FACT SHEET

Sicherheit auf höchstem Niveau

G/On und der richtige Umgang mit Keyloggern / Spyware

Ein Keylogger (dt. Tasten-"Rekorder") ist eine Hard- oder Software, die dazu verwendet wird, sämtliche Eingaben eines Anwenders an einem PC aufzuzeichnen. Die Protokollierung erfolgt je nach System permanent oder schlüsselwortbasiert, um Speicherplatz zu sparen. Ein automatisierter Versand der Informationen via Internet ist möglich, ebenso die lokale Speicherung der Daten, um sie zu einem späteren Zeitpunkt abzuziehen. Besonders Hacker verwenden solche Systeme, um auf einfachste Weise an private Informationen wie PIN, TAN oder Passworte zu gelangen bzw. diese aus dem Datenstrom zu rekonstruieren.

G/On kann dabei helfen, mobile Anwender vor den Gefahren durch softwarebasierte Keylogger zu schützen, da praktisch alle Sicherheitsfeatures integrierbar sind.

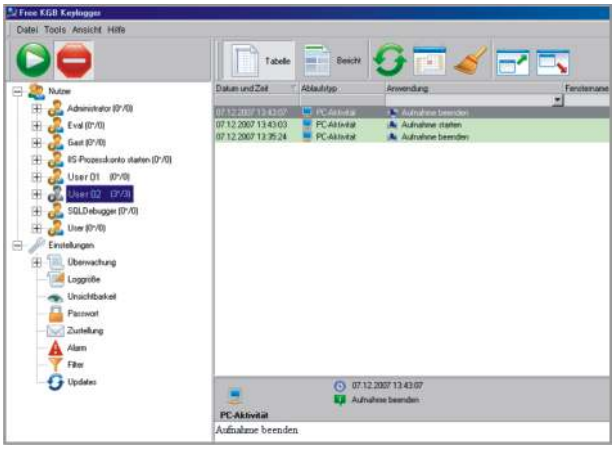
Anerkannte Schutzverfahren

Während Hardware-Keylogger (als Blackbox zwischen Tastatur und PC) in der Regel nur optisch erkannt und dann auch vermieden werden können, hinterlassen Software-Keylogger verräterische Spuren auf dem Computer. Deshalb gibt es von führenden Sicherheits-experten anerkannte Methoden, um sich gegen das Ausspähen privater Informationen durch Keylogger zu schützen:

- verwenden einer **virtuellen Tastatur** (On-Screen-Keyboard, OSK)
- überprüfen des Systems mit **Anti-Spyware-** und dedizierten **AntiVirus**-Programmen, um auch als ungefährlich eingestufte Keylogger, wie den "Free KGB Keylogger" zu enttarnen

G/On On-Screen-Keyboard

Bereits in der Grundausstattung bietet G/On ein OSK (On-Screen-Keyboard), das für den Loginvorgang genutzt werden kann. Entsprechend konfiguriert wird die virtuelle Tastatur beim Einstecken des USB Access Keys automatisch aufgerufen, so dass der Benutzer seine Zugangsdaten (Name und Passwort) gar nicht mehr über die normale Tastatur eingeben kann sondern zwingend das On-Screen-Keyboard verwenden muss. Keylogger können so die Anmeldedaten am G/On Server nicht mehr ausspähen. Unterstützt die Applikation zusätzlich Single-Sign-On, dann können die per virtueller Tastatur



Richtig konfiguriert kann G/On dabei helfen, Keylogger und Spyware zu erkennen und Gegenmassnahmen zu ergreifen - auch wenn nicht alle Keylogger (wie hier der "Free KGB Keylogger") als gleichermassen gefährlich eingestuft sind.

eingegebenen Passwortdaten direkt an die Anwendung weitergegeben werden, so dass keine weitere, sichtbare Authentifizierung im Klartext mehr notwendig ist.

Automatische Spyware-Prüfung mit G/On

Soll G/On im mobilen Einsatz auf nicht vertrauens-würdigen PCs genutzt werden (z. B. in Internet Cafes oder an Kiosk-PCs), dann ist eine automatische Prüfung auf Keylogger bzw. Spyware wie folgt implementierbar:

1. Die erforderlichen Prüfprogramme können als mobile Anwendung auf dem G/On USB Access Key zur Verfügung gestellt werden. Per "Auto-Launch" Funktion starten diese sofort beim Einstecken des Access Keys und prüfen den lokalen PC. Im Vergleich mit SSL-VPNs wird für diesen Vorgang weder eine administrative Berechtigung noch das Recht zum Starten oder Installieren von Plugins benötigt. Für die Überprüfung via G/On ist ein gewöhnliches User-Konto ausreichend.

2. Alternativ kann das Scanning direkt vom G/On Server aus initiiert werden. Die Überprüfung des lokalen PCs startet dann automatisch, sobald sich der Anwender mit Benutzername und Passwort (über das On-Screen-Keyboard) am Server authentifiziert hat.

Grundsätzlich bleibt es dem G/On User überlassen, ob er die Prüfung des PCs abwartet oder während des aktiven Scanvorgangs weiter arbeitet und im Einzelfall auf entsprechende Meldungen reagiert.

Schutz durch 2-Faktor Authentifizierung

Ein Exploit von Benutzername und Passworts hat bei G/On im Gegensatz zu herkömmlichen SSL VPNs keine direkten Konsequenzen, denn aufgrund der integrierten 2-Faktor-Authentifizierung müsste ein potenzieller Hacker auch in den Besitz der eindeutig freigeschalteten Hardware kommen (USB Access Key mit weltweit eindeutiger EDC-Nummer). Ohne die Hardware kann er von ausserhalb des Unternehmens nicht einmal auf die Anmeldemaske von G/On gelangen, geschweige denn, sich mit irgend einer Anwendung im Firmennetzwerk verbinden. Die EDC-Nummer ist ein hardware-gebundener Token, der weder extern abgefragt noch durch eine fremde Software an den G/On Server gesendet werden kann (hierfür wäre das von Giritech entwickelte, patentierte, proprietäre Protokoll EMCADS™ sowie AES 256 Verschlüsselung mit privaten und öffentlich signierten Keys notwendig).

Regeln und Zonen

Zusätzlich verfügt G/On über Regeln und Zonen-Definitionen, die eine Identifizierung erlauben, wo der Benutzer gerade arbeitet. Im Falle eines unbekannten und damit unsicheren Computers, kann die Access-Nutzung auf die Bereitstellung unkritischer Applikationen beschränkt werden. Zwar eliminiert dies ein potenzielles Keylogger-Szenario nicht, aber im Gegensatz zur (SSL)VPN lässt G/On dann ortsabhängig nur noch diejenigen Anwendung zu, bei denen ein geringes Sicherheitsrisiko besteht.

Keine sicherheitsrelevanten Daten am Client

Alle Applikationsdaten sind ausschliesslich zentral am G/On Server gespeichert - der Client besitzt keinerlei verwertbare Daten des Servers, des LANs oder der Benutzer. Während traditionelle Lösungen den (unsicheren) VPN-Client zum Bestandteil des Netzwerks machen, gibt es bei G/On keinerlei IP-Konnektivität (nodeless client), kein lokales Caching von Daten und auch sonst keine verwertbaren Informationen auf dem Computer. Der nodeless G/On Client hat aufgrund des Designs zu keinem Zeitpunkt Zugriff auf IPs, sprich: Es gibt keinen technischen Weg, über G/On solche Adressen offenzulegen. Einzig der G/On Server hat Zugriff auf die Adressen der Zielsysteme, der Client arbeitet nur auf der Loopback-Adresse und kennt maximal die öffentliche IP des G/On Servers (die natürlich kein sicherheitsrevelantes “Geheimnis” ist, denn ohne Access Key ist auch kein Zugriff möglich).

Fakten: G/On und Keylogger / Spyware

Durch die integrierbare Kombination aller hier genannten Features in Verbindung mit der 2-Faktor-Authentifizierung geht G/On deutlich über die Standardsicherheit traditioneller VPNs hinaus. Die Einbindung der entsprechenden Security-Prozesse in die G/On Umgebung wird abhängig von den Sicherheitsanforderungen in Zusammenarbeit zwischen Anwender und Giritech bzw. einem durch Giritech autorisierten Partner realisiert.
Grundsätzlich gilt aber auch für G/On wie für jede andere Anwendung, dass ein Sicherheitsverständnis beim Anwender vorhanden sein muss und sich dieser an die Security Policy des Unternehmens hält.

G/On ist ein sicheres und leistungsstarkes Produkt, das allen mir bekannten Lösungen in diesem Bereich überlegen ist.

Otto Schröder
Diakonie Kassel

G/On ist eine genial einfache und sichere Lösung, um mobilen Menschen sicheren Zugriff auf zentrale Systeme zu ermöglichen.

Thomas Merkel
altro consult Deutschland GmbH
Geschäftsbereichsleiter IT-Services

Giritech GmbH | Mariabrunnstr. 123 | 88097 Eriskirch | Tel. +49 (0) 7541 971099-0 | Fax 971099-99 | info@giritech.de | www.giritech.de