

## Netzwerkweite Überwachung der Ereignisprotokolle leicht gemacht

Wie GFI LANguard S.E.L.M. zum Erkennen von Netzwerk-Angriffen und zur Ereignisprotokoll-Überwachung eingesetzt werden kann

In diesem White Paper wird erklärt, warum eine netzwerkweite Überwachung von Ereignisprotokollen notwendig ist und wie Sie GFI LANguard S.E.L.M. dabei unterstützt. Dieses White Paper wurde von Randy Franklin Smith verfasst, dem Autor einer ausführlichen Artikelserie zum Windows-Sicherheitsprotokoll, veröffentlicht im Windows 2000 & .NET Magazine.

---

## Einführung

Die Überwachungsfunktionen von Microsoft Windows ermöglichen zwar ein grundlegendes Auditing, erfüllen jedoch längst nicht alle Anforderungen des täglichen Geschäftslebens (z. B. die Überwachung der Windows-Rechner in Echtzeit oder die periodische Analyse sicherheitsrelevanter Aktivitäten und die Bereitstellung eines Überwachungsprotokolls, mit dessen Hilfe sich Aktivitäten über einen längeren Zeitraum nachvollziehen lassen). Daher sollte ein auf Ereignisprotokoll-Dateien basierendes Tool eingesetzt werden, mit dem sich Netzwerk-Angriffe erkennen und analysieren lassen – wie der GFI LANguard Security Event Log Monitor (S.E.L.M.). In diesem White Paper wird erklärt, wie sich dank der innovativen Architektur von GFI LANguard S.E.L.M. die Log-Funktionalität von Microsoft Windows kostengünstig erweitern lässt, ohne dabei die Netzwerk-Leistung zu beeinträchtigen. Das Dokument erörtert die Verwendung von GFI LANguard S.E.L.M. zur Einhaltung von "Best Practice"-Richtlinien und Anforderungen, die öffentliche Prüfer und Regulierungsbehörden an die unternehmerische Sorgfaltspflicht stellen. Erfahren Sie auch, wie Sie die Leistungsfähigkeit von GFI LANguard S.E.L.M. optimal ausnutzen können.

Über den Autor: Dieses White Paper wurde von Randy Franklin Smith verfasst, dem renommierten Experten im Bereich "Windows-Ereignisprotokolle" und Autor der ausführlichen Serie zum Windows-Sicherheitsprotokoll, erschienen im *Windows 2000 & .NET Magazine*.

Einführung .....	2
Funktionsweise von GFI LANguard S.E.L.M.....	2
Sorgfältigkeitsanalyse .....	6
Strategien für maximalen Schutz .....	6
Wahl der geeigneten Sicherheitsstufen einzelner Rechner .....	6
Ausgewogenes Verhältnis zwischen Ressourcenbelastung und rechtzeitigen Warnmeldungen.	7
Gewährleistung der Pflege und Integrität von Sicherheitsprotokollen .....	8
Überwachung des Dateizugriffs für erhöhte interne Sicherheit.....	9
Erkennen unbefugter Web-Server-Zugriffe und -Manipulationen .....	11
Überwachung des Administrators .....	12
Erstellen eines langfristigen Überwachungspfads .....	12
Zusammenfassung .....	12
Über GFI .....	13

---

## Funktionsweise von GFI LANguard S.E.L.M.

### Übersicht über die Architektur

GFI LANguard Security Event Log Monitor (S.E.L.M.) erkennt Angriffsversuche und überwacht die Netzwerk-Sicherheit, indem er die Ereignisprotokolle sämtlicher mit Windows

2000/NT/XP/2003 betriebenen Server und Workstations kontrolliert. Bei möglicherweise unberechtigten Zugriffsversuchen und potenziellen Angriffen werden Sie in Echtzeit alarmiert.

Um eine reibungslose Integration mit der gesamten Windows-Umgebung zu gewährleisten, greift GFI LANguard S.E.L.M. auf standardmäßige Windows-Technologien zurück, z. B. Microsoft Message Queuing (MSMQ), die Microsoft Management Console (MMC), den Microsoft Windows Installer und die Open Database Connectivity (ODBC).

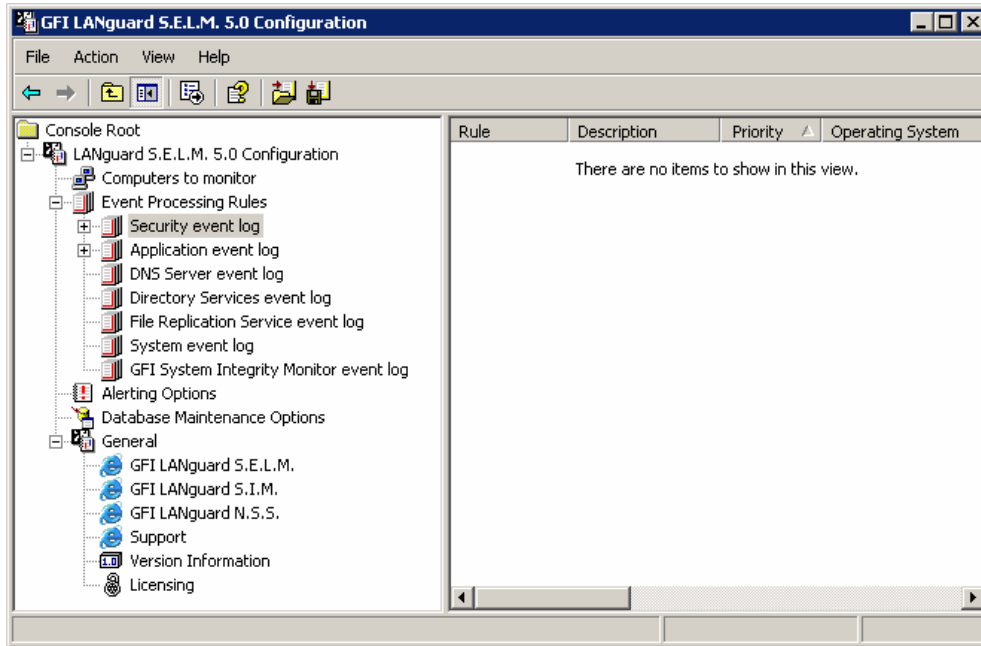
Die Implementierung einer netzwerkweiten Überwachung mit GFI LANguard S.E.L.M. erfolgt ohne großen Aufwand, da auf keinem der zu überwachenden Rechner zusätzliche Client-Software installiert werden muss. Administratoren brauchen S.E.L.M. auf nur einem Host-Computer installieren, um dann einfach nur die Systeme anzugeben, die kontrolliert werden sollen. Der Collector Agent von S.E.L.M. verwendet native Win32-APIs, um Sicherheitsereignisse von den gewählten Computern abzurufen und speichert diese Ereignisse in einer Microsoft Access-Datenbank oder auf einem MS SQL Server. Dank der ODBC-Architektur können Standard-Tools für die Berichterstellung verwendet werden, z. B. Crystal Reports von Crystal Decisions, um Berichte nach eigenen Vorgaben erstellen zu lassen.

Beim nächsten Schritt vergleicht der Alerter Agent von GFI LANguard S.E.L.M. dann die gesammelten Ereignisse mit einer Tabelle für Kategorisierungsregeln und weist den Ereignissen die Gefahrenstufen niedrig, mittel, hoch oder kritisch zu. Bei kritischen Ereignissen versendet der Alerter Agent sofort SMTP-Benachrichtigungen, beispielsweise an die E-Mail-Adresse eines Administrators, um ihn sofort über unautorisierte Zugriffsversuche zu alarmieren. Zudem kann der Sicherheitsbeauftragte für jeden überwachten Computer die Häufigkeit der Ereignissammlung vorgeben, normale Arbeitszeiten festlegen und Rechner-Sicherheitsebenen mit den Stufen niedrig, mittel oder hoch einrichten. Die Einstellung der Sicherheitsebene bewirkt, dass der Alerter Agent jedes verdächtige Ereignis, das auf Systemen mit sensiblen Informationen und Prozessen eintritt, als entsprechend schwer wiegender interpretiert. Hierdurch wird die Anzahl unnötiger Fehlalarme reduziert.

Administratoren können den erweiterten Ereignis-Monitor oder das Bericht-Modul von GFI LANguard S.E.L.M. verwenden, um regelmäßig alle sicherheitsrelevanten Ereignisse zu analysieren. Um ein ausgewogenes Verhältnis zwischen Ressourcen-Beanspruchung und zeitnaher Alarmierung zu erzielen, kann für jeden Rechner eine andere Sammelfrequenz vorgegeben werden. Ältere Protokolldaten werden zudem regelmäßig aus der aktiven Datenbank entfernt und archiviert. GFI LANguard S.E.L.M. verwendet die MSMQ-Technologie, um eine leistungsfähige Kommunikation zwischen den internen Agents zu gewährleisten.

### **Echtzeit-Überwachung und Klassifizierung von Sicherheitsereignissen**

Im Mittelpunkt der intelligenten Alarmierungsfunktionen von GFI LANguard S.E.L.M. steht der Knoten für die Ereignis-Verarbeitungsregeln aus dem Konfigurations-Snap-In der Microsoft Management Console (MMC).



### MMC-Snap-In zur Sicherheitskonfiguration von GFI LANguard S.E.L.M.

Die standardmäßigen Kategorisierungsregeln von GFI LANguard S.E.L.M. sind so konzipiert, dass das Produkt wichtige Ereignisse erkennen und den Sicherheitsbeauftragten entsprechend benachrichtigen kann, ohne ihn mit Fehlalarmen zu belasten. Die Regeln erlauben es GFI LANguard S.E.L.M., nach auffälligen Hinweisen zu suchen, z. B. Ereignisse, die zu ungewöhnlichen Zeiten oder auf Computern mit hoher Sicherheitsstufe auftreten. Ereignisse niedriger Priorität lösen keinen sofortigen Alarm aus, bleiben aber immer für eine tägliche oder wöchentliche Analyse durch den Administrator verfügbar. GFI LANguard S.E.L.M. filtert Sicherheitsereignisse nach den Gefährdungsgraden niedrig, mittel, hoch oder kritisch. Dafür analysiert das Produkt die Ereignis-ID (z. B. die Ereignisnummer eines fehlgeschlagenen Logins, Anwenderkonto-Blockierung, Dateizugriff) und die Eigenschaften des Rechners, auf dem das Ereignis eingetreten ist – einschließlich Betriebssystem, Rollenfunktion in der Domain, Sicherheitsebene und normale Betriebszeiten. Anschließend werden die Kategorisierungsregeln auf diese Daten angewandt. Alle Verarbeitungsregeln von GFI LANguard S.E.L.M. lassen sich dabei an die Netzwerk-spezifischen Merkmale anpassen.

### Kategorisierung auf Grundlage der Ereignisquelle

Bei Windows NT und Windows 2000/XP/2003 werden Ereignisse unerklärlicherweise unterschiedlich protokolliert. Aus diesem Grund berücksichtigt GFI LANguard S.E.L.M. auch das jeweilige Betriebssystem, das überwacht werden soll. Das Produkt kann auch zwischen Arbeitsplatzrechnern, Member-Servern und Domain-Controllern unterscheiden und interpretiert ein Ereignis je nach Funktion des Rechners in der Domain auf unterschiedliche Weise.

Netzwerk-Logins sind nur ein Beispiel dafür, warum das Produkt zwischen den

unterschiedlichen Betriebssystemen und Domain-Rollen differenzieren muss. Wenn sich jemand mit einem Computer über das Netzwerk verbindet (z. B. bei Zugriff auf einen Shared Folder), wird von Windows NT das Ereignis mit der ID 528 und Logon-Typ 2 protokolliert, wohingegen es von Windows 2000 als Ereignis mit der ID 540 geloggt wird. Weil GFI LANguard S.E.L.M. das Betriebssystem berücksichtigt, kann er die Ereignisnummer richtig identifizieren, je nachdem ob das Ereignis auf einem Windows NT- oder einem Windows 2000/XP/2003-System eingetreten ist. Netzwerk-Logins auf Domain-Controllern oder Servern sind während der regulären Arbeitsstunden nichts Ungewöhnliches und sollten daher nicht als verdächtig eingestuft werden. Normalerweise müssen Anwender bei ihrer Arbeit jedoch nicht auf andere Workstations zugreifen.

Logins auf Arbeitsplatz-Rechnern über das Netzwerk sollten daher als verdächtig eingestuft werden, da Unberechtigte, die remote auf einen Arbeitsplatz-Rechner zugreifen wollen, sich als autorisierte Anwender dieser Workstation ausgeben und versuchen könnten, über die Identität dieses Anwenders auf andere Server im Netzwerk zuzugreifen. Aus diesem Grund stuft GFI LANguard S.E.L.M. Netzwerk-Logins auf Arbeitsplatz-Rechnern mit höherer Wichtigkeit ein als auf Domain-Controllern oder Servern.

### **Netzwerkweite Überwachung von Workstations und Servern**

Da die sicherheitsrelevanten Aktivitäten von Windows über alle Rechner einer Domain verteilt sind, ist ein netzwerkweiter Einsatz von GFI LANguard S.E.L.M. am sinnvollsten. Indem man S.E.L.M. alle Arbeitsplatz-Rechner, Member-Server und Domain-Controller eines Netzwerkes überwachen lässt, kann das Produkt eine umfassende Abbild der Netzwerk-Sicherheit erstellen. Die voreingestellten Kategorisierungsregeln erkennen vielfältige Szenarien wie:

- Fehlgeschlagene Logins
- Blockierte Zugangsberechtigungen
- Erstellte Zugangsberechtigungen und Änderungen von Gruppenzugehörigkeiten außerhalb der regulären Arbeitszeit.
- Logins auf Hochsicherheitssystemen außerhalb der regulären Arbeitszeiten
- Zugriff auf Arbeitsplatz-Rechner durch Netzwerk-Logins
- Änderungen der Überwachungsregeln
- Gelöschte Sicherheitsprotokolle
- Erfolgreiche oder fehlgeschlagene Dateizugriffe (inklusive Zugriffe auf bestimmte Dateien)

Ein Ereignis kann je nach den Umständen des Eintritts auf verschiedene Arten interpretiert werden. Daher liefert GFI LANguard S.E.L.M. bei dessen Kategorisierung eine Erklärung für die gewählte Einordnung. Zudem wird erklärt, auf welche Art von Sicherheitsproblem das Ereignis möglicherweise hindeutet. Administratoren werden sogar weitere Schritte empfohlen, die sie zur Klärung der Situation und als weitergehende Maßnahmen einleiten können.

Die Standardeinstellung von GFI LANguard S.E.L.M. sieht eine Benachrichtigung über kritische

Ereignisse per SMTP-Mail vor. Administratoren können jedoch eine Benachrichtigung bereits bei Ereignissen mit einer niedrigeren Sicherheitsebene auslösen lassen. Um einen Überblick über weniger wichtige Ereignisse zu behalten, für die keine Benachrichtigung verschickt wird, kann der Sicherheitsverantwortliche den Vorschlägen einer Sorgfältigkeitsanalyse folgen.

---

## Sorgfältigkeitsanalyse

Um Prüfungsanforderungen bei allgemeinen Kontrollen durch öffentliche Prüfer und Regulierungsbehörden erfüllen zu können, sollten Unternehmen zusätzlich zu einer Echtzeit-Überwachung auch eine regelmäßige Überwachung geringfügiger Ereignisse vornehmen. Damit Administratoren nicht zu viel Zeit mit dieser Aufgabe verbringen müssen, werden von GFI LANguard S.E.L.M. mehrere vorgefertigte Berichte bereitgestellt. Sicherheitsverantwortliche können somit Ereignissen aller Sicherheitsstufen nachgehen, indem sie einfach Berichte wie "Yesterday's High Security Events", "Last Week's Medium Security Events" oder "Last Month's Low Security Events" täglich, wöchentlich oder monatlich durchsehen. Zusätzliche Berichte ermöglichen eine Überwachung der Aktivitäten des laufenden Tages oder von mittleren und niedrigen sicherheitsrelevanten Ereignissen in kürzeren Zeitabständen.

---

## Strategien für maximalen Schutz

GFI LANguard S.E.L.M. bietet flexible Funktionen für die Verwaltung von Sicherheitsprotokollen. Bei der Implementierung des Produkts ist es jedoch wichtig, die individuellen Bedürfnisse des Unternehmens zu berücksichtigen und die Anzahl der Fehlalarme möglichst gering zu halten. Bereits bei den Vorbereitungen für die Implementierung von GFI LANguard S.E.L.M. sollte der Administrator die relativen Sicherheitsstufen der Netzwerk-Rechner, die potenzielle Leistungsbeanspruchung im Verhältnis zur Rechtzeitigkeit der Alarmierung und die für die Netzwerk-Umgebung spezifischen Risikoszenarien berücksichtigen.

---

## Wahl der geeigneten Sicherheitsstufen einzelner Rechner

Bei GFI LANguard S.E.L.M. muss für jeden zu überwachenden Rechner die erforderliche Sicherheitsstufe vom Administrator einzeln festgelegt werden. Bei der Registrierung eines Arbeitsplatz-Rechners sollte auch der Aufgabenbereich des Benutzers des jeweiligen Rechners berücksichtigt werden. Rechnern von Anwendern, die Zugang zu wichtigen Daten haben – z. B. Administratoren – und solche, die Finanzdaten verwalten, sollte eine hohe Sicherheitsstufe zugewiesen werden. Zu weiteren Workstations, die unter Umständen eine höhere Sicherheitsstufe erfordern, zählen Rechner, die innerhalb des Rechenzentrums installiert oder die für kritische Prozesse verantwortlich sind, z. B. das physikalische Zugangssystem eines Unternehmens-Netzwerkes. Arbeitsplatz-Rechner von Mitarbeitern, die eingeschränkten Zugriff auf kritische Daten oder Prozesse haben, sollten mit einer niedrigen Sicherheitsstufe konfiguriert werden. Die mittlere Sicherheitsstufe lässt sich somit für Arbeitsplatz-Rechner aller

anderen Anwender verwenden, die zwischen diesen beiden Sicherheitsstufen liegen.

Da Domain-Controller eine wichtige Sicherheitsrolle einnehmen, sollten Administratoren diese Rechner einer mittleren bis hohen Sicherheitsstufe zuordnen. Üblicherweise wird Rechnern in einer entmilitarisierten Zone (DMZ – z. B. E-Mail-Gateway und Web-Server) eine hohe Sicherheitsstufe zugewiesen. Dies gilt auch für Rechner, auf denen Personal-, Finanz-, Forschungs- oder Entwicklungsdaten gespeichert sind. Applikations- und Datenbank-Server speichern normalerweise wichtige Informationen oder Prozesse und sollten normalerweise mit einer mittleren oder hohen Sicherheitsstufe versehen werden. Niedrige und mittlere Sicherheitsstufen sollten für Datei-Server verwendet werden, die allgemeine Informationen auf Abteilungsebene speichern. Unternehmen, die bereits ein System zur Klassifizierung der Informationssicherheit besitzen, können dieses verwenden, um Arbeitsplatz-Rechner und Server zu bestimmen, die für vertrauliche oder geheime Daten zuständig sind.

## Ausgewogenes Verhältnis zwischen Ressourcenbelastung und rechtzeitigen Warnmeldungen

Die Frequenz, mit der GFI LANguard S.E.L.M. Ereignisse von jedem überwachten Computer sammelt, hat einen direkten Einfluss auf die CPU-Belastung des Computers und die allgemeine Netzwerk-Bandbreite. Rechner einer höheren Sicherheitskategorie werden selbstverständlich öfter abgefragt, aber auch die Rolle des Computers beeinflusst die Abfragefrequenz. Ein Arbeitsplatzrechner mit einer hohen Sicherheitseinstufung ist für gewöhnlich weniger wichtig als ein Server mit einer ebenfalls hohen Sicherheitsebene. Die Tabelle auf der folgenden Seite zeigt Vorschläge für Abfragefrequenzen, je nach Domänenrolle und Sicherheitseinstufung eines Systems. In Anbetracht der hohen Anzahl von Workstations in den meisten Unternehmen kann durch eine niedrigere Abfragefrequenz für Arbeitsplatzrechner das größte Einsparpotenzial bei der Netzwerk-Bandbreite erzielt werden.

Rolle	Sicherheitsebene	Abfragefrequenz
Domain-Controller	Hoch	1 Minute
	Mittel	5 Minuten
	Niedrig	15 Minuten
Member-Server	Hoch	1 Minute
	Mittel	5 Minuten
	Niedrig	1 Stunde
Workstation	Hoch	5 Minuten
	Mittel	6 Stunden
	Niedrig	1 Tag

### Empfohlene Abfrageintervalle

---

## Gewährleistung der Pflege und Integrität von Sicherheitsprotokollen

Aus technischer Sicht könnte ein gut geplanter Angriff auf ein schlecht konfiguriertes System einem Angreifer Zugriff auf Administratorebene verschaffen. So ließe sich das Ereignisprotokoll löschen, bevor es durch GFI LANguard S.E.L.M. abgerufen wird. Windows speichert jedoch stets einen speziellen Ereigniseintrag, wenn das Protokoll gelöscht wird – auch wenn die Auditing-Funktion ausgeschaltet ist – und GFI LANguard S.E.L.M. klassifiziert dieses Ereignis dann auf jedem System als kritisch.

Daher sollten Sie es sich zur Regel machen, Sicherheitsprotokolle auf Rechnern, die von GFI LANguard S.E.L.M. überwacht werden, niemals manuell zu löschen. Hierdurch ist stets sichergestellt, dass alle Ereignisse nachvollziehbar bleiben und Verantwortlichkeiten unter den Administratoren beibehalten werden. GFI LANguard S.E.L.M. löscht das Sicherheitsprotokoll automatisch, nachdem das Programm die Ereigniseinträge abgerufen hat, so dass ein manuelles Löschen niemals notwendig ist.

Unter Windows muss für jeden Rechner die maximale Größe der Log-Dateien angegeben werden. Ist die voreingestellte Größe erreicht, werden vom Betriebssystem keine weiteren Aktivitäten gespeichert. Daher könnten wichtige Informationen verloren gehen, wenn die Protokolldatei zwischen den Abfragevorgängen durch GFI LANguard S.E.L.M. den eingestellten Wert überschreitet. Aus diesem Grund sollten Administratoren die Maximalgröße des Sicherheitsprotokolls jedes Systems an die für den jeweiligen Rechner festgelegte Abruffrequenz und den Umfang der darauf ablaufenden Prozesse anpassen. Für Systeme mit kurzen Abfrageintervallen durch GFI LANguard S.E.L.M. wird selbst eine ungewöhnlich kleine Protokolldatei niemals voll werden. Bei den heute üblichen Festplattengrößen ist es zudem nicht sehr sinnvoll, die Speichergröße von Protokolldateien zu begrenzen. Sicherheitsverantwortliche können sich jedoch absichern, indem sie standardmäßig eine Protokollgröße zwischen 5 MB und 10 MB angeben. In einem Active Directory-Umfeld können Administratoren einfach ein mit einem Domain-Root verknüpftes Group Policy Object (GPO) verwenden, um für Rechner mit Windows 2000 eine Standard-Protokollgröße festzulegen. Rechner mit Windows NT und Windows 2000, die nicht unter AD verwaltet werden, sind manuell zu konfigurieren.

Windows kann so eingerichtet werden, dass das System abstürzt, wenn die Log-Datei voll ist. Für unternehmensrelevante Hochsicherheitsrechner oder zur Erfüllung rechtlicher Überwachungsanforderungen (z. B. auf Systemen für den Zahlungsverkehr) kann eine solche Einstellung durchaus notwendig sein. Um die Möglichkeit eines Absturzes minimal zu halten, sollten Administratoren jedoch eine große Protokolldatei und ein kurzes Abrufintervall festlegen. Dadurch ist sichergestellt, dass die Protokolldatei vor dem nächsten Abruf durch GFI LANguard S.E.L.M. nicht vollständig gefüllt sein wird.

---

## Überwachung des Dateizugriffs für erhöhte interne Sicherheit

Die Dateiüberwachung unter Windows ermöglicht es Administratoren, bei bestimmten Dateien verschiedene Zugriffsarten zu protokollieren. Diese Windows-Funktion ist sehr hilfreich um zu prüfen, wie Anwender auf bestimmte Dokumente, z. B. Dateien aus Microsoft Excel und Microsoft Word, zugreifen. Diese Kontrollfunktion kann aber auch dazu verwendet werden, beispielsweise Änderungen an Dateiverzeichnissen, die ausführbare Dateien enthalten, oder unzulässige Zugriffsversuche auf Dateien einer Datenbank festzustellen. Sicherheitsverantwortliche können fehlgeschlagene sowie erfolgreiche Zugriffsversuche auf bestimmte Dateien und Verzeichnisse entsprechend der Zugriffsarten *Lesen*, *Schreiben*, *Löschen*, u. ä. prüfen. (Um Änderungen an einem Objekt zu überwachen, aktivieren Sie die Überwachung für erfolgreiche Schreibvorgänge. Um Anwender zu überwachen, die versuchen, auf Dateien zuzugreifen, für die sie keine Zugriffsberechtigung haben, ist die Überwachung für fehlgeschlagene Lesevorgänge zu aktivieren.) Zusätzlich ist zu beachten, dass Windows potenzielle, nicht jedoch definitive Änderungen protokolliert: Objektüberwachungsereignisse werden zum Zeitpunkt des Dateizugriffs erstellt. Wenn ein Anwender z. B. ein Word-Dokument mit Lese- und Schreibberechtigung öffnet und es anschließend einfach wieder schließt, ohne eine Änderung vorgenommen zu haben, dann protokolliert Windows die Ereignisse als *Open* (Ereignis-ID 560) und *Close* (Ereignis-ID 562) um zu zeigen, dass der Anwender das Objekt für einen Schreibzugriff geöffnet hat.

GFI LANguard S.E.L.M. bietet, wie für eine Sicherheitslösung dieser Art erwartet wird, Kategorisierungsregeln für alle Objektereignisse. Das Produkt ermöglicht es jedoch auch Objektzugriffereignisse, die mit sicherheitsrelevanten Dateien oder Verzeichnissen (je nach Administrator-Vorgabe) verbunden sind, in ihrer Wichtigkeit hochzustufen. Hierdurch können beliebig viele Dateien und Verzeichnisse überwacht werden, und gleichzeitig kann GFI LANguard S.E.L.M. aber auch so konfiguriert werden, dass besonders kritische Dateien/Verzeichnisse bei der Überwachung Vorrang haben. Der Sicherheitsverantwortliche muss lediglich alle für die Überwachung vorgesehenen Objekte festlegen und dann mit Hilfe von S.E.L.M. die Sicherheitsebene derjenigen Ereignisse hochstufen, die mit bestimmten Datei- oder Verzeichnisnamen verbunden sind.

Windows ist durchaus in der Lage, erfolgreiche Zugriffe und fehlgeschlagene Zugriffsversuche auf Objekte aufzuzeichnen, aber auf Grund der immensen Datenmenge, die normalerweise anfällt, ist die Analyse der Objektüberwachung am aufwendigsten. Um wichtige Aktivitäten auf Dateiebene zu erkennen, ohne viel Zeit mit dem Durchsuchen von Sicherheitsprotokollen zu verbringen, sollten Administratoren den Einsatz von GFI LANguard S.E.L.M. mit einem durchdachten Objekt-Auditing kombinieren. Bei der Konfigurierung der Objektüberwachung sind drei Aspekte zu berücksichtigen:

- Welche Objekte sollen überwacht werden?

- Welche Bereiche (z. B. Anwender/Gruppen) sollen für jedes Objekt protokolliert werden?
- Welche Zugriffsarten sollen für jeden Bereich überwacht werden?

Bei ihrer Entscheidung, welche Objekte zu überwachen sind, sollten Administratoren bedenken, dass sich GFI LANguard S.E.L.M. so konfigurieren lässt, dass Untergruppen dieser Objekte bei der Beobachtung besonders berücksichtigt werden. An erster Stelle sollte der sparsame Umgang mit den System-Ressourcen stehen. Je mehr Objekte überwacht werden, desto mehr CPU-Zeit, Netzwerk-Bandbreite und Festplatten-Speicher werden beansprucht.

Für die Wahl der Anwender oder Gruppen, die für ein bestimmtes Objekt verfolgt werden sollen, ist die Gruppe "JEDER" wohl die beste Wahl. Findet eine Überwachung nur für bestimmte Anwender statt, könnte einem Unternehmen Voreingenommenheit oder die gezielte Überwachung von Angestellten vorgeworfen werden, falls das Sicherheitsprotokoll einmal als Begründung für Disziplinarmaßnahmen eingesetzt werden sollte. Die Verwendung anderer Gruppen als "JEDER" ist zudem riskant, weil wichtige Zugriffsereignisse übersehen werden könnten, wenn jemand versehentlich Zugriff auf ein Objekt erhält.

Die Entscheidung, welche Zugangsarten zu überwachen sind, muss besonders überlegt sein. Mit dieser wichtigen Einstellung kann der Umfang der ebenfalls protokollierten irrelevanten Ereigniseinträge eingegrenzt werden. Im Allgemeinen sollten erfolgreiche Lesezugriffe ignoriert werden – ansonsten würde sich die Log-Datei zu schnell mit harmlosen Ereignissen füllen. Erfolgreiche Schreibzugriffe hingegen sind nützlich, wenn es für Sie wichtig ist zu wissen, wer Objekte geändert hat oder wenn Sie über verdächtige Änderungen an Objekten informiert werden müssen (z. B. HTML- und Bilddateien oder Active Server Pages (ASP) auf einem Web-Server), deren Aktualisierung nur in einem kontrollierten Umfeld erfolgen sollte. Mit der Überwachung fehlgeschlagener Lese- oder Schreibzugriffsversuche lassen sich Anwender identifizieren, die ein Objekt ohne die dafür notwendige Autorisierung öffnen wollten und dank der Zugangskontrollliste des Objekts (Access Control List, ACL) abgewiesen wurden.

Eine Beschränkung des Auditing auf eine bestimmte Gruppe (anstatt der Gruppe "JEDER") ist nur dann nützlich, wenn der Administrator alarmiert werden möchte, falls die ACL des Objekts den Zugriff durch einen unautorisierten Anwender nicht verhindern konnte. Zum Beispiel könnte ein Finanzdienstleister Abteilungen für das Investment-Banking und Maklergeschäfte haben. Um den Insider-Handel zu unterbinden, sollten die Makler niemals Zugriff auf die Access-Datenbank der Investment-Banker haben. Als Absicherung kann der Administrator nun Windows so konfigurieren, dass erfolgreiche Lesezugriffe von der Gruppe "Makler" auf die Investment-Banking-Datenbank überwacht werden. Auf diese Weise verzeichnet Windows die Aktivitäten eines Maklers, wenn er auf die Datenbank zugreift, selbst wenn die ACL der Datenbank den Anwender unbeabsichtigt zugelassen hat oder er aus Versehen der Gruppe "Investment-Banker" hinzugefügt wurde. Hat der Sicherheitsverantwortliche GFI LANguard S.E.L.M. so konfiguriert, dass Ereignisse in Verbindung mit dem Dateinamen der Investment-Banking-Datenbank einer höheren Sicherheitsstufe zugerechnet werden, wird er

benachrichtigt, sobald ein Zugriff stattfindet.

Dieses Beispiel verdeutlicht, wie wichtig es ist, Anwender, Gruppen und Zugriffsarten, die Sie von Windows überwachen lassen, richtig einzugrenzen. Sie können GFI LANguard S.E.L.M. so konfigurieren, dass nur bestimmte Objekte überwacht werden, aber die vom Programm protokollierten Zugriffsarten (z. B. fehlgeschlagene Lese- bzw. Schreibzugriffe und erfolgreiche Lese- bzw. Schreibzugriffe), sind abhängig von den Zugriffsarten, die Sie in Windows einrichten. Daher sollten Sie versuchen, nur die für Sie notwendigen Bereiche der Windows-Überwachung zu konfigurieren, abhängig davon, welche Zugriffsarten GFI LANguard S.E.L.M. als kritisch betrachten soll. Nehmen Sie zum Beispiel an, Sie möchten die Datei *payroll.xls* auf fehlgeschlagene Lesezugriffe überwachen. Wenn Sie die Windows-Überwachung für alle Zugriffsarten aktivieren und dann GFI LANguard S.E.L.M. so konfigurieren, dass *payroll.xls*-spezifische Ereignisse überwacht werden, erhalten Sie von GFI LANguard S.E.L.M. nicht nur dann eine Benachrichtigung, wenn jemand ein Ereignis aufgrund eines fehlgeschlagenen Lesezugriffs verursacht hat, sondern auch, wenn generell auf *payroll.xls* zugegriffen wird. Um dieses Übermaß an Alarmierungen zu vermeiden, brauchen Sie das Windows-Auditing nur für fehlgeschlagene Lesezugriffe aktivieren.

---

## Erkennen unbefugter Web-Server-Zugriffe und - Manipulationen

Für Web-Server ist eine Echtzeit-Überwachung der Sicherheitsprotokolle sehr wichtig – und effektiv, weil auf einem Web-Server verdächtige Aktivitäten einfacher festgestellt werden können als auf einem internen Netzwerk-Server. Die Überwachung des Dateizugriffs ist besonders hilfreich bei der Erkennung von Web-Site-Modifizierungen. Ein nach "Best-Practice"-Richtlinien konfigurierter Web-Server hat klar definierte Unterverzeichnisse für HTML-, ASP- und Bilddateien. Diese Dateien bleiben, verglichen mit Datenbanken oder anderen Dateien, die aufgrund von Web-Site-Besuchen von Anwendern modifiziert werden, mehr oder weniger unverändert. Indem man Windows so konfiguriert, dass alle erfolgreichen Änderungen an diesen Verzeichnissen überwacht werden und die Sicherheitsstufe von Zugriffereignissen für darin enthaltene Dateinamen mit GFI LANguard S.E.L.M. erhöht, kann der Administrator bei Änderungen an der Web-Site sofort benachrichtigt werden. Um Fehlalarme zu vermeiden, die bei einer notwendigen zulässigen Änderung der Web-Site entstehen würden, ist es notwendig, die Überwachung von erfolgreichen Objektzugriffs-Ereignissen in diesem Fall zeitweilig zu deaktivieren. Windows wird dadurch daran gehindert, die Aktualisierungen zu protokollieren. Wenn Administratoren das Versenden von Alarmmeldungen verhindern möchten, kann alternativ auch der jeweilige Verzeichnisname aus der Special-Watchlist von GFI LANguard S.E.L.M. entfernt werden. Änderungen werden dann zwar weiterhin von Windows protokolliert und in der Datenbank von GFI LANguard S.E.L.M. entsprechend den Kategorisierungsregeln klassifiziert, aber die Sicherheitsstufe der Ereignisse wird nicht auf "kritisch" erhöht. Infolge dessen werden auch keine Warnmeldungen versendet.

---

## Überwachung des Administrators

Eine der Schwachstellen des Windows-Sicherheitsprotokoll besteht darin, dass Administratoren nicht hinreichend kontrolliert werden können. Windows speichert zwar die Aktivitäten des Administrators (Pflege der Zugangskonten, Rechte, usw.), aber es besteht immer die Gefahr, dass er die Log-Datei löscht, die Überwachungsfunktion deaktiviert oder die Protokolldatei direkt modifiziert, indem er das System herunterfährt und mit einer 3,5" DOS-Diskette bootet.

Eine gesicherte Installation von GFI LANguard S.E.L.M. kann diese Probleme lösen, damit auch Sicherheitsverantwortliche für Fehler oder Missbrauch zur Verantwortung gezogen werden können. Die Standardeinstellungen von GFI LANguard S.E.L.M. bieten voreingestellte Berichte zu Administrator-Aktivitäten und bewerten Ereignisse wie das Löschen eines Protokolls oder eine Änderung der Audit-Regeln als kritisches Ereignis. Da GFI LANguard S.E.L.M. oft Ereignisse von Hochsicherheitsrechnern in einer physikalisch getrennten Datenbank sammelt, bedeutet eine Sicherung der Produktinstallation, dass der Rechner, auf dem die Datenbank von GFI LANguard S.E.L.M. installiert ist, physikalisch zu schützen ist. Dieser Rechner sollte zudem so vor Netzwerk-Angriffen gesichert sein, wie in den Richtlinien "National Security Recommendation Guides for Windows" der amerikanischen National Security Agency (NSA) empfohlen (kostenlos unter <http://www.nsa.gov> erhältlich).

---

## Erstellen eines langfristigen Überwachungspfads

Um die Nachverfolgbarkeit von Administrator-Aktionen, rechtliche Untersuchungen und Trendanalysen zu unterstützen, sollten Sie die Sicherheitsprotokolle auf einem einmal beschreibbaren Medium speichern, z. B. auf einer CD-R. Darauf auf einer solchen CD lassen sich auch Audit-Datenbanken sichern, die mit der automatischen Archivierungsfunktion von GFI LANguard S.E.L.M. erstellt wurden.

---

## Zusammenfassung

Windows unterstützt die vollständige Protokollierung von Sicherheitsereignissen, stellt jedoch kaum Möglichkeiten bereit, die Daten zu analysieren, zu archivieren und in Echtzeit zu überwachen. Neben den oft kryptischen Ereignisbeschreibungen verursacht auch die Tatsache, dass auf jedem Rechner eine eigene Protokolldatei geführt wird, größere Probleme. Dennoch ist es heute in unserer vernetzten Geschäftswelt äußerst wichtig, sicherheitsrelevante Aktivitäten nachverfolgen und auf Zugriffsverletzungen sofort reagieren zu können. GFI LANguard S.E.L.M. baut auf den grundlegenden Überwachungsfunktionen von Windows auf, um diese Anforderungen umfassend zu erfüllen. Eine durchdacht eingesetzte Installation von GFI LANguard S.E.L.M. ermöglicht eine Reduzierung von Fehlalarmen, selbst Administratoren können für Missbrauch zur Verantwortung gezogen werden, und es lassen sich sichere Protokollarchive erstellen.

Weitere Informationen zu GFI LANguard S.E.L.M. und eine kostenfreie Testversion finden Sie

unter <http://www.gfisoftware.de/de/lanselm/>.

---

## Über GFI

GFI ([www.gfisoftware.de](http://www.gfisoftware.de)) ist ein führender Entwickler und Anbieter von Produkten für Netzwerk- und Inhaltssicherheit sowie von Kommunikationslösungen. Das Produktportfolio von GFI umfasst unter anderem den Netzwerk-Fax-Server GFI FAXmaker for Exchange/SMTP, die Sicherheitslösung GFI MailSecurity for Exchange/SMTP zur Überprüfung von E-Mail-Inhalten und zum Schutz vor E-Mail-basierten Exploits und Viren, die Server-basierte Anti-Spam-Software GFI MailEssentials for Exchange/SMTP, GFI LANguard Network Security Scanner (N.S.S.) für Sicherheits-Scans und Patch-Management, GFI Network Server Monitor zum automatischen Versand von Warnmitteilungen und zur Fehlerbehebung bei Netzwerk- und Server-Problemen, GFI LANguard Security Event Log Monitor (S.E.L.M.) zur Ereignisprotokoll-basierten Eindringlingserkennung und netzwerkweiten Verwaltung von Ereignisprotokollen sowie GFI LANguard Portable Storage Control (P.S.C.) zur netzwerkweiten Kontrolle wechselbarer Speichermedien. GFI-Produkte sind im Einsatz bei Microsoft, Telstra, Time Warner Cable, Shell Oil Lubricants, NASA, DHL, Caterpillar, BMW, der US-Steuerbehörde IRS und der USAF. GFI unterhält Niederlassungen in den USA, Großbritannien, Deutschland, Zypern, Rumänien, Australien und Malta und wird von einem weltweiten Netzwerk von Distributoren unterstützt. GFI ist "Microsoft Gold Certified Partner" und erhielt die Auszeichnung "Microsoft Fusion (GEM) Packaged Application of the Year". Weitere Informationen erhalten Sie unter <http://www.gfisoftware.de>.

© 2004 GFI Software Ltd. Alle Rechte vorbehalten. Die in diesem Dokument aufgeführten Informationen geben den von GFI zum Zeitpunkt der Veröffentlichung vertretenen Standpunkt zum Thema des White Papers wieder. Änderungen aufgrund von veränderten Marktbedingungen sind vorbehalten. Die in diesem Dokument präsentierten Informationen stellen keine Verpflichtung seitens GFI dar, und für ihre Genauigkeit wird nach dem Datum der Veröffentlichung keine Garantie übernommen. Dieses White Paper dient nur der Produktinformation. GFI ÜBERNIMMT KEINE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE HAFTUNG FÜR DIE IN DIESEM DOKUMENT PRÄSENTIERTEN INFORMATIONEN. GFI, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI LANguard, GFI Network Server Monitor, GFI DownloadSecurity und die zugehörigen Produkt-Logos sind eingetragene Marken oder Marken von GFI Software Ltd. in den Vereinigten Staaten und/oder anderen Ländern. Alle in diesem Dokument aufgeführten Produkte oder Firmennamen sind Eigentum der jeweiligen Inhaber.

