

**öffentlich**

## **Vorlage zur Behandlung im Verwaltungs- und Finanzausschuss**

Sitzung am 25.06.2012

### **TOP 8: IT-Sicherheit im Landratsamt**

#### A. Beschlussvorschlag:

Kenntnisnahme

#### B. Kosten/Finanzielle Auswirkungen:

Für Sofortmaßnahmen stehen im laufenden Haushalt Mittel zur Verfügung;  
Größere Maßnahmen sind ggf. im Haushalt 2013 vorzusehen

Anlagen:

**öffentlich**

## **IT-Sicherheit im Landratsamt**

### **1. Sachverhalt:**

Das Landratsamt ist in verschiedenen Organisationseinheiten zuständig für die Bewilligung und Auszahlung von EU-Fördergeldern und damit Teil der „EU-Zahlstelle Baden-Württemberg“. Dieser EU-Zahlstelle zuzuordnen sind das Landwirtschaftsamt, das Umweltamt sowie aus dem Vermessungsamt das Sachgebiet Flurneuordnung.

Für die „EU-Zahlstelle BW“ wurde vom Land eine IT-Sicherheitsleitlinie erlassen mit der verbindlichen Einführung des „IT-Grundschutzes“ nach Vorgaben des Bundesamtes für Sicherheit in der Informationstechnologie (BSI). Das BSI hat für den IT-Grundschutz ein „Handbuch“ erstellt, das laufend der sehr dynamischen technischen Entwicklung aber auch genauso dynamischen Gefährdungssituation angepasst wird. Die in diesem Handbuch, das in der aktuellen Version 12 4.000 Seiten Text und ca. 1.400 Maßnahmen umfasst, gelisteten Bausteine sind von der Verwaltung anhand der eigenen technischen und organisatorischen Gegebenheiten auf Relevanz zu prüfen und ggfs. umzusetzen.

Für die bei uns eingesetzte Hard- und Software sind rund 1.000 Maßnahmen einschlägig. Die Maßnahmen umfassen dabei nicht nur die EDV-Arbeitsplätze im engeren Sinne, sondern auch die internen und externen Datennetze, Telefonanlagen, Multifunktionsgeräte (drucken, kopieren, scannen, faxen), die Zutrittskontrolle, die Einhaltung von Brandschutzvorschriften, die Elektro- und Haustechnik bis hin zur Aufbewahrung und Entsorgung von Datenträgern.

Das Ministerium für Ländlichen Raum und Verbraucherschutz Baden-Württemberg (MLR) hat am 2.11.2011 angekündigt, die Umsetzung und Einhaltung des IT-Grundschutzes im Landratsamt Zollernalbkreis (Teilbereiche EU-Zahlstelle) zu prüfen und hat vorab umfangreiche Prüfdokumente angefordert. Die Vorort-Prüfung erfolgte dann am 7.2.2012. Drei EDV-Fachleute des MLR sowie ein Mitarbeiter der Europäischen Finanzkontrolle (EFK) prüften einen Tag lang, ob die in den Prüfdokumenten („auf dem Papier“) dargestellten Schutz- und Sicherheitsvorkehrungen auch tatsächlich umgesetzt und wirksam sind.

Die Vorbereitung auf die Prüfung war für unser EDV-Team neben dem laufenden Tagesgeschäft sehr arbeitsintensiv, u.a. auch deshalb, weil viele Sicherheitsmaßnahmen bei uns gelebter Alltag, aber nicht lückenlos schriftlich dokumentiert waren. Man kann die Prüfkation vom Aufwand und von den Abläufen mit einem Zertifizierungsverfahren, wie es in der Privatwirtschaft üblich ist, vergleichen, mit dem Unterschied, dass sie per Gesetz vorgesehen ist.

Bei der Prüfung wurde ein Maßnahmen-Check anhand von 178 Kontrollfragen durchgeführt. Zusätzlicher Bestandteil der Prüfung war eine einstündige Begehung. Hier wurden Büro- und Serverräume sowie weitere Räume der technischen Infrastruktur sehr genau besichtigt.

Mit Schreiben vom 26.4.2012 ging der Prüfbericht beim Landratsamt ein.

**öffentlich**

**2. Auszug aus dem Prüfbericht „6. Gesamtbewertung“**

*„Die Erstellung der Dokumentation nach Vorgaben des BSI ist beim Landratsamt Zollernalbkreis mehrheitlich umgesetzt. Die Dokumentenprüfung hat eine vergleichsweise geringe Beanstandungsquote ergeben...*

*Die Qualität der Angaben des Basis-Sicherheitschecks (BSC) ist hoch bis mittel.*

*Die Vor-Ort-Prüfung ergab eine Abweichungsquote\* von ca. 25%. Dies ist erhöht und zeigt, dass die Umsetzung einer Vielzahl von Maßnahmen zwar auf den Weg gebracht, aber noch nicht vollständig abgeschlossen ist. Zu den beanstandeten Maßnahmen befinden sich in den jeweiligen Kapiteln dieses Berichts konkrete Hinweise zur korrekten Maßnahmenumsetzung.*

*Informationssicherheit nach dem IT-Grundschutz ist eine Daueraufgabe. Änderungen in der Organisation und in der Technik sowie aktualisierte Vorgaben des BSI führen zu einer Überprüfung der Referenzdokumente (BSC etc.). Diese Dynamik bewirkt, dass die IT-Grundschutz konforme Etablierung und Dokumentation von Prozessen zum Zeitpunkt der Prüfung eine Momentaufnahme darstellt.*

***Vor diesem Hintergrund ist durch das gegenwärtig erreichte und im Prüfbericht dokumentierte Sicherheitsniveau die Informationssicherheit der EU-Zahlstelle gewährleistet.\****

Die beanstandeten Maßnahmen sind entsprechend den Hinweisen zur korrekten Maßnahmenumsetzung abzuarbeiten. Eine aktualisierte Dokumentation zur Maßnahmenumsetzung ist bereits im Juli 2012 dem MLR vorzulegen.

Bemängelt wurden insbesondere folgende Punkte:

Die im Hauptgebäude des Landratsamtes eingesetzte **Schließanlage** entspricht nicht mehr den aktuellen Sicherheitsanforderungen, weil der Schlüsselschutz der Schließanlage abgelaufen ist. Aktuell werden deshalb die Kosten für die Installation einer neuen zentralen Schließanlage ermittelt und für den Haushaltsentwurf 2013 eingebracht. In diesem Zusammenhang ist anzumerken, dass die vorhandene Schließanlage nach 30 Dienstjahren ohnehin nicht mehr zeitgemäß aufrecht zu erhalten ist und jede Raumveränderung erhebliche Kosten mit sich bringt.

\* Wobei hier auch nur „teilweise“ umgesetzte oder „nicht beurteilbare“ Maßnahmen als Abweichungen gewertet wurden“.

Die **manuelle Dokumentation** der Vergabe von Berechtigungen im EDV-System (welcher Mitarbeiter darf welche Daten sehen, ändern, drucken, löschen?) wurde im Grundsatz bemängelt. Die enorme Komplexität, die ein Betrieb von knapp 700 Benutzern mit sich bringt, erfordert einen schnelleren Überblick über die eingerichteten Zugriffsrechte. Eine bessere Revisionssicherheit ist nur über die Einführung eines automatisierten Verfahrens zum Berechtigungsmanagement möglich. Auch hierfür werden die Kosten ermittelt und in den Haushalt 2013 eingebracht.

### öffentlich

Im Elektrobereich gilt es vor allem, die **Dokumentation des Elektronetzes** zu verbessern, sowie die BGV A3 Geräteprüfung (Elektrogeräteprüfung) zeitnah umzusetzen.

Weitere geforderte Maßnahmen im Bereich der Netzwerksicherheit werden derzeit umgesetzt. Hierfür sind entsprechende Haushaltsmittel bereits vorhanden.

### **3. Ausblick:**

Rechtlich zwingend anzuwenden ist der IT-Grundschutz derzeit lediglich bei den Organisationseinheiten der „EU-Zahlstelle“. Viele Maßnahmen lassen sich aber sinnvollerweise nur für „keinen oder alle“ Arbeitsplätze umsetzen. Dies ist kein übertriebener Standard, weil in anderen Ämtern (Jugendamt, Sozialamt, Gesundheitsamt...) sensiblere Daten als in der EU-Zahlstelle verwaltet werden. Der Bund hat angekündigt, für die Waffenbehörden ebenfalls die Anwendung des IT-Grundschutzes vorzuschreiben. Wir werden nicht umhin kommen, auf absehbare Zeit in der gesamten Kreisverwaltung das Sicherheitsniveau vergleichbar des BSI-Grundschutzhandbuches einzurichten und zu dokumentieren.