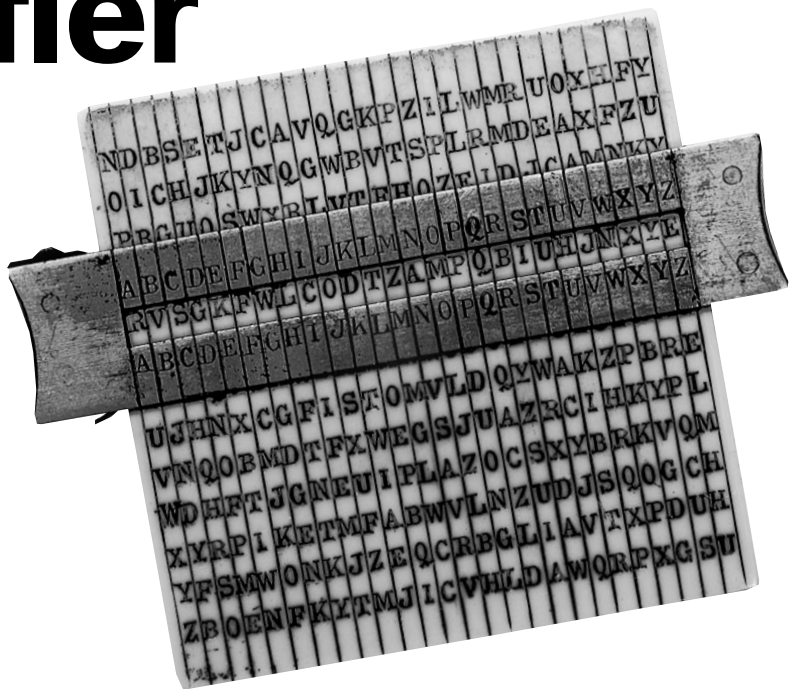
Hintertüre für Schnüffler

Windows NT gilt als besonders sicheres Betriebssystem. Tatsächlich taugt seine Verschlüsselung weniger, als sie verspricht. Schuld ist die amerikanische Regierung.



Etwas zu verbergen haben nicht nur Kriminelle. Eine vertrauliche Nachricht für einen Kollegen, ein Kostenvoranschlag, die Umsatzzahlen des letzten Quartals – nichts Ungesetzliches oder Unsittliches also, aber auch nichts, das in die Hände Fremder oder gar der Konkurrenz gelangen sollte. Wie gut, daß es Verschlüsselungsverfahren gibt, die dafür sorgen, daß solche Daten und Nachrichten geheim bleiben oder – oft noch wichtiger – nicht verändert werden können, ohne daß es auffällt.

Und noch schöner ist, daß das dazu nötige Werkzeug gleich frei Haus mit dem Betriebssystem kommt: Microsoft hat in die neue Version 4.0 von Windows NT eine sogenannte CryptoAPI integriert. Diese Programmierschnittstelle stellt Software-Entwicklern die Ver- und Entschlüsselung von Daten als fest integrierte Betriebssystemfunktionen zur Verfügung, so daß jede Anwendung leicht mit Sicherheitsfunktionen ausgestattet werden kann.

NT-Sicherheit ausgehebelt

Schöne heile NT-Welt also? Leider nein. Die Sache hat einen Haken: Was Microsoft frei Haus liefert, ist weit von dem entfernt, was sicherheitsbewußte Anwender haben wollen, nämlich eine praktisch nicht zu brechende Verschlüsselung.

Schuld ist ein amerikanisches Gesetz, das die Ausfuhr von Kriegswaffen reguliert: Es stuft kryptographische Programme als militärische Produkte ein und unterwirft deren Export schweren Auflagen. Solche Software darf nur das Land verlassen, wenn ihre Schlüssel nicht zu lang sind, sich also mit vertretbarem Aufwand knacken lassen. Gerechtfertigt wird dieses Vorgehen mit dem Kampf gegen das organisierte Verbrechen.

Eine Schlüssellänge von 40 Bit gilt derzeit als Schmerzgrenze. Ihr verdankt die Öffentlichkeit einen Anhaltspunkt für die Leistungsfähigkeit der staatlichen Codeknacker: 40 Bit sind für technisch gut ausgestattete Spezialisten offensichtlich längst keine harte Nuß mehr.

Microsoft beugt sich

Unter dem Druck der Exportvorschriften arbeiten Microsoft wie auch andere US-Unternehmen – nicht nur in den Exportversionen ihrer Software – mit einer Schlüssellänge von maximal 40 Bit. Das dabei eingesetzte DES-Verfahren nutzt normalerweise 64 Bit lange Schlüssel, von denen 56 Bit für die tatsächliche Verschlüsselung verwendet werden.

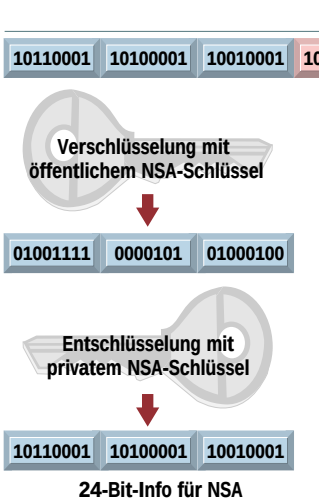
Je länger der Schlüssel, desto größer der Aufwand beim Knacken: Nur zehn Bits mehr verlängern die dazu benötigte Zeit um etwa den Faktor 1000. Ein sicherer Schlüssel muß so lang sein, daß auch die schnellsten verfügbaren Rechner in vernünftiger Zeit nicht in der Lage sind, den Schlüssel zu finden. So schlug denn eine Gruppe von Kryptographen und Computerwissenschaftlern Anfang diesen Jahres vor, künftig mindestens 75 Bit lange Schlüssel zu verwenden. Zuverlässigen Schutz über die nächsten 20 Jahre bieten Schlüssel mit mindestens 90 oder besser 128 Bit, so die Experten. Netscape beherrscht diese Sicherheitsstufe schon heute, in einer Version allerdings, die für den Export aus den USA tabu ist.

So verschlüsselt Windows NT

Das Kernstück der Verschlüsselungseinheit von Windows NT ist der Cryptographic Service Provider (CSP). Ein CSP ist im Prinzip eine zum Betriebssystem gehörende Programmdatei, die ein kryptographisches Verfahren umsetzt. Windows NT delegiert jeden Aufruf einer CryptoAPI-Funktion an sie.

Der Clou an der Sache: CSPs sind auswechselbar. Welches Verfahren die Verschlüsselung übernimmt, hängt von der Installation des Betriebssystems und des jeweiligen CSP ab. Microsoft liefert Windows NT 4.0 standardmäßig mit einem CSP aus, der mit dem heute sehr verbreiteten Verschlüsselungsalgorithmus Data Encryption Standard (DES) arbeitet.

Amerikanischer Schlüsseltrick



Quelle: Lotus

Die Lotus-Lösung: Unangetastet bleibt der 40 Bit lange, rot markierte Teil des Schlüssels, der dem Anwender die Vertraulichkeit seiner Botschaft gewähren soll. Der „überstehende" Teil wird mit dem öffentlichen Schlüssel der National Security Agency (NSA) codiert und zur Nachricht gepackt. Mit ihrem geheimen Schlüssel ist auf diese Weise nur die NSA in der Lage, diesen Teil des 64 Bit langen Anwenderschlüssels bequem zu rekonstruieren.

0 Kuhhandel erlaubt

Damit die im Exportfall nur mit schwachem Kryptoschutz ausgelieferte Software aus den USA jedoch nicht aus Furcht vor Spionage verschmäht wird, akzeptiert die amerikanische Regierung einen technisch aufwendigeren Kuhhandel: Längere Schlüssel sind o.k., wenn der 40 Bit übersteigende Teil des Schlüssels bei einer US-Behörde hinterlegt wird. Dieses Vorgehen soll amerikanischen Polizeibehörden und Geheimdiensten den bequemen Zugriff auf verschlüsselte Daten sichern, technisch weniger gesegnete Angreifer aber außen vor lassen.

Wie man das „Hinterlegen" der Schnüffelinformation in der Praxis bei ständig neu generierten Schlüsseln technisch lösen kann, hat Lotus in ihrer Software Notes gezeigt (siehe Grafik): Das Programm packt die ungesetzlichen Bits des kompletten Schlüssels – ebenfalls per Kryptotechnik – in einer nur für amerikanische Behörden lesbaren Form zur verschlüsselten Nachricht dazu. Der gewöhnliche Industriespion müßte den langen Schlüssel knacken; die amerikanischen Staatsschützer müssen sich nur noch mit 40 Bits herumplagen.

0 Zensur für Entwickler

Mit dem Manko der durchlöcherten Vertraulichkeit sieht sich auch Microsoft mit dem Cryptographic Service Provider in Windows NT konfrontiert. Europäische Anwender müssen sich also mit einer 40-Bit-Verschlüsselung zufriedengeben, wenn sie auf die integrierten Verschlüsselungsmethoden zurückgreifen. „Verschlüsselungsprodukte sind in den USA eben ab einem bestimmten Level nicht mehr frei verfügbar", kommentiert Thomas Baumgärtner, Pressesprecher bei Microsoft in Unterschleißheim, wenig begeistert die Situation.

Würde die abgeschwächte Sicherheit nur Spezialsoftware zum Verschlüsseln von Dateien und ähnliche Anwendungen betreffen, wäre guter Rat leicht zu erteilen: einfach einheimische Produkte nehmen. An einem Betriebssystem wie Windows NT kommen aber viele Firmen nicht vorbei. Die Entwickler greifen zu den eingebauten schwachen Verschlüsselungsroutinen, weil sie auf diese Weise ihr Produkt mit „fertigen" kryptographischen Sicherheitsfunktionen ausstatten können, ohne selbst solche Algorithmen programmieren zu müssen. Dabei treten auch keine Lizenzprobleme auf, da die Kryptofunktionen fester Bestandteil des Betriebssystems sind.

Angesichts der Exportreglementierungen für die „starke" Kryptographie ist damit zu rechnen, daß sehr viele amerikanische Softwarehäuser bei Programmen für Windows NT 4.0 darauf verzichten werden, eigene Kryptographie in ihre Produkte einzubauen. Statt dessen werden sie sich der CryptoAPI bedienen.

Einen Ausweg aus dem Dilemma könnten theoretisch europäische Softwarehersteller weisen, die eigene CSPs für NT entwickeln; ausgestattet etwa mit längeren Schlüsseln, anderen Algorithmen oder mit zusätzlicher Hardware. Doch auch diesen Weg versperrt die Politik: Jeder CSP muß, um in Windows NT 4.0 integriert werden zu können, von Microsoft zertifiziert werden. Bei dieser Gelegenheit wird im amerikanischen Redmond geprüft, ob die gelieferte Programmbibliothek fehlerfrei mit NT zusammenarbeitet. Die DLL wird dann mit einem geheimen Schlüssel versehen, wodurch Windows NT die Datei als legitimen Cryptographic Service Provider erkennt und einbindet. Damit wird der neue CSP zu einem festen Bestandteil des Betriebssystems NT, der über die CryptoAPI angesprochen werden kann – und fällt damit prompt wieder unter die einschlägigen Exportbestimmungen der USA – auch wenn der CSP von einem europäischen Anbieter stammt.

Hiesige Anwender amerikanischer Software mit integrierten Verschlüsselungsfunktionen müssen sich entweder mit dem – wenigsten vor US-Behördenaugen – auf 40 Bit geschrumpften Sicherheitsniveau zufriedengeben oder für zusätzliches Geld hierzulande entwickelte Sicherheitsprodukte darüberstülpen (siehe Kasten). Nur so kommen sie in den Genuß einer Verschlüsselung, die dem Stand der Kunst entspricht.

Ulrike Pröller, Jan Vollmuth (kk)

So können Sie sich schützen

Müssen Windows-NT-Anwender auf eine sichere Verschlüsselung ihrer Daten verzichten? Nein. Software-Entwickler sind nicht gezwungen, auf die via CryptoAPI im CSP angebotenen Funktionen zurückzugreifen. Wer den Aufwand für Eigenentwicklungen scheut oder das Know-how nicht hat, kann es sich bei Spezialisten einkaufen.

So will beispielsweise Utimaco im Frühjahr 1997 das Produkt Safeguard Easy vorstellen, das die FAT- und NTFS-Partitionen (NT File System) von Windows NT sektorweise verschlüsselt. Dabei verwendet es die Verschlüsselungsalgorithmen Blowfish, Stealth und DES mit voller Schlüssellänge. „Dabei wird kein API verwendet, weder von Microsoft noch ein anderes", betont Pressesprecherin Jutta Stolp. Im Gegenteil: „Über ein API ließe sich diese systemnahe Form der Verschlüsselung gar nicht realisieren."

Adressen: Microsoft, Edisonstr. 1, 85716 Unterschleißheim, Tel. (089) 3176-0

Lotus, Baierbrunner Str. 35, 81379 München, Tel. (089) 78509-0

Utimaco Safeguard Systems, Dornbachstr. 30, 61440 Oberursel, Tel. (06171) 917-0