT-Sicherheitskonzept und auf welchen Grundlagen beruht dieses?

Gemäß § 4 des Sächsischen Informationssicherheitsgesetzes (SächsISichG) werden im Landratsamt Erzgebirgskreis angemessene organisatorische und technische Vorkehrungen zur Gewährleistung der Informationssicherheit getroffen. Alle Maßnahmen unterliegen einem Informationssicherheitsmanagementsystem (ISMS), das nach dem BSI-Standard 200-2 aufgebaut, betrieben und kontinuierlich verbessert wird.

2. Werden die Empfehlungen des BSI berücksichtigt und umgesetzt?

Für den Aufbau des ISMS sind die Bausteine und Anforderungen des IT-Grundschutz-Kompendiums des BSI maßgeblich. Empfehlungen über das IT-Grundschutz-Kompendium hinaus – beispielsweise technische Richtlinien oder Warnmeldungen des BSI – werden ebenso berücksichtigt und bei Bedarf

umgesetzt. Zum Beispiel legten Presseveröffentlichungen nahe, dass die IT-Systeme des Landratsamtes Anhalt-Bitterfeld durch die Ausnutzung der Schwachstelle „PrintNightmare“ kompromittiert wurden. Die dazu von Microsoft bereitgestellten Workarounds und Patches wurden jeweils unmittelbar nach Veröffentlichung eingespielt. Wie bisher auch werden Medienmeldungen und Empfehlungen von Sicherheitsbehörden aktiv verfolgt und bei Bedarf umgesetzt.

3. Wurden optimale Sicherheitsvorkehrungen bei mobilen Geräten, Netzwerk-Anbindungen von Home-Office-Arbeitsplätzen, Schulen usw. getroffen?

Die Anbindung von Homeoffice-Arbeitsplätzen erfolgt über eine Plattform für virtuelle Anwendungsbereitstellung. Hierbei werden nicht wie bei klassischen VPN-Lösungen die VPN-Clients netztechnisch integriert, sondern es wird per SSL-gesichertem Kanal ein virtueller Desktop übertragen. Das Risiko einer Infektion durch Schadsoftware durch angeschlossene (Homeoffice)-Clients wird dadurch auf ein Minimum reduziert. Als Endgeräte kommen nur vom Sachgebiet IT meines Hauses installierte bzw. geprüfte Systeme zum Einsatz. Die Authentifikation am zentralen Einwahlknoten erfolgt je nach Endgerät entweder zusätzlich durch ein SSL-Zertifikat oder bevorzugt durch einen Token (hard- und softwarebasierend).

4. Wird regelmäßig zu Sicherheits- und Datenschutzaspekten geschult?

Belehrungen zu Datenschutz und EU-DSGVO finden bei Neueinstellung der Mitarbeiter statt. Sensibilisierungen zur Informationssicherheit finden gemäß BSI-Baustein „ORP.3“ regelmäßig und anlassbezogen statt.

5. Wird der Datenbestand regelmäßig und ausreichend gesichert, so dass auch im Falle eines Totalausfalls oder von Naturkatastrophen eine Wiederherstellung möglich ist?
Werden die Datensicherungen an einem zweiten Standort gespiegelt?
Wird die Wiederherstellung der gesicherten Daten in regelmäßigen Abständen getestet?

Die Datensicherungen der Landkreisverwaltung unterliegen einem Datensicherungskonzept. Gesichert werden alle Daten von Servern für Anwendungs- und Betriebssoftware, Systemdaten, Benutzerdaten, Datenbanken, Software und E-Mail-Postfächer. Als Datensicherungsstrategie wird das Konzept „Disk-to-Disk-to-Tape“ (D2D2T) umgesetzt. Die Sicherungsbänder werden mit speziellen Koffern in ein anderes Dienstgebäude transportiert und dort standortgetrennt vom zentralen Rechenzentrum aufbewahrt. Die inkrementellen Backups werden zusätzlich auf ein System an einem weiteren Standort gespiegelt. Die Wiederherstellung einzelner Daten erfolgt im Live-Betrieb bei beispielsweise versehentlich gelöschten oder überschriebenen Daten. Komplette Server werden beispielsweise vor dem Einspielen größerer Updates zurückgesichert, um diese vorher auf einem Zweitsystem testen zu können.

6. Existiert ein Disaster-Recovery-Konzept, um den Betrieb der zentralen IT-Infrastruktur (z. B. Verzeichnisdienste) nach einem größeren Ausfall in einem angemessenen Zeitraum wiederherstellen zu können?

Ein vollumfängliches Business Continuity Management nach dem BSI-Standard 200-4 existiert derzeit noch nicht. Ein Wiederherstellen der zentralen IT-Infrastruktur, wie z. B. Domain-Controller, E-Mail-Server, usw. ist jedoch auch jetzt schon möglich.

7. Existieren Redundanzen bzw. Hochverfügbarkeitskonzepte für kritische, zentrale IT-Komponenten, um den Betrieb bei Ausfall einzelner Systembestandteile aufrechtzuerhalten?

Das zentrale Rechenzentrum ist redundant ausgelegt. Dabei befinden sich in getrennten Gebäuden zwei Serverräume, die sich bei Unterbrechung zu einem gewissen Grad gegenseitig stützen können. Eine 100%ige Hochverfügbarkeit wird nicht gewährleistet.

8. Erfolgt eine externe Beratung oder Überprüfung hinsichtlich der Datensicherheit?

Die Informationssicherheit wird durch externe Dritte in Form von Audits und Revisionen überprüft. Zuletzt 2020 und 2021 im Rahmen der Einführung von „i-Kfz" (internetbasierte Fahrzeugzulassung) und durch die EU-Zahlstelle. Prüfaspekte sind dabei jeweils auch Regelungen, die über den jeweiligen Informationsverbund hinausgehen. Festgestellte Mängel werden in Form von Maßnahmenbehandlungsplänen bearbeitet.

9. Gibt es explizit Verantwortliche für die Netz- und Datensicherheit?

Die Gesamtverantwortung für die Informationssicherheit trage ich als Landrat entsprechend der BSI-Anforderung ISMS.1.A1. Für die Steuerung und Koordination des Sicherheitsprozesses wurden jeweils ein IT- und Informationssicherheitsbeauftragter und ein Vertreter bestellt und gemäß § 8 SächsISichG dem Beauftragten für Informationssicherheit des Freistaat Sachsen gemeldet. Innerhalb des Sachgebietes IT haben sich Teamstrukturen etabliert, bei dem durch Spezialisten innerhalb der Teams auch die Belange der Server- und Netzsicherheit berücksichtigt und verantwortet werden.

Mit freundlichen Grüßen

F. Vogel