Newsletter 25.07.2008
Ausgabe 1/2008

blossey & partner

Tipps für Ihren Urlaub & den Geschäftsreisenden

- Datendiebstahl im Urlaub
- Wichtige Daten für die Reise sichern

Vorsicht vor Datendiebstahl im Urlaub!

Risiko am Strand: Im Internet surfen an fremdem PC kann gefährlich sein.

Ein Internetzugang in einem Internetcafé findet sich an beinahe jedem Urlaubsort. Das Versenden vertraulicher Daten, zum Beispiel geschäftliche Korrespondenz, Behördenschreiben oder gar Online-Banking sollte man dabei gänzlich unterlassen, sonst droht unter Umständen großer finanzieller Schaden.
Die Uhren ticken im Urlaub anders und auf die Details sieht der Reisende eher selten. Neue und nette Bekanntschaften oder einfach die Tatsache fernab vom Alltag zu sein, verleiten dazu gewohntes Misstrauen schnell mal unter den Tisch fallen lassen, ebenso wie die Klamotten. Wer in dieser Laune mal eben im Internetpoint um die Ecke seinen Kontostand prüfen will, riskiert dabei jedoch schnell mal ein gut aufgeräumtes Konto nach der Rückkehr aus dem Urlaub vorzufinden.
Der Grund dafür liegt in der starken Anfälligkeit dieser öffentlichen PC´s für Schadprogramme jeglicher Art. Die Geräte werden häufig durch Ihre Betreiber nicht auf dem aktuellen Stand gehalten oder gewartet, so dass aktuelle Sicherheitsupdates für Betriebssystem oder die Antivirensoftware (wenn vorhanden) nicht installiert sind. Dabei ist die Gefahr groß, dass ein Programm heimlich im Hintergrund mitläuft und übermittelte Daten aufzeichnet.

Keine vertraulichen Daten übermitteln

Egal, ob Sie Onlinebanking oder einen Einkauf im Internet tätigen wollen, Sie sollten grundsätzlich vermeiden sensible Daten wie Passwörter, Kontoverbindungen oder Kreditkartennummern (PIN`s) einzugeben. Das gilt auch, wenn Sie ihr eigenes Notebook benutzen, denn die öffentlichen Hotspots, über die sich Urlauber ins drahtlose Netz (WLAN) einwählen können, arbeiten meistens unverschlüsselt. Da kann schon der nette Herr am Nebentisch in legerer Urlaubskleidung zum potentiellen Risiko werden, weil er Ihre Daten leicht abfangen kann.

Erst die Arbeit, dann das Vergnügen

Auch wenn nach Ihrem Arbeiten im Netz das Meer und die Wellen locken, ist zunächst einmal Aufräumen angesagt. Dazu gehört die eigenen Surfspuren auf dem Rechner zu beseitigen, sonst könnte der Nächste darauf zugreifen. Dazu empfiehlt es sich immer die Cookies unter Internetoptionen oder unter Extras des jeweiligen Browsers (z.B. Internetexplorer oder Firefox) zu löschen. Auch temporäre Dateien wie Zugänge (Benutzernamen) werden dabei gelöscht, wenn auch hier ein Haken gesetzt wird. Im Bedarfsfall sollte der Reisende sich VOR dem Urlaub über die notwendigen Maßnahmen informieren. UND GANZ WICHTIG: Vor dem Verlassen des öffentlichen PC´s unbedingt prüfen, ob Sie sich auch richtig ausgeloggt haben.
TIP: Die Nutzung des eigenen portablen Webbrowsers auf Ihrem USB-Stick verhindert zumindest das Hinterlassen von Spuren auf dem genutzten Computer.

blossey & partner

Newsletter 25.07.2008
Ausgabe 1/2008

Wichtige Daten für die Reise sichern

Kontrollen durch Zoll: **Wie sie Ihre Daten vor unerwünschter Einsichtnahme schützen können.**

Wenn man weiß, was auf einen zukommen kann, dann kann man sich auch vor Antritt einer Geschäftsreise auf den richtigen Umgang mit den sensiblen Firmendaten und den damit verbundenen personenbezogenen Daten einstellen und entsprechende Maßnahmen treffen. Führende Softwareunternehmen Unternehmen weisen Ihre Mitarbeiter an, sensitive Daten auf dem Firmenserver zu hinterlegen und vom Ausland dann nur über einen sicheren Remotezugang zuzugreifen.

Sensibilisierung erforderlich

Das Zauberwort für Qualität und Sicherheit heißt immer noch Schulung der Mitarbeiter. „Was ich nicht weiß, macht mich nicht heiß“ - trifft hier wohl eher nicht zu, denn sind erst einmal sensitive Informationen bei einer Durchsuchung des Arbeitsnotebooks am Zoll (z.B. US-Zoll) gesichtet, kopiert oder sichergestellt, dürfte der weitere Datenverlauf eher schwerlich nachvollziehbar sein. Der Mitarbeiter oder der Auslandsreisende sollte hinsichtlich relevanter lokaler und internationaler Bestimmungen geschult und geprüft sein, sollte dieser häufig geschäftlichen Auslandsaufenthalt antreten. Dazu gehört nicht nur die Kenntnisnahme des Gesetzestextes, als vielmehr die speziellen Schulungen über Besonderheiten zum Thema.

Sollte es trotzdem zu Kontrollen kommen, bei welchen Daten schließlich kopiert werden, wirkt sich ein unkooperatives Verhalten gegenüber den Behörden zudem schnell negativ aus. Bevor jedoch Passwörter oder PIN´s bekannt gegeben werden, sollte ggf. der Vorgesetzte oder der Sicherheitsbeauftragte des Unternehmens kontaktiert werden.

Bei den aktuellen technischen Möglichkeiten benötigt die vollständige Kopie aller Daten eines Notebooks für die Zollbehörden nur noch etwa 20 Minuten. Es ist davon auszugehen, dass diese Kontrollen künftig verstärkt vorgenommen werden, gerade im Hinblick auf die Bekämpfung der Piraterie beziehungsweise das Anti-Counterfeiting Trade Agreement (ACTA), in dessen Rahmen auch über Durchsuchungen von Datenträgern ohne konkreten Anlass beim Grenzübertritt diskutiert werden soll. Selbst die Übertragung von Funkbefehlen, zum Beispiel zur Selbstzerstörung eines Rechners wird wissenschaftlich längst erarbeitet.

Was Sie dagegen tun können

- Eine Möglichkeit, so offerieren verschiedene Anbieter von Internet-Dienstleistungen, ist die Nutzung von freiem „webspace“ im Internet. Hier hinterlegen Sie verschlüsselt Ihre sensitiven Daten und greifen auf diese erst am endgültigen Zielort ihrer Reise zu.

Achtung! Wir warnen vor dieser Maßnahme, da solche Anbieter von Internetdienstleistungen, in deren Leistungsumfang die Bereitstellung von freiem „webspace“ enthalten ist, ihre Technologie oftmals weder mit entsprechender Datenverschlüsselung noch mit hinreichendem Zugriffsschutz „up to date“ halten.

- Alle sensitiven Daten und Dateien, die vor dem Zugriff Dritter zu schützen sind, sollten gar nicht erst mit auf die Reise genommen werden (Passwörter, E-Banking-Daten, private Fotos, etc.).

- Wird auf dem Gerät durch eine Behörde etwas gefunden, besteht die Möglichkeit, dass Ihr Gerät einbehalten wird. Sie sollten also auf Nummer sicher gehen, dass vor Reiseantritt ein entsprechender Backup (Sicherheitskopie aller Daten) vorgenommen wurde.

- Untersucht werden können alle Geräte, auf welchen Daten gespeichert werden können, also nicht nur Notebooks, sondern auch Digicams, iPods, mobile Festplatten, etc.

- Von Seiten des Unternehmens können für reisende Mitarbeiter unter bestimmten Voraussetzungen sog. Mobile VPN-Verbindungen eingerichtet werden, die dann in Abhängigkeit von firewalls am Firmenserver (mehrere firewalls hintereinander + Clustering) und mit entsprechender Softwareeinrichtung über das Internet sicheren Serverzugriff gewährleisten. Hierzu ist eine fachliche Beratung unerlässlich.

- Speichern Sie Ihre sensiblen Daten extern auf einem portablen Speichermedium (USB-Stick mit großer Speicherkapazität oder auf einer externen Festplatte). Sichern Sie Ihre Daten auf diesen Medien mittels einer effektiven und zertifizierten passwort-geschützten Verschlüsselungssoftware. Diese Medien werden im Falle einer Untersuchung des Notebooks nicht gesichtet.

.