Sicherheitseinstellungen

mit NetSupport Manager

Da die Belegschaft zunehmend in hybriden Arbeitsumgebungen verteilt ist, wird es für jedes Unternehmen immer wichtiger, über Technologien zu verfügen, die effektives Arbeiten ermöglichen und gleichzeitig für Sicherheit sorgen.

Hier kommt NetSupport Manager ins Spiel. Mit Sicherheitsfunktionen wie Aktivitätsprotokollen, Benutzerbestätigungen, 256-Bit-Verschlüsselung, Smartcard-Unterstützung und AD-Integration ist es kein Wunder, dass militärische und finanzielle Institutionen weltweit darauf vertrauen.

Sicherheitsoptionen für den NetSupport Connectivity (Gateway) Server

Gateway-Schlüssel

Ein NetSupport Connectivity Server kann mit mehreren Gateway-Schlüsseln konfiguriert werden. Jeder Client, der eine Verbindung zum NetSupport Connectivity Server herstellen möchte, muss mit einem Gateway-Schlüssel konfiguriert werden, der mit dem am NetSupport Connectivity Server festgelegten Schlüssel übereinstimmt. Wenn der Schlüssel auf dem Client-Computer nicht übereinstimmt, wird keine Verbindung zum NetSupport Connectivity Server zugelassen. Das Control kann mit unterschiedlichen Gateway-Symbolen konfiguriert werden, um Clients auf dem NetSupport Connectivity Server mit verschiedenen Gateway-Schlüsseln zu durchsuchen. So können Sie steuern, welche Clients für welches Control sichtbar sind. Auch hier gilt: Wenn das Control nicht mit einem Gateway-Schlüssel konfiguriert ist, der mit einem der Schlüssel auf dem NetSupport Connectivity Server übereinstimmt, wird keine Berechtigung erteilt, den NetSupport Connectivity Server zu durchsuchen oder die Liste der Clients abzurufen, um eine Verbindung herzustellen.

SSL/TLS-Zertifikate

Für höchste Datensicherheit wurden SSL/TLS-Zertifikate hinzugefügt, um sicherzustellen, dass alle über das Gateway übertragenen Daten verschlüsselt sind. Kunden können entweder ihr eigenes Zertifikat eingeben oder für das Gateway ein Let's Encrypt-Zertifikat erstellen und verwenden lassen.

Gateway-Operatoren

Eine weitere Möglichkeit, den Zugriff auf den NetSupport Connectivity Server einzuschränken, ist die Einführung von Gateway-Operatoren. Dabei handelt es sich um

Benutzerkonten, die Sie auf dem NetSupport Connectivity Server konfigurieren können, sodass nur die angegebenen Operatoren den Server durchsuchen dürfen. Dies kann beispielsweise nützlich sein, wenn eine Person, die den Gateway-Schlüssel kennt, das Unternehmen verlässt. Statt den Gateway-Schlüssel zu ändern, können Sie einfach das Operator-Konto entfernen, sodass diese Person keinen Zugriff mehr auf den NetSupport Connectivity Server hat.

Ereignisprotokollierung

Die Aktivitätsprotokollierung des NetSupport Connectivity Servers ist standardmäßig aktiviert und wird unter folgendem Pfad gespeichert:

C:\Program Files\Common Files\NSL\Connectivity Server\

Die Einstellungen für die NetSupport Connectivity Server-Komponente werden über den Connectivity Server Configurator vorgenommen. Dieser ist zugänglich, indem Sie mit der rechten Maustaste auf das NetSupport Connectivity Server-Symbol in der Systemleiste klicken.

Client-Sicherheitsoptionen

Benutzerauthentifizierung

Es ist möglich, den Client so zu konfigurieren, dass ein lokal gespeicherter Benutzername und ein Passwort für die Verbindung verwendet werden, die in der Client-Konfigurationsdatei gespeichert werden. Alternativ können Sie den Zugriff auf den Client über NT-Authentifizierung oder AD-Authentifizierung steuern, indem Sie eine Gruppe aus Ihrer Domäne zur Authentifizierung auswählen. Wenn eine dieser Optionen am Client eingestellt ist und ein Control versucht, eine Verbindung herzustellen, wird eine Eingabeaufforderung für Benutzername und Passwort angezeigt. Die eingegebenen Daten müssen mit den beim Client festgelegten Details übereinstimmen, um die Verbindung zu erlauben.

Falls sich der Name der Client-Ausführungsdatei ändert, wird deren Ausführung verhindert, um vor Exploits und Malware zu schützen. Eine praktische Funktion, die sicherstellt, dass keine unerwünschten Aktivitäten stattfinden.

Sicherheitsschlüssel

Zusätzliche Sicherheit bietet die Möglichkeit, dass Control-Benutzer nur dann eine Verbindung herstellen können, wenn das Control denselben Sicherheitsschlüssel wie der Client verwendet. Optional kann dies als Seriennummer in Ihrer NetSupport-Lizenzdatei festgelegt werden. Der Sicherheitsschlüssel muss sowohl beim Client als auch beim Control eingerichtet werden.

Benutzerbestätigung

Wenn ein Control-Benutzer versucht, eine Verbindung herzustellen, wird dem Client eine Nachricht angezeigt. Sofern der Benutzer am Client die Anfrage nicht ausdrücklich akzeptiert, wird die Verbindung abgelehnt.

Verschlüsselung

Wenn die Verschlüsselung aktiviert ist, wird die gesamte zwischen Control und Client übertragene Information so verschlüsselt, dass sie für Dritte nur schwer lesbar ist. NetSupport Manager bietet eine Vielzahl an Verschlüsselungsoptionen, die von 56-Bit-DES bis zu 256-Bit-AES reichen. Dadurch können Sie das erforderliche Gleichgewicht zwischen Sicherheit und Leistung finden. Je höher das Verschlüsselungsniveau, desto höher kann der Leistungsverlust ausfallen. Wählen Sie das Verschlüsselungsniveau aus, das während einer Verbindung zwischen Control und Client verwendet werden soll. Standardmäßig ist die Verschlüsselung für alle Verbindungen auf „keine“ und für HTTP-Verbindungen auf 56-Bit-DES eingestellt.

„Hervorragender Kundenservice. Das Produkt ist sicher, effektiv und stabil. Ich bin mit der Software sehr zufrieden und empfehle sie gerne für IT-Support-Zwecke.“

James Hill – Premiserv

Smartcard-Authentifizierung

Wenn diese Option am Client ausgewählt ist, muss der Control-Benutzer bei der Verbindung zum Client eine Benutzer-ID und ein Passwort sowie die Smartcard und die PIN eingeben.

Zugriffsberechtigungen

Mithilfe der Client-Konfiguration können bestimmte Fernsteuerungsfunktionen deaktiviert werden, z. B. das Verhindern von Dateiübertragungen oder das Deaktivieren des Steuerungsmodus während der Anzeige.

Client-Profile

Es ist möglich, unterschiedliche Zugriffsrechte für Control-Benutzer zu konfigurieren, je nachdem, welcher Benutzer sich bei der Verbindung über den Client authentifiziert. Dies erfolgt mithilfe der Client-Profile.

Anpassbarer Text

Mit dieser Funktion können Sie anpassbare Nachrichten hinzufügen, die auf dem Client-Rechner angezeigt werden, wenn eine Verbindung mit dem Control hergestellt wird, damit der Endbenutzer über die Remote-Verbindung informiert ist.

Replay-Dateien

Wenn diese Option aktiviert ist, wird bei jeder Ansicht eines Client-PCs durch die Steuerung eine Replay-Datei aufgezeichnet – vorausgesetzt, die Option ist aktiviert.

Client-Protokollierung

Protokolldateien zeichnen die Aktivitäten auf, die auf einem Client-Computer während der Fernsteuerung stattfinden. Standardinformationen umfassen den Namen des Control-Benutzers, der die Verbindung initiiert hat, sowie Datum und Uhrzeit des Sitzungsbeginns und -endes. Die erstellten Textdateien bieten eine nützliche Prüfspur, mit der die Sicherheit des Clients zusätzlich verbessert werden kann.

Das Client-Protokoll kann bearbeitet werden, um nur ausgewählte Informationen anzuzeigen und so den Datenschutz weiter zu unterstützen. Beispielsweise können persönliche Daten wie Benutzernamen beim Empfang von Support geschützt werden. Zudem ist es möglich, Client-Protokolle zu löschen, die älter als „x“ Tage sind, falls erforderlich.

Passwort für den Client-Konfigurator

Das Passwort für den Client-Konfigurator ermöglicht es, den Zugriff auf den Client-Konfigurator einzuschränken. Dies kann durch ein lokal gespeichertes Passwort für das Client-Profil oder durch die Angabe einer NT-Gruppe von Benutzern erfolgen, die sich für den Zugriff authentifizieren können.

Die oben genannten Optionen für den NetSupport Manager Client/Control können lokal auf einem Client mit dem NetSupport Manager Konfigurator angewendet werden. Alternativ können sie mit den AD-Vorlagendateien sowohl für AD-Gruppenrichtlinien als auch für Intune-Konfigurationsprofile verwendet werden. Einstellungen, die über Gruppenrichtlinien angewendet werden, überschreiben alle lokal konfigurierten Einstellungen.

Control-Sicherheitsoptionen

Der NetSupport Manager Control bietet ebenfalls eine Vielzahl von Sicherheitsoptionen, um den Zugriff zu sichern und die Funktionalität einzuschränken.

Control-Passwort

Ermöglicht das Festlegen eines Passworts für das Control. Sie werden dann bei jedem Start des Controls zur Eingabe dieses Passworts aufgefordert.

Control-Protokollierung

Wenn aktiviert, wird die Aktivität jeder Sitzung, in der das Control mit einem Client verbunden ist, protokolliert.

Replay-Dateien

Wenn aktiviert, wird bei jeder Ansicht eines Client-PCs durch das Control eine Replay-Datei erstellt.

Control-Schnittstelleneinstellungen

Mit den Schnittstelleneinstellungen des Controls können Sie konfigurieren, welche Komponenten für die benannte Konfiguration verfügbar sind. Beispielsweise kann der Zugriff auf die Abschnitte „Automatische Gruppen“ oder „Gateway-Liste“ der Control-Schnittstelle deaktiviert werden.

Control-Funktion

Die Einstellungen der Control-Funktion ermöglichen es, bestimmte Funktionen einzuschränken, wie beispielsweise die Dateiübertragung oder die Neustart-Option.

Control-Profile

Der NetSupport Control kann mit unterschiedlichen Control-Konfigurationen eingerichtet werden, sodass Sie verschiedene Profile für unterschiedliche Control-Benutzer erstellen können.

Die oben genannten Optionen für den NetSupport Manager Control können lokal über die NetSupport Manager Control-Einstellungen angewendet oder mithilfe der AD-Vorlagendateien für den NetSupport Manager Control über Gruppenrichtlinien erzwungen werden. Einstellungen, die über Gruppenrichtlinien angewendet werden, überschreiben alle lokal vorgenommenen Konfigurationen.