CORONIC
Software & Security

Sicher arbeiten in kompromittierten IT-Umgebungen

Frank Bock

Online-Banking-Schnittstellen sind ein beliebter Angriffspunkt. Um sichere Transaktionen selbst auf bereits infizierten Computern durchführen zu können, hat CORONIC die PROTECT-Technologie entwickelt. Als ausführbare EXE-Datei kann das Schutz-Programm auf jedem Rechner ohne Installation eingesetzt werden. Weder das Hooking zentraler Systemfunktionen noch Echtzeit-Trojaner vermögen den auf vier Säulen basierenden Schutz zu überwinden.

Im letzten Jahr hat die Zahl der Personalcomputer in Deutschland mit 46 Millionen registrierten Geräten die Zahl der zugelassenen Pkw überstiegen. Das Internet ist vom Tummelplatz für Computerfreaks und Wissenschaftler zum Online-Medium für alle Deutschen geworden. Eine Bestellung bei Amazon, eine Überweisung im Online-Banking und das Ummelden der Wohnung via Internet sind heute genauso einfach wie Autofahren. Leider hat der große Erfolg der Online-Geschäftsprozesse auch seine Schattenseiten: Mit jedem umgesetzten Euro und mit jedem online bestellten Artikel wird der private PC mehr und mehr zum Lieblingsziel von Computerkriminellen und Trickbetrügern.

Fragt man die Hersteller von Sicherheitssoftware, so gibt es natürlich für jeden Computerschädling ein geeignetes Sicherheitspaket, für jeden Virus einen Antivirus und für jede Sicherheitslücke die passende Firewall. Trotzdem nimmt die Zahl der Computerviren und der ausspionierten PC weiter zu. Hierbei liegen Banken nach wie vor im Fokus der Internet-Kriminellen, denn sie allein verfügen über einen massentauglichen Geschäftsprozess, aus dem man direkt Bargeld entwenden kann: das Online-Banking.

Autor:
Dr. Frank Bock ist Geschäftsführer der CORONIC GmbH

Die Entwicklung des Online-Bankings

Banken sind schon seit zehn Jahren mit aggressiver Schadsoftware, Spionage-Programmen und den kriminellen Methoden der Internet-Mafia vertraut. Im Rahmen ihres Abwehrkampfes wurden Software und Verfahren mehrfach ausgetauscht. Die Authentifizierung des Nutzers wurde verbessert, Zertifikate eingeführt und teilweise auf externe Hardware ausgelagert. Am Ende wurden mathematisch nicht mehr knackbare Zwei-Schritt-Transaktionssysteme eingeführt, um dem Treiben der Banking-Trojaner ein Ende zu setzen. Beispielsweise setzten die VR-Banken auf smartTANplus oder die Sparkassen auf chipTANcomfort. Inzwischen sind jedoch auch diese Systeme überlistet worden, denn auf dem infizierten PC kann der Trojaner schalten und walten wie er möchte. Er kann die Bildschirmdarstellung beliebig manipulieren und so den Nutzer zum Aushebeln aller Sicherheitsfunktionen missbrauchen.

Wenn der PC erst einmal infiziert und der Echtzeit-Trojaner aktiv ist, lässt sich auch mit noch so viel Schutzsoftware und Sicherheitsverfahren kaum noch etwas gegen diese Schädlinge unternehmen. Das umso mehr, als sich Trojaner heute mit Rootkit-Technologie vor der Entdeckung verbergen und erst dann aktiv werden, wenn es darum geht, die Manipulation tatsächlich durchzuführen. Der Trick ist immer der gleiche, solange der Trojaner die Bildschirmanzeige manipulieren kann, kann er den Nutzer zu jedem beliebigen Fehlverhalten verleiten. Am Ende muss das Kryptoverfahren gar nicht gebrochen werden, der Nutzer betrügt sich praktisch selbst.

Gelungene Manipulation

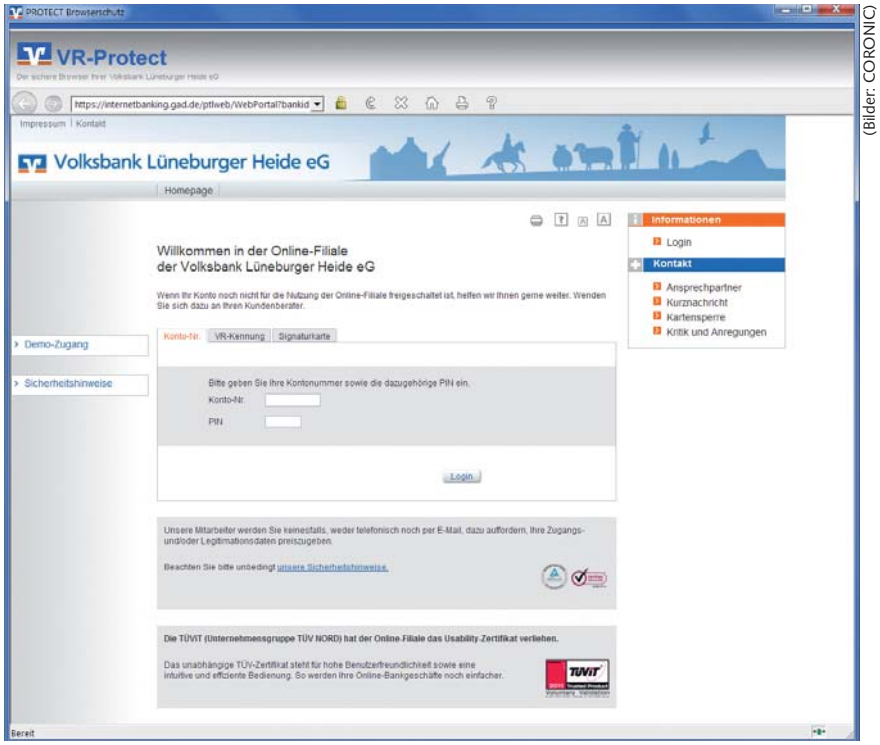
Moderne Echtzeit-Trojaner wie Zeus oder SpyEye umgehen die SSL-Verschlüsselung von Windows und manipulieren den dargestellten Browserinhalt so glaubwürdig, dass der Nutzer sich gewissermaßen selbst beklaut. Ein Beispiel: Herr Müller meldet sich beim Online-Banking an und sieht, dass der Kontostand 5.000 Euro zu hoch ist. Diesen Umstand erklärt ein vorgetäuschtes elektronisches Schreiben seines Bankberaters: Ihm sei versehentlich ein Betrag der Firma XY gutgeschrieben worden, ob Herr Müller wohl so nett wäre, das Geld noch heute zurück zu überweisen. „Kein Problem“, sagt sich Herr Müller und überweist die 5.000 Euro zurück. Erst beim nächsten Gang zum Kontoauszugsdrucker in den Geschäftsräumen der Bank erfährt er, dass es diese Überweisung und das Schreiben des Bankberaters in Wahrheit nie gegeben hat. Technisch hatte Müller alles richtig gemacht. Er hat sich korrekt angemeldet und authentifiziert. Er hat das vorgesehene Verschlüsselungsverfahren der Bank eingesetzt und sich sogar von der Echtheit der SSL-Zertifikate überzeugt.

Ein Blick auf die aktuelle Situation im Online-Banking gibt einen guten Vorgeschmack, was anderen Geschäfts-Prozessen in den kommenden Jahren noch bevorstehen mag. Ob das aktuelle Zusammenspiel aus Schutzsoftware, Verfahren und Kryptographie wirklich sicher ist, bemerkt man erst, wenn intelligente und organisierte Angreifer in Heerscharen dem System zu Leibe rücken. Es ist daher dringend geraten, die eigenen Anwendungen als zentrales Element der Kommunikation gegen gezielte Angriffe mit Spionageprogrammen zu schützen. In einer Zeit, in der Baukasten-Trojaner die Netzwerkkommunikation der wininet.dll verbiegen, Tastatureingaben ausspionieren und alle dargestellten Internetseiten manipulieren, helfen einem auch Verschlüsselung, Secoder-Hardware und Antivirenlösungen nicht mehr weiter.

PROTECT: Vier Säulen für die Prozesssicherheit

Die PROTECT-Technologie von CORONIC ist genau an dieser Stelle besonders stark. Sie bringt ihre eigene Netzwerkschicht, eigene Protokolle und eigene Verschlüsselungsmechanismen mit und kann so weder durch das Hooking zentraler Systemfunktionen noch durch Echtzeit-Trojaner beeinträchtigt werden. PROTECT ist das perfekte Instrument, um eine sichere Transaktion auf einem bereits infizierten System durchzuführen. Es spielt dabei überhaupt keine Rolle, welche Art von Trojaner sich auf dem Arbeitsplatz bereits eingenistet hat, der Prozess bleibt immer sicher.

Die technischen Schutzverfahren für das Programm PROTECT beruhen im Wesentlichen auf vier Säulen. Jede einzelne Säule ist durch mehrere hintereinander gestaffelte technische Methoden abgeschottet. Der Charme des Produktes liegt hierbei sowohl in der Einzigartigkeit der eingesetzten Techniken als auch in der Kombination mehrerer voneinander unabhängiger Sicherheitsmechanismen zur Härtung jedes einzelnen Angriffspunktes. Dadurch bleibt der Schutz erhalten, auch wenn eine einzelne Methode oder gar eine ganze Sicherheitssäule angegriffen werden sollte.



(Bilder: CORONIC)

PROTECT Browserschutz im Einsatz bei der Volksbank Lüneburger Heide

- **Säule 1: Programm- und System-härtung**

Mehrere Anti-Hacking-Mechanismen kontrollieren die Funktion und Unversehrtheit von Browser und Programmcode. Leicht angreifbare Betriebssystemkomponenten wie die Netzwerkzugriffsschicht inklusive SSL-Layer werden durch sichere PROTECT-Komponenten zur Laufzeit ersetzt. Weitere Kontrollmechanismen überwachen die Injektion von Fremd-DLL-Dateien, verhindern Windows-Hooks und kontrollieren aktive Threads.

- **Säule 2: Zertifikats-Überwachung**

Die SSL-Zertifikat-Whitelist überwacht die SSL-Zertifikate auf Signatur-Basis. Nur die bekannten, fest einprogrammierten Zertifikatssignaturen von Servern werden bei den obligatorischen SSL-Verbindungen akzeptiert. So wäre nicht einmal ein derzeit nur theoretisch möglicher Pre-Image-Angriff über den HashCode des Zertifikats erfolgreich.

- **Säule 3: Whitelist-Verfahren**

Die URL-Whitelist führt eine Kontrolle auf Domain-Namen-Basis durch; die IP-Adress- und -Port-Whitelist auf IP-Ebene. Dadurch kann der gesamte Internet-Verkehr auf die wenigen bekannten „guten" Internetseiten des Unternehmens beschränkt werden.

- **Säule 4: Beste Usability**

Das Schutz-Programm wird als ausführbare EXE-Datei geliefert. Es muss weder installiert noch konfiguriert werden. Ebenso sind keine Administrator-Rechte erforderlich. Die Anwendung agiert minimal-invasiv und verändert nichts auf dem zu schützenden Arbeitsplatz. Die PROTECT-Schutzfunktionen sind beim Programmstart sofort aktiv.

Über die CORONIC GmbH

CORONIC ist auf dem Gebiet der Browser- und Systemhärtung sowie der Absicherung von Webframeworks langjährig erfahren. Zu den Kunden des Unternehmens gehören verschiedene deutsche und ausländische Großbanken sowie namhafte Konzerne aus Industrie und Rüstung.