Special Innovation

Lösungen für Überflieger

Der österreichische Flugzeugbauer Diamond Aircraft kann sich keinerlei Sicherheitslücken leisten. Heikle Unternehmensdaten und das IT-Netz müssen ausreichend geschützt werden. Gelöst wurde das Problem mit einem ausgeklügelten Self-Defending Network, das interne und externe Bedrohungen zu identifizieren imstande ist.

Sonja Gerstl

Gerade in der Flugzeugindustrie spielt das Thema Sicherheit eine entscheidende Rolle. Um sich vor Werksspionage zu schützen, müssen Security-Experten alle Register ziehen – damit Betriebsgeheimnisse auch tatsächlich solche bleiben. Foto: Fotolia.com

Der internationale Flugzeughersteller Diamond Aircraft hat sich auf den Bau von fortschrittlichen, einsitzigen Flugzeugen spezialisiert. Die Produktion erreicht neue Höhen, wenn heuer der erste Jet an den Start geht. Das Unternehmen stammt aus Österreich, hat aber inzwischen auch Werke in Kanada und China eröffnet. Der Entwicklungszyklus ist in Bezug auf Technik und Konstruktion sehr kurz und beträgt nur ein Fünftel des Zeitraums, den andere Unternehmen bis zur Neuvorstellung eines Flugzeugs benötigen.

Hans-Peter Planer, Leiter des IT-Bereichs von Diamond Aircraft, erklärt: „In der Flugzeugindustrie dauert die technologische Entwicklung eines neuen Flugzeugs generell etwa zehn Jahre. Bei Diamond beträgt dieser Zeitraum ungefähr zwei Jahre. Es ist ein großer Erfolg, Flugzeuge in einer so kurzen Zeit bauen zu können, aber es besteht neben anderen Risiken auch die Gefahr, dass uns Konkurrenten ausspionieren."

Ein Unternehmen, dessen Entwicklungszyklus dem seiner Wettbewerber um bis zu acht Jahre voraus ist, ist stets auch ein offensichtliches Ziel für den Datendiebstahl durch Dritte. Umso wichtiger war es für Diamond, ein entsprechendes Sicherheitskonzept für das gesamte Unternehmen zu erstellen, das mittelfristig auch die Auslandsdependancen berücksichtigen soll. Mit dieser heiklen Aufgabe beauftragt wurde der IT-Konzern Cisco, der in weiterer Folge eine komplette End-to-End-Security-Lösung erstellte. Herzstück ist dabei das Cisco Self-Defending Network, das eine langfristige Strategie zum Schutz der Geschäftsabläufe des Unternehmens und zur Datensicherheit beinhaltet. Dabei werden sowohl interne als auch externe Bedrohungen identifiziert, vermieden und in der Planung berücksichtigt. Dieser Schutz hilft Organisationen darüber hinaus auch, die in ihren Netzwerk-Ressourcen gespeicherten Betriebsgeheimnisse besser zu nutzen und so nicht nur die Geschäftsabläufe zu verbessern, sondern auch die Kosten zu senken.

Umfassende Lösung

Umgesetzt wurde das Konzept in einem abgestuften Realisierungsplan, der mit einem Upgrade auf ein durchgängiges Cisco-Netzwerk startete. In weiterer Folge kam ein Cisco Security Manager hinzu. Schlussendlich erfolgte ein Upgrade auf ein komplettes Cisco-Sicherheitsüberwachungssystem mit kontrolliertem Netzwerkzugang. Für Diamond Aircraft gewinnt diese Lösung noch mehr an Gewicht, wenn das Unternehmen wie geplant VPN-Verbindungen nach Kanada, China, England und Deutschland einrichtet.

www.cisco.at

Sicherheitslücken im Arbeitsalltag

Die rasante Entwicklung der Informationstechnologie fordert Unternehmen in Sachen Security stark heraus.

Firmen sind heute mit einer Vielzahl von elektronischen Gefahren konfrontiert, und es gibt auch eine Vielzahl von Lösungen. Trotzdem gelingt es Angreifern, mitunter enormen Schaden anzurichten. Vor allem die rasante Entwicklung der Branche stellt hierbei ein großes Problem dar.

Wilfried Pruschak, Geschäftsführer von Raiffeisen Informatik, konstatiert: „Das ist eine echte Herausforderung für Sicherheitsexperten und sollte daher in erster Linie von Profis gemacht werden. Sich hausintern einen solchen Profi zu leisten, ist sehr kostspielig. Hier kann Outsourcing die Lösung sein. Die Vergabe der Unternehmens-IT an einen professionellen IT-Dienstleister ermöglicht dem Unternehmen, stets die aktuellsten Sicherheitsvorkehrungen eingesetzt zu haben, ohne hier erheblichen Mehraufwand leisten zu müssen." Unternehmensdaten stellen ein wertvolles Gut dar. Der Handel mit Daten und der Diebstahl sensibler Daten erreichte im vergangenen Jahr Rekordhöhe. Hier gilt es, mit umfassender IT Security Policy und dementsprechenden Maßnahmen wie etwa geregelten und administrierten Zutritts- und Zugriffsbeschränkungen dem Missbrauch einen Riegel vorzuschieben.

Ausgefeilte Attacken

Beim E-Mail wiederum wird Spam zur Plage. „Wir rechnen in Zukunft vermehrt mit gezielten Attacken auf Computer- und Systemschwachstellen. Die Attacken sind immer ausgefeilter und zielgerichteter und auf den ersten Blick schwer als Spam zu erkennen. Hier sind alle IT-Security-Verantwortlichen gefordert, den stets steigenden Attacken entgegenzuwirken und immer neue Mechanismen der Abwehr zu entwickeln", betont Pruschak. Kopfzerbrechen bereitet den IT-Experten auch das Thema Mobilität. Eine von Riverbed Technology bei Forrester Consulting in Auftrag gegebene Studie belegt, dass Unternehmen zunehmend dezentral aufgestellt sind und WDS (Wide-Area Data Services) immer mehr als strategische Komponente sehen. Die zunehmende Bedeutung mobiler Mitarbeiter und Zweigstellen für das Wachstum der Unternehmen bringt aber eine Menge von Risiken mit sich.

Ebenso begehrt sind die Geräte selbst: Nicht nur, dass sie aufgrund ihres Wertes interessant für Diebe sind, auch finden sich teils sensible Geschäfts- oder Kundendaten zum Teil schwach oder gar nicht verschlüsselt auf ihnen. Vertrauliche Behandlung der Daten und der Kommunikation ist hier unbedingt gefordert. *sog*

www.raiffeiseninformatik.at

Vertrauliche Unternehmensdaten sind in vielen Fällen oft nur unzureichend geschützt. Foto: Fotolia.com