

# Das Schweizerische Rote Kreuz

Die kostensparenden FortiGate-Appliances schützen die Berner Zentrale und die angeschlossenen Institutionen vor Gefahren aus dem Internet

Fallbeispiel

## Situation

Als nationale Rotkreuzgesellschaft der Schweiz und Teil der weltweiten Rotkreuz- und Rothalbmond-Bewegung, unterstützt das von General Guillaume-Henry Dufour und Bundesrat Jakob Dubs im Jahr 1866 gegründete Schweizerische Rote Kreuz (SRK) weltweit Menschen in Not. Kantonalverbände und Mitgliedsorganisationen wie die Rettungsflugwacht, der Samariterbund, die Lebensrettungsgesellschaft oder der Verein für Katastrophenhunde „Redog“ erhalten Unterstützung von zahlreichen Gönnern, 50.000 Freiwilligen und über 400.000 Mitgliedern. Die Kerntätigkeiten im Inland konzentrieren sich auf Gesundheitswesen, den sozialen und sozialmedizinischen Bereich, die Migration und Integration von Flüchtlingen sowie Erste Hilfe und Rettungswesen. Im Ausland engagiert sich das SRK in der humanitären Hilfe in Kriegs- und Katastrophengebieten, im Wiederaufbau und in der sozialen Entwicklung zur Schaffung menschenwürdiger Lebensbedingungen.

SRK ICT Services bietet seine ICT Dienste allen Rotkreuz-Institutionen (z.B. Samariterbund, Rettungsflugwacht, Schweiz. Lebensrettungsgesellschaft und viele mehr) in der gesamten Schweiz an und fungiert als ASP-Provider. Die Bürostandorte der Institutionen, die das ASP-Angebot des SRK wahrnehmen möchten, werden via Internet mit dem Rechenzentrum in Bern verbunden. Um ein sicheres Arbeiten auf den Terminalservern des SRK gewährleisten zu können, werden die Daten zwischen dem Berner Rechenzentrum und den angeschlossenen Institutionen über einen VPN-Tunnel transportiert.

Das breite Aufgabenspektrum des SRK bringt es mit sich, dass in einigen Abteilungen des Hauptsitzes des SRK in Bern personenbezogene Daten, wie etwa Patientendaten von Kriegsfolteropfern oder Organspendern beziehungsweise den Organempfängern, elektronisch vorgehalten werden. Die Sicherheit dieser Datenbestände wird innerhalb des SRK sehr ernst genommen und der Zugriff auf diese muss 7x24 Stunden gewährleistet sein. Die bisherige Security-Lösung des SRK basierte auf zwei geclusterten Inhouse-Appliances, die von einer externen Firma im Rahmen eines Outsourcing-Vertrages betreut wurden. Die Nachteile dieses Verfahrens machten sich mit der Zeit immer störender bemerkbar: Für jede kleinste Konfigurationsänderung musste bei der betreuenden Firma ein schriftlicher Änderungsantrag gestellt werden; darüber hinaus wurden die gewünschten Changes oft mit Verzögerung implementiert. Schlimmer noch: Die alte Lösung war nicht zuverlässig – es gab mehrere markante Hardware-Ausfälle zu verzeichnen. Beim SRK entstand zudem der Eindruck, dass das Produkt nicht mehr aktiv weiter entwickelt wurde. So verfügte die Lösung beispielsweise nicht über eines der doch immer wichtiger werdenden Intrusion-Prevention-Systeme. Auch waren keine Auswertungsmöglichkeiten über die Firewall-Aktivitäten vorgesehen, das SRK erhielt lediglich einmal pro Monat ein einfaches Reporting über die momentan aktuellen Gefahren (Viruswarnungen) und über das von der Firewall geprüfte Verkehrsvolumen in Megabytes.

## Lösung

All das führte schließlich dazu, dass man sich beim SRK dafür entschied, den Betrieb der Firewall nicht länger in fremde Hände zu geben, sondern vielmehr eine Inhouse-Lösung zu suchen. Dabei waren Aspekte wie Hochverfügbarkeit, Markenbekanntheit des Produkts und gute Referenzen wichtige Auswahlkriterien. Zudem musste das neue System einfach in der Handhabung sein und kostengünstig im Unterhalt.

Das SRK machte sich auf die Suche. Zunächst verschafften sich die Verantwortlichen in einer ersten Sondierungsphase durch das intensive Studium von Fachliteratur einen umfassenden Überblick. Ebenso wurden die Erfahrungsberichte anderer Anwender und Whitepapers mit ins Kalkül gezogen. Der langjähriger Netzwerk-Implementierungspartner des SRK, die Netlan AG in Belp brachte schließlich Fortinet ins Spiel und berichtete von erfolgreichen Implementierungen bei anderen Kunden. Darauf verglich man beim SRK die Ergebnisse der eigenen Recherchen mit den von Netlan gelieferten Daten sowie den technischen Daten von Fortinet.

Das Vertrauen in eine sichere ICT-Infrastruktur ist dem SRK so wichtig, dass es bis auf die Anwenderebene bei den Mitarbeitern gewährleistet sein muss. Hier spielte der Einsatz einer Firewall eine zentrale Rolle. Darüber hinaus sollte sich die Lösung nahtlos in die bestehende Infrastruktur einbinden lassen und alle Sicherheitsbedürfnisse des Perimeterschutzes vollumfänglich abdecken. Die Lösung sollte auch über genügend Performancereserven verfügen, damit nach der Beschaffung auch der Investitionsschutz für einige Jahre gesichert bleibt. „Als Non-Profit-Organisation sind wir ganz besonders darauf angewiesen, unsere Hilfsmittel kostengünstig zu beschaffen und zu betreiben“, erklärt Benno Stucki.

In den beiden Rechenzentren in Bern setzt das SRK nun zwei größere FortiGate Appliances im HA-Modus (High Availability) mit einem FortiAnalyzer ein. Für den Remote-Zugriff setzen die Systemadministratoren auf ihren Notebooks und PCs FortiClient ein. Kleinere Außenstellen, die von dem ASP-Angebot der Berner Zentrale Gebrauch machen möchten, können ebenfalls mit Fortinet-Appliances ans Internet angeschlossen werden.

## Erfolg

In Bern ist man sehr zufrieden. Das Produkt besticht durch einfache Konfigurier- und Wartbarkeit und ist vom Userinterface verständlich aufgebaut. „Die Administratoren schätzen es außerordentlich, dass das Webinterface für jeden Firewall-Typ (kleine oder große Firewall) immer gleich aufgebaut ist“, führt Benno Stucki aus. „Dies reduziert den Trainingsaufwand und verhindert Konfigurationsfehler weitgehend. Erstaunlich ist auch, dass die Spam-Erkennung recht gut ist, obwohl Fortinet klar zum Ausdruck bringt, dass die integrierte Spam-Erkennung nicht als vollwertiges Werkzeug gedacht ist und nebenher nach wie vor eine separate Spam-Appliance, die FortiMail, eingesetzt werden sollte. Last but not least ermöglicht der FortiAnalyzer dem IT-Verantwortlichen, die immer umfassender werdenden Compliance-Erfordernisse auf einfache Art und Weise nachzuweisen.“

„Sicherheit kann nicht monetär quantifiziert werden. Erst wenn ein Schaden entstehen würde, wäre die Rechnung gewissermaßen interessant, der Schaden hingegen könnte katastrophal sein – man denke nur an den Image- und Vertrauensverlust ins SRK“, resümiert Benno Stucki. „Verglichen mit der alten, ausgelagerten Lösung sparen wir mit Fortinet auf alle Fälle jährlich ungefähr 40 % wiederkehrende Kosten.“

## Fortinet

### Über Fortinet Inc.

Fortinet ist einer der führenden Anbieter von ASIC-beschleunigten Multi-Threat-Sicherheitssystemen, die in Unternehmen und bei Service-Providern genutzt werden, um den Sicherheits-Level zu erhöhen und gleichzeitig die Betriebskosten zu senken. Die Lösungen von Fortinet sind von Grund auf dafür konzipiert, mehrere Level von Schutz- und Sicherheitsanwendungen zu kombinieren – beginnend mit Firewall, Antivirus, Intrusion Prevention, VPN, Schutz vor Spyware bis hin zu umfassenden Antispam-Lösungen. Die Kunden können sich damit vor den verschiedenen bekannten Bedrohungen sowie vor verborgenen Angriffen schützen. Durch die Verwendung eines kundenspezifischen ASIC und einer einheitlichen Schnittstelle bieten die Lösungen von Fortinet herausragende Sicherheitsfunktionen, die vom Schutz dezentraler Niederlassungen bis hin zu Hardware-Lösungen mit integrierten Management- und Protokollfunktionen. Die Lösungen von Fortinet wurden weltweit mit verschiedenen Awards ausgezeichnet und sind die einzigen Sicherheitsprodukte, die bereits sechs mal durch die ICSA in den Kategorien Firewall, Antivirus, IPSec, SSL, IPS und Antispyware ausgezeichnet wurden. Fortinet ist in privater Hand und hat seinen Hauptsitz in Sunnyvale, Kalifornien. Weitere Informationen über Fortinet finden Sie unter [www.fortinet.com](http://www.fortinet.com)

CAS172