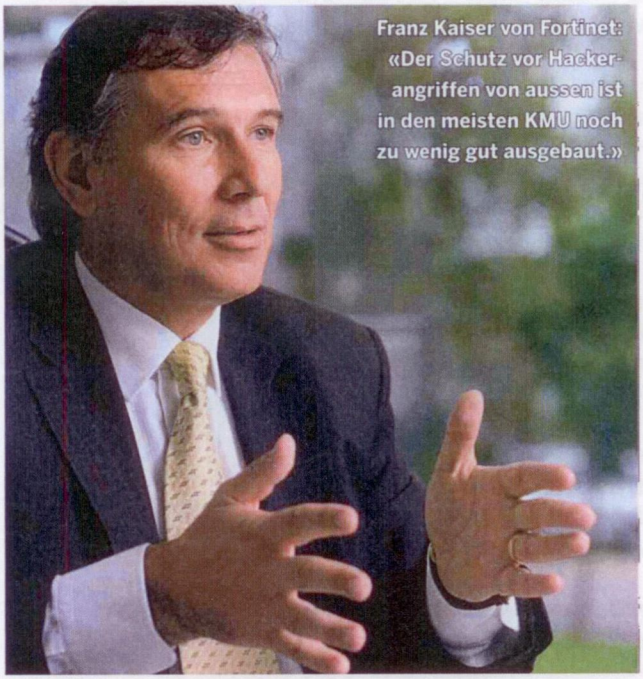
ICT

Drahtlose Netzwerke als Sicherheitsrisiko.

Auch KMU werden vermehrt zur Zielscheibe von Cyber-Kriminellen. Zu einer Schwachstelle entwickeln sich zunehmend die drahtlosen Netzwerke. Moderne Firewalls bieten aber auch hier immer besseren Schutz vor Hackern.

VON THOMAS BERNER



Franz Kaiser von Fortinet: «Der Schutz vor Hackerangriffen von aussen ist in den meisten KMU noch zu wenig gut ausgebaut.»

«IT-Manager sind zunehmend gezwungen, aus ihrer Komfortzone ‹sicheres LAN› herauszutreten und ihre Netzwerkarchitektur zu überdenken. Denn die verschiedenen mobilen Geräte und Applikationen im Einsatz werden über kurz oder lang das bestehende System samt Sicherheit in die Knie zwingen.» Dies sagt Franz Kaiser, Regional Director Österreich und Schweiz bei Fortinet, einem der grössten Anbieter von IT-Sicherheitslösungen. Die Bedürfnisse von KMU sind ihm durchaus bekannt: «KMU haben kaum Zeit für IT-Sicherheit.

Deshalb ist ihnen eine Box-Lösung, welche Firewall, Virenschutz etc. einschliesst, am liebsten: Anschliessen, einschalten – und es läuft.»

Drahtlose Netzwerke benötigen Leistung. Die Leistungsfähigkeit einer Firewall ist das eine: Immer mehr mobile Geräte müssen darüber laufen können, zumal «Bring your own device» (BYOD) einem starken Trend entspricht. So hat etwa das Reiseunternehmen Globetrotter in seinem Stammsitz sowie den 23 Filialen ein drahtloses Netzwerk eingerichtet, das mit einer Firewall zentral im Rechenzentrum gesteuert wird. «Uns war es ein grosses Anliegen, dass sich die WLAN-Geräte zentral verwalten und formneutral in unser Filialbild einpassen lassen, falls mal ein AccessPoint sichtbar platziert werden müsste», sagt Michael Bucher, IT-Support-Verantwortlicher der Globetrotter Travel Service AG.

Internet-Kriminelle mit ihren eigenen Waffen schlagen. Doch auch bei der Sicherheit müssen Firewalls laufend nachgerüstet werden. Für die Cyber-Kriminalität wie etwa Industriespionage oder Datenklau werden besonders KMU, welche in ihren Bereichen eine führende Position einnehmen oder als Zulieferer bedeutender Konzerne fungieren, zu lohnenden Zielen. Anbieter wie Fortinet bieten inzwischen Lösungen an, welche sich immer genauer und benutzerfreundlicher auf die Sicherheitsbedürfnisse von Unternehmen einstellen lassen und mit verbesserten Sicherheitstools vor sogenannten Langzeit-Multi-Vektor-Angriffen schützen.

Intelligent reagieren. Den Internet-Kriminellen einen Schritt voraus zu sein, ist immer noch eher gesagt als getan. Mit zusätzlichen und immer ausgefeilteren Firewall-Funktionen wird das Möglichste versucht, wie Franz Kaiser im folgenden Interview erläutert.

Herr Kaiser, wie beurteilen Sie die derzeitige Situation: Machen Unternehmen genug für die IT-Sicherheit?

Franz Kaiser: Es geht immer um eine Risikoabwägung. Je mehr ein Unternehmen in IT-Sicherheit investiert, desto sicherer kann es sich fühlen. In der Regel wird aber eher noch zu wenig unternommen. Gerade KMU verlassen sich da voll und ganz auf ihren IT-Outsourcing-Partner, häufig ohne genau zu überlegen, was sie in Sachen IT-Sicherheit eigentlich bräuchten.

Worin bestehen die derzeit grössten Risiken? Wo besteht Nachrüstbedarf?

Der Schutz vor Hackerangriffen von aussen ist in den meisten KMU noch zu wenig gut ausgebaut. Gerade in den sogenannten Advanced Persistent Threats (APT; fortschrittliche anhaltende Bedrohung) besteht heute das Hauptproblem. Das heisst: Internet-Kriminelle betreiben einen hohen Aufwand, um in IT-Systeme einzudringen und dort z.B. zwecks Spionage längere Zeit unbemerkt verweilen zu können.

Und dagegen hilft nun Ihr Produkt Next Generation Firewall. Was ist konkret neu daran?

Wir versuchen, intelligenter zu reagieren, als dies etwa mit herkömmlichen Virenschutz-Programmen passiert. Dort besteht zwischen dem erstmaligen Erkennen eines Schadcodes und dem Schreiben eines Schutzprogramms ein Zeitfenster von in der Regel vier bis sechs Stunden. In dieser Zeit besteht kein Schutz. Wir wollen dieses Zeitfenster weiter verkürzen. Eine unserer Strategien besteht im sogenannten «Sandboxing». Eingehende Codes werden analysiert, indem man sie in einer geschützten Umgebung, eben dem «Sandkasten», unter Laborbedingungen ablaufen lässt. Hat der Code ein Schadenspotenzial, wird darauf reagiert. Ferner loggen wir mit. Wenn häufig auf eine bestimmte IP-Adresse zugegriffen wird, schöpfen wir Verdacht und sperren diese gleich. Denn diese Zugriffe können die Ursache in einem Virus haben, der im Rahmen von APT verwendet wird.

Nun kommen ja immer mehr auch mobile Geräte ins Spiel, damit erhöht sich die Komplexität. Einschalten und es läuft, ist dann wohl zu einfach?

Grundsätzlich sind unsere Geräte nicht viel anders. Sie erkennen selbst, ob der Datenverkehr von einem mobilen oder einem festinstallierten Rechner stammt. Sie «wissen» also, um welchen User es sich handelt. Sind diese Informationen vorhanden, lassen sich unternehmensweite Regeln festlegen, welche Zugriffe von welchen Geräten gesperrt sind oder nicht. Unsere Systeme sind so konfiguriert, dass alle Geräte, die sich darüber einloggen, zuerst als ungeschützt betrachtet werden. Sie werden entsprechend gescannt. Damit lassen wir Probleme im Zusammenhang mit BYOD gar nicht erst entstehen.

Mit welchen Kosten wird dies erkauft?

Einen Kostenfaktor bilden Firewalls nicht mehr; für das gleiche Geld erhalten Sie immer mächtigere Maschinen.

Nun erweitert Fortinet ihre Network-Security-Plattform mit neuen Funktionen. Eine davon ist die Advanced Threat Protection. Worin bestehen da die Kernelemente?

Das eine ist das erwähnte «Sandboxing», das andere ist eine

Botnet-Datenbank. Diese wird laufend aktualisiert.

Welche Tipps können Sie Unternehmen geben, um ihr bestehendes System zu checken, ob Nachrüstbedarf besteht?

In jedem Fall: Sprechen Sie mit einem IT-Security-Spezialisten. Mit ihm zusammen können Sie Ihre bestehende Lösung am besten analysieren. Auch wenn KMU durch Firewalls gut geschützt sind, geht oft vergessen, dass sie ihre internen Netze segmentieren sollten, d.h. die Zugriffsberechtigungen für verschiedene User-Gruppen definieren. Am meisten Nachholbedarf besteht bei der Integration von Wireless-Netzwerken. Die Daten werden dort zwar verschlüsselt, dies bildet aber noch keinen Schutz vor APT. Die Internet-Kriminalität ist mittlerweile lukrativer als Drogenhandel; mit gestohlenen Daten lässt sich in dunklen Kanälen viel Geld verdienen ...