

Erhöhte Sicherheit durch dezentral geschützte Produktionszellen

Produktionsnetze sind meist komplex aufgebaut und dadurch störanfällig. Für die sichere Vernetzung von Produktionsmaschinen und Anlagen setzt ein Unternehmen in Österreich auf ein Konzept mit abgeschotteten Produktionszellen und dezentralen Industrie-Firewalls. Ein darauf folgender Virenangriff konnte verhindert werden.

HERBERT DIRNBERGER UND MARTIN ORTGIES

Im Jahre 2006 sollten bei der Umdasch AG in Amstetten (Österreich) 30 neue Roboterschweißzellen und Produktionsanlagen in das Unternehmensnetzwerk integriert werden. Für den Ausbau war es notwendig, die Strategie und Vorgehensweise weiterzuentwickeln. Weil das Produktionsnetzwerk schnell gewachsen und sehr komplex geworden war, war für die Administration des Un-

ternehmens eine neue Sichtweise notwendig geworden.

Informationssicherheitskonzept für komplette Automatisierung

Für die angepasste Behandlung des Risikos, wie zum Beispiel eines Virenbefalls von Produktionsrechnern mit einem verbundenen Stillstand von Produktionslinien, wurde ein

Informationssicherheitskonzept für die Prozess-, Fertigungs- und Gebäudeautomatisierung erstellt. Die Serviceabteilung Elektro-

Herbert Dirnberger ist Automatisierungs- und Systemtechniker bei der Umdasch AG in Amstetten (Österreich). Martin Ortgies ist Fachjournalist in Königslutter. Weitere Informationen: Innominate Security Technologies AG, 12489 Berlin, Tel. (0 30) 92 10 28-0, contact@innominate.com



Bild: Umdasch

Ein Produzent von Betonschalungssystemen setzt bei der Prozess-, Fertigungs- und Gebäudeautomatisierung auf ein Informationssicherheitskonzept mit dezentralen Industrie-Firewalls.

und Automatisierungstechnik und die zentrale Informationstechnik entwickelten gemeinsam mit externen Partnern eine Plattform für innovative Produktions- und Unterstützungsprozesse im Umdasch-Konzern.

Kern des Konzepts ist die Bildung von kleinen, dezentralen Produktionszellen

Die aktuell wichtigsten Anforderungen an die Informationssicherheit in der Produktion sind eine durchgängige und sichere Kommunikation im Office- und Produktionsnetz, flache Netzwerke mit möglichst geringer Komplexität, eine hohe Flexibilität für die Integration neuer Anlagen und hohe Sicherheit bei externen Zugriffen, wie zum Beispiel bei der Fernwartung von Anlagen. Kern des Konzepts ist die Bildung von kleinen, überschaubaren und dezentralen Produktionszellen. Die Produktionssysteme für Bearbeitungsprozesse wie Schneiden, Bohren, Fräsen, Schweißen und weitere sind jeweils in mehrere Zellen aufgeteilt und mit einer Industrie-Firewall abgeschottet. Insgesamt über 40 solcher Zellen bilden den Übergang zum Informationsnetz. So wird der Informationsfluss zwischen den Schichten des Pro-

Umdasch Group

170 Niederlassungen und Standorte in 70 Ländern mit mehr als 7000 Mitarbeitern

Die Umdasch Group zählt mit den beiden Divisionen Doka Group (Beton Schalungstechnik) und Umdasch Shopfitting Group (Ladeneinrichtungen) zu den jeweils international marktführenden Anbietern und ist damit einer der aktivsten Global Player der österreichischen Wirtschaft.

Gegenwärtig ist die Umdasch Group mit nahezu 170 Niederlassungen und Standorten in rund 70 Ländern der Welt vertreten. Mehr als 7000 Mitarbeiter erwirtschaften bei einer Exportquote von rund 80% jährliche Umsätze von nahezu einer Milliarde Euro.

duktionsnetzes und den administrativen Informationssystemen kontrolliert und abgesichert (Bild 1). Neue Automatisierungs- und Steuerungssysteme können mit diesem Konzept relativ einfach und schnell in die Systemlandschaft der Umdasch AG eingebunden werden.

Einsatz von dezentralen Firewalls ist die wichtigste Schutzmaßnahme

Der Einsatz von dezentralen Firewalls ist die wichtigste Schutzmaßnahme. Trotz der sehr

vielen vernetzten Produktionssysteme wurden bei dem österreichischen Unternehmen gut administrierbare und überschaubare Teilnetze geschaffen. Neben den dezentralen Firewalls gehören ein Konzept für Back-up und Recovery sowie die Vorhaltung von Ersatzgeräten zu den nächstwichtigsten Schutzmaßnahmen. Umgesetzt werden außerdem weitere Schritte zur Systemhärtung, ein Schutz vor Malware, sichere Authentifizierung und Autorisierung sowie Punkte zur physikalischen Sicherheit und Systemresis-

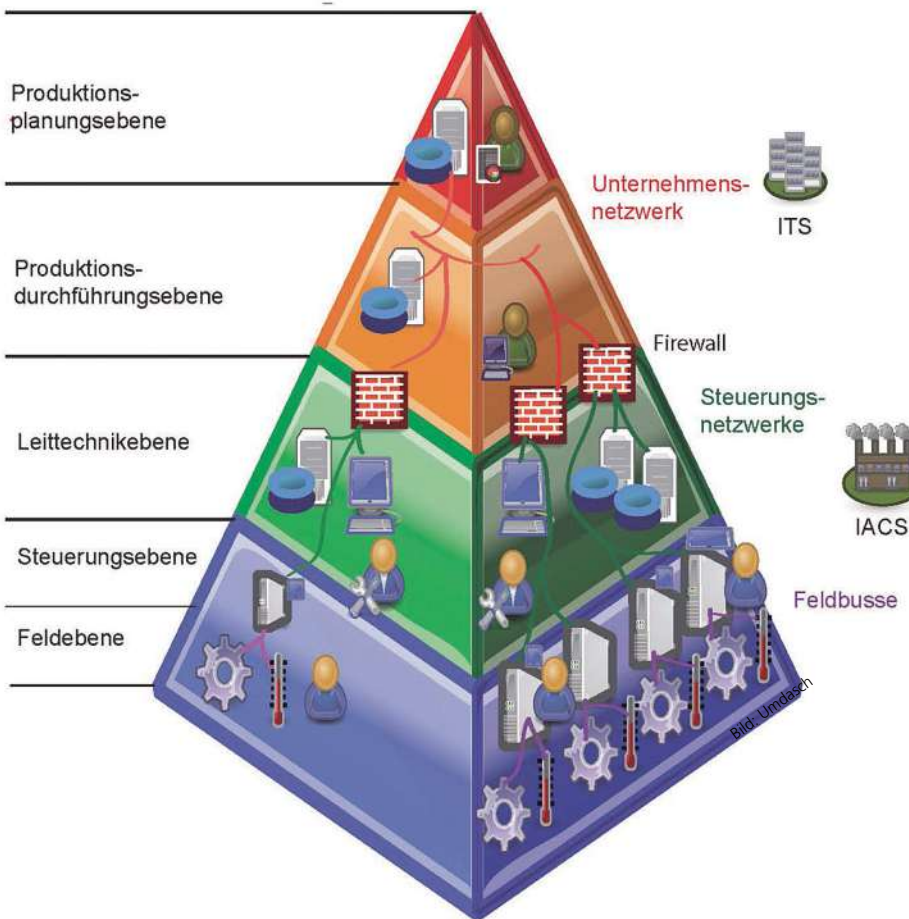


Bild 1: Der Informationsfluss zwischen den Schichten des Produktionsnetzes und dem Unternehmensnetz wird durch kleine abgeschottete Produktionszellen kontrolliert und abgesichert.

tenz. Bei der Auswahl der geeigneten Sicherheitstechnik fiel die Entscheidung zugunsten der Mguard-Security-Appliance-Technik von Innominate. Maßgeblich dafür waren die bessere Serviceunterstützung, die Indus-

trietauglichkeit, die Einfachheit des Systems und des Linux-Betriebssystems. Weil das Unternehmen eine Servicehotline bevorzugt, die auch am Tag erreicht werden kann, verzichtete man auf Geräte aus Übersee.

Im Vergleich zu Produkten aus der Officewelt sind Anforderungen wie ein erweiterter Temperaturbereich, die Schutzart oder die Montagemöglichkeit in Schaltschränken ausschlaggebend. Weil viele Funktionen aus der Officewelt im Produktionseinsatz nicht gebraucht werden und eher störend sind, zeigt sich die Industrietechnik als einfacher und besser administrierbar. Die Linux-Softwarebasis ist hilfreich, um mit eigenen Skripten die Funktionalitäten erweitern zu können oder per Command Line-Logging- und Konfigurationsdateien der Firewalls einzusehen.

Zwischen den einzelnen Systemen werden sichere Übergänge geschaffen

Durch die eingesetzte Mguard-Technik werden sichere Übergänge zwischen den Systemen geschaffen, weil der Netzwerkverkehr mittels Paketfilterung und Routing nach dem Prinzip des sogenannten Least Privilege eingeschränkt wird. Es wird nur das erlaubt, was unbedingt notwendig ist. Für die Sicherheitsexperten von Umdasch ist außerdem die Logging-Funktion der Security Appliances (Bild 2) ein wichtiges Sicherheitselement. Weil sich die Netze ständig dynamisch verändern, neue Netzteilnehmer eingepflegt oder Fehler im Datennetz korrigiert werden, wird der Verkehr im Datennetz sehr aufmerksam beobachtet.

Die Meldungen über abgelehnte oder akzeptierte Datenverbindungen werden zentral an einen Syslog-Server weitergeleitet und kontinuierlich überwacht. Veränderungen werden gezielt mittels automatisierter Skripte herausgefiltert und analysiert.

Durch das Logging wurde beispielsweise ein aktueller Virusbefall frühzeitig erkannt. Das Virus war in der Lage, innerhalb von einer Stunde mehr als 100.000 Netzadressen zu kontaktieren. Durch die Firewalls wurden die Produktionszellen allerdings erfolgreich geschützt. Lediglich eine Zelle hatte Probleme. Die Ursache war ein ungepatchtes Gerät, das nicht dem Stand der Technik entsprach.

Konfiguration von Firewalls ist keine triviale Aufgabe

Die Konfiguration von Firewalls mit individuellen Regeln für die einzelnen Zellen ist zunächst keine triviale Aufgabe. Mit einer Schulung, etwas Übung und den Best-Practice-Erfahrungen, wie sie zum Beispiel die Experten von Innominate haben, lässt sich allerdings recht schnell ein strukturiertes Verfahren entwickeln. Dann geht es in kleinen Schritten immer nach dem gleichen Muster. 80% der einmal entwickelten Konfiguration können auch für andere Zellen genutzt werden.

Für die Verwaltung der Firewall-Systeme überlegt das Unternehmen Umdasch, in Zukunft auch den Innominate Device Manager (IDM) einzusetzen. Damit lässt sich der administrative Aufwand bei Systemumstellungen oder bei Anpassungen an Ausführungsrichtlinien und Standards deutlich verringern.

Ein größerer Anpassungsaufwand entsteht zum Beispiel immer dann, wenn ein Fileserver ausgetauscht wird oder sich Adressen des Fileservers ändern. Weil dann bei allen Firewalls die gleichen Einträge angepasst werden müssen, kann der IDM für



Bild 2: Dieses industrietaugliche Sicherheitsgerät ist auf der Hutschiene montierbar.

wartung durch externe Serviceanbieter sorgt die Mguard-Technik für ein kontrollierbares und sicheres Verfahren.

Externe Zugriffe über die Hintertür gehören der Vergangenheit an

Beim Umdasch entscheiden die Servicetechniker jetzt von Fall zu Fall, ob für eine einzelne Zelle eine externe Einwahl erfolgen soll. Externe Zugriffe über die Hintertür gehören damit der Vergangenheit an. Erst wenn die Techniker per Serviceknopf die Einwahl freischalten, ist ein Verbindungsaufbau möglich. Dann wird die Verbindung zwischen der Produktionszelle und der Office-Firewall, also dem äußeren Schutzwall an der Außengrenze des Unternehmens, freigeschaltet. Dort sind die Office- und Industrie-Firewalls eng aufeinander abgestimmt.

Nach den Erfahrungen bei Umdasch gehören Sicherheitsvorfälle im Datennetz zum Alltag. Immer wieder wird Schadsoftware über infizierte USB-Sticks oder versehentlich von externen Servicetechnikern ins Netz gebracht. Die Folgen solcher Infektionen sind nun allerdings entscheidend eingedämmt, weil die Produktionssysteme jetzt gut geschützt sind. Das erarbeitete Informationssicherheitskonzept mit dezentralen Industrie-Firewalls hat zusätzliche Vorteile: Das Netzwerk ist weniger komplex, besser kontrollierbar und die Verfügbarkeit wird dadurch erhöht. Außerdem lassen sich neue Anlagen besser integrieren. **MM**