konradin MEDIENGRUPPE

www.windowsitpro.de

12/2006

Windows IT Pro

Das Magazin für den Windows-Administrator

Datensicherheit & Massenspeicher

Kryptographie schützt die Daten
Dynamische Paging-Architektur
Viel Speicher im Netz

LAB-REPORT:

- Workstation mit 64-Bit-Windows im Test
- NAS-System mit einem Terabyte
- SBS 2003 R2

SPECIAL:

- Neue Wege für Remote-Access
- Terminal-Server erweitern

TOOLKIT:

- Imagefrage: Deployment von Windows Vista
- Datenrettung mit BartPE
- PowerShell: Noch mehr Kraft!

Sicherheit und Flexibilität für Remote Access

Auf neuen Wegen

von Michael Bleicher & Joachim Seibold

Remote-Access-Lösungen kommen zum Einsatz, wenn sich die Anwendungen im Firmennetz befinden und die Nutzer auch von ihren mobilen Client-Systemen aus direkt auf die Host-basierten Lösungen zugreifen sollen. Unser Autor stellt eine Lösung aus diesem Umfeld vor, die nicht den üblichen Weg über VPNs geht, um solche Verbindungen sicher aufzubauen.

Firmen, die sensible Daten beim Transport über das Internet schützen wollen, setzen für den Remote-Access über öffentliche Netze traditionell auf VPNs (Virtual Private Networks). Diese bauen sie entweder selbst auf oder mieten sie von externen Dienstleistern. Solche VPNs sind aber keine Plug&Play-Lösungen sondern erfordern vielmehr eine umfassende Planungsphase, in der alle Kommunikations- und Sicherheitsanforderungen im Unternehmen berücksichtigt werden müssen. Die folgende Liste fasst die fünf wichtigsten Herausforderungen zusammen, denen sich ein Administrator dabei stellen muss:

- Authentifizierung der Anwender,
- Absicherung der (End-)Geräte,
- Schutz der Daten beim Transfer über das Internet,
- Filtern des Netzwerkzugriffs und
- Kontrolle sowie Verwaltung der Identitäten.

Wer als Administrator diese Faktoren verantwortungsbewusst umsetzen möchte, muss sich darüber im Klaren sein, dass neben den reinen Client- und Rollout-Kosten schnell weitere Investitionen für Token-Server, Zertifikatsserver, Intrusion Detection Systeme, DMZ, Identity-Management-Systeme und so weiter anfallen können.

Ohne Grundlage geht es nicht: die Basistechniken. Als Basistechniken zur Absicherung von Remote-Verbindungen über ein VPN stehen IPSec und SSL VPN zur Verfügung. Dabei schützt ein IPSec VPN den Datenverkehr zwischen zwei festverdrahteten, abgesicherten Netzen und stellt im Vergleich zu privaten oder geleasten Verbindungsstrecken eine preisgünstige Alternative dar. Da dabei jedoch auf jedem PC ein Client installiert sein muss, kann der Anwender keine Ad-hoc-Verbindung aufbauen, wenn er beispielsweise von einem Internet-Café oder einem unsicheren Kunden-PC aus arbeiten will.

Das SSL VPN benötigt hingegen keinen Client, denn hier kommt ein herkömmlicher Browser für den Verbindungsaufbau zum Einsatz. Theoretisch ist damit ein weltweiter Remote-Zugang von jedem Rechner aus möglich. In der Praxis stellt allerdings gerade der Browser eine gravierende Sicherheitslücke dar. Er kann zum Einen relativ einfach infiziert werden (durch Malware, Viren, intelligente Angreifer), zum Anderen muss beim Beenden der Session dafür gesorgt sein, dass keine Daten (-Fragmente) im lokalen Cache zurück bleiben.

Ein weiterer Weg: Remote Connectivity – on the fly. Ein anderes Konzept liefert Giritech mit der Lösung G/On, deren wesentlichen Eigenschaften in einem Kasten auf der Seite 26 den traditionellen Methoden des Remote-Zugriffs gegenübergestellt werden. Statt das LAN über VPNs zu öffnen, ermöglicht das Paket den Zugriff auf Applikationen im Netzwerk. Diese Lösung ist eine Client/Server-Plattform, die eine sichere, virtuelle Verbindung auf Unternehmensressourcen ermöglicht, ohne dabei VPN-Strukturen oder Security-Mechanismen zu benötigen. Der Client wird entweder von einem speziellen USB-Stick aktiviert oder kann bei definierten Endgeräten auch fest installiert sein.

G/On setzt auf der patentierten EMCADS-Technik (Encrypted Multipurpose Content and Application Deployment System) auf. Die für End-to-End Remote-Connectivity entwickelte Kombination aus Hard- und Software unterscheidet sich vor allem in einem Punkt von klassischen VPNs: Dem Gerät, das die Verbindung hostet wird keine interne IP-Adresse zugewiesen. Deshalb wird der angebundene PC kein direkter Bestandteil des Netzwerks, stattdessen werden die Nutzer mit den spezifischen, für sie freigegebenen Anwendungen auf dem lokalen Loopback verbunden. Sie erhalten aber keine Verbindung zum gesamten Netz. Auf diese Weise kann der Administrator auch

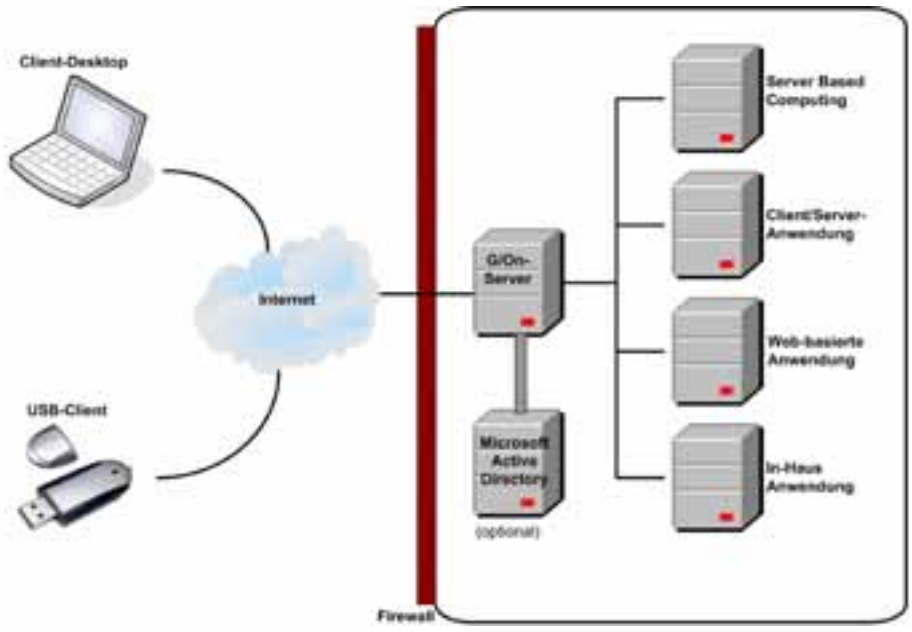

Bild 1: Der andere Weg zum Server-Centric-Computing: Die G/On-Anwendung baut eine direkte Verbindung zu den benötigten Programmen im Firmennetz auf. (Quelle: Griritech)

die traditionell mit Remote-Connectivity verbundenen Risiken reduzieren. Mögliche Interaktionen und Anwendungen steuert er dabei abhängig vom Standort des Users über Regeln und Zonen: Wählt sich beispielsweise ein Mitarbeiter im Außendienst mit dem Firmen-Notebook ein, so kann der Server den vollen Zugriff gewähren. Verwendet er hingegen ein Hotel-Terminal, so erhält er nur Zugriff auf seine E-Mails. Ressourcen und Applikationen werden zentral mit dem G/On Administrator freigeschaltet und über Menüs bestimmten User-Gruppen zur Verfügung gestellt.

Die Bausteine der Lösung: Server und Clients. Der Server wird hinter der Perimeter-Firewall des Netzwerks eingerichtet und so konfiguriert, dass er Informationen an spezifische Anwendungen, Datenbanken, Server und PCs weiterleitet. Sobald der Server installiert ist, muss der Administrator über ihn die Client-Menüs erstellen sowie die Applikationen, Protokolle und Ports definieren. Zudem kann er an dieser Stelle optionale Software zum Download auf das Client-Gerät vorbereiten. Die Sicherheitsfunktionen enthalten eine Zwei-Faktor-Authentifizierung: Der Client kann eindeutig an einen Computer des Anwenders gebunden werden. Er stellt damit den Zugangsschlüssel dar. Im Netzwerk kommen aber zusätzlich noch Identity-Datei, Login-Name sowie das Passwort zur Anwendung. Alle Daten sind mit 256-Bit-AES verschlüsselt und durch Prüfziffern gegen Hacking oder Man-in-the-Middle-Angriffe geschützt.

Sollen mobile Anwender die USB-Variante der Lösung einsetzen, wird diese auf einem speziellen USB-Key eingerichtet. Dieser Key wird in den aktiven USB-Port eines Internet-fähigen PCs eingesteckt (ab Windows 2000 aufwärts) und startet den Client automatisch von der so genannten CD-Partition des USB-Keys. Sobald die Login-Dialogbox erscheint, kann der Anwender die Verbindung durch Eingabe von Benutzername und Passwort aufbauen. Alle für den Benutzer und die aktuelle Zone freigegebenen Anwendungen stehen dann über ein Menü in der Taskleiste zur Verfügung (Bild 2).

So genannte Trusted-Applications kann der Systembetreuer optional auch in die sichere Verbindung einbinden und auf dem USB-Key ablegen, was per Push vom Server auf die unveränderbare CD oder auf die Read/Write-Partition des Keys geschehen kann. Wird der USB-Stick aus dem Anschluss entfernt, so schließt die Anwendung die aktive Session automatisch, ohne dass Spuren auf dem PC zurück bleiben.

Will der Anwender den optionalen Desktop-Client der Lösung einsetzen, so kann der Systemverwalter diese Software auf einem PC installieren und am Server dann über einen spezifischen Hash-Code eindeutig freischalten. Auf diese Weise wird der jeweilige PC zum Bestandteil der Authentifizierung. Es ist danach nicht mehr möglich, beispielsweise mit einem kopierten Desk-

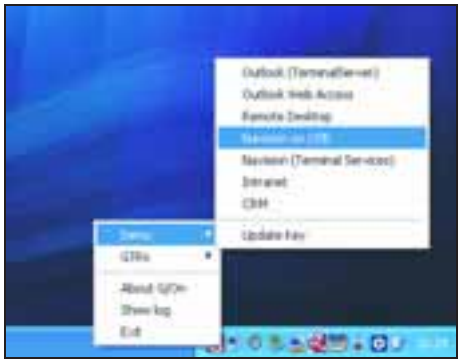

Bild 2. Alle Anwendungen im Überblick: Hat sich der Anwender angemeldet, so stellt ihm die Lösung über ein spezielles Menü die Applikationen zur Verfügung, die er verwenden darf.
(Quelle: Giritech)

top-Client den Remote-Access über ein anderen als den definierten PC aufzubauen.

Soll die Software der Lösung aktualisiert werden, so wählt der Administrator die Anwendungen oder Einstellungen aus, die ausgerollt werden müssen. Meldet sich der Anwender das nächste Mal an, so werden diese Upgrades automatisch per Push auf den USB-Stick oder den PC übertragen. Sollte eine solche Übertragung gerade aufgrund langsamer Leitungen oder einem anderen Zeitproblem nicht möglich sein, kann der Anwender die Aktualisierung auf einen späteren Zeitpunkt verschieben. Der Administrator kann mit diesem Push-Befehl parallel auch zusätzliche Dateien wie beispielsweise Preislisten, Telefonlisten oder Produktpräsentationen gleich mit übertragen.

Sicherheit: Unterschiedliche Technologien stehen zur Verfügung. Sowohl bei IPSec- als auch bei SSL-VPNs steht die stärkste heute verfügbare Authentifizierung (mutual device authentication und multifactor user authentication) nur durch die Integration von Drittanbieter-AddOns zur Verfügung. Diese Methoden sind in G/On bereits vollständig implementiert: Dabei authentifizieren sich Client und Server zunächst gegenseitig, noch bevor sich der User anmeldet. Diese Vorgehensweise kann Phishing- und Pharming-Angriffe verhindern. Wenn die Lösung außerdem mit der integrierten One-Time-Passwort-Option eingesetzt wird, kommt die Multifactor-Authentication zum Einsatz.

Während VPNs einen verschlüsselten Tunnel zwischen zwei Endpunkten aufbauen, wobei sich die Daten teilweise auch direkt im Tunnel verschlüsseln lassen, arbeitet die hier vorgestellte Anwendung nicht mit einem Tunnel: Die Daten werden einfach mit 256-Bit-AES verschlüsselt und mit Prüfsummen versehen, um auf dieser Weise Man-in-the-Middle- Angriffe zu verhindern.

Auch wenn es um die so genannte Server-Visibility geht, haben die Entwickler dieser Lösung einen anderen Weg gewählt: Es kommt keine Broadcast-Adresse zum Einsatz, da der Server hier nur als Zuhörer agiert. Er antwortet ausschließlich auf einen autorisierten Datenstrom. Deshalb erhalten tatsächlich nur solche User überhaupt einen Logon-Prompt, die eine Identität und ein Device erhalten haben und deren Informationen zusätzlich am Server aufgenommen worden sind. Diese Anwender werden dabei kein Bestandteil eines Netzwerks, wodurch auch keine verwertbaren Informationen zu den Endpunkten zur Verfügung stehen. Im Bereich der Remote-Connectivity ist aber der Endpunkt immer der verwundbarste Punkt. So speichern IPSec VPNs alle Informationen auf dem Endpunkt und erstellen dann einen offenen Tunnel in das Unternehmensnetzwerk. Auch SSL-VPNs sind aufgrund der Footprints angreifbar, die sie auf den PCs zurücklassen.

Wie die Tabelle auf der Seite 25 zeigt, existieren zwischen den drei Remote-Connectivity-Lösungen auch Unterschiede in der Verwaltung. So muss bei IPSec VPNs der IT-Administrator für die spezifische Konfiguration und Wartung der Endpunkte sorgen. SSL VPNs bringen keinerlei Endpoint-Management mit, dennoch müssen Sicherheitsrichtlinien entwickelt und implementiert werden, um die zwischengespeicherten Informationen nach der Session zu löschen und bestimmte Sicherheitsstandards bei den Webbrowsern zu erzwingen. Die G/On-Lösung wird vom Backend über ein integriertes Nutzer-orientiertes Managementsystem verwaltet. Der Client wurde im so genannten Monolithic-Programming-Verfahren entwickelt. Das bedeutet, dass bei dieser Software keine DLLs oder externe Dateien benötigt werden. Da viele Schwachstellen dadurch entstehen, dass DLLs ausgetauscht werden, ist dies ein wirkungsvoller Schutz vor Trojanern, die sich in den Datenstrom zwischen Executable und DLL einklinken. Zusätzlich ist die ausführbare Client-Datei komprimiert und ver-

schlüsselt, um den Code vor Missbrauch, Reverse Engineering oder anderen Veränderungen zu schützen.
Das vom Hersteller entwickelte EMCADS-Protokoll verwendet 163-Bit-ECC für das signierende Schlüsselpaar zwischen dem Server und dem USB- beziehungsweise Desktop-Client. Auch für den sicheren Schlüsselaustausch und die Übertragung der Client-Identity-Facility (CIF) kommt 163-Bit-EXX zum Einsatz. Alle über die Remote-Strecke transportierten Informationen werden mit 256-Bit-AES verschlüsselt, wobei die Lösung auf die Datenpakete den SHA-1-Hash-Algorithmus anwendet, um sicherzustellen, dass die Pakete während der Übertragung nicht manipuliert werden können.
Bei der Installation des Servers wird eine spezielle Datei erzeugt, das so genannte Identity File. Diese Datei enthält eindeutige, verschlüsselte Informationen, die problemlos weitergegeben werden können und dem Client die Möglichkeit geben, auf einen spezifischen G/On Server zuzugreifen. Die ursprüngliche Verbindung wird aufgebaut, wenn der Client das erste Mal aufgerufen wird. Er entschlüsselt dann das Identity File und erhält IP-Name/Adresse des Servers, der kontaktiert werden soll. Anschließend baut der Client die Verbindung über den TCP-Port 3945 auf (IANA Default, kann individuell verändert werden), der Server antwortet mit einer Begrüßung, und der Prozess für den sicheren Schlüsselaustausch wird angestoßen. Die Begrüßungsinformation enthält einen öffentlichen ECC-Schlüssel, der pro Session einmalig ist, sowie eine Signatur, die vom Server gesendet wird. Nur der Client mit dem Identity File, das von diesem Server erzeugt worden ist, kann den öffentlichen Key nutzen und die Signatur validieren. Dies stellt die Basis für die wechselseitige Authentifizierung dar: Auf diese Weise wird sichergestellt, dass Client und Server füreinander konfiguriert sind. Der Client antwortet darauf mit der Client-Identity-Facility (CIF). Sendet der Client nicht die korrekte Antwort, so wird die TCP-Verbindung sofort abgebrochen. Dies ist auch die Antwort auf Verbindungsversuche, die nicht von einem G/On-Client stammen, wie beispielsweise ein Versuch, per Telnet auf den Port 3945/tcp des Servers zuzugreifen.
Die Client-Identity-Facility (CIF) enthält die Seriennummer des EMCADS-Data-Carrier (EDC). Es ist entweder die eindeutige auf dem USB-Stick eingebrannte Seriennummer oder um die eindeutige Festplatten-Seriennummer des Geräts, auf dem der Desktop-Client installiert. Die CIF enthält außerdem eine Anzahl von Identifizierungsmerkmalen des Geräts, auf dem der Client ausgeführt wird, wie beispielsweise EDC-Seriennummer, Device Volume Label, Device Volume Serial, EDC-Hersteller, PC-Name und -Domain, Betriebssystem oder primäre MAC-Adresse. Diese Informationen verwendet das Gerät um während des Adopt-Prozesses den Client zu identifizieren, in die richtige globale Zone einzuordnen und spezielle Regeln anzuwenden. Dies ist der erste Teil der Zwei-Faktor-Authentifizierung.
Im CIF ist zudem auch die gewählte Verschlüsselungsmethode (derzeit 256-Bit AES) enthalten. Der zweite Bestandteil der Zwei-Faktor-Authentifizierung ist der Anmeldedialog. Wurde das Gerät authentifiziert, auf dem sich der Client befindet, so muss der Anwender seine User-ID und sein Passwort eingeben. Die Benutzer lassen sich auch gegenüber dem Active Directory (AD) authentifizieren, um so zu verhindern, dass Passwörter auf dem Server gespeichert werden müssen. Nach der erfolgreich Authentifizierung ist der Anmeldeprozess abgeschlossen. Nun erhält der Anwender sein Applikationsmenü je nach Gerät, Zonen, Regeln, Gruppe und User-ID in die Taskleiste gepusht. *(fms)*

Methoden des Remote-Zugriffs im Vergleich

Kategorie	IPSec	SSL	G/On
Anwender kann Applikationen starten...	nur von logischen Laufwerken	über Browser von logischen Laufwerken	auf dem G/On Key, logischen Laufwerken oder auf einem Terminal Server bzw. einem Arbeitsplatz mit Remote Desktop Zugriff
2-Factor Authentication	3rd Party AddOn	3rd Party AddOn	2-Factor Authentication und gegenseitige Authentifizierung ist Bestandteil der Lösung
Host	Abschottung durch Antivirus, Personal Firewall und Filter	Abschottung durch Antivirus, Personal Firewall und Filter. Durch Applets, die im Browser heruntergeladen werden.	Lock to process –Client ist niemals Bestandteil des Netzwerks. Antivirus und Firewall nur für den lokalen PC sinnvoll..
Beenden der Sitzung	Trennung beim Ausloggen	Anwender muss Browser-Cache löschen und Browser beenden	Abziehen des USB-Keys oder Beenden des Desktop Clients schließt alle Prozesse und Applikationen.
Netzwerk	vollständig geöffnet, 3rd Party Produkte und Firewalls ermöglichen das Schließen nicht benutzter Ports	Browser voll geöffnet für Anwendungskonnektivität, 3rd Party Schutz für Browser-Port und HTTP-Daten z. B. durch einen Secure Proxy erforderlich	kein direkter Zugriff, nur Anwendungskonnektivität, Daten der kontrollierten Prozesse werden über den definierten Port an ein Zielsystem weiter geleitet.
Server Management	Management der User typischerweise durch Tools von Drittanbietern	Management der User typischerweise durch Tools von Drittanbietern	AD-Synchronisation mit Benutzern und Gruppen oder individuelle Benutzer und Gruppendefinition in G/On eigenen Tools
Verschlüsselung	basierend auf verschiedenen Standards, maximal 256 Bit AES mit statischen Schlüsseln	SSL (typischerweise 128 Bit AES, maximal 256 Bit AES mit statischen Schlüsseln	256 Bit AES mit Prüfsummen und wechselnden Schlüsseln während der Sitzung, 163 Bit ECC für Sitzungsaufbau