Giritech GmbH, Mariabrunnstr. 123, 88097 Eriskirch

Deutschland · Österreich · Schweiz

Sicherheit und Flexibilität für Remote Access

Auf neuen Wegen gehen

Wenn die Interessensgruppe der externen DV-Anwender mit den Gralshütern der EDV zusammentrifft, enden Begierlichkeiten nicht selten in Verteidigungsmassnahmen. Das Thema „Remote Access“ wird einerseits zur unverzichtbaren Anforderung und sorgt andererseits bei den IT-Verantwortlichen für Kopfzerbrechen. Dass dies nicht zwangsläufig so sein muss, zeigt der folgende Beitrag.

Autoren: Michael Bleicher
Joachim Seibold
Thomas Bleicher

Die Auswirkungen des Internet auf unsere Arbeitswelt stellt hohe Anforderungen an die IT-Infrastruktur im Unternehmen. Ergeben sich einerseits völlig neue Möglichkeiten zur Dezentralisierung von Arbeitsplätzen und Neuorganisation von Geschäfts- und Entscheidungsprozessen, so erfordern diese andererseits den Einsatz neuer, sicherer und teils aufwändiger Technologien: Road Warrior müssen heute von ihren mobilen Arbeitsplätzen aus zu jeder Zeit von jedem beliebigen Ort auf zentrale Datenbeständige und Applikationen zugreifen können. Geschäftspartner, Berater, Kunden oder Zulieferer benötigen einen flexiblen sowie kostengünstigen Zugriff auf gemeinsame Ressourcen und schließlich muss auch das typische Homeoffice abgesichert in die Infrastruktur integrierbar sein. Die Möglichkeit, dieses Potenzial voll auszuschöpfen, ist ein Schlüsselfaktor für den Unternehmenserfolg doch gleichzeitig wirft die Freigabe von Ressourcen - selbst an vertrauenswürdige Teilnehmer - viele Sicherheitsfragen auf.

Um den Transport sensibler Daten über das Internet zu schützen, setzen Firmen für den Remote-Access über öffentliche Netze traditionell auf VPNs, die sie entweder selbst aufbauen oder von externen Dienstleistern anmieten. Nun sind aber VPNs keine plug&play Lösungen - sie erfordern vielmehr eine umfassende Planungsphase, in deren Rahmen alle Kommunikations- und Sicherheitsanforderungen im Unternehmen berücksichtigt werden müssen. Die fünf wichtigsten Herausforderungen hierbei sind zusammengefasst:

1. Authentifizierung der Anwender
2. Absicherung der (End)Geräte
3. Schützen der Daten über das Internet
4. Filtern des Netzwerkzugriffs
5. Kontrolle und Verwaltung der Identitäten

Wer als Administrator diese Faktoren verantwortungsbewusst umsetzen möchte, muss sich darüber im klaren sein, dass neben den reinen Client- und Rolloutkosten schnell weitere Investitionen für Token-Server, Zertifikatsserver, Intrusion Detection Systeme, DMZ, Identity Management Systeme usw. anfallen können. Dies wirkt sich nicht nur nachteilig auf die TCO aus, sondern führt aufgrund der komplexen Topologie zu deutlich erhöhtem Administrationsaufwand.

Basistechnologien

Um in VPN´s Remote-Verbindungen auf Netzwerkressourcen über das Internet abzusichern sind als Basistechnologien IPSec VPN und SSL VPN verfügbar. Dabei schützt IPSec VPN den Datenverkehr zwischen zwei festen, abgesicherten Netzen und ist im Vergleich mit privaten oder geleasten Verbindungsstrecken eine preisgünstige Alternative. Da auf jedem PC ein Client installiert sein muss, kann keine ad hoc Verbindung etabliert werden, z. B. von Internet-Cafés oder unsicheren Kunden-PCs aus.
Das SSL VPN benötigt hingegen keinen Client, denn es wird ein herkömmlicher Browser für den Verbindungsaufbau verwendet. Theoretisch ist damit ein weltweiter Remote-Zugang von jedem Rechner aus möglich, in der Praxis stellt allerdings der Browser eine gravierende Sicherheitslücke dar. Er kann nämlich einerseits recht einfach kompromittiert werden (durch Malware, Viren, intelligente Angreifer), andererseits muss beim Beenden der Session dafür gesorgt werden, dass keine Daten(fragmente) im lokalen Cache

zurück bleiben. Solche klar lesbaren Informationen wären das Aus für jede sichere Kommunikation und könnten dramatische wirtschaftliche Schäden nach sich ziehen.
Hier wird deutlich, wie wichtig das Thema Sicherheit für die Planung der Remote Connectivity ist:
Da ein VPN das Netzwerk nach außen erweitert und jeden Teilnehmer als Knoten in das LAN einbindet, muss sich das Unternehmen gegen alle (un)denkbaren Angriffe und Bedrohungen schützen, die aus einer solchen Integration resultieren können. Eine denkbare Lösung wäre, in zusätzliche Sicherheitslösungen von Drittanbietern zu investieren, beispielsweise Aufbau einer DMZ, Einsatz von Token Servern, Certificate Servern und Authentifizierungssystemen. Leider hat aber so viel Sicherheit ihren Preis: Einerseits belasten hohe Investitionen und aufwändiges Systemmanagement den Administrator (sind alle Lücken erkannt und wirklich geschlossen?), andererseits führen komplizierte Verfahren zu einer Ablehnung bei den Anwendern, die schlicht mit der Technik überfordert sind. Letztlich fallen Bedienungskomfort und Performance der Sicherheit zum Opfer. Ebenso problematisch: Sowohl VPN-Client und Browser als auch die Security Hardware sind nur vor bekannten Angriffen sicher. Werden durch weiter entwickelte Angriffsstrategien neue Sicherheitslücken gefunden, dann sind die Remote Verbindungen bis zur Verfügbarkeit eines Patches und dem folgenden Rollout durch den Administrator jederzeit kompromittierbar. So wird aus der Chance „Remote Connectivity“ schnell ein unternehmensweites Verteidigungsprojekt, das Ressourcen bindet, hohe Kosten produziert und die Frage aufwirft: Wie kann Remote Access einfacher gemacht werden? Der dänische Hersteller Giritech A/S beantwortet diese Frage mit einer integrierten Lösung, die als dritte Basistechnologie zu IPSec- und SSL-VPN positioniert ist.

Remote Connectivity “on the fly”
Ein völlig anderes Konzept verfolgt dagegen Giritech mit „G/On“. Statt das LAN über VPNs zu öffnen, ermöglicht G/On den einfachen Zugriff auf netzwerkseitige Applikationen. G/On ist eine Client/Server Plattform, die eine sichere, virtuelle Verbindung auf Unternehmensressourcen ermöglicht, ohne dabei VPN Strukturen oder Security-Mechanismen zu benötigen. Der G/On Client wird entweder von einem speziellen USB Stick aktiviert oder kann – bei definierten Endgeräten – fest installiert sein.
Basierend auf der patentierten EMCADS™ (Encrypted Multipurpose Content and Application Deployment System) Technologie ist G/On eine proprietäre Lösung. Die für end-to-end Remote Connectivity entwickelte Kombination aus Hard- und Software unterscheidet sich von klassischen VPNs technisch dadurch, dass G/On dem Gerät, das die Verbindung hostet, keine interne IP-Adresse zuweist. Deshalb wird der via G/On konnektierte PC niemals Bestandteil des Netzwerks, stattdessen verbindet G/On die Anwender lediglich mit den spezifischen, für sie freigegebenen Anwendungen auf dem lokalen Loopback - aber nicht mit dem gesamten Netz. Damt werden die traditionell mit Remote Connectivity verbundenen Risiken signifikant reduziert. Mögliche Interaktionen und Anwendungen können abhängig vom Standort des Users über Regeln und Zonen gesteuert werden (wenn sich beispielsweise eine Mitarbeiterin im Außendienst mit dem Firmen-Notebook einwählt, kann der G/On Server vollen Zugriff gewähren, während sie am Hotel-Terminal nur Zugriff auf ihre E-Mails erhält). Ressourcen und Applikationen werden zentral mit dem “G/On Administrator” freigeschaltet und über Menüs bestimmten Usergruppen zur Verfügung gestellt.

G/On Server und Clients
Der G/On Server wird hinter der Perimeter-Firewall des Netzwerks eingerichtet und so konfiguriert, dass er Informationen an spezifische Applikationen, Datenbanken, Server, PCs usw. weiterleitet. Sobald der G/On Server installiert ist, werden über ihn die Client-Menüs erstellt, die Applikationen, Protokolle und Ports definiert - und es wird optionale Software zum Download auf das Client-Gerät vorbereitet. Die Sicherheitsfeatures beinhalten eine 2-Factor Authentifizierung: Während der G/On Client eindeutig auf einen Computer Anwenders gebunden ist und damit den „Zugangsschlüssel“ darstellt, kommen zusätzlich Identity-Datei, Login Name sowie Passwort im Netzwerk zur Anwendung. Alle Daten sind mit 256-bit AES verschlüsselt und durch Prüfziffern gegen Hacking oder „Man-in-the-Middle“ Angriffe geschützt. G/On implementiert somit Sicherheitsfunktionen, für die ansonsten oft Drittprodukte erforderlich wären (z. B. Secure Tokens zur Authentifizierung und VPNs für Datenverschlüsselung). Die kleine Serverkomponente stellt keine besonderen Anforderungen an CPU oder RAM-Ausstattung, das Client-Modul ist einfach zu bedienen und kann nicht verändert werden, was die Wartungskosten minimiert.

Die G/On USB-Variante wird auf einem speziellen USB Key eingerichtet und eignet sich für mobile Anwender, die sehr flexibel auf Applikationen im Unternehmen konnektieren möchten. Der Key wird einfach in den aktiven USB-Port eines Internet-fähigen PCs eingesteckt (ab Windows 2000 aufwärts) und startet den G/On Client automatisch von der CD-Partition. Sobald die Login-Dialogbox erscheint, kann die Verbindung durch Eingabe von Benutzername und Passwort aufgebaut werden. Alle für den Benutzer und die aktuelle Zone freigegebenen Applikationen stehen sofort über das G/On Menü in der Taskleiste zur Verfügung. Trusted Applications können optional in die sichere Verbindung eingebunden und auf dem G/On USB-Key abgelegt werden (per Push vom Server auf die unveränderbare CD- oder die Read/Write-Partition). Wird der USB Stick aus dem Anschluss entfernt, schließt G/On automatisch die aktive Session ohne dass Spuren auf dem PC zurück bleiben. Der optionale G/On Desktop Client wird auf einem PC installiert und am G/On Server über einen spezifischen Hash-Code eindeutig freigeschaltet. Somit wird der jeweilige PC zum Bestandteil der Authentifizierung. Es nicht möglich, mit einem kopierten G/On Desktop Client den Remote Access über ein anderen als den definierten PC aufzubauen.

Die Aktualisierung von G/On ist ebenfalls einfach: Der Administrator wählt die Anwendungen oder Einstellungen, die ausgerollt werden müssen und das nächste Mal, wenn sich der Anwender anmeldet, werden diese Upgrades automatisch per Push auf den USB Stick oder den PC übertragen. Falls die Übertragung z. B. aufgrund langsamer Leitungen oder einem Zeitproblem nicht sinnvoll ist, kann der Anwender die Aktualisierung auf einen späteren Zeitpunkt verschieben. Parallel ist im Push auch das Senden zusätzlicher Dateien (z. B. Preislisten, Telefonlisten, Produktpräsentationen) möglich. Datenübertragung sowie Aktualisierung des Sticks können interaktiv oder lautlos ohne Benutzereingriff erfolgen.

Der Anwender selbst muss weder Software installieren noch Security-Updates aufspielen oder Konfigurationen vornehmen, so dass sich G/On auch für weniger technisch orientierte Anwender eignet.

Unterschiedliche Technologien

Die stärkste heute verfügbare Authentifizierung (mutual device authentication und multifactor user authentication) ist bei IPSec- und SSL-VPNs nur durch die Integration von Drittanbieter-AddOns realisierbar. Diese Methoden sind in G/On bereits vollständig implementiert: Zunächst authentifizieren sich Client und Server gegenseitig, noch bevor sich der User anmeldet – dies verhindert Phishing- und Pharming-Angriffe. Wird G/On außerdem mit der integrierten One-Time-Passwort Option eingesetzt, greift die Multifactor Authentication.

Zur Datenverschlüsselung etablieren VPNs einen verschlüsselten Tunnel zwischen zwei Lokationen, wobei sich optional auch die Daten im Tunnel kodieren lassen. Im Gegensatz hierzu wird von G/On kein Tunnel aufgebaut, wodurch eine extrem stabile Verbindung gewährleistet ist. Daten werden einfach mit 256-bit AES codiert und mit Prüfsummen versehen, um Man-in-the-Middle Angriffe zu verhindern.

Zugriffsseitig bieten IPSec VPNs dem User immer vollen Netzwerkzugang. Da dies verständlicherweise nicht erwünscht ist, sind zusätzliche Investitionen für den Aufbau einer DMZ notwendig, in der alle Informationen, die verfügbar sein sollen, repliziert werden. SSL VPNs wurden ursprünglich für den Einsatz als Web-Proxy entwickelt, weshalb sie nur minimalen Schutzmechanismen für den Datenverkehr von und zu Websites mitbringen. Einige SSL-Anbieter bieten inzwischen IPSec-ähnliche, offene Verbindung in ein Unternehmensnetzwerk an, wenn Applikationen gestartet werden müssen. Sobald die Verbindung in diesen Modus wechseln, entsteht die selben Probleme, wie beim Einsatz einer IPSec VPN: Das Netzwerk wird vollständig nach außen geöffnet. G/On etabliert hingegen keine direkte Verbindung in das Netzwerk, da nur authentifizierte Anwender auf spezifische Applikationen verbunden werden.

Im Bereich der Server Visibility geht die dänische Lösung ebenfalls einen anderen Weg, denn G/On hat keine Broadcast Adresse. Der Server ist nur „Zuhörer“ und 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.

Da G/On User niemals Bestandteil eines Netzwerks werden, gibt es keine verwertbaren Endpoint-Informationen. Im Gegensatz zu SSL VPNs werden keine Daten lokal zurück gelassen, die ein Angreifer

ausnutzen könnte. Ohne Key ist nicht einmal eine Adresse bekannt, über die der Hacker den Server finden und versuchen könnte, die Verbindung nochmals aufzubauen.
Im Bereich der Remote Connectivity ist der Endpoint immer der verwundbarste Punkt. IPSec VPNs speichern alles auf dem Endpoint und erstellen einen offenen Tunnel in das Unternehmensnetzwerk. Auch SSL VPNs sind aufgrund der Footprints, die Sie auf den PCs zurücklassen, angreifbar - zusätzlich bestehen im Applikationsmodus die selben Gefahren, wie bei IPSecs. Durch das Bundling mit Sicherheitstools versuchen SSL VPN Anbieter, das Problem auf Drittprodukte zu verlagern, doch Tests belegen, dass die Endpoint Security bei SSL VPNs derart schlecht designed ist, dass sie nur in sehr eingeschränkten Umgebungen funktionieren (Joel Snyder in NetworkWorld Clear Choice Tests, Dez. 2005). G/On USB verhindert ein solches Szenario wirkungsvoll. Da die Anwendung als protected monolithic code mit minimalen lokalen Ressourcen läuft, werden am Endpunkt keine verwertbaren Informationen offengelegt, gecached oder in anderer Form hinterlassen.
Letztlich gibt es zwischen den drei Remote Connectivity Lösungen auch Unterschiede in der Verwaltung. Bei IPSec VPNs sorgt der IT-Administrator für die spezifische Konfiguration und Wartung der Endpoints. SSL VPNs bringen keinerlei Endpoint Management mit, dennoch müssen Sicherheitsrichtlinien entwickelt und ausgerollt werden, um die zwischengespeicherten Informationen nach der Session zu löschen und bestimmte Sicherheitsstandards bei den Webbrowsern zu erzwingen. G/On hingegen wird zu 100% vom Backend über ein integriertes User-orientiertes Managementsystem verwaltet. Der Zugriff durch G/On User auf Applikationen wird vom Administrator in vollem Umfang kontrolliert, definiert und gewartet. Ebenso kann der IT-Admin alle Updates zentral über den G/On Server kontrollieren und zum Endgerät distribuieren.

Sicherheit
Der G/On Client ist im monolithic programming Verfahren entwickelt, d. h. es werden keine DLLs oder externe Dateien benötigt. Da viele Exploits auf dem Austausch von DLLs basieren, ist dies ein wirkungsvoller Schutz vor Trojanern, die sich gerne in den Datenstrom zwischen Executable und DLL einklinken. Zusätzlich ist die ausführbare Client Datei komprimiert und verschlüsselt, um den Code vor Missbrauch, Reverse Engineering oder anderen Veränderungen zu schützen.
Das von Giritech entwickelte EMCADS™ Protokoll verwendet 163-bit ECC für das signierende Schlüsselpaar zwischen dem G/On Server und dem G/On USB- bzw. Desktop-Client. 163-bit EXX wird auch für den sicheren Schlüsselaustausch und die Übertragung der Client Identity Facility (CIF) verwendet.
Alle über die Remote-Strecke transportierten Informationen werden mit 256-bit AES verschlüsselt, auf die Datenpakete wird der SHA-1 Hash-Algorithmus angewendet, um sicherzustellen, dass die Pakete während der Übertragung nicht manipuliert werden.

Mit der Installation des G/On Server wird eine spezielle Datei, das Identity File, erzeugt. Diese Datei enthält eindeutige, codierte Informationen, die problemlos weitergegeben werden können und dem G/On Client die Möglichkeit geben, auf einen spezifischen G/On Server zuzugreifen. Die initiale Verbindung wird aufgebaut, wenn der G/On Client das erste Mal aufgerufen wird. Der Client entschlüsselt das Identity File und erhält IP Name/Adresse des G/On Servers, der kontaktiert werden soll. Der Client baut dann die Verbindung über 3945/tcp auf (IANA Default, kann individuell umkonfiguriert werden), der Server antwortet mit einer „Begrüßung“ and der Prozess für den sicheren Schlüsselaustausch wird angestoßen. Eine 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 bei G/On die Basis für die wechselseitige Authentifizierung dar, denn es wird sicher gestellt, dass Client und Server für einander konfiguriert sind. Der Client antwortet darauf mit der Client Identity Facility (CIF).
Falls der Client die korrekte Antwort sendet, wird die TCP Verbindung sofort abgebrochen. Dies ist auch die Antwort auf Verbindungsversuche, die nicht von einem echtem G/On Client stammen (wie z. B. von einem Telnet auf Port 3945/tcp auf den Server).

Die Client Identity Facility (CIF) enthält die EMCADS™ Data Carrier (EDC) Seriennummer, welche entweder die eindeutige auf dem USB-Stick eingebrannte Seriennummer ist – oder die eindeutige Festplatten-Seriennummer des Geräts, auf dem der Desktop-Client installiert ist. Der CIF enthält außerdem eine Anzahl von Identifizierungsmerkmalen des Geräts, auf dem G/On ausgeführt wird, wie beispielsweise:

EDC Seriennummer, Device Volume Label, Device Volume Serial, EDC Hersteller, EDC Media Class, EDC Interface, EDC Class, EDC Firmware, öffentliche IP, Quellnetzwerk, Client Hash, Client Version, PC-Name und -domain, Betriebssystem, primäre MAC Adresse usw.
All diese Informationen können verwendet werden, um das Gerät während des Adopt-Prozesses zu identifizieren, den Client in die richtige globale Zone einzuordnen und spezielle Regeln anzuwenden. Dies ist der erste Teil der 2-Factor Authentication.

Im CIF ist übrigens auch die gewählte Verschlüsselungsmethode (derzeit 256-bit AES) beinhaltet. Werden später einmal bessere Codierungsalogorithmen entwickelt werden, können diese einfach in das EMCADS™ Protokoll integriert und sofort zum Einsatz kommen.

Zonen und Regeln.
Globale Zonen können, abhängig von der eigenen Sicherheitsdefinition, unterschiedliche Bedeutungen haben: standardmäßig sind sie definiert als „innen, außen und unbekannt“. Sie könnten aber ebenso „vertrauenswürdig, eingeschränkt und nicht vertrauenswürdig“ heißen. Die grundsätzliche Idee hinter diesem Konzept ist, dass abhängig vom weltweiten Standard des Anwenders, bestimmte Zugriffe freigegeben oder gar nicht erst nicht verfügbar gemacht werden können. Parallel hierzu erlauben Regeln das Zulassen oder Sperren eines Gerätes sowie die Zuordnung eines Geräts auf eine Zonendefinition.

Login mit Single Sign-On
Der zweite Bestandteil der 2-Factor-Authentication ist das Anmeldedialog. Wurde das Gerät, auf dem sich der Client befindet authentifiziert, muss der Anwender seine User-ID und sein Passwort eingeben. Dabei kann der Anwender auf das Device, das Device kann auf den Anwender und Geräte aneinander gebunden werden.
User lassen sich gegenüber dem Active Directory (AD) authentifizieren, um zu verhindern, dass Passworte auf dem G/On Server gespeichert werden müssen. Sobald der Anwender authentifiziert ist, dann ist der Anmeldeprozess abgeschlossen (die 2-Factor Merkmale wurden geprüft). Nun erhält der Anwender sein Applikationsmenü in die Taskleiste gepushed, basierend auf Gerät, Zonen, Regeln, Gruppe und User-ID.

Der Login-Dialog ist mit verschiedenen Funktionen ausgestattet, um brute-force Angriffe zu verhindern:

- fehlgeschlagene Logins
- Fenster wird an einer zufälligen Position auf dem Monitor angezeigt
- verhindern der Navigation per TAB Taste
- wechseln der Funktionsweise von „OK“ und „Cancel“
- Nutzung des On-Screen-Keyboards (OSK) zur Eingabe
- OSK automatisch aufrufen
- Verbindungsabbruch, sobald der Bildschirmschoner aktiv wird

Die Kombination der Möglichkeiten sollte auf die internen Sicherheitsrichtlinien sowie die Umgebung abgestimmt sein, in der G/On genutzt wird.

Anwendungskonnektivität
Im Gegensatz zu traditionellen Anbindungen, bietet Application Connectivity wie mit G/On den entscheidenden Vorteil, dass keine Netzwerk zu Netzwerk Verbindung notwendig ist. Der Client konnektiert ausschließlich auf einen Server, der die Verbindung zu den einzelnen Applikationsservern herstellt. Stellt man ein solches System über Internet zur Verfügung, entfallen die zusätzlichen Kosten für Extranets, Portale und andere Technologien, die üblicherweise eingesetzt werden, um Remote Access anzubieten. Gleichzeitig reduziert sich die Zahl der an der Firewall zu öffnenden Ports auf einen einzelnen TCP Port – ein wichtiger Sicherheitsfaktor, der zusätzlich für geringeren Traffic im Netzwerk sorgt, da sich weniger Geräte per Broadcast miteinander unterhalten. Die direkte Verbindung mit einer Applikation anstatt einem Netzwerk macht das Aushandeln gemeinsamer Sicherheitsstandards, kompatibler Geräte oder die Aufsplittung von Kosten überflüssig, denn tatsächlich wird der Netzwerkinhaber selbst zum Provider, der für Partner, Kunden und Mitarbeiter einen Service anbietet, den sie mit einfachsten Mitteln ad hoc nutzen können.

Das Loopback Interface und Split DNS
Die Verbindung zwischen dem G/On Server und dem Desktop- oder USB-Client über Port 3945/tcp ist auf das Loopback Device des Clients gebunden, genauer gesagt auf 127.0.0.2. Das Socket Gateway (das Teil des G/On Clients ist) öffnet einen Socket für den verwendeten Port, z. B. 127.0.0.2:80 für http Traffic. Nun werden alle Daten, die an einen eingerichteten Socket auf 127.0.0.2 gesendet werden, verschlüsselt und durch den Port 3945/tcp an den Server geschickt.
Split DNS wird verwendet, wenn der Server einen Redirect von 127.0.0.2 auf einen tatsächlichen Hostnamen sendet. Dies bedeutet, dass nach innen der Hostname in die korrekte IP-Adresse aufgelöst wird, nach außen jedoch 127.0.0.2 bestehen bleibt. Schöner Nebeneffekt: Jeder Hacking-, Viren-, Backdoor-Angriff und Scanningvorgang findet auf dem Loopback Interfaces des Hackers statt, da alle IP-Adressen der zu attackierenden Server in 127.0.0.2 auf der externen DNS aufgelöst werden.

Viren, Spyware, Trojaner, Phising usw.
Da die G/On Konnektivität nicht netzwerk- sondern anwendungsbasiert arbeitet, ist es für Viren, Spyware und Trojaner sehr schwierig, das Unternehmensnetzwerk zu kompromittieren. Natürlich ist G/On - wie jede andere Anwendung - selbst nicht resistent gegen Viren, Trojaner usw. aber mit der richtigen Konfiguration ist es praktisch unmöglich, dass parasitäre Software die vom Unternehmensnetzwerk zur Verfügung gestellten Services infizieren kann.
Auch Phishing-Angriffe lassen sich mit G/On effektiv eliminieren, wenn Anwender generell den G/On Client für den Verbindungsaufbau nutzen und keine E-Mail Links zum Online-Bank usw. ausführen. Da die Konnektivität auf Anwendungen durch das Loopback Interface geleitet wird, bleiben Versuche, die URL zu ändern ohne Erfolg, denn der Client verbindet auf 127.0.0.2 und die vollständige URL ist ausschließlich auf der G/On Serverseite bekannt.

G/On bietet im bisher von IPSec- und SSL-VPN dominierten Remote Connectivity Markt eine unkomplizierte und sichere Methode, um Anwender via Internet oder im LAN mit Applikationen virtuell zu verbinden. Das Spektrum reicht dabei von einer administrationsfreundlichen Umgebung, in der „leere“ Windows-PCs durch Einstecken des G/On USB-Keys zu vollwertigen Arbeitsplätzen gemacht werden, bis zur Integration externer Dienstleister oder dem sofortigen Zugriff auf fusionierte, neue Unternehmensstandorte.
Typische Einsatzgebiete sind: Klassische Telearbeit, Aussendienst-, CRM- und PPS- Anbindung über Email und Intranet Zugang, Conferencing, (Audio)Chat, Filetransfer, Remote Control und webgestützte, dynamischen Lernumgebungen sowie Zugriff auf Remote Desktops sowie Terminal Server und Citrix.

Für Administratoren ergeben sich durch G/ON vielfältige Möglichkeit, um Kosten deutlich zu reduzieren und traditionelle Sicherheitslösungen (wie z. B. VPNs und/oder Secure Tokens) zurückzufahren bzw. in bestimmten Bereichen vollständig zu ersetzen. Gleichzeitig wird durch die äußerst einfache Client-Handhabung eine sehr gute Akzeptanz bei den Endanwendern erreicht.

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 – es muss nichts abgeschottet werden, da der Client niemals Bestandteil des Netzwerks ist. Antivirus und Firewall nur für den lokalen PC sinnvoll aber für die Connectivity nicht zwingend erforderlich.
Endpoint Information (Caching nutzbarer Daten, z. B. Passworte)	keine	ja	keine
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, G/On verwendet 163 bit ECC für Sitzungsaufbau
Anwendungsmanagement	AddOn Identity Manager oder Replikation einer gewählten Infrastruktur auf eine DMZ	Add-On Identity Manager	Volles Applikations-management mit AD Integration. Kein Benutzereingriff notwendig.

Über Giritech
Giritech entwickelt sichere Remote Connectivity Lösungen, welche die Produktivität erhöhen, Kosten senken und Kunden in die Lage versetzen, neue Geschäftsbeziehungen vorteilhaft zu nutzen.
Unser Ziel ist es, in diesem schnell wachsenden Markt eine weltweit führende Position einzunehmen. G/On, das erste auf unserer patentierten EMCADS™ Technologie basierende Produkt, wird exklusiv durch ein Netzwerk zertifizierter Reseller vertrieben.

"Giri" ist ein japanisches Konzept, das Ehre und Pflichtbewußtsein beinhaltet. Giritech fühlt sich diesen Idealen verpflichtet - sowohl technologisch als auch unternehmerisch.
Hinter Giritech stehen zwei der größten Venture Capital Fonds in Nordeuropa. Das Unternehmen wird von einem erfahrenen Management-Team geleitet, im Board of Directors sind einige der erfolgreichsten Unternehmer der IT-Industrie tätig.

Das Team der Giritech GmbH ist seit über 15 Jahren im Bereich Remote Control und Remote Access erfolgreich und betreut die Regionen Deutschland, Österreich und Schweiz (DACH).

Kontakt
Giritech GmbH; Mariabrunnstr. 123; 88097 Eriskirch
Tel. (0 75 41) 97 10 99-0
Fax (0 75 41) 97 10 99-99

www.giritech.de
info@giritech.de

Giritech reserves the right to change the information contained in this document without prior notice. Giritech®, EMCADS™ and G/On™ are trademarks or registered trademark of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property includes the patented systems and methods called EMCADS™. Other product names and brands used herein are the sole property of their owners. Giritech denies any and all responsibility for damages caused directly or indirectly as a result of using this document. This document could include technical inaccuracies or typographical errors to which Giritech is not liable. The content of this document is subject to change without notice. . © November 2006 Giritech GmbH and Giritech A/S.