UNTERNEHMENS-GEHEIMNISSE SCHÜTZEN

Nicht nur Virenscanner, Firewalls und Netzwerkkontrollen sind für den schwäbischen Maschinenbauer SFB wichtig, sondern auch der Schutz von Kundendaten und Firmengeheimnissen.

Der Name „SFB Schwäbische Formdrehteile GmbH & Co. KG" verrät es bereits: Mitten im beschaulichen Schwaben zwischen Ulm und Memmingen produziert das Familienunternehmen nun seit über 70 Jahren Präzisionsteile und Baugruppen für die Automobil-, Luftfahrt-, Maschinenbau- sowie Lebensmittel- und Medizinbranche.

Mit über 350 Mitarbeitern gehört SFB damit zu den größten Arbeitgebern in der Region, wobei sich der Kundenkreis keineswegs nur auf Schwaben, Bayern oder Deutschland beschränkt. „Kunden aus aller Welt, wie zum Beispiel aus Dubai oder China, vertrauen auf unsere schwäbische Gründlichkeit und Präzision", verrät der verantwortliche IT-Leiter Michael Geller.

Um diesem Vertrauen immer wieder gerecht zu werden, muss auch die gesamte Technik im Werk und der Verwaltung aktuellsten Sicherheitsanforderungen genügen. „Das macht selbstverständlich auch vor unserer IT keinen Halt", erklärt der IT-Mitarbeiter Jürgen Keller. Er betont ganz ausdrücklich: „Datensicherheit endet bei SFB nicht bei der Einlasskontrolle am Tor. Unsere Kunden vertrauen uns oft streng geheime Entwicklungspläne an. Da darf es nicht passieren, dass ein Dokument das Werk unbemerkt verlässt oder durch einen eingeschleppten Virus zerstört wird."

Der Zeit voraus

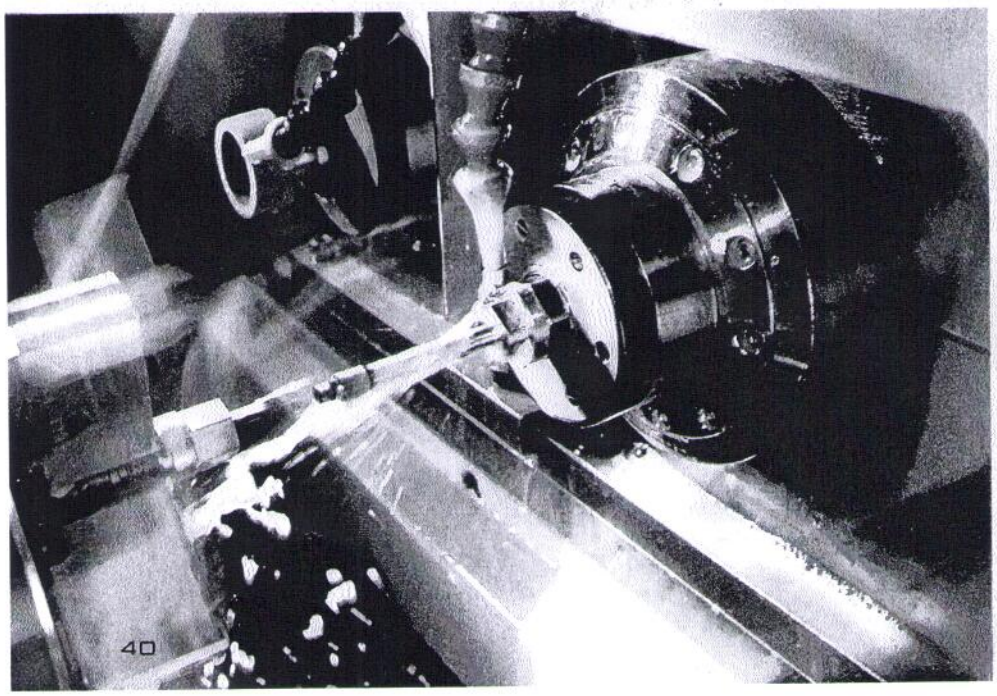
SFB hat deshalb schon vor einigen Jahren erkannt, dass neben Virenscannern, Firewalls, Spamschutz und Netzwerkkontrollen noch andere Maßnahmen ergriffen werden müssen, um neben vertraulichen Kundendaten auch die eigenen Unternehmensgeheimnisse zu schützen. „Bei unseren Mitarbeitern war es bis vor einigen Jahren völlig normal, sich seinen USB-Stick mitzubringen und diesen an den eigenen PC im Werk oder im Büro anzuschließen. Mit der steten Zunahme dieser kleinen Speichergeräte wurde uns schnell klar, dass wir etwas tun mussten. Es ging dabei weniger um die Angst, dass Mitarbeiter Kundenpläne oder Ähnliches unbemerkt entwenden, sondern vielmehr darum, dass sie mit ihrem privaten USB-Stick keinen Virus in unser Netzwerk einschleppen", betont Jürgen Keller.

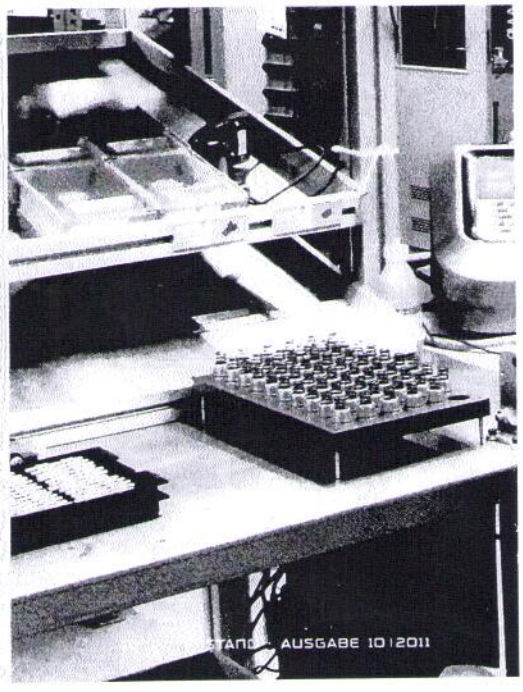
Auf der Suche nach einer geeigneten Software zur Kontrolle dieser anfälligen Hardwareschnittstellen wurde man schnell fündig. Die Lösung „Security.Desk" der Nürnberger Firma FCS Fair Computer Systems wurde eingeführt. Anfangs stießen die beiden IT-Fachleute auf wenig Verständnis bei den Kollegen. Denn bisher unbekümmert eingesetzte private USB-Sticks, Kameras oder andere Speichermedien konnten nicht mehr ohne vorherige Erlaubnis am Firmen-PC genutzt werden. „In einigen Gesprächen mit unseren Kollegen konnten wir aber relativ zügig Verständnis erwirken. Die Argumentation, dass es uns nicht um Kontrolle, sondern um Schutz für unser Unternehmen geht, haben die meisten doch schnell verstanden", erinnert sich Jürgen Keller.

Livebetrieb ohne Probleme

Security.Desk läuft nunmehr seit fünf Jahren, in der vierten Version – und das völlig problemlos. „Eine schnelle Einführung und eine einfache Handhabung im Livebetrieb mit möglichst wenig Administrationsaufwand war einer unserer größten Wünsche", erinnert sich der IT-Leiter Michael Geller. „Wir sind eine kleine IT-Abteilung, da können wir es uns nicht leisten, stundenlangen Administrationsaufwand für eine einzige Lösung zu betreiben", ergänzt sein Mitar-

SFB Schwäbische Formdrehteile GmbH & Co. KG Babenhausen
Branche: Maschinenbau
Mitarbeiter: 350
Sitz: Babenhausen
Gründung: 1941
www.sfb-vab.de





beiter Jürgen Keller. So kam vor allem Jürgen Keller, der bei SFB für die Lösung zuständig ist, der intuitive Aufbau von Security.Desk entgegen. Die zentrale Konsole, auf einem Server installiert, ermöglicht es, individuelle Sicherheitsrichtlinien für die Verwendung aller Hardwareschnittstellen zu definieren. Ein Security Service auf jedem einzelnen Rechner übernimmt schließlich die Überwachung und Einhaltung dieser Regeln. Verstöße und jegliche Steckaktionen werden just in Time an die zentrale Konsole zurückgemeldet und können dort an übersichtlichen Anzeigen schnell abgelesen werden. Jürgen Keller ist so stets informiert, welcher Mitarbeiter welche Hardwareschnittstelle nutzen möchte und welche Daten darüber gerade transferiert werden.

Die Strategie der beiden IT-Fachleute ging auf. Alle Mitarbeiter von SFB sind mittlerweile in Security.Desk analog ihrer Active-Directory-Gruppen organisiert. Diese Gruppen besitzen unterschiedliche Nutzungsrechte in Bezug auf die Hardwareschnittstellen im Unternehmensnetzwerk. „Im Grunde dürfen alle Mitarbeiter erst mal gar nichts. Wir sperren jeglichen Zugriff auf USB- und sonstige Schnittstellen. Natürlich gibt es aber auch einige Gruppen, die beispielweise eigens angeschaffte, unternehmenseigene USB-Sticks nutzen dürfen. Alle anderen USB-Speicher werden dennoch geblockt", erklärt Jürgen Keller. „Wenige Mitarbeiter haben aber natürlich Vollzugriff, auch das gibt es. Hier besteht dennoch die Möglichkeit, über ein Dateiprotokoll zu kontrollieren, welche Dateien transferiert werden. Wir haben also immer noch eine gewisse Übersicht, ohne den Mitarbeiter in seinem Arbeitsalltag einzuschränken. Außerdem lässt sich über eine temporäre Freigabe erwirken, dass Mitarbeiter, die normalerweise gesperrt sind, für eine gewisse Zeit von mir freigegebene Schnittstellen nutzen dürfen. Das kostet mich lediglich zwei Mausklicks. Diese Möglichkeit nutzen wir relativ häufig", ergänzt er.

Dass die Einführung der Endpoint-Security-Lösung ein wichtiger Baustein für eine wirksame Sicherheitsstrategie von SFB ist, bestätigen nicht zuletzt die erfolgreichen ISO-Zertifizierungen der letzten Jahre. Kunden wie auch Datenschützer können sich sicher sein, dass bei SFB keine Daten unbemerkt in das Netzwerk hinein-, geschweige denn hinausgelangen. Schwäbische Gründlichkeit eben. ↩

Angela Mähringer

Produziert *werden bei der SFB seit 70 Jahren Präzisionsteile und Baugruppen für die Automobil-, Luftfahrt-, Maschinenbau- sowie Lebensmittel- und Medizinbranche.*