

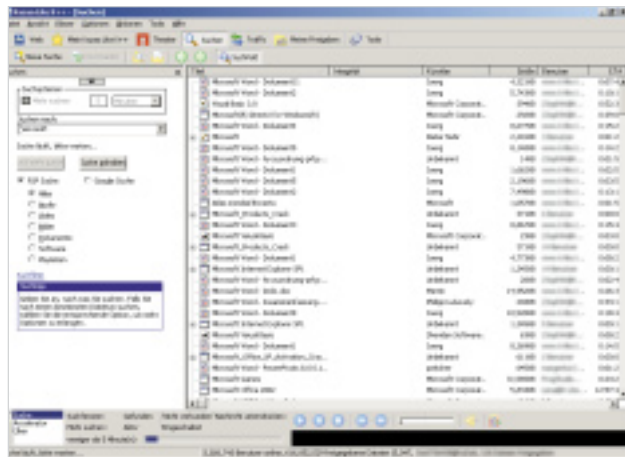
dieser Aufzählung – es könnte die Anwender verschrecken. Gerold Hübner, Sicherheitschef bei Microsoft Deutschland, versichert: „NGSCB hat nicht zum Ziel, die Durchsetzung von Leistungsschutzrechten zu ermöglichen.“ Allerdings, räumt Hübner ein, sei eine DRM-Anwendung sehr viel sicherer, wenn sie im geschützten Bereich des Rechners ablaufe. Anders ausgedrückt: Es ist nicht das Ziel, aber es wird erreicht.

NGSCB braucht neue Hardware

Auf herkömmlichen Rechnern arbeitet NGSCB nicht, es fehlen die notwendigen sicheren Hardwarekomponenten. Dazu zählen: ein neuer Prozessor und Chipsatz; ein Sicherheits-Chip auf dem Motherboard, Secure Service Component (SSC) genannt, und neue Tastaturen, Grafikkarten und Schnittstellen, die Datenverschlüsselung unterstützen. Longhorn selbst soll auch auf alten PCs laufen, doch die neuen NGSCB-Anwendungen werden den Dienst verweigern, sobald auch nur eine unsichere Komponente im Spiel ist.

So weit, so harmlos. Doch die kritischen Aspekte der Technologie blendet Microsoft geflissentlich aus, etwa die Frage der Zertifizierung. Prinzipiell kann es auch „böse“ NGSCB-Programme geben, trojanische Pferde etwa. Damit der Anwender diese von den „guten“, vertrauenswürdigen Programmen unterscheiden kann, soll es eine optionale Zertifizierung geben; ähnlich wie heute schon bei Treibern. Microsoft betont den freiwilligen Charakter der Zertifizierung. In der Praxis könnte daraus dennoch ein Zwang erwachsen. Windows wird mit an Sicherheit grenzender Wahrscheinlichkeit eine Option anbieten, die nicht zertifizierten Programmen die Starterlaubnis verweigert – und Sysadmins werden diese Funktionen nutzen, so wie sie heute schon oftmals die Installation nicht zertifizierter Treiber unterbinden. Auch das ist nur eine Windows-Option.

Zu bezweifeln ist ferner, dass nicht zertifizierte Programme auf Dateien zugreifen können, die zertifizierte Programme angelegt haben. Das widerspricht einem der vier wesentlichen NGSCB-Aspekte, der Attestation (siehe „Die Grundlagen“ auf dieser Seite).



Tauschbörsen-clients wie Kazaa Lite laufen laut Microsoft auch unter Longhorn – dafür gibt es den ungeschützten Modus.

Stellt Scientology Zertifikate aus?

Microsoft will angeblich keinesfalls die Rolle der zentralen Zertifizierungsstelle übernehmen – zu leicht würde das Unternehmen zur Zielscheibe von Kartellrechtsklagen. Wer aber dann? Microsofts offizielle Position: Viel zu früh, um darüber zu diskutieren. Einige Mitarbeiter nennen staatliche oder gemeinnützige Einrichtungen als mögliche Stellen, beispielsweise auch Stiftungen oder Kirchen. Institutionen eben, denen die Anwender vertrauen (sollen). Wie das Ganze in der Praxis aussehen soll, bleibt

ein Rätsel. Wird der heimische PC-User einem Zertifikat vertrauen, das die syrische Regierung ausgestellt hat? Darf auch Scientology ran? Immerhin ist die Sekte in den USA eine anerkannte Kirche. Eine realistischere Variante scheinen kommerzielle Zertifizierungsstellen zu sein.

Offen ist, wie viel eine Zertifizierung kosten wird – zu viel für Open-Source-Projekte? Wird daher Windows künftig bei jedem Start eines Open-Source-Programms vor dessen Benutzung warnen – da es ja nicht zertifiziert ist? Diktiert

Das sind die Grundlagen von NGSCB

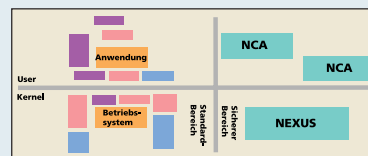
NGSCB baut auf vier Säulen auf: einem sicheren, abgeschotteten Computerbereich (Process Isolation), sicherer Datenein- und -ausgabe (Trusted Path), versiegeltem Speicher (Sealed Storage) und Beglaubigung (Attestation), also Zertifizierung von Benutzern, Anwendungen und Dokumenten. Ein konkretes Beispiel: Fängt sich ein Anwender auf einem herkömmlichen PC einen Trojaner ein, kann dieser die volle Kontrolle über das System übernehmen: Tastatureingaben mitprotokollieren, Antivirenprogramme ausschalten, gespeicherte Daten ausspähen, manipulieren oder an Dritte verschicken – und das alles, ohne dass der Anwender etwas davon mitbekommt.

Auf einem NGSCB-System kann das auch weiterhin passieren, allerdings nur bei alten Anwendungen. Eine neue NGSCB-Anwendung, auch Nexus Computing Agent (NCA) genannt, arbeitet im „Trusted Mode“. Sie wird in einen abhörsicheren

Speicherbereich geladen, empfängt verschlüsselte Tastatureingaben, speichert die Daten verschlüsselt und erlaubt die Weiterverarbeitung der Dateien nur entsprechend zertifizierten Anwendungen. Der Trojaner bekommt von alledem nichts mit, er bleibt aus diesem Hochsicherheits-trakt ausgesperrt.

Sichere Anwendungen haben keinen direkten Hardware-Zugriff. Sie können sich auch nicht gegenseitig beschneffeln oder manipulieren. Der Sicherheitskern, Nexus genannt, soll manipulierte Anwendungen erkennen und ihre Ausführung stoppen. Nexus ist für die Verwaltung sämtlicher NGSCB-Anwendungen zuständig. Er kann direkt mit dem

Betriebssystem starten, aber auch nachträglich ge- und entladen werden. Microsoft liefert mit Longhorn einen Sicherheitskern mit, Fremdhersteller sollen aber in der Lage sein, ihren eigenen Nexus zu schreiben.



Bisherige Programme werden unter Longhorn weiterhin laufen, doch nur NCAs nutzen die neuen Sicherheitsfeatures.