Stadt St.Gallen

Stadtrat

Vorlage an den Grossen Gemeinderat vom 22. Januar 2002 Nr. 1532

Informatik

Errichtung von zwei Firewall-Systemen

1 Ausgangslage

Im Frühjahr 2001 wurde durch einen externen Partner eine umfassende Risikoanalyse über die städtische Informatik-Infrastruktur durchgeführt. Daraus resultierte ein Schwachstellenkatalog, der neben den physischen (baulichen) Schwachstellen auch diejenigen der eingesetzten Serversysteme (inkl. Polizei Einsatzleitsystem (PELIX) der Stadtpolizei), der Remote-Access-Lösung (RAS) sowie der Anbindung an das kantonale Kommunikationsnetzwerk (KOMSG) beinhaltete. Die Analyse zeigte u.a. unmissverständlich auf, dass die Anbindung des städtischen Netzwerkes an das KOMSG und damit an andere Netzwerke der St.Gallischen Gemeinden sowie zum Bundesnetzwerk (KOMBV) ungenügend geschützt ist.

Bei der Installation der IT-Anlagen wurde früher sehr grosses Gewicht auf den Aspekt der „Verfügbarkeit" gelegt. So sind die Hauptserver redundant ausgelegt und entsprechen einem hohen Verfügbarkeitslevel. Doch bezüglich Authentisierung, Integrität von Daten, Autho-risierung wurden Mängel entdeckt. Das städtische Netzwerk ist zudem ein Perimeter-Netzwerk des kantonalen Netzwerkes KOMSG. Auch hier sind keine einschränkenden Massnahmen im Einsatz, welche es z.B einem Angestellten einer anderen, am KOMSG angeschlossenen Gemeinde verunmöglicht hätten, Attacken auf die städtischen Systeme durchzuführen. Umgekehrt sind auch die Server in den am KOMSG angeschlossenen Gemeinden ohne einschränkende Mittel erreichbar.

Auf den städtischen Serversystemen wird heute eine beachtliche Datenmenge verwaltet. Viele dieser Informationen sind potentiell für Aussenstehende interessant und/oder unterliegen direkt oder indirekt dem Datenschutzgesetz. Weiter steht fest, dass ein längerer Ausfall der Systeme zu erheblichen Unterbrüchen in allen Arbeitsprozessen führen würde. Dies nicht zuletzt auch aufgrund der heute umfassend integrierten Informatik.

Weiter hat sich die Flut an schädlichen oder gar gefährlichen Computer-Viren im Jahr 2001 nahezu vervierfacht und auch hier zeichnet sich eine bedenkliche Entwicklung ab. In Fachkreisen besteht die einhellige Meinung, dass mehrere, kombinierte Strategien nötig sind, um ein wirkungsvolles Sicherheitsnetz zu schaffen. Mit der Installation eines Firewall-Systems wird auf jeden Fall eine wichtige Hürde zur Risikoverminderung geschaffen. Die Stadtpolizei betreibt aufgrund der erwähnten Sicherheitslücken für die Einsatzleitzentrale bereits heute ein Firewall-System, um die hochsensiblen Daten dieses Systems effektiv gegen Angreifer zu schützen.

2 Zielsetzungen

Zur Risikoverminderung wurden insbesondere die nachstehenden Ziele festgelegt:

- Sicherstellung des störungsfreien Betriebs der eigenen Anlagen
- Gewährleistung des Datenschutzes gemäss Datenschutzgesetz
- Überwachung des gesamten eingehenden und ausgehenden Datenverkehrs
- Absicherung gegen aktive Angriffe von aussen und innen
- Schaffung der technischen Basis für diverse geplante Projekte
- Das System verfügt über die Protokollierung aller Zugriffe sowie deren Auswertung
- Das System verfügt über ein Intrusion Detection System (IDS) zur Überwachung von Hackerangriffen
- Das System verfügt über ein Content Filtering , womit die Daten, welche übermittelt werden, auf deren Inhalt nach Rubriken (Pornografie, Rassismus etc.) geprüft und deren Übermittlung gesperrt werden kann.
- Das System kann für verschlüsselte Zugriffe auf das Stadtnetz über das Internet mit VPN-Verbindungen ausgebaut werden
- Die Firewall verfügt über einen Virenschutz der neusten Technologie
- Das System darf nicht Microsoft-basierend sein.

3 Lösungsbeschrieb

Der geplante Einsatz der Firewall-Systeme umfasst alle nötigen technischen Aspekte inkl. eines Load-Balancing (ausfallsicheres, redundantes System, welches die Netzwerklast auf zwei Subsysteme verteilt) Die beiden Firewall werden so angelegt und ausgewählt, dass ein eventueller, späterer Ausbau ohne Probleme und ohne nötig werdende Ablösung bestehender Infrastruktur möglich ist. Die Firewall sollen mit den Bedürfnissen wachsen können. Die geplante Lösung sieht wie folgt aus:

- Zwischen beiden Verbindungen zum KOMSG-Netz wird neu je ein Firewall-System eingesetzt.

- Das System wird redundant ausgelegt und an geografisch unterschiedlichen Orten installiert (Rathaus-Serverfarm und Amtshaus), um eine höhere Verfügbarkeit zu gewährleisten
- Die Firewall-Systeme werden durch eine noch zu evaluierende Partnerfirma installiert.
- Das OIA definiert zusammen mit dem externen Partner die Sicherheits-Anforderungen für die Installation solcher Systeme.
- Für die regelmässige Kontrolle, Wartung und Erweiterung der Firewall-Systeme wird ein externer Partner eingesetzt.
- Das OIA lässt zwei Mitarbeiter zur Überwachung der Firewalls ausbilden. Diese Mitarbeiter sollen in der Lage sein, kleinere Wartungsarbeiten durchzuführen, die Einhaltung der Sicherheits-Anforderungen zu garantieren, Angriffe zu erkennen und in diesen Situationen somit angemessen zu reagieren.
- Beide Systeme werden gleichzeitig in Betrieb genommen.

Das OIA definiert entsprechende Grundbedingungen für die Firewall-Systeme. Dazu wird den offerierenden Parteien ein Anforderungskatalog (inkl. Firewall-Anforderungen der IG KOMSG) abgegeben.

Im Hinblick auf die schnellen Entwicklungen in diesem Markt und der in den letzten Jahren erheblich gestiegenen Gefahren im Netzwerk wird die neuste verfügbare Firewall-Technologie eingesetzt. Die Firewall muss ICSA-zertifiziert sein. Die nötige Hardware wird optimal auf die Firewall-Software abgestimmt. Als Betriebsystem soll nicht Microsoft-Windows eingesetzt werden, da Windows nicht die nötige sichere Grundlage für eine professionelle Firewall bietet.

Die Firewall unterstützt die heute gängigen Methoden des Filterings sowie die Möglichkeit einer Rückverfolgung von Angriffen. Es wird kein Firewall-Produkt eingesetzt, welches bei den möglichen Providern für die Zukunft bereits eingesetzt wird. (Kaskadierung ist nur mit unterschiedlichen Produkten sinnvoll). Die Systeme sollen soweit skalier- und ausbaubar sein, dass sie auch den geplanten Umstellungen und Ausbauten der Informatikinfrastruktur Rechnung tragen (z.B.: Providerwechsel, Ablösung RAS, öffentliche Webzonen, Metaframe, CMS, eGov).

Mit diesem Projekt sollen die bestehenden Sicherheitslücken zwischen dem Stadtnetz und dem KOMSG mittels einem Firewall-System der neusten Generation eliminiert werden und für das EZ-LAN der Stapo ein zusätzlicher Schutz geboten werden.

4 Mittelbedarf

Aufgrund vorliegender Offerten ergeben sich folgende Aufwendungen:

4.1 Einmalige Kosten	Fr.
4.1.1 Hardware	
Firewall-Systeme	17’000.--
Fireproof Application-Switches / Cisco Catalyst	86’000.--
Reserve 12 %	12’360.--
MwSt	8'840.--
Zwischentotal inkl. MwSt	124’200.--
4.1.2 Software	
Lizenzkosten für Firewallsoftware (Clusterlizenz)	56’000.--
Reserve 10 %	5'600.--
MwSt	4’700.--
Zwischentotal inkl. MwSt	66’300.--
4.1.3 Installation durch externe Partner	
Engineering / Aufsetzen / Konfigurieren / Testen	45'000.--
Reserve 10 %	4'500.--
MwSt	3'800.--
Inkl. MwSt	53’300.--
4.1.4 Ausbildung	
Schulung zweier OIA-Mitarbeiter	4'000.--
MwSt	300.--
Zwischentotal inkl. MwSt	4'300.--
Total Projektkosten inkl. MwSt	248’100.--

4.2 Wiederkehrende Kosten	
Jährliche Wartungsgebühr	
Wartung durch externen Partner (12 Monate)	33'000.--
Reserve 10 %	3'300.--
MwSt	2’800.--
Total inkl. MwSt	39’100.--

Ein Teil dieser Kosten fällt bereits im Realisierungsjahr an.

5 Terminplan und weiteres Vorgehen

Der Informatiklenkungsausschuss hat am 12. Dezember 2001 dem Lösungskonzept zur Einführung zweier Firewall-Systeme zwischen dem Stadtnetz und dem KOMSG zugestimmt und das Projekt genehmigt. Nach dem Beschluss des Grossen Gemeinderates wird zur Auswahl des Lieferanten ein Einladungsverfahren durchgeführt. Die Realisierung des Projektes bzw. die Einführung der Firewall-Systeme ist im Sommer / Herbst 2002 geplant.

6 Wirtschaftlichkeit und Nutzenüberlegungen

Für die Firewall-Lösung lässt sich nur schwer ein quantifizierbarer Nutzen nachweisen. Die Stadtverwaltung St. Gallen beugt damit System- und Arbeitsausfällen vor, erfüllt die Pflichten und Verantwortungen betreffend Datenschutz und erweitert ihre eigene Hardware-Infrastruktur auf ein zeitgemässes Niveau. Eine Verwaltung dieser Grösse muss zudem die Basis für ein zukünftiges Wachstum im Intranet- sowie Internetbereich in dieser Art schaffen. Bei Nichtrealisation wird ein übermässiges Risiko betreffend Datenschutz und Betriebssicherheit für die Zukunft eingegangen. Im Falle einer tatsächlichen Attacke ist unter Umständen mit sehr langen Ausfallzeiten der städtischen Systeme zu rechnen. Ausserdem ist die Gefahr zu gross, dass sensible Daten in falsche Hände geraten.

7 Finanzierung

Den Betrieben und Spezialfinanzierungen werden die folgenden Anteile belastet:

Stadtwerke sgsw	Fr.	27'000.--
VBSG	Fr.	4'500.--
KVA	Fr.	2'300.--
Feuerwehr	Fr.	4'500.--
Parkierung	Fr.	4'500.--
Entsorgungsamt	Fr.	9'000.--

Der auf die Betriebe mit eigenen Rechnungskreisen entfallende Betrag von Fr. 33'800.-- wird über dort vorhandene Kredite finanziert und kann daher bei der Ermittlung des Kreditbetrages in Abzug gebracht werden.

8 Antrag

Dem Lösungskonzept zur Einführung zweier Firewall-Systeme zwischen dem Stadtnetz und

dem KOMSG im Betrag von Fr. 248'100.– wird zugestimmt und für den auf den allgemeinen Haushalt entfallenden Anteil ein Verpflichtungskredit von Fr. 214‘300.– erteilt.

Der Stadtpräsident:
Christen

Im Namen des Stadtrates
Der Stadtschreiber:
Linke