LANline

März 2009

konradin mediengruppe

Das Magazin für Netze, Daten- und Telekommunikation www.lanline.de

Mobile Security und Remote Access

Anwendungssicherheit

Data Loss Prevention

mit Marktübersicht Verschlüsselungs-Tools für mobile Endgeräte

Sonderdruck für Giritech

Anwendungsbindung

Über das Internet auf Programme und Daten des Unternehmens zugreifen zu können, gehört selbst bei den kleinsten Unternehmen heute zum Standard. Bei der Suche nach einfachen und sicheren Remote-Access-Lösungen bietet sich das System G/On von Giritech als eine spannende Alternative zu VPN & Co. förmlich an.

Typischerweise werden Verbindungen von Heimarbeitsplätzen oder mobilen Geräten auf ein Firmennetzwerk per VPN (Virtual Private Network) auf Basis von IPSec oder SSL aufgebaut. Dabei kommt eine direkte Verbindung zwischen den Nodes zustande. Außerdem ist der technische und administrative Aufwand beim Aufbau einer VPN-Umgebung mit DMZ, Firewall, Authentication-Server, Certificate-Server, IPSec-VPN-Terminator, SSL-VPN-Applikation und eventuell Intrusion Detection System (IDS) hoch und verlangt Spezialwissen. Hinzu kommt, dass aufgrund der vielen benötigten Funktionen die DMZ zunehmend zu einem Zweitnetzwerk verkommt, auch wenn dort höhere Sicherheitsmaßstäbe gelten. Eine weitere Schwierigkeit beim Einsatz von IPSec-VPN stellt die Installation des Clients selbst dar. Für die Einrichtung werden üblicherweise Administrationsrechte auf dem Rechner verlangt, somit fällt der sofortige Einsatz beliebiger PCs aus. Bei SSL-VPN reduziert sich der Installationsaufwand zwar auf die Einrichtung des Plug-ins für den Browser, doch auch über dieses Recht verfügt ein normaler Benutzer nicht immer.

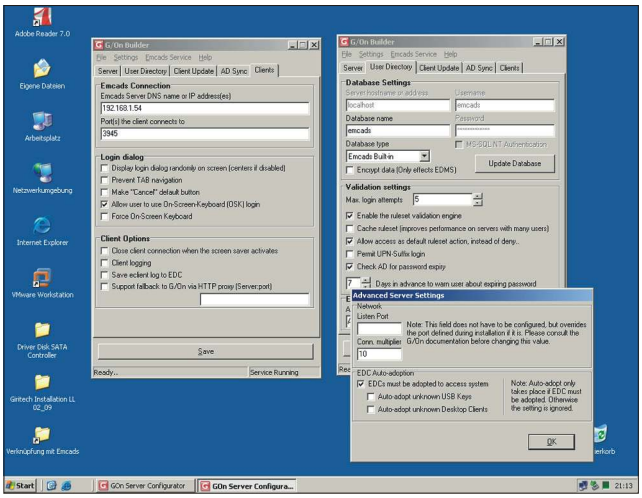
Das Produkt G/On der dänischen Firma Giritech versucht, dieser Problematik bei der Einrichtung von VPN-Zugriffen mithilfe der patentierten EMCADS-Technik (Encrypted Multipurpose Content and Application Deployment System) elegant aus dem Weg zu gehen. G/On ist eine Server-Software, die Anfragen von Clients über eine gesicherte Verbindung an einem einzigen freigeschalteten Port entgegennimmt und wie eine Art Proxy-Server weiterreicht. Die Client-Software wird dabei typischerweise von einem USB-Stick aus gestartet, auf dem alle benötigten Programme abgelegt sind. Die Besonderheit im System G/On stellt dabei die Art der Verbindung selbst dar. Dabei handelt es sich um eine Verbindung auf Applikationsebene anstelle einer klassischen VPN-/TCP-Verbindung.

Einfache Installation

Das für die Teststellung verwendete Paket von G/On besteht aus zwei 1-GByte-USB-Sticks, einer deutschsprachigen Kurzanleitung, einer Installations-CD und einem Freigabeschlüssel, der uns per E-Mail erreichte. Das gesamte Material findet problemlos in einer Kartongröße einer Netzwerkkarte Platz.

Als Grundlage benötigt G/On eine Microsoft-Windows-Server-2000-SP4- oder Server-2003-SP1-Server-Installation auf einer typischen Standardhardware. Der Hersteller empfiehlt die Einrichtung auf einer dedizierten Server-Hardware oder den Betrieb auf einem Proxy- oder Terminal-Server. Von der Installation auf einem Domänen-Controller oder Web-Server rät der Hersteller indes ab. Die Hardwareempfehlungen des Herstellers beschreiben ein 3-GHz-Single-Core-Pentium-System mit 512 MByte Arbeitsspeicher für maximal 100 Benutzer und ein Doppelprozessorsystem mit 3 GHz und 2 GByte RAM für maximal 500 gleichzeitig aktive Anwender. Je nach Art der Einrichtung ist auf der Server-Seite der Einsatz eines USB-Tokens erforderlich – bei der von uns betrachteten Version handelte es sich um eine „Token-less-Installation".

Die Installation der Software selbst ist innerhalb weniger Augenblicke geschehen. Für die Konfiguration und die Ersteinrichtung der Applikationen benötigten wir im Test gerade einmal eine halbe Stunde. Die Dialogfenster des G/On-Administrationsfensters sind weitgehend selbsterklärend und müssen lediglich Register für Register von links nach rechts abgearbeitet werden. Leider wird der Anwender nicht vor Fehleingaben bewahrt – wird beispielsweise die öffentliche IP-Adresse des G/ON-Servers nicht eingegeben, so hindert die Software den Anwender nicht daran, den Konfigurationsvorgang abzuschließen. Der Support des Deutschlandvertriebs konnte in einer Telefonsitzung das Problem innerhalb weniger Minuten eingrenzen, und die Software ließ sich wie geplant verwenden.



Bevor eine gesicherte Verbindung zwischen Client und Server aufgebaut werden kann, ist wie üblich eine Konfiguration notwendig. Im Gegensatz zu der von VPN-Produkten ist dies bei G/On jedoch in rund einer halben Stunde abgeschlossen.

Alle Daten wie Zugriffsversuche, Verbindungsinformationen oder Einstellungen werden in einer mitgelieferten Datenbank abgespeichert. Auf Wunsch ist auch die Nutzung einer vorhandenen MySQL- oder Microsoft-SQL-Installation möglich.

Die Konfiguration beginnt mit der Erstellung eines privaten und eines öffentlichen

Schlüssels. Diese können entweder direkt per Tastatur eingegeben oder – einfacher – mithilfe einer Schaltfläche automatisch erzeugt werden. Es folgen weitere allgemeine Grundeinstellungen wie das Administrationskonto für G/On, Zielpfade und Active-Directory-Zugriffsinformationen. Der Abgleich mit dem Active-Directory-Verzeichnisdienst ist optional und vereinfacht die Bereitstellung bei einer größeren Nutzeranzahl. Mehrere spezielle Einstellungen wie beispielsweise das Unterbrechen einer Datenverbindung, sobald ein Client-PC den Bildschirmschoner aktiviert, sind über Optionskästchen auszuwählen. Netzwerkseitig ist nur eine wichtige Anpassung erforderlich: Ein einziger Port, in der Standardeinstellung 3945, ist auf der Firewall so einzustellen, dass er auf den G/On-Server weitergeleitet wird. Dadurch entfällt die Notwendigkeit, den Server in der DMZ zu positionieren. Selbst der Verwendung einer dynamischen DNS-Adresse steht im Zusammenspiel mit G/On nichts im Wege.

Mit dieser Konfiguration ist die Einrichtung des Servers mithilfe des „G/On Builders“ abgeschlossen. Der private und öffentliche Schlüssel sollten an einem sicheren Ort aufbewahrt werden, da diese Informationen, gemeinsam mit den speziellen Sicherungen, für eine Wiederherstellung auf einem Reserve-Server von Bedeutung sind.

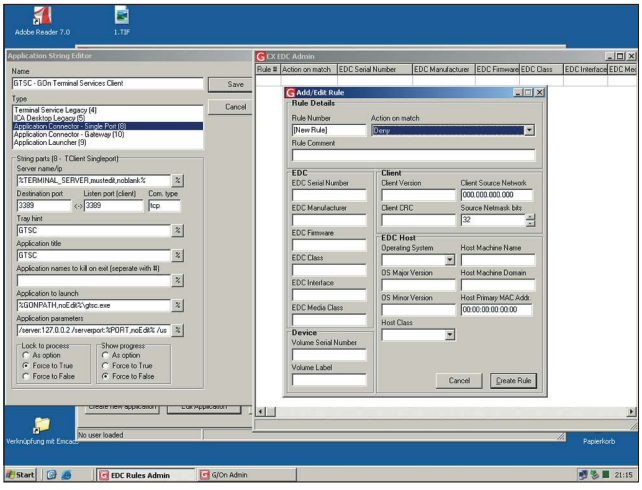
Im Gegensatz zu VPN-Verfahren handelt es sich bei G/On um eine Remote-Access-Lösung auf Applikationsbasis. Entsprechend müssen dem späteren Benutzer Anwendungen wie Terminalsitzungen für Microsoft RDP oder Citrix ICA, Browserverbindungen ins Intranet, Outlook, Navision, SAP, CRM oder MS Dynamics in einer Menüstruktur von „G/On Admin“ freigegeben werden. Je nach Einsatzgebiet ist aber auch die Freischaltung einzelner Ports für Clients auf festgelegte Zielmaschinen möglich. Zur Konfiguration der Applikationen sind Informationen wie die benötigten Port- und IP-Adressen oder die DNS-Namen der Zielmaschinen notwendig.

Da der Einsatz der Client-Software auf den USB-Sticks das primäre Ziel der Lösung darstellt, findet sich eine zusätzliche Zonenverwaltung in der Verwaltungsoberfläche. Anhand von IP-Adressen, Hersteller- oder Server-Informationen ist es der Client-Software so möglich, festzustellen, ob sie in einem „trusted“ oder „untrusted“ Netzwerk aktiviert wurde. Je nach Einstellungen hat dies eine unterschiedliche Ausstattung an Menübefehlen zur Folge.

Sicherer Zugriff über USB-Stick

Neben den Applikationen, die über die Verbindung mit dem Unternehmensnetz kommunizieren, lassen sich auf dem USB-Stick auch „Portable Applications“ wie der Firefox-Browser unterbringen. Die von uns getesteten Sticks bieten mit 1 GByte Speicher für Zusatzprogramme ausreichend Platz.

Der G/On-Client arbeitet auf jedem Computer mit Windows 2000 SP4, XP, 2003 oder Vista. Der Client läuft außerdem auch auf x64-Windows, jedoch nicht als native 64-Bit-Anwendung, sondern als 32-Bit-WOW-Task. Auf der Entwicklungs-Roadmap steht für die nähere Zukunft ein Client für MacOS an. Windows XP Embedded auf Thin Clients wird bereits heute unterstützt, jedoch ist beispielsweise bei Geräten von Hewlett-Packard oder Igel zunächst die administrative Freischaltung des USB-Tokens erforderlich. Thin Clients von Wyse arbeiten ohne Konfigurationsänderung automatisch mit G/On zusammen.



Anstelle einer Netzwerkverbindung wird dem Client der Zugriff auf zuvor freigeschaltete Applikationen ermöglicht. Die Regelwerke können für Gruppen oder einzelne Clients festgelegt werden.

Die G/On-Client-Software lässt sich entweder direkt auf dem Rechner installieren oder auf dem speziellen USB-Stick von G/On ablegen. Bei diesen USB-Sticks der Firma Hagiwara ist die üblicherweise unsichtbare „Read Only“-Partition aktiviert und mit dem ISO-Image der Client-Software gefüllt. Die Verwendung der Read-Only-Partition macht Änderungen am Client-PC durch Anwender oder Programme unmöglich. Manipulationsversuche werden anhand von Hash-Werten der Dateien erkannt.

Bevor ein Client mit dem Server in Verbindung treten kann, ist die Freischaltung auf dem Server erforderlich. Dieser Vorgang wird bei der Software als „Adopt“ bezeichnet. Unveränderbare Merkmale des Clients, Eckdaten des Clients oder beim USB-Stick die weltweit eindeutige Seriennummer dienen als Erkennungszeichen.

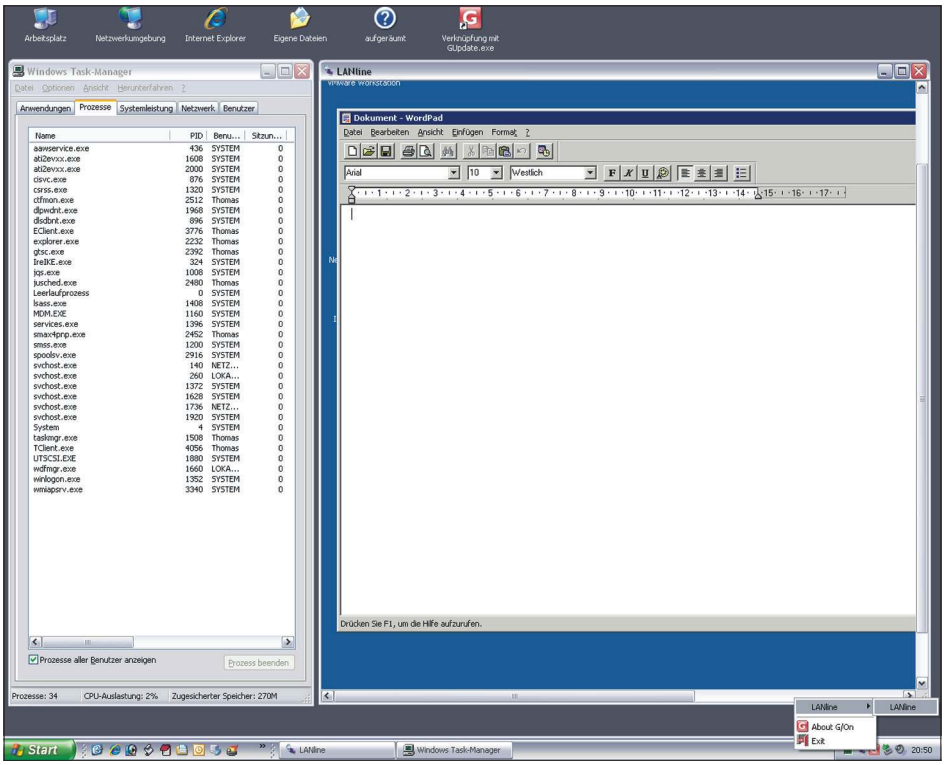
Nach der Freischaltung, die im Test lediglich eine Minute Zeit kostete, baut der G/On-Client eine Verbindung zum G/On-Server auf, um eine Identifikation des Anwenders mit Benutzername und Passwort vorzunehmen. Auch ein zufällig aufgefundener Stick stellt somit ohne die Kenntnis der Zugangsdaten kein Sicherheitsrisiko dar. Zudem lassen sich sowohl Client-Installationen als auch USB-Sticks mit einem Mausklick auf dem Server deaktivieren.

Im Task-Tray des Client-Windows erscheint in der Nähe der Uhrzeitangabe ein Menü mit dem roten Buchstaben „G“. Je nach vorgefundener Zone zeigen sich die zuvor festgelegten Programme im Menü. Die komplette Kommunikation ist mit 256 Bit AES verschlüsselt und wird über einen einzigen Port abgewickelt – quasi ein Port-Multiplexing. Die Verteilung der für die Anwendungen benötigten Datenpakete übernimmt auf der Seite des Firmennetzwerks der G/On-Server als Proxy.

Der G/On-Client ist bewusst im monolithischen Programmverfahren entwickelt worden. Es werden keine DLLs, externe Dateien oder Registrierungsdaten vom Client-Computer verwendet. Malware, die versucht, Exploits auszunutzen, kann die Sicherheit von G/On somit nicht unterwandern. Zusätzlich wurde die Client-Software komprimiert und

verschlüsselt, um ein Reverse Engineering zu unterbinden. Selbst auf die Speicher- und Task-Zuordnung durch Windows über den Microsoft Memory Manager verlässt sich der G/On-Client nicht, sondern verwendet eine eigene Speicherverwaltung.

on von G/On arbeitet über „TCP over HTTP“ und ist somit für das Zusammenspiel mit Servern wie dem Microsoft ISA oder dem JANA2-Proxy gewappnet. Verschiedene optionale Erweiterungen wie Wake on LAN für angesteuerte PCs, Remo-



Eine G/ON-Terminalsitzung auf dem Client-Computer: Die benötigten Applikationen befinden sich auf dem speziellen USB-Stick. Die Netzwerkverbindung ist für die einzelne Applikation gekapselt.

Die auf dem Client über die G/On-Software gestarteten Applikationen kommunizieren ausschließlich mit dem lokalen Loopback-Adapter der Maschine auf der Standard-IP-Adresse 127.0.0.2. Der Client-PC ist somit nie ein Mitglied des Netzwerks, auf das eigentlich zugegriffen wird. Die G/On-Software lässt nur die Datenpakete durch das Loopback in Richtung G/On-Server passieren, die von den erwünschten und gestarteten Applikationen stammen – „Lock to Process“. So ist es im Test beispielsweise möglich, über http://127.0.0.2 auf das Test-Intranet im LAN zuzugreifen, sofern der Browser über das G/On-Menü gestartet wurde. Wird eine weitere Browser-Instanz geöffnet und versucht, über die Adresse zuzugreifen, so blickt die zweitgestartete Instanz lediglich auf Port 80 des Client-PCs. Viele Internet-Anbindungen werden über Proxy-Server realisiert. Die aktuelle Version bietet Access oder ein Connector für Novell Edirectory bieten sich bei Bedarf an.

Fazit

Es ist schon schwer, dem Charme des kleinen roten USB-Sticks nicht zu verfallen. Dass die von Giritech entwickelte EMCADS-Verschlüsselungs- und Kommunikations-Engine nach FIPS 104-2 zertifiziert wurde, erhöht die gefühlte Sicherheit noch weiter. Der Preis für eine Business Lizenz für kleinere und mittlere Unternehmen beginnt bei 583,10 Euro. Eine Client-Lizenz kommt auf 166,60 Euro und der USB Access Key auf weitere 78,54 Euro.

Thomas Bär/wj

■ Info: Giritech
Tel.: 07541/9710990
Web: www.giritech.de