Ralph Lehmann
IT-Sicherheitsanalyse
und Beratung

Ralph Lehmann • IT-Sicherheitsanalyse und Beratung • Kochstraße 34 • 04275 Leipzig

Kochstraße 34
04275 Leipzig

Tel.: (03 41) 3 06 99 05
Fax: (03 41) 3 08 10 31
mobil: (01 70) 3 11 37 35

e-mail: info@ralph-lehmann.de
Web: www.ralph-lehmann.de

Sicherheitshinweise für Anwender von Microsoft Windows

Steuernummer: 231/244/00473
Bankverbindung: Sparkasse Leipzig, BLZ: 860 555 92, Kto-Nr.: 1 895 153 928

Sichern Sie regelmäßig Ihre Daten und bewahren Sie die Backups in einem anderen Raum (besser: in einem anderen Gebäude) auf. Testen Sie hin und wieder, ob die Wiederherstellung der Daten fehlerfrei funktioniert.

Verwenden Sie ausschließlich NTFS als Dateisystem. Vergeben Sie Rechte möglichst restriktiv. Verschlüsseln Sie sensible Daten. Ziehen Sie - insbesondere bei Laptops - eine Verschlüsselung des gesamten Dateisystems in Betracht.

Verwenden Sie nur sichere Kennwörter. Halten Sie Kennwörter unter Verschluss. Verwenden Sie keine Kennwörter gemeinsam mit anderen Personen. Wählen Sie für Anwendungen mit unterschiedlichem Sicherheitsniveau (z.B. unverschlüsselter Emailverkehr und Ihr Bankprogramm) keinesfalls die gleichen Kennwörter.

Meiden Sie unsichere Software und Verfahren (Internet Explorer, Outlook Express, Filesharing, Instant-Messaging etc.). Vermeiden Sie den Besuch dubioser Seiten im Internet.

Betrachten und versenden Sie Email als reinen Text. Signieren Sie Ihre Nachrichten und fordern Sie Ihre Kommunikationspartner auf, dies ebenfalls zu tun. Verschlüsseln Sie vertrauliche Nachrichten. Sorgen Sie dafür, dass Anhänge nicht automatisch geöffnet werden. Holen Sie eine telefonische Bestätigung des angeblichen Absenders ein, falls Sie an dessen Urheberschaft zweifeln. Speichern Sie Anhänge lokal ab und öffnen Sie diese direkt mit der geeigneten Anwendung.

Informieren Sie sich regelmäßig über neu entdeckte Sicherheitslücken Ihres Systems und Ihrer Anwendungen und installieren Sie Sicherheitsupdates zeitnahe. Beenden Sie alle nicht benötigten Dienste. Installieren Sie nur Software, die Sie tatsächlich benötigen. Installieren Sie nur Software aus vertrauenswürdigen Quellen. Verwenden Sie keine illegalen Kopien.

Verlassen Sie sich nicht auf Personal Firewalls. Verwenden Sie diese nur, wenn Sie mit der Filtertechnologie vertraut sind, für die Änderung des Regelwerkes besondere Berechtigungen abgeprüft werden (Kennworteingabe) und zum Einsatz eines solchen Filters keine Alternative verfügbar ist.

Verlassen Sie sich nicht auf Virenscanner. Denken Sie daran, dass Virenschutz im Kopf des Anwenders beginnt, dass ein Virenscanner prinzipiell nicht vor Unachtsamkeit schützen kann und dass zwischen der erstmaligen Entdeckung bösartiger Software und der Aktualisierung Ihres Scanners immer eine gewisse Zeit vergeht. Informieren Sie sich über die Wirkungsweise der einzelnen Typen von Schadsoftware.

Versuchen Sie nicht, im Falle einer Infektion mittels entsprechender Tools die Schadsoftware von Ihrem Rechner zu entfernen. Bedenken Sie, dass die Mehrzahl der heute verbreiteten Schädlinge weitere - auch legale - Software nachlädt, die von Virenscannern prinzipiell nicht erkannt werden kann und trotzdem zur Fernsteuerung Ihres Rechners missbraucht werden kann. Eine Entfernung kann deshalb nur dann erfolgreich sein, wenn die Schadsoftware mit Sicherheit keine weiteren Komponenten nachlädt. I.d.R. ist deshalb nach einer Kompromittierung immer die Neuinstallation des Betriebsystems und aller Anwendungen erforderlich.

Rufen Sie sicherheitskritische Seiten nicht über Links auf. (Phishing-Gefahr!) Besuchen Sie sicherheitskritische Seiten mit einem frisch gestarteten Browser. Achten Sie darauf, dass sicherheitskritischer Datenverkehr ausschließlich verschlüsselt erfolgt. Prüfen Sie Zertifikate sorgfältig.

Arbeiten Sie nicht als Administrator sondern immer als Benutzer mit den geringst möglichen Rechten. Passen Sie Ihr System so an, dass Ihre Software auch für normale Benutzer ausführbar ist. Benutzen Sie "Ausführen als" oder "runas", falls Ihr System nicht entsprechend angepasst werden kann.

Misstrauen Sie unbekannten Datenträgern. Deaktivieren Sie die Autostartfunktion Ihres DVD/CD-ROM-Laufwerkes.

Achten Sie auf die physische Sicherheit Ihres Computers. Denken Sie daran, dass der Zugriff auf die dort gespeicherten Daten i.d.R nicht verhindert werden kann, wenn für einen Angreifer die Möglichkeit zum lokalen Zugriff besteht.

Denken Sie daran, dass die Konfiguration eines Microsoftsystems nach der Installation nicht sicher ist. Nutzen Sie Sicherheitsvorlagen und Tools wie z.B. den MBSA oder die BSI OSS Security Suite zur Optimierung der Sicherheit. Nutzen Sie die verfügbaren Angebote zur externen Suche nach offenen Ports sowie zur Aufdeckung von Sicherheitslücken in Browsern und Mailclients.

Stand: 08.09.2007
Die jeweils aktuellste Version dieses Dokuments können Sie unter
www.ralph-lehmann.de/Service___Downloads/service___downloads.html
herunterladen.