TRISEC
YOUR WAY INTO SECURITY

SUCCESS STORY

Zentral administrierter Virenschutz und Desktop Security

Der Kunde

Main-Kinzig-Kliniken gGmbH
Gelnhausen Schlüchtern Bad Soden-Salmünster

Die Main-Kinzig-Kliniken sind im Jahr 1997 aus dem Eigenbetrieb der drei Kreiskrankenhäuser mit Standorten in Gelnhausen, Schlüchtern und Bad Soden-Salmünster in der Rechtsform einer gemeinnützigen GmbH entstanden.

Alleiniger Eigentümer ist der Main-Kinzig-Kreis. Heute bieten sie als eine Klinik an drei Standorten auf allen Gebieten der Grund- und Regelversorgung stationäre und ambulante Behandlungen an.

Die Main-Kinzig-Klinken behandeln in 12 Fachrichtungen und bieten, auf die drei Standorte verteilt, 689 Betten.

Sie sind Träger einer Schule für Pflegeberufe und nehmen als akademisches Lehrkrankenhaus an der studentischen Ausbildung in der Medizin und in den Pflegewissenschaften teil.

Als gemeinnütziges Unternehmen sind sie einer der größten Arbeitgeber der Region.

Gelnhausen

Schlüchtern

Bad Soden-Salmünster

Die Anforderungen

Aufgrund der drastisch gestiegenen Viren-Vorfälle im Jahr 2003 und der Aussicht auf einen weiteren Anstieg in 2004, sollte die Sicherheit an allen 3 Standorten durch eine Anti-Virus-Lösung für die ca. 380 Workstations und 20 Server zusätzlich zur bereits implementierten Firewall erhöht werden.

Da sich Viren, Würmer und Backdoor- Programme hauptsächlich über Anhänge in Emails verbreiten, sollte zusätzlich zum internen Schutz der Email-Verkehr an allen möglichen Schnittstellen auf schadhaften Code überprüft und - bei positivem Ergebnis - automatisch von diesem befreit werden können.

Folgende Anforderungen wurden zusammen mit den Anti-Virus-Experten der TriSec GmbH erstellt:

- zentrale Verwaltung und Distribution der Software-Lösung
- Zugriff auf die Administrationsoberfläche von unterschiedlichen Arbeitsplätzen
- automatisches und zentrales Viren-Signaturen Update
- zentrales Email-Scanning, zusätzlich auf den einzelnen Workstations lokal (ein- und ausgehend)
- Berücksichtigung von PCs mit geringer Rechenleistung oder veralteten Betriebssystemen
- Verwendung unterschiedlicher Regelwerke nach Abteilungen gruppiert
- lokalen Benutzern soll ausschließlich das Starten eines manuellen Scan-Prozesses möglich sein
- zentrales Alerting und Reporting aller Workstations und Server

TRISEC
YOUR WAY INTO SECURITY

SUCCESS STORY

Zentral administrierter Virenschutz und Desktop Security

Die Softwarelösung

Aufgrund der umfangreichen Anforderungen an eine entsprechende Software, einer zukünftig verstärkten Ausrichtung auf Applikationen aus dem Open-Source-Segment und den in großem Umfang benötigten Management-Funktionen, fiel die Wahl sehr schnell auf den Hersteller F-Secure und dessen Produkt Anti Virus Total Suite.

F-SECURE
BE SURE.

Diese Suite beinhaltet, neben der derzeit am Markt funktionsreichsten Software Anti Virus Client Security und der Administrations-Oberfläche F-Secure Policy Manager, weitere Versionen für den Schutz von (Email-) Server-Farmen (Windows/Linux), Linux-Gateways, Microsoft Exchange und MIMEsweeper.

Ebenfalls enthalten ist der Internet Gatekeeper, welcher den HTTP- und SMTP-Datenstrom scannt, Dateien anhand von Größe und Art, sowie den Besuch unerwünschter Webseiten zum Erhalten der Produktivität blockiert.

Das Management

Da alle 3 Standorte der Main-Kinzig-Kliniken über performante Standleitungen direkt miteinander verbunden sind, es keine mobilen Mitarbeiter oder Home-Offices anzubinden galt, platzierte die TriSec GmbH den Server für das zentrale Management innerhalb der bestehenden LAN-Struktur.

Der hauptsächlich für das Verteilen und Konfigurieren der unterschiedlichen Softwareversionen zuständige Server ist zentraler Knotenpunkt der gesamten Anti-Virus Lösung. Er verwaltet das Regelwerk aller in das Management eingepflegten Systeme und stellt täglich aktuelle Viren-Signaturen bereit, welche er automatisch von den Servern des Herstellers updatet.

Die F-Secure Software auf den einzelnen Workstations / Servern im LAN und/oder der DMZ verbindet sich in frei konfigurierbaren Zeitintervallen zum Management Server und übernimmt etwaige Änderungen am Regelwerk in Echtzeit.

Bei Funktionsstörungen oder Viren-Befall /-Verdacht werden Alarmierungen an selbigen übermittelt (auch per Email an zuständige Personen möglich) und können dort über die grafische Administrations-Oberfläche eingesehen werden. Diese wurde auf mehreren Systemen installiert um auch von unterschiedlichen Arbeitsstationen im LAN die Lösung administrieren zu können.

Warum F-Secure ?

„Aufgrund langjähriger Erfahrungen mit unserem Partner F-Secure und dem, mit keinem anderen Hersteller am Markt vergleichbaren, Umfang an Funktionalitäten und Reporting-Optionen, fiel unsere Wahl sehr schnell auf F-Secure“.

M.Soukup
Security Consultant der TriSec GmbH

Keine Viren in Emails

Um den Email-Verkehr am Gateway abfangen und auf schadhaften Code überprüfen zu können, wurde der F-Secure Gatekeeper direkt auf dem Mailserver des Kunden platziert. Dieser greift den SMTP-Datenstrom vor der Weiterleitung an den internen Mailserver ab und leitet diesen an den Content Scanner Server weiter. Dort werden ein-, sowie ausgehende Email-Anhänge gescannt, die Email mit einem frei konfigurierbaren Header versehen und wieder an den Gatekeeper zurückgegeben. Bei positivem Scan-Ergebnis werden infizierte Dateien unter Quarantäne gestellt und der Administrator (und/oder Email-Absender / -Empfänger) über den gefundenen Virus informiert.

SUCCESS STORY

Zentral administrierter Virenschutz und Desktop Security

Um den Versand von Email-Anhängen auf die im Unternehmen wichtigen Daten zu beschränken, wurde der Gatekeeper so konfiguriert, dass unerwünschte Anhänge, wie Video-, Bild- oder Audio-Dateien, direkt geblockt werden. Darüber hinaus wurde eine Beschränkung auf die Größe der Anhänge vorgenommen, um die Auslastung der Standleitungen gering zu halten.

Keine Viren auf den Servern

Für den Viren-Schutz auf allen Servern wurde die Software F-Secure Anti-Virus für Server installiert. Diese stellt sicher, dass Benutzer, die mit einem infizierten Rechner eine Verbindung zu Unternehmens-Servern aufbauen, keine Viren an andere Teilnehmer im Netzwerk weitergeben können.

Keine Viren auf den Workstations

Alle Workstations der 3 Standorte wurden zentral gesteuert mit der Software Anti-Virus Client Security ferninstalliert und mit einem Basis-Regelwerk versehen. Dieses wurde später anhand der Standorte, Gebäude, Abteilungen und Leistungsgrenzen der Systeme untergliedert. Die Software enthält:

- → 3 parallel arbeitende Scan-Engines
- → Echtzeit-Virenschutz
- → automatisches Signaturen-Update
- → Email-Scanning (ein- / ausgehend)
- → Desktop-Firewall
- → Anwendungssteuerung

Nicht vom Administrator freigegebene Applikationen, die eine Internetverbindung aufzubauen versuchen, werden solange blockiert (an den Management Server gemeldet), bis eine Freigabe durch den Administrator erfolgt. Entsprechend frei zu formulierende Meldungen werden anhand eines Pop-Up-Fensters an den Clients lokal angezeigt und informieren den Benutzer warum eine Verbindung unterbunden wird.

Um sich grundlegend einen Überblick über solche Applikationen verschaffen zu können, wurden in einer Test-Phase alle Verbindungen blockiert und anhand des Reportings am Management Server entschieden, welche Applikationen eine Verbindung ins Internet aufbauen können, welche nicht und ob dies generell oder innerhalb bestimmter Zeiten geschehen darf.

Kundenzitat

„Eine solche Funktion ist genau das, wonach ich gesucht habe“, erzählt EDV- Administrator B. Bischof. *„Sogar anhand der unterschiedlichen Softwareversionen können Reglementierungen vorgenommen werden.“*

Umgesetzt durch

TriSec GmbH – Your Way Into Security
Senefelderstr. 1 / T1
D – 63100 Rodgau

Tel.: +49 (0) 6106 - 7079 – 180
Fax.: +49 (0) 6106 – 7079 – 189
http://www.trisec.de
eMail : info@trisec.de

Ansprechpartner
Main-Kinzig-Kliniken gGmbH

B.Bischof