Mobiler Zugriff

Segen und Gefahr

Bald sind sie wieder da, die warmen Tage mit viel Sonnenschein. Schnell den Laptop unter den Arm gepackt und ab an die Sonne. Mit VPN ist es ja kein Problem, auch vom Schwimmbad aus weiterzuarbeiten. Dass sich hier aber viele Gefahren tummeln, wird oft vernachlässigt.

Autor: Andreas Wisler

Der mobile Zugriff von Unterwegs ist eine beliebte Möglichkeit, noch schnell seine Termine abzugleichen, die neuesten E-Mails zu beantworten oder an einem wichtigen Dokument weiterzuarbeiten. Der Zugriff geschieht dabei wahlweise von einem Public Access Point via Wireless LAN oder direkt via GSM/UMTS. Damit nicht alle Personen in der Nähe den gesamten Verkehr mithören, wird VPN (Virtual Private Network) verwendet.

Mit dieser Technik werden alle Datenpakete verschlüsselt an den Endpunkt, oft die Firewall des Unternehmens oder eine spezielle VPN-Endpunktlösung, geschickt. Dies ist umso wichtiger, da öffentliche Wireless Access Points keine Verschlüsselung mit WPA oder WEP bieten (siehe auch BlickPunkt KMU 2.05 – Einsatz und Risiken von Wireless LAN). Ist einmal eine VPN Verbindung aufgebaut, ist ein Mithören der Daten nicht mehr möglich. Die Gefahren bei der mobilen Kommunikation liegen aber an einer anderen Stelle.

Schutz des mobilen Gerätes

Es ist erstaunlich, wie unachtsam mit den mobilen Geräten umgegangen wird. Alleine in den Londoner Taxis bleiben jährlich hunderte von PDAs und Laptops liegen. Nicht nur die Vergesslichkeit zeigt seine Wirkung, es werden auch viele Laptops gestohlen. Ein Wiedersehen ist in praktisch allen Fällen ausgeschlossen.

Daher ist es angebracht, die Daten auf diesen Maschinen zu schützen. Ein BIOS-Passwort oder das Anmelde-Passwort von Windows sind dabei kein Schutz. Das BIOS Passwort kann mit einem einfachen Stecker auf dem Motherboard gelöscht werden. Der Schutz von Windows kann mit einer einfachen Diskette und dem entsprechenden Programm innert Sekunden ausgehebelt werden. Nur eine Harddisk- oder Datenverschlüsselung hilft, dass die Daten nicht in fremde Hände geraten.

Der Wert dieser Daten wird oft unterschätzt. Selbst wenn der Inhalt für eine fremde Person keinen direkten Nutzen bringt, ist doch sehr viel Arbeit für die Wiederherstellung (bzw. Neu-Erstellung) notwendig.

Nicht zu vergessen sind aber die lokal gespeicherten Passworte. So werden beispielsweise im Internet Explorer zu zahlreichen Internetseiten die Passworte abgespeichert. Eventuell finden sich hier auch gleich noch die Login-Informationen zum Outlook Web Access (E-Mails) oder gar der VPN-Zugriff in die Firma. Und schon geht es nicht mehr um die auf dem mobilen Gerät gespeicherten Daten, sondern die gesamte Firma ist schutzlos ausgeliefert. Daher gilt immer, wenn ein

mobiles Gerät abhanden kommt, ist umgehend der Netzbetreuer zu informieren, damit dieser den VPN-Zugriff sperren kann.

Schutz des Firmennetzwerkes

Eine VPN-Verbindung ist auf beiden Seiten, dem Client und dem Firmennetzwerk schnell eingerichtet. Wichtig ist aber das Prinzip des Minimalnotwendigen. In vielen Firmen wird der VPN-Zugang auf der Firewall terminiert und von dort kann der VPN-Benutzer auf alle Server und Daten zugreifen. Aber ist dies auch notwendig? In den wenigsten Fällen! Es gilt, auch VPN-Verbindungen in der Firewall einzuschränken, wie dies für andere Zugriffe (zum Beispiel Mail Ein- und Ausgang) geschieht. Die Angriffsfläche muss so klein wie möglich gehalten werden.

Aktualität des mobilen Gerätes

Ein weiterer Punkt, der regelmässig vergessen geht, ist die Aktualität des mobilen Gerätes. Wer lädt schon gerne via GSM die aktuellen Patches von Microsoft herunter? Das bremst nur und macht ein Arbeiten zur Qual. Schnell ist der Download abgebrochen …

Viele Firmen setzen eine zentrale Antivirenlösung ein. Die Pattern (Informationen zu neuen Viren) werden von einem Server an alle Geräte verteilt, auch an die mobilen Geräte. Da diese sich nicht regelmässig einwählen, ist der Aktualisierungsstand oft einige Tage, wenn nicht sogar Wochen, alt. Leicht kann es so geschehen, dass der Notebook zu Hause, in einer anderen Firma oder per Wireless mit dem Internet verbunden wird und sich ein Virus oder ein trojanisches Pferd einnisten kann. Beim nächsten Zugriff in die Firma kopiert sich die Schadsoftware gleich mit und kann eine Epidemie auslösen. Davon sind nicht nur kleine Firmen betroffen, wie vor einiger Zeit die Schweizerische Post bewies. Der Wurm SQL-Slammer hat sich via einen Datenbank-Administrator von zu Hause auf die produktiven Server der Post verteilt. Der Ausfall von Postomaten und PCs war die Folge. Damit die ungenügende Aktualität des mobilen Gerätes nicht zu einem Problem wird, haben einige Hersteller eine Lösung bereit. Vor dem Einwahl in das Firmennetzwerk wird das Gerät untersucht. Erfüllt es die von der Firma definierten Bedingungen, wird die Verbindung zugelassen oder das Gerät zuerst aktualisiert. (Vgl. hierzu auch „Sünder unter der Sonne“, Seite 60)

„Ein weiterer Punkt, der regelmässig vergessen geht, ist die Aktualität des mobilen Gerätes.“

Adminrechte?

Braucht es lokale Administratorrechte auf dem mobilen Gerät? Ein heikles Thema. Nimmt man diese weg, ist ein Aufschrei garantiert. „Ich kann meine Software nicht mehr nutzen“, „ich muss doch beim Kunden Einstellungen verändern“, „ich möchte dies und das ausprobieren“, und so weiter prasselt es auf dem Netzbetreuer ein. Doch es geht auch ohne. Nicht umsonst heissen diese Rechte „Administratorrechte“. Sie sind für den Administrator gedacht. Microsoft bietet zum Beispiel mit dem Tool „runas“ die Möglichkeit, ein Programm mit anderen Rechten zu betreiben. Mit dem Aufruf auf der Kommandozeile kann sogar das Passwort gespeichert werden. Dies ist aber in den wenigsten Fällen notwendig. Mit etwas Geschick findet man schnell heraus, welche Registrywerte und Dateiordner das Programm verwendet.

Zum Autor

Andreas Wisler (Tel. 052 320 91 20), CISSP, ist Geschäftsführer der GO OUT Production GmbH, welche sich mit IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt. Er unterrichtet in der Klubschule Migros den Lehrgang „IT-Security Manager“, darüber hinaus veröffentlicht er regelmässig einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.gosecurity.ch bestellt werden kann. Für Blickpunkt:KMU beleuchtet er in jeder Ausgabe einen neuen Aspekt der IT-Sicherheit.

Kann das Programm darauf zugreifen, ist einem eingeschränkten Arbeiten kein Stein mehr im Weg. Ein Zeitaufwand, der sich in Anbetracht der vielen Gefahren im Internet, garantiert lohnt.

Unbeschwertes Arbeiten

Die VPN-Technik ermöglicht das einfache und schnelle Zugreifen auf interne Daten. Da über diesen Weg aber nicht immer nur Gutes kommt, ist eine umfassende Planung notwendig. Wie erwähnt gilt es, die mobilen Geräte immer auf dem aktuellsten Stand zu halten und diese Daten vor fremden Zugriffen zu schützen. Gleichzeitig muss der Zugriff so eingeschränkt werden, dass nur das erreichbar ist, was auch benötigt wird. Mit der richtigen Planung und einer durchdachten Konfiguration ist dem Arbeiten aus dem Schwimmbad kein Hindernis mehr im Weg. Geniessen Sie die Sonne. ◆