Versicherung gegen unliebsame Zwischenfälle in der IT-Sicherheit

SecuSurf gewährleistet einen ungehinderten Internetzugang bei hoher Sicherheit.

„Gerade als akademisches Lehrkrankenhaus müssen wir dem Wunsch der Anwender nach ungehindertem Internetzugang Rechnung tragen. Schließlich gehören zum wissenschaftlichen Arbeiten weltweite Recherchen, Studienvergleiche und Kommunikation mit Kollegen. Auf der anderen Seite entstehen im WorldWideWeb ständig neue Mechanismen, die Unternehmen schaden." So beschreibt Ralf Plomann, IT-Leiter des St.-Marien-Hospitals Lünen, die Zwickmühle, in der er sich befindet. Er fühlt sich oft als Hase der dem Igel hinterherläuft und nicht wirklich gewinnen kann. „Sicherheitspatches der Softwarehersteller sind oftmals nicht schnell genug verfügbar und wir können sie nicht im Arbeitsalltag testen, um Inkompatibilität zu bestehenden Lösungen auszuschließen." Firewalls bieten lediglich Support-Sicherheit, Antivirenprogramme reagieren nur auf bekannte Viren und Trojaner. Was also tun, um sich gegen Sicherheitslücken zu wappnen und den Mitarbeitern einen sicheren und einfachen Zugang zum weltweiten Datennetz zu ermöglichen? „Wir haben uns nach einer Lösung umgeschaut, die verhindert, dass Mitarbeiter Programmcodes ausführen, die nicht von der IT freigegeben wurden", erläutert Plomann seinen Ansatz. In diesem Zuge ist das St.-Marien-Hospital auf SecuSurf gestoßen und hat sehr schnell festgestellt, dass die Software viele Probleme lösen hilft. Mittlerweile werden so in beiden Häuser der St. Rochus GmbH etwa 650 Rechner geschützt – Tendenz steigend. 2011 soll die Lösung klinikweit im Einsatz sein.

Einfache Konfiguration einer White List

„Aufgrund der Leistungsfähigkeit des Produktes kann ich vielen Problemen sehr gelassen entgegensehen, die Kollegen in anderen Häusern Kopfzerbrechen bereiten", sagt der IT-Leiter. Die IT-Security-Suite SecuSurf stellt technisch sicher, dass ausschließlich Software installiert oder ausgeführt werden kann, die vorher auf einer zentralen Positivliste, der sogenannten White List, als vertrauenswürdig eingestuft wurde. Das bedeutet im Umkehrschluss: Jede Software, die nicht erfasst ist, kann nicht ausgeführt werden. So lassen sich alle Computer zu dem machen, was sie eigentlich sind: Arbeitsgeräte mit nur der Software, die für die Arbeit notwendig sind. Und die Sicherheit geht über den reinen PC hinaus. Genauso können USB-Geräte und alle Wechseldatenträger verwaltet werden. Auch hier gilt: Was nicht bekannt und erlaubt ist, kann auch nicht verwendet werden.

„Bei einer White List denken viele, dass ein enormer Arbeitsaufwand hinter der Er-

stellung steckt. Das wäre auch so, wenn in SecuSurf nicht clevere Mechanismen eingebaut wären, die den gesamten Aufwand sehr überschaubar machen. Das ist genau der Clou dieser Sicherheitslösung“, stellt Plomann begeistert heraus. Bei tausenden von exe-Dateien pro Rechner wäre es sehr aufwändig, die komplette White List manuell freizuschalten. Daher bietet SecuSurf bei der Erstkonfiguration des Systems einen „Learning-Mode“. „Dazu haben wir einen definitiv sicheren und sauberen Rechner ausgewählt, der auf dem aktuellen Softwarestand war und über einen Internetzugang sowie USB-Devices verfügte. Dieser Musterrechner wurde mit seiner kompletten Konfiguration in die Positivliste importiert”, beschreibt Plomann das Vorgehen.

Im Anschluss wird der Lernmodus zentral aktiviert und die SecuSurf Client/Agent-Software mit der V erteilsoftware von SecuLution an alle Netzwerkrechner ausgerollt. Nun arbeiten die Anwender etwa einen Monat ganz normal mit ihren Programmen. So wird jegliche zusätzliche Software, die nicht auf dem Musterrechner vorhanden war, erfasst und automatisch in die zentrale Freigabekonfiguration übernommen. Während der Lernphase ist der Nutzer nicht eingeschränkt. Nach Ablauf des Monats schaut der Systemadministrator sich die Liste der durch den Lernmodus hinzugefügten Programme an und kann dann gegebenenfalls unerwünschte oder nicht der Arbeit dienliche Programme entfernen. Hier wartet oftmals die erste Überraschung, wenn der Administrator sieht, was die Benutzer alles an nicht der Arbeit dienlichen Software auf ihrem Rechner verwenden.

Ralf Plomann, IT-Leiter Krankenhausverband St. Rochus GmbH

SecuSurf löst Versprechen ein

„Uns hat bei SecuSurf besonders die ausgesprochen hohe Funktionstiefe überzeugt. So können beispielsweise einzelne Versionen von Ausführungsdateien geblockt werden, wozu vergleichbare Programme nicht in der Lage sind. Dazu ist SecuLution ein inhabergeführtes mittelständisches Unternehmen mit sehr hohem Know-how und großer Kundennähe. Das hat sich in intensiven persönlichen Gesprächen und Präsentationen gezeigt”, erläutert Plomann die Gründe für die Zusammenarbeit. Nicht zuletzt hat auch ein überzeugendes Preis-Leistungs-Verhältnis die Entscheidung maßgeblich unterstützt. So kann selbst die ans Hospital angegliederte Krankenpflege-Schule mit einem eher bescheidenen IT-Budget die Lösung einsetzen.

Nichtsdestotrotz war der IT-Leiter vor der Einführung in Bezug auf die Sicherheit und den Administrationsaufwand sehr skeptisch. „Wir mussten erst die Anwender und Administratoren von der Sinnhaftigkeit des Projektes und der Lösung überzeugen. Dabei galt es primär, die Angst vor einem zusätzlichen Arbeitsaufwand zu nehmen und die Vorteile der Lösung für die tägliche Routine zu kommunizieren“, erläutert der IT-Leiter. Das Projekt startete deshalb auch mit einer kleinen Installation. Dort hat SecuSurf dann aber sehr schnell überzeugt und wurde schrittweise ausgerollt. „Mittlerweile genießt die Lösung eine sehr hohe Akzeptanz und alle Administratoren sind von ihr überzeugt.“

Einfache Konfiguration und schneller Rollout

Wie aber genau arbeitet SecuSurf eigentlich? Nach Ablauf der Lernphase hat das System ein Inventar jeglicher Software angelegt, die im Netzwerk eingesetzt wird. Diesen Status quo kann der Administrator nun beliebig bearbeiten oder einfach „einfrieren“. SecuSurf ist ein Client-Server-System. Dabei werden die Systemserver mit dem Netzwerk verbunden und der Client auf jedem zu sichernden Host installiert. Auf den Servern kann so zentral für alle Systeme festgelegt werden, welche Programme benutzt werden dürfen.

Jeder Angriff auf ein Netzwerk setzt voraus, dass ein entsprechendes Programm auf einem Rechner gestartet wird. SecuSurf identifiziert jedes Programm, das auf dem Host ausgeführt werden soll, anhand eines elektronischen Fingerabdrucks – und zwar unmittelbar vor der Ausführung. Auf den SecuSurf-Servern kann mit der Administrationskonsole, dem Admin-Wizard, zentral festgelegt werden, welche Programme auf

Das St.-Marien-Hospital Lünen

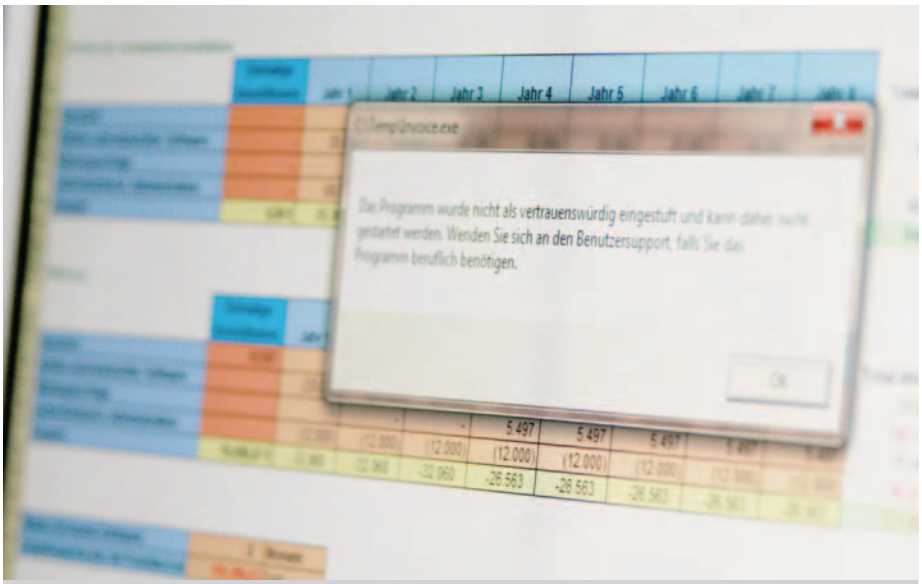
ist mit 590 Betten eines der größten katholischen Krankenhäuser im Ruhrgebiet und Münsterland. Von insgesamt 16 Fachabteilungen werden im Schwerpunktklinikum mit Anteilen der Maximalversorgung jährlich 20.000 stationäre und fast 40.000 ambulante Patienten versorgt.

Das Akademische Lehrkrankenhaus der Westfälischen Wilhelms-Universität Münster bildet mit dem St. Christophorus-Krankenhaus Werne (216 Betten, 9.000 stationäre und 12.000 ambulante Patienten pro Jahr) den Krankenhausverbund St. Rochus GmbH.

SecuLution

SecuLution ist der führende Anbieter von proaktiven Sicherheitslösungen für Unternehmensnetzwerke. Die selbst entwickelte und international patentierte Lösung SecuSurf schützt Netzwerke auf revolutionär neue Weise gegen jegliche Angriffsformen. Neben Schulungen und Beratungsdienstleistungen zum Thema Sicherheit erstellt SecuLution auch anerkannte Gutachten zu bestehenden Netzwerk- und Sicherheitsstrukturen oder analysiert und dokumentiert Angriffe.

Im Zentrum der Unternehmensphilosophie stehen die Sicherheit und die Zufriedenheit der Kunden. Konsequent und kompetent unterstützen die Mitarbeiter diese bei der Konzeption und Implementierung von Sicherheit – ohne dabei die Wirtschaftlichkeit aus den Augen zu verlieren. Sicherheit wird als ein Mittel zur Steigerung der Produktivität von Systemen bei gleichzeitiger Senkung der Betriebskosten verstanden. Hierauf sind sowohl die Produkte als auch Dienstleistungen ausgerichtet.



SecuSurf gewährleistet einen ungehinderten Internetzugang bei hoher Sicherheit.

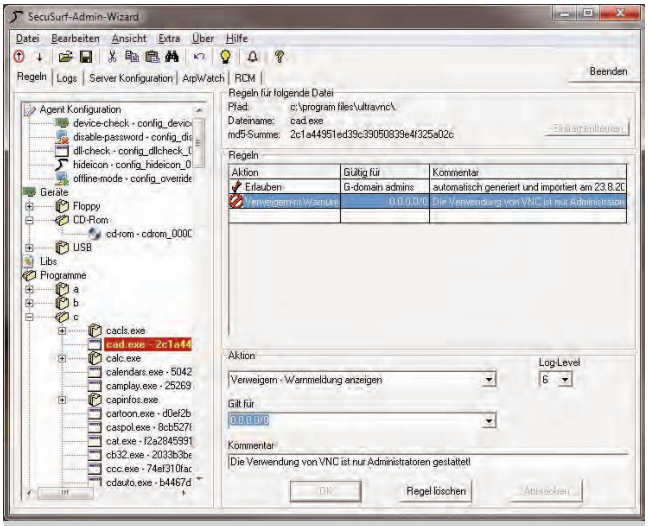
welchem Rechner von wem gestartet werden dürfen. Versucht nun ein Anwender ein nicht autorisiertes Programm zu starten, löst dies schon vor der Ausführung einen Alarm in SecuSurf aus und das Programm wird blockiert. „Wir können individuell festlegen, wie sich ein Rechner verhalten soll, an dem eine ungewollte Aktion ausgeführt wird“, erläutert Plomann. „In der Regel wird die Ausführung des Programms verhindert, dem Benutzer ein definierter Warnhinweis eingeblendet und an den IT-Support verwiesen. Es sind aber auch andere Aktionen möglich, bis zum erzwungenen sofortigen Herunterfahren des Rechners.“ Da die Ausführung nicht explizit autorisierter Codes technisch nicht möglich ist, wird ein außerordentlich hohes Maß an Sicherheit gewährleistet.

Meldet ein User eine Anwendung neu, die er nutzen möchte, ist die Aufnahme in die White List und damit die Autorisierung mit einem Mausklick in der zentralen Management-Konsole erledigt. Der Anwender kann sie ohne Zeitverzögerung sofort verwenden. Der Administrator hat vielfältige Möglichkeiten, das Regelwerk anzupassen. Die Installation von neuer Software bringt genauso wie das Updaten von bestehender Software die Veränderung der Checksummen mit sich und erfordert daher eine Anpassung des Regelsatzes. Doch dies ist ohne zusätzlichen Aufwand erledigt: Es reicht, wenn der Administrator die Installation auf einem beliebigen Rechner unter einem Benutzeraccount durchführt, der vorab als ständiger Lernbenutzer definiert wurde. Die neue Software kann ohne weitere Anpassungen sofort auf allen anderen Rechnern im Netzwerk installiert werden. Auch Windows-Updates werden vollautomatisch integriert, so dass hier keine manuellen Interaktionen nötig sind. Während des normalen Betriebs entsteht kein zusätzlicher Administrationsaufwand.

Hohe Sicherheit zu geringen Kosten

„In meinen Augen ist SecuSurf das Beruhigungsmittel für Administratoren. Ich bin wirklich froh, mit dem System arbeiten zu können. Es erspart mir eine Menge Aufwand und schafft Zeit für andere Tätigkeiten“, bringt IT-Leiter Plomann seine Erfahrungen der vergangenen fünf Jahre auf den Punkt. Da die Anwender in der Klinik ihre Systeme nicht mehr durch das Starten unerwünschter Software schwächen können, sinkt vor allem der Aufwand im Bereich des First- und Second-Level-Usersupports beträchtlich. Die Systeme werden langfristig stabiler, was sich sowohl bei den Kosten für die Administration als auch durch eine höhere Produktivität positiv auswirkt. Darüber hinaus sinken die Kosten für die sicherheitstechnische Administration merklich. Es entfällt jegliche Suche nach erfolgreichen Angriffen oder Virenbefall, es sind keine Audits des Netzwerkverkehrs oder Logfiles aus IDS-Protokollen notwendig. „Und selbst wenn der Server einmal ausfällt, arbeitet SecuSurf sicher weiter, da einmal autorisierte Programme lokal auf jedem PC gecached werden, sodass auch mobile Geräte, die keine stetige Verbindung zum internen Netz haben, gesichert werden können“, ergänzt Plomann.

Nicht zuletzt unterstützt die Software die IT-Abteilung auch bei der Konsolidierung der Anwendungslandschaft. Anhand von dedizierten Auswertungen kann sehr schnell festgestellt werden, welche Programme eigentlich nicht mehr benötigt und deshalb von den Servern gelöscht werden können.



Mit wenig Aufwand können neue Anwendungen gesperrt oder freigeschaltet werden.

„Der Wert der Investition für eine Sicherheitssoftware in der IT bemisst sich nach der Zahl nicht eingetretener unliebsamer Zwischenfälle – und wir hatten noch nie einen“, so Plomann abschließend.

Anbieter

SecuLution GmbH
Alter Hellweg 6 b
59457 Werl
Tel.: 02922 958921-0
Fax.: 02922 958921-9
E-Mail: info@4ss.de
http://www.4ss.de

Referenzgeber

Krankenhausverbund St. Rochus GmbH
Ralf Plomann
IT-Leiter
Altstadtstraße 23
44534 Lünen
Telefon (02 3 06) 77-21 70
E-Mail: plomann.ralf@klinikum-luenen.de