Fluch oder Segen?

Mobile Datenverarbeitung

Fluch oder Segen?

Kein Sicherheitssystem ist perfekt, neue Risiken tauchen immer wieder auf. Dies gilt es schnell wahrzunehmen.

Der Trend im Geschäftsleben geht in Richtung mobile Datenverarbeitung. Manager treten via Laptop mit ihrem Headquarter in Verbindung, Marketing-Leiter können sich die neue Marketing-Strategie von ihrem Homeoffice herunterladen, Vertriebsmitarbeiter haben unterwegs Zugang zu vertraulichen Kundeninformationen aus dem Unternehmensnetzwerk. Darin liegen Chancen und Risiken zugleich.

Die mobile Datenverarbeitung und das Teleworking sollten eine neue Ära in der Wirtschaft einläuten, doch sie brachten zugleich Sicherheitsprobleme mit sich: Die Technologie, die Mitarbeitern den Zugang zu ihrem Unternehmensnetzwerk ermöglicht, kann von Hackern missbraucht werden. Diese vermögen in fremde Systeme einzudringen, Viren zu verbreiten oder auf andere Weise die Sicherheit eines Unternehmens zu gefährden. Die New Economy ist durch die mobile Datenverarbeitung flexibler und produktiver, aber auch verletzlicher geworden. M-Commerce läuft ausserhalb der Unternehmens-Firewall ab, sodass jedes Endgerät mit Internetzugang anfällig für Missbrauch wird. Der Netzzugang über Breitband- oder DSL-Standleitungen ist fast schon eine Einladung für Hacker.

Beträchtliche Schäden für Unternehmen

Die Kosten einer Attacke sollten nicht unterschätzt werden. Ein Unternehmen, das sensible Daten über mobile oder Fern-PCs verliert, kann Wettbewerbsvorteile einbüssen. Es entstehen darüber hinaus indirekte finanzielle Kosten, wenn der Eindringling das Unternehmensnetzwerk beispielsweise mit einem Virus infiziert und zum Erliegen bringt. M-Commerce ist dann nicht möglich. Ausserdem kann ein Unternehmen seinen Ruf aufs Spiel setzen, seinen Markennamen gar, wenn der Eindringling firmeneigene Fern-PCs missbraucht, um in das System eines ungeschützten Kunden einzudringen. Wenn von seinen Fern-PCs oder mobilen Geräten «Denial of Service»-Attacken ausgehen, kann ein Unternehmen rechtlich und finanziell haftbar gemacht werden.

Abwehr der Risiken

Die moderne Sicherheitstechnologie hat Massnahmen gegen diese neuen Bedrohungen ergriffen: Sie setzt auf Virenschutzprogramme, die auf Fern- und mobilen Endgeräten ebenso wichtig sind wie auf dem Unternehmensnetzwerk. Technologien wie Virtual Private Networks (VPN) sichern die Verbindung zwischen Ferngerät und Unternehmensnetzwerk.

Dennoch bleiben Fern-PCs und Mobilcomputer verwundbar. Sie sind wie Satelliten vielfältigen Risiken ausserhalb des Unternehmensnetzwerks ausgesetzt. Hat ein Eindringling erst die Schutzwälle des individuellen Geräts durchbrochen, so ist der Zugang zum VPN oder dem Unternehmensnetzwerk kinderleicht.
PC-Firewalls lösen das zuvor beschriebene Problem. Firewalls sind Filter, die Datenübertragungen über das Internet blockieren oder erlauben. Sie sind direkt auf mobilen Computern oder Fern-PCs angesiedelt und wehren Hackerangriffe auf die Geräte und damit auf das Unternehmensnetzwerk ab.
PC-Firewalls schützen die Datenübertragung an ihrer verwundbarsten Stelle: Sie überwachen alle ein- und ausgehenden Daten auf den Fern-PCs selbst und ermöglichen dadurch einen sicheren Zugang zum Netzwerk, selbst über «unsichere» Breitbandverbindungen. In Kombination mit bestehenden Sicherheitstechnologien von Virenschutzprogrammen bis zu VPNs sorgen PC-Firewalls für umfassende Sicherheit.
Besonders leistungsfähige Firewalls können noch mehr. Diese Firewalls sind:

- *Anpassungsfähig an Kundenbedürfnisse:* Die Regeln, nach denen der Internet-Zugriff gewährt oder verwehrt wird, sind so flexibel, dass unvorhergesehene Hackerattacken pariert, aber gleichzeitig autorisierten Benutzern der Fernzugriff ermöglicht wird. Dieses Detail ist besonders wichtig für Teleworker, deren Heimarbeitsplatz von der Zentrale aus über Fernzugang gewartet werden muss.
- *Leicht zu verwalten:* Der Wert einer PC-Firewall bemisst sich an ihrer Integrationsfähigkeit in das unternehmensweite Sicherheitssystem und an ihren Wartungsmöglichkeiten.
- *Sorgen für umfassenden Schutz des einzelnen Geräts:* Ein- und ausgehende Daten werden streng auf ihre Zugangsberechtigung geprüft.

Der Schutz aus Distanz ist ein Puzzle aus verschiedenen Sicherheitsbausteinen. Eine Kette ist so stark wie ihr schwächstes Glied. Die beste Firewall bringt nichts, wenn sie nicht mit gleichwertigen Komponenten kombiniert ist. Diese Komponenten sind:

Aktueller Virenschutz
Selbst ein gut funktionierender PC kann mit einem so genannten Trojanischen Pferd oder einem Virus infiziert sein, die im Hintergrund ihr zerstörerisches Werk verrichten. Ein leistungsfähiges, leicht zu aktualisierendes Virenschutzprogramm gehört daher zur Grundausstattung jedes Fern- oder Mobilgeräts.

VPNs
Firewalls und Virenschutzsoftware schützen die beiden grossen Säulen des M-Commerce: das Unternehmensnetzwerk und die angeschlossenen Ferngeräte. Die Verbindung zwischen diesen muss jedoch auch abgeschirmt werden. Ein VPN sichert die dritte Säule des M-Commerce, die Verbindung zwischen Fern-PC und Unternehmen.

Sicherheitstraining für Mobil- und Fernarbeiter
Das Sicherheitssystem eines Unternehmens braucht die Wachsamkeit seiner Mitarbeiter. Alle Mitarbeiter, die mobile und Ferngeräte benutzen, sollten über die speziellen Risiken der mobilen Datenverarbeitung aufgeklärt und über neue Gefährdungen umfassend informiert werden.

Software für Fernzugang
Jedes Datenverarbeitungsgerät muss regelmässig gewartet werden. Ein gutes Datenverarbeitungssystem für Mobilcomputer enthält für gewöhnlich Remote Access Software, die es Datenschutzbeauftragten in der Zentrale ermöglicht, alltäglich auftretende Probleme zu lösen und die Leistungsfähigkeit aller Ferngeräte zu steigern.
Die PC-Firewall ist das letzte Teil im Sicherheitspuzzle. Alle Komponenten zusammen ergeben ein Sicherheitssystem, das sich vom Herzstück des Unternehmens, dem Unternehmensnetzwerk, bis zu den äusseren Gliedmassen erstreckt; das heisst, bis zu den Mitarbeitern, die zu Hause Telearbeit verrichten oder unterwegs am Laptop arbeiten. Kein Sicherheitssystem ist perfekt, neue Risiken tauchen immer wieder auf. Flexible Sicherheitssysteme sind die Antwort darauf. Die PC-Firewall schliesst eine Sicherheitslücke und beschleunigt damit den Siegeszug des M-Commerce. 4

Quelle: Symantec

Symantec (Switzerland) AG
Grindelstrasse 6
CH-8303 Bassersdorf
Tel. 01 838 49 32
Fax 01 838 49 01
E-Mail: Heike_Faller@symantec.com

Summary

Mobile Data Processing – a Blessing or a Curse?

Business is moving towards mobile data processing. Managers can contact company headquarters via their laptops, marketing heads can download the latest marketing strategy using their home office, and sales staff can access confidential customer information on the company network when on the move. These developments are opening up new opportunities and risks at the same time. Modern security technology contains measures against these new threats in the form of virus protection programmes, which are just as vital for remote and mobile terminals as they are for company networks. No security system is perfect, and new risks are constantly arising. The answer to this is flexible security systems. The PC firewall closes a security loophole, thereby speeding up the breakthrough of m-commerce. Firewalls are filters that block or permit data transmissions via the Internet. They are located on mobile computers and remote PCs themselves, and protect terminals and therefore ultimately company networks against hacker attacks from outside. The PC firewall is the last piece in the security jigsaw. All the components together comprise a security system stretching from the core of a company, the company network, to the outermost branches, i.e. teleworkers or staff working on a laptop while travelling.