



Weltweit

sicher vernetzt



KASTO, Hersteller von Metallsägen und Lagersystemen, setzt bei IT-Sicherheit auf zweistufiges Firewall-Cluster und verschlüsselten Datenaustausch via Internet

Wenn irgendwo Metall gesägt wird, ist sehr wahrscheinlich eine Maschine von KASTO am Werk. Die Maschinenbau-firma aus dem badischen Achern ist Weltmarktführer bei den Bügel-, Band- und Kreissägen, von den Werkstatt-maschinen für Handwerker bis hin zu den Hochleistungsautomaten für die industrielle Massenproduktion. Diese computergesteuerten Maschinen zerlegen Stahlrohre oder auch Autoblech mit schnellen, präzisen Schnitten – auf den Zehntelmillimeter genau. Außerdem entwickelt und realisiert KASTO eine breite Palette an halb- und vollauto-matischen Langgut- und Blechlager-systemen. Die Position als globaler

Marktführer – in Technologie und Stück-zahlen – bei Metallsägemaschinen und automatischen Lagersystemen basiert auf über 120 Patenten und wird durch über 120.000 in alle Welt gelieferte Säge-maschinen sowie über 1.200 installierte Automatik-Lager eindrucksvoll dokumen-tiert. Für die Produktion, den Vertrieb und weltweiten Wartungsservice müssen sensible Daten zwischen den Firmenstand-orten sowie mit Kunden in der ganzen Welt ausgetauscht werden – gegen un-befugte Zugriffe und Ausfälle zuverlässig abgesichert. Hier setzten die Maschinen-bauer auf zweistufige, hochverfügbare Firewall-Systeme und VPN-Appliances für den verschlüsselten Datenaustausch.



Auf hohem Level zertifiziert: Zweistufige Firewall GeNUGate

KASTO produziert die leistungsstarken Sägemaschinen und Lagersysteme am Stammsitz in Achern und einem zweiten Werk im thüringischen Schalkau. Für den internationalen Vertrieb und Kundenservice vor Ort unterhält die Firma weitere Niederlassungen im Ausland, darunter größere Tochtergesellschaften im englischen Southampton und Obernai im Elsass. Der reibungslose Geschäftsbetrieb erfordert, dass die rund 600 Mitarbeiter an den verschiedenen Standorten ständig untereinander, mit Kunden und Interessenten kommunizieren und Daten via Internet austauschen können.

Großen Kommunikationsbedarf hat zudem das Service-Center: Auf Wunsch der Kunden werden die weltweit installierten Anlagen per Fernzugriff von KASTO überwacht. Dazu greifen Service-Spezialisten von der badischen Firmenzentrale via Internet auf die Steuerungssysteme der Maschinen zu und kontrollieren die Betriebsdaten. So werden Unregelmäßigkeiten frühzeitig erkannt und behoben, bevor sie zu Betriebsstörungen oder sogar kostspieligen Ausfallzeiten führen. Dieser Service ist für das kontinuierliche Monitoring auf eine zuverlässige Internet-Anbindung unbedingt angewiesen.

Unverschlüsselte Daten sind digitale Postkarte

Die erwünschten Kommunikationsverbindungen via Internet müssen sichergestellt werden,

gleichzeitig sind die übertragenen Daten und das Firmennetz von KASTO aber gegen unerwünschte Zugriffe zu schützen. Denn Kunden-, Betriebs- oder auch Konstruktionsdaten dürfen nicht in die Hände unbefugter Dritter, beispielsweise der Konkurrenz, gelangen. Werden Daten jedoch ohne Verschlüsselung übertragen, sind sie auf ihrem Weg durch das weltweite Web vor neugierigen Blicken so sicher wie eine Postkarte in der gelben Briefpost.

Auch an der Schnittstelle zwischen öffentlichem Internet und dem lokalen Firmennetz (LAN) muss sorgfältig kontrolliert werden: Verbindungen für E-Mail-Kommunikation, WWW-Daten sowie zum Informationsaustausch mit Niederlassungen und Kunden sollen stets zugelassen werden, unbefugte Zugriffe und Angriffe vom Internet in das LAN sind dagegen zuverlässig abzublocken. Bei der Absicherung von Netzwerken und Daten wird KASTO seit 20 Jahren von dem IT-Spezialisten BWG Informationssysteme aus Ettlingen unterstützt. Die Spezialisten lösten diese Aufgabe mit Firewalls des Typs GeNUGate sowie VPN-Appliances zur Datenverschlüsselung vom Typ GeNUBox.

„Die Firewall GeNUGate bietet aufgrund der Zweistufigkeit eine starke Sicherheitsleistung, die von unabhängigen Experten auf einzigartig hohem Level zertifiziert ist. Dies ist ein entscheidendes Merkmal, denn beim Schutz sensibler



Sägen von KASTO zerlegen Stahl und Blech mit präzisen Schnitten



Daten und Firmennetze sollte kein Risiko eingegangen werden“, erläutert Thomas Zeller, Leiter Security Services bei BWG, die Auswahl der Firewall. Bei der GeNUGate des deutschen Herstellers GeNUA sind zwei unterschiedliche Firewalls zu einer Lösung kombiniert: Ein Application Level Gateway und ein Paketfilter. Beide Systeme laufen auf separater Hardware, sind jedoch in Reihe geschaltet. Daten auf dem Weg vom Internet in das LAN müssen also zwei unterschiedliche Firewalls passieren.

Alles verboten – außer was ausdrücklich erlaubt ist

Das zweistufige Firewall-System folgt bei der Datenkontrolle einer strikten Regel: Jeglicher Datenaustausch ist verboten – außer den ausdrücklich zugelassenen Verbindungen. Daten aus dem Internet erreichen zuerst das Application Level Gateway. Dies ist das aufwändigere der beiden Firewall-Systeme und überprüft den Inhalt des Datenstroms. Dazu stoppt es die eintreffenden IP-Pakete und setzt sie zu Datensätzen zusammen. Denn nur anhand kompletter Datensätze kann der Inhalt überprüft werden. Jetzt analysieren spezielle Prüfprogramme so-

wie zusätzlich ein integrierter Virens Scanner den Inhalt der empfangenen Daten. Unerwünschter und auch gefährlicher Code wie aktive Inhalte und Viren werden so zuverlässig identifiziert und abgeblockt. Auch Datenpakete, die Angreifer mit gefälschten IP-Adressen versehen haben um als erwünschter Kommunikationspartner zu erscheinen, werden bei der Prüfung erkannt und zurückgewiesen.

Danach gelangen die Daten zum zweiten Firewall-System, einem Paketfilter unmittelbar vor dem LAN. Er lässt generell nur Datenpakete ins LAN passieren, die zuvor von dort angefordert wurden, beispielsweise WWW-Daten beim Surfen im Internet. Dazu werden die formalen Kennzeichen im Header der Pakete überprüft: Sind die Absenderadresse, der verwendete Protokolltyp sowie die angesteuerte Port-Nummer zugelassen? Erst wenn die Daten auch diese Prüfung bestanden haben, dürfen sie zum Empfänger im LAN passieren. Die zweistufige Prüfung und die Inhaltskontrollle durch das Application Level Gateway unterscheiden die GeNUGate von vielen anderen Firewalls, die ausschließlich als Paketfilter arbeiten.



VPN-Appliance GeNUBox für verschlüsselten Datenaustausch



Die Zweistufigkeit ermöglicht zudem den einfachen Aufbau einer so genannten Demilitarisierten Zone (DMZ) zwischen den beiden Firewalls. In diesem separaten Bereich stehen WWW- und E-Mail-Server – also die Systeme, auf die sowohl vom Internet als auch vom LAN aus zugegriffen werden kann. Das LAN ist von den Servern in der DMZ aber immer noch durch die zweite Firewall getrennt und somit vor direkten Zugriffen aus dem Internet abgeschirmt. „Eine DMZ ist ein wichtiger Baustein, um die IT-Sicherheit in Firmennetzen deutlich zu steigern“, so Thomas Zeller von BWG.

Penetration-Test kommt nicht durch

KASTO hat im Oktober 2007 von der Wirtschaftsprüfungs-Gesellschaft Ernst&Young eine externe IT-Sicherheitsuntersuchung durchführen lassen. Dabei haben die Spezialisten einen Penetration-Test gegen die Firewall gefahren. Das Ergebnis: kein Durchkommen. „Die beiden Firewalls ergeben im Zusammenspiel einen zuverlässigen Schutzriegel. Wir hatten an dieser Stelle noch nie irgendwelche Sicherheitsprobleme“, resümiert Robert Ganter, IT-Leiter bei KASTO. Seit 2002 schützt die GeNUGate das Netz der Maschinenbaufirma. Anfang 2008 wurde die Sicherheitslösung mit einer zweiten Firewall zu einem Cluster erweitert. Beide Firewalls teilen sich seitdem die Arbeit und beobachten dabei stets den Partner, um bei einem Ausfall sofort dessen Aufgaben zu übernehmen

und so die hochverfügbare Verbindung zum Internet sicherzustellen.

Die unabhängigen Experten vom Bundesamt für Sicherheit in der Informationstechnik (BSI) haben die GeNUGate nach dem internationalen Standard Common Criteria (CC) geprüft. Dabei wird das System ausführlich getestet und die korrekte Umsetzung aller Sicherheitsmechanismen bis hinunter zum Quellcode nachgeprüft, der vom Hersteller vorgelegt werden muss. Das Ergebnis: Sicherheitszertifikat in der Stufe EAL 4+ mit dem Zusatz „Highly Resistant“. EAL 4+ ist der höchste Level, der auf ein komplexes System wie eine Firewall vollständig anwendbar ist. Da die GeNUGate aber beim wichtigen Merkmal Selbstschutz noch höhere Anforderungen erfüllt – selbst sorgfältig vorbereiteten und unter günstigen Bedingungen geschickt ausgeführten Angriffen wird stärkster Widerstand entgegengesetzt – hat das BSI den Zusatz Highly Resistant vergeben. Die GeNUGate ist die einzige Highly Resistant Firewall der Welt.

Verschlüsselter Datentransfer via Internet

Wenn die Daten jetzt das sichere LAN der Firmenzentrale verlassen, Richtung weiterer Niederlassungen oder zu betreuten Maschinen bei Kunden, müssen sie ebenfalls vor unbefugten Zugriffen geschützt werden. Hier nutzt KASTO ein Virtual Private Network (VPN). Mit



der VPN-Technologie werden über das öffentliche Internet verschlüsselte Verbindungen aufgebaut, über die Daten sicher abgeschirmt übertragen werden können. Dazu müssen an den jeweiligen Endpunkten VPN-Gateways installiert sein.

In der Firmenzentrale sowie den Niederlassungen in Thüringen, Großbritannien und Frankreich sind VPN-Appliances des Typs GeNUBox installiert, um die sicheren Verbindungen aufzubauen. Kleinere Niederlassungen sowie die Steuerungssystemen der Maschinen bei den Kunden sind mit software-basierten Client-Lösungen an die verschlüsselte Kommunikation angebunden. Dieses VPN basiert auf Schlüsseln mit 128 Bit und ist mit heutigen Methoden und Kapazitäten nicht zu knacken. So wird zwischen den Firmenstandorten sowie für den Kundenservice zu den

weltweit betreuten Maschinenanlagen ein zuverlässig geschütztes Datennetz geknüpft.

Betreut wird der Firewall-Cluster und die VPN-Appliances vom Kundenservice des Herstellers. Die Spezialisten von GeNUA überwachen – ebenfalls via VPN-Verbindung – die Systeme und übernehmen die komplette Administration von der Konfiguration bis hin zum regelmäßigen Einspielen neuer Updates. Robert Ganter von KASTO: „Der Kundenservice ist sehr schnell und kompetent. Wir können uns darauf verlassen, dass unsere wichtigen IT-Systeme stets reibungslos funktionieren.“ Davon profitieren wiederum die Kunden von KASTO, die irgendwo Metall sägen. Denn sie können sich darauf verlassen, dass der Fernwartungsservice des badischen Maschinenbauers ihnen jederzeit via Internet zur Seite steht.

GeNUA mbH
Gesellschaft für Netzwerk- und Unix-Administration mbH
Domagkstraße 7, 85551 Kirchheim b. München
tel +49 (89) 99 19 50-0