Geschäft 3498

Eing.-Datum: 14.1.2004

Bericht der Wirkungsprüfungskommission:

„Informatik (IT)–Sicherheit der Gemeinde Allschwil“

Beilage: Kurzfassung ‚Security Audit' vom 17.7.2003

0. Ausgangslage

Wie im Bericht Nr. 3439A (Bericht der WiKo zum Schlussbericht des Gemeinderates zum Projekt Allwo, ‚Allschwil wirkungsorientiert') dargelegt, hat sich die WiKo im 1. Quartal 2003 eingehend mit den Leistungsaufträgen, im 2. Quartal 2003 dann mit den zugehörigen Leistungsberichten 2002 befasst. Im Zusammenhang damit fand der **Leistungsauftrag/Leistungsbericht Nr. 193 „Produktgruppe Informationstechnik IT“ bezüglich Sicherheitsfragen besondere Beachtung**. Anlässlich der Diskussionen mit dem Gemeinderat zu den diesbezüglichen Fragen der WiKo wurde die WiKo darüber informiert, dass auch der Gemeinderat sich mit diesem Thema speziell befasste. Er beauftragte ein hierfür spezialisiertes Unternehmen mit der Durchführung eines umfassenden Sicherheitstestes, der im Frühjahr 2003 durchgeführt wurde. D.h. der Gemeinderat hatte bereits parallel zu den Diskussionen mit der WiKo zum Leistungsauftrag als solchem Schritte in der von der WiKo gewünschten Richtung unternommen.

Die mit der Prüfung beauftragte Firma Netcloud legte mit einem rund 70 Seiten starken ‚Security-Audit' ein sehr technisches und komplexes Werk vor, welches zu einer auch für Nichtfachleute verständlichen Kurzfassung überarbeitet wurde (siehe Beilage).

Mit Brief vom 22. August 2003 erhielt die WiKo vom Gemeinderat zusammen mit der Kurzfassung des Security-Audits einen ausführlichen Brief mit weiteren Informationen und Beschlüssen zum Thema IT-Sicherheit. In gewohnter Art und Weise erstellte die WiKo sowohl zum Brief (inkl. Beschlüssen des Gemeinderates) wie zur Kurzfassung des Security Audits einen Fragenkatalog, welcher seitens des Gemeinderates ebenfalls in gewohnter Manier ausführlich beantwortet wurde.

Der nachfolgende Bericht fasst die unter den Titel ‚Controlling' zu stellende Arbeit der WiKo zusammen und kommentiert die beiden aus dem Sicherheitstest resultierenden Papiere:

1. Kurzfassung ‚Security Audit' vom 17. Juli 2003 à siehe Beilage

2. Ergebnisse Sicherheitstests und eingeleitete Massnahmen (Brief mit IT-Sicherheitsbezogenenen Beschlüssen des Gemeinderates an die WiKo vom 22. August 2003)

3. Würdigung der Berichte: Weiteres Vorgehen

4. Anträge

1. Kurzfassung ‚Security Audit'

Dieses Kapitel enthält **ergänzende** Bemerkungen der WiKo zu einzelnen Kapiteln der Kurzfassung ‚Security Audit' à siehe Beilage zu diesem Bericht. Die Zusammenfassung ist auch für IT-Laien verständlich abgefasst ist: Danke!

1.1. Ziel des Audits

Die WiKo fragte nach ausführlicherer Definition der Ziele und erhielt von Markus Rudolf von Rohr folgende Antworten, die teilweise wörtlich zitiert sind.

1.1.1. ‚die interne IT-Infrastruktur so gut wie möglich zu schützen' (siehe Security Audit, Seite 2, Kapitel 2: 1. Ziel des Audits)

Sicherheitsrelevante Anpassungen der Netzwerkkomponenten und Konfigurationen an den Servern sind durchgeführt worden (Neudefinition von Passwörtern, Entfernen von unnötigen Protokollen auf den Servern und im Netzwerk). Entsprechende bauliche Massnahmen sind bereits im Zuge des Neubaus des Gemeindezentrums realisiert worden.

1.1.2. ‚die Ausfallquote der IT-Infrastruktur so klein wie möglich zu halten' (siehe Security Audit, Seite 2, Kapitel 2: 2. Ziel des Audits)

Durch eine optimale Ausrichtung und eine bedarfsorientierte Bewirtschaftung der Infrastruktur kann die Informatik eine Ausfallquote von unter 2% gewährleisten. Die Verfügbarkeit der Rechner und des Netzwerkes liegt derzeit über 98 % (bezogen auf die SOLL-Betriebszeiten). Serviceverträge mit den Lieferanten garantieren diese hohe Betriebsbereitschaft.

1.1.3. ‚die Datensicherheit und Datenkonsistenz zu gewährleisten' (siehe Security Audit, Seite 2, Kapitel 2: 3. Ziel des Audits)

Folgende Punkte sind in diesem Zusammenfang von Wichtigkeit:

- Bauliche Massnahmen wurden im Zuge des Neubaus des Gemeindezentrums realisiert (siehe auch Kapitel 2.1 dieses Berichtes (Einschätzung der Situation), letzter Abschnitt). Es steht ein separater, nicht dem Rechenzentrum angegliederter Backup-Raum zur Verfügung.

- Durch tägliche Jobs (Ausführung von Programmen, welche die Software-Lieferanten zur Verfügung stellen) werden die wichtigsten Daten der Kernapplikationen (NEST/ABACUS, INOVA-Time, CostController) gesichert und auf Konsistenz überprüft. Dadurch sind die Daten widerspruchsfrei und können somit als korrekt angesehen werden.

- Stromausfälle werden durch eine USV-Anlage (Notstromanlage) überbrückt, welche die Stromversorgung der IT für rund 2.5 Std. sichert. Dies ermöglicht die ordentliche Datensicherung und das korrekte Herunterfahren der Rechner.

- Im Bereich der Server wird mit RAID-Controller (Spiegelungen) gearbeitet; im Einsatz stehen RAID 1 und RAID 5.

- Regelmässig wiederkehrende Wartungen an der Infrastruktur tragen dazu bei, dass allfällige Fehler frühzeitig erkannt und behoben werden können.

- Die Netzwerksteigzone wird redundant geführt.

Diese Ziele enthalten nach Meinung der WiKo allerdings keines, welches die Datensicherung als solche, d.h. einen Backup in Fällen von Datenverlust, garantieren. Ein solches Datensicherungs-Konzept bestand bereits vor der Durchführung des Security Audits und musste deshalb nicht mehr als Ziel des Security Audits definiert werden: Die Daten werden täglich im 3-Generationen-Prinzip gesichert und die Bänder dezentral in einem Bankschliessfach aufbewahrt.

1.2. Ausgangslage und angewandte Methodik

1.2.1. 14 Server für > 90 Arbeitsplätze

Die WiKo interessierte sich dafür, weshalb 14 Server für die mehr als 90 Arbeitsplätze benötigt werden. Sie erhielt darauf folgende Antworten, welche uns auch als Information für den Einwohnerrat als wichtig erscheinen:

- Durch den Einsatz mehrerer gleicher Server, die als Terminalserver eingesetzt werden, wird eine höhere Ausfallsicherheit erreicht.

- Die Vielfalt der verschiedenen Applikationen erfordert zudem mehrere Rechner (Server), da nicht jede Programmversion mit der gleichen Datenbankplattform, mit gleichen ‚Servicepatches' oder dem gleichen Office-Paket zusammenarbeitet.

- Zwei Server sind reserviert für den Einsatz in der IP-Telephonie (Call-Manager und Voice-Box).

- Alle Server sind miteinander vernetzt. Die IT legt grossen Wert auf die optimale Nutzung der Server-Farm.

1.2.2. IT-Grundschutzhandbuch

Auf Seite 3 des Security Audits wird unter dem Titel ‚Interview' ein IT-Grundschutzhandbuch erwähnt. Es handelt sich hierbei um BS ISO/IEC 17799:2000 und BS 7799-1:2000, welche Standardsicherheitsmassnahmen für typische Systeme, d.h. in vorliegenden Fall die in Allschwil angewandten, empfehlen. Ziel dieser IT-Grundschutz-Empfehlungen ist es, durch geeignete Anwendung von organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmassnahmen ein Sicherheitsniveau zu erreichen, das für den normalen Schutz angemessen und ausreichend ist und als Basis für hochschutzbedürftige IT-Systeme und Anwendungen dient (siehe dazu auch Kapitel 2.1 dieses Berichtes: Einschätzung der Situation).

1.2.3. Notfallkonzept

Auf Seite 4 des Security Audits fehlt der WiKo unter dem Titel ‚Sicherheitsprozess als Planungsinstrument' ein vierter Punkt, nämlich ein Notfallkonzept. Wie auch am Schluss des Kapitel 2 des WiKo-Berichtes erwähnt, gibt es bereits verschiedene Unterlagen, Aufzeichnungen und Richtlinien für den Umgang mit Notfällen. Daraus sollen gemäss Terminplan für die Umsetzung des Security Audits ab Dezember 2003 in einem ‚Notfallkonzept, 1. Teil' alle wichtigen sicherheitsrelevanten Punkte für das jetzige Tagesgeschäft zusammengefasst werden.

1.3. Ergebnisse der Sicherheitsprüfung

Das auf Seite 5 oben (des Security Audits) erwähnte Risiko eines unerwünschten Zugriffs auf Allschwiler-Daten durch die direkte Anbindung des Gemeindenetzes an das kantonale Netz wurde in der Zwischenzeit durch den Einbau einer Firewall bereits eliminiert (Beschluss 1 im Schreiben des Gemeinderates vom 22.8.2003).

Auch die im nächsten Abschnitt angeregten Massnahmen wurden und werden sukzessive in Angriff genommen (siehe auch Kapitel 2.2.2 des WiKo-Berichtes)., wie u.a. auch aus Beschluss 3 im Schreiben des Gemeinderates vom 22.8.2003 hervorgeht.

1.4. Umsetzung der aufgezeigten Massnahmen

Dieses Kapitel (siehe Seite 6 des Security Audits) umfasst ausschliesslich Sofort- und kurzfristige Massnahmen. Die WiKo interessierte sich zusätzlich dafür, ob auch mittelfristige und langfristige Massnahmen ins Auge zu fassen wären. Dazu Markus Rudolf von Rohr:

- Die Informationstechnologien sind sehr schnelllebig. Ein jährlicher Security Check-up zur Kontrolle der bestehenden Security-Policy (Berechtigungen, Sicherheitspolicen) wird angestrebt.

- Mittelfristige personelle Massnahmen sind die Erarbeitung eines Schulungs- und Sensibilisierungskonzeptes sowie von IT-Arbeitsrichtlinien für alle Mitarbeitenden.

- Weitere, langfristige technische Massnahmen wären: Zentraler Authentisierungs-Server, VPN zu den Aussenstellen, Datenverschlüsselung für kritische Daten und Intrusion Detection (Ueberwachung des Netzwerkverkehrs).

Vor allem diese letzt genannten Massnahmen sind mit Kosten verbunden, d.h. das Kosten/Nutzen-Verhältnis wäre von Fall zu Fall genau zu evaluieren.

2. Ergebnisse Sicherheitstests und eingeleitete Massnahmen

2.1. Einschätzung der Situation

Zitat aus dem Brief des Gemeinderates an die WiKo vom 22. August 2003:

- Die Firma Netcloud beurteilt den Sicherheitsstand bei Ablieferung ihres Berichtes als ‚mittelmässig'.

- Mit der Umsetzung der verschiedenen Massnahmen (betrieblich und organisatorisch) kann ein Standard erreicht werden, der als ‚gut' bezeichnet werden kann.

- Die Integration einer Firewall (Prüfinstanz, welche die Zugriffe auf das interne Netzwerk regelt) hebt den Sicherheitslevel markant an.

‚Mittelmässig' in diesem Zusammenhang heisst, dass eine Verbesserung angestrebt werden muss, dass also nicht alle Möglichkeiten voll ausgeschöpft sind; ‚gut' dagegen bedeutet, dass alle zum aktuellen Zeitpunkt organisatorisch und systemtechnischen Möglichkeiten unter Berücksichtigung der in der Gemeinde vorhandenen Mittel ausgeschöpft sind.

Die Kurzfassung des Security-Audits (siehe Kapitel 1 des WiKo-Berichtes) enthält eine Liste direkter und kurzfristig umzusetzender Massnahmen. Sind alle aufgeführten Massnahmen erfolgt, darf der Sicherheitszustand im IT-Umfeld als ‚gut' bezeichnet werden. Damit sind nach Ansicht des Gemeinderates die Sicherheitsanforderungen für die Gemeinde Allschwil erfüllt. Bei der Einführung zusätzlicher Sicherheitseinrichtungen wäre das Kosten/Nutzen-Verhältnis sehr genau abzuwägen (zusätzlicher Personalaufwand!).

2.2. Sicherheitsrisiken

2.2.1. Firewall und Virenschutz

Mit der in Kapitel 2.1. des WiKo-Berichtes erwähnten Integration einer Firewall kann das externe als grösstes aller Sicherheitsrisiken eliminiert werden. Der Gemeinderat hat deshalb beschlossen (Beschluss 1 im Brief vom 22. August 2003), für die Integration einer Firewall den im Rahmen der gemeinderätlichen Finanzkompetenz liegenden Kredit von Fr. 26'000.-- zu Lasten des verbliebenen Restkredites aus dem Projekt NILA zu bewilligen. Dieser Kredit beinhaltet nicht nur die Hardware sondern alle anderen Dienstleistungen wie Ausarbeitung des Firewall-Konzeptes, Vorkonfiguration der Hardware, Installation vor Ort und Anpassungen der bestehenden Netzwerk-Infrastruktur sowie Schulung der Systembetreuer. Die Firewall wurde in der Zwischenzeit durch eine Fremdfirma in die bestehende Infrastruktur integriert; es wurden ebenfalls sicherheitsrelevante Anpassungen der Netzwerkkomponenten und Konfigurationen durchgeführt.

Mit der eingesetzten Firewall werden alle unberechtigten Zugriffe von extern gesperrt. Ausschliesslich bei Applikationen, welcher der Kanton bereitstellt, sind die Zugänge so konfiguriert, dass ein Datenaustausch möglich ist. Direkte Zugänge ins Web (Internet-Homepage) sind nicht vorhanden, vom Kanton nicht erlaubt und zudem über den Kanton resp. den Bund geregelt. Die Datenbank der Allschwiler-Homepage wird bei einer Fremdfirma gehostet, d.h. sie ist auf einem externen Server gelagert und befindet sich somit nicht im Umfeld der Gemeinde-IT.

Da eine Firewall nur ein bedingter Virenschutz ist, werden die verbleibenden Prüfungen durch eine tagesaktuell gehaltene Virenschutz-Software durchgeführt, welche im Hintergrund läuft. Hiezu kommen die Schutzvorrichtungen von Bund und Kanton, was von Bedeutung ist, da der gesamte Mail-Verkehr über diesen Weg abgewickelt wird.

2.2.2. Interne Massnahmen

Die Behebung der anlässlich des Sicherheitstest festgestellten Mängel in der IT-Administration wurden bereits als Jahresziele 2003 / 2004 für den Bereich Informatik definiert. Der Aufbau einer Kontrolle über die durch die Informatik erteilten Benutzerrechte wurde neu organisiert und die daraus resultierenden Arbeitsabläufe definiert. Zudem müssen die Zuständigkeiten innerhalb der Informatik überprüft werden, was besondere Aktualität erhielt durch den Weggang einer der beiden Informatiker der Gemeinde. *Ziel muss dabei die Festlegung klarer Verantwortlichkeiten sein, welche sowohl den Mitarbeitenden als auch den Drittfirmen bekannt sind* (Zitat aus dem Brief des Gemeinderates vom 22.8.2003).

Im weiteren wurden (Zitat des Beschlusses 3 im Brief des Gemeinderates vom 22.8.2003)

die Mitarbeitenden der IT beauftragt, in Zusammenarbeit mit dem Personalwesen und dem Rechtsdienst die erforderlichen Vorarbeiten für die Erarbeitung eines Schulungskonzeptes sowie die Erstellung umfassender IT-Arbeitsrichtlinien an die Hand zu nehmen (Berichterstattung per Ende März 2004).

Dieser Beschluss beinhaltet auch, dass die erwähnten IT-Arbeitsrichtlinien als Teil des Anstellungsvertrages von den Mitarbeitenden zu unterzeichnen sind.

Bis zur Umsetzung dieses Beschlusses müssen die diversen umfassenden, bereits bestehenden Unterlagen, Aufzeichnungen und Richtlinien als Notfall-Konzept (siehe auch Kapitel 1.2) genügen.

3. Würdigung der zwei Berichte im Hinblick auf das weitere Vorgehen

3.1. Würdigung der Berichte (Brief GR vom 22.8.2003 und Kurzfassung Security Audit

Die WiKo stellte mit Genugtuung fest, dass ihre Bedenken hinsichtlich IT-Sicherheit in Allschwil durch

- die Kurzfassung des Security Audits

- den Brief des Gemeinderates vom 22. August 2003

- die ausführliche Beantwortung der Fragen zu den beiden obgenannten Berichten

ernst genommen wurden. Entsprechende Massnahmen sind bereits während der beiden ‚Frage/Antwort-Perioden' zum Leistungsauftrag sowie Leistungsbericht Nr. 193 (Produktgruppe Informationstechnik IT) in Angriff genommen worden.

Wir danken dem Gemeinderat für seine Offenheit und Bereitschaft zur Zusammenarbeit.

3.2. Weiteres Vorgehen

Die WiKo erachtet es als sinnvoll, dass regelmässig solche Security Audits durchgeführt werden, wenn möglich jeweils durch andere Firmen als die jetzt zum Einsatz gekommene Firma Netcloud. Der Gemeinderat hat noch nicht abschliessend über dieses Thema beraten:

- Zitat aus dem Brief vom 22.8.2003: *Ein idealer Zeitintervall wäre alle 2-4 Jahre, je nach dem, in welchem Umfang an der bestehenden Infrastruktur Modifikationen vorgenommen wurden.*

- Auch der Gemeinderat ist der Meinung, dass es sinnvoll wäre, jeweils eine andere Firma zu beauftragen.

- In jedem Fall jedoch spielt auch hier das Kosten-/Nutzen-Verhältnis eine nicht zu vernachlässigende Rolle.

Trotz ihrer beschränkten Kenntnisse auf diesem Spezialgebiet schliesst sich die WiKo diesen Schlussfolgerungen aus dem ersten Security Audit an. Sie wird im übrigen im Rahmen ihrer Controlling-Tätigkeit darüber wachen, dass die aufgeführten Massnahmen auch wirklich wie dargestellt durchgeführt werden.

4. Anträge

Die WiKo beschloss an ihrer Sitzung vom 7. Januar 2004 einstimmig, dem Einwohnerrat folgende Anträge zu stellen:

1. Die WiKo beantragt, dass der Einwohnerrat den vorliegenden Bericht der WiKo zur Kenntnis nimmt.

2. Die WiKo beantragt dem Einwohnerrat, von den bereits durch den Gemeinderat eingeleiteten innerbetrieblichen Massnahmen im technischen und administrativen Bereich und den teilweise erfolgten neuen Aufgabenzuweisungen Kenntnis zu nehmen.

3. Die WiKo beantragt, dass in zwei Jahren, d.h. zu Beginn des Jahres 2006, ein weiterer Security Audit durchgeführt wird.

Für die Wirkungsprüfungskommission:
Verena Meschberger, Co-Präsidentin

Mitglieder der WiKo:

seitens der FiReKo:	seitens der GPK:
Max Amsler	Guido Beretta
Stevie Brügger (entsch.)	Karl Frei (entsch.)
Kurt Kneier (entsch.)	Peter Humbel
Verena Meschberger (Präsidentin)	Alice Märky
Thomas Pfaff	Mathilde Oppliger (Präsidentin)
Robert Richner	Bruno Steiger (entsch.)
Iris Zihlmann (entsch.)	Margaret Wagner (entsch.)