Solstice Pod Baseline Security Standard (BSS)

Zur Bereitstellung des höchstmöglichen Sicherheitsstandards empfehlen wir, vor der Installation von Solstice Pods in Unternehmensnetzwerken die Konfiguration bestimmter IT-Grundschutzmaßnahmen vorzunehmen.

Im Folgenden beschreiben wir den Baseline Security Standard (BSS), welchen Mersive für sicherheitsrelevante Umgebungen empfiehlt. Pods, die nicht entsprechend konfiguriert sind, können Sicherheitsrisiken für Benutzer und Netzwerke sein, u.a. durch nicht autorisierte Benutzerzugriffe, Screenshots, sonstige Aufzeichnungen, nicht autorisierte Änderungen von Konfigurationseinstellungen sowie durch Denial-of-Service Angriffe.

Der Solstice Pod ist ein an das Netzwerk angeschlossenes Gerät, welches über ein Host-IT-Netzwerk einen einfachen und sicheren drahtlosen Zugriff auf die vorhandene Display-Infrastruktur ermöglicht. Mit der entsprechenden Konfiguration des Sicherheitsstandards des Pods können Benutzerinhalte schnell und sicher auf Displays in Pod-aktivierten Räumen geteilt werden.

Adressaten
Diese Richtlinie gilt für alle Organisationen, die in sicherheitsrelevanten Umgebungen arbeiten. Kleinere Implementierungen, Collaboration-Hotspots und die öffentlich zugängliche Verwendung von Pods erfordern in der Regel keine strikte Einhaltung der in diesem Dokument beschriebenen Sicherheitsstandards. Für größere bzw. zentral verwaltete Pod-Bereitstellungen sollten diese Maßnahmen jedoch getroffen werden.

Da die Pods mit einem Netzwerk verbunden werden, empfehlen wir, bei der Planung ihrer Bereitstellung den IT-Administrators und die Verantwortlichen für Netzwerksicherheit einzubeziehen. Der BSS, Solstice Pod Baseline Security Standard, ermöglicht eine sichere Bereitstellung der Pods durch die Möglichkeit ihrer Anpassung an die Spezifikationen der individuellen Netzwerkkonfiguration und Datenschutzrichtlinien Ihres Unternehmens.

Ersteinrichtung
Richten Sie Ihre Pods vor Bereitstellung im Unternehmensnetzwerk stets in einem separaten Netzwerk ein. So stellen Sie sicher, dass die Konfiguration den Empfehlungen der BSS Sicherheitsrichtlinie entspricht. Installieren Sie das Solstice Dashboard auf einem sicheren Windows Host PC oder Server. Führen Sie Dashboard und Pods stets auf demselben Netzwerk aus.

1. Richten Sie ein separates Netzwerk ein und konfigurieren Sie hier die Pods, bevor diese mit dem Unternehmensnetzwerk verbunden werden.

2. Schalten Sie hierzu jeweils den Pod ein und stellen Sie ihn auf dem eigenständigen Netzwerk bereit. Der Pod wird sowohl mit DHCP / Ethernet als auch mit dem WAP des Geräts ausgeliefert. Schließen Sie das Ethernet-Kabel an Ihr separates Konfigurationsnetzwerk an, damit das Gerät eine lokale IP-Adresse empfangen kann.

3. Standalone-Konfiguration (Optional): Sie können den Pod auch mithilfe der folgenden Schritte ohne Netzwerk konfigurieren. Dazu müssen Tastatur und Maus über einen USB-

Hub direkt mit dem Gerät verbunden sein. Mersive empfiehlt jedoch, zum Konfigurieren Ihrer Pods das Solstice-Dashboard zu verwenden.

4. Starten Sie das Solstice Dashboard im separaten Netzwerk. Verwenden Sie das Dashboard zur Konfiguration Ihrer Pods und führen sie es auf dem Standalone-Netzwerk zusammen mit den Pod-Geräten aus.

   Zum Starten des Dashboards im Netzwerk müssen Sie es zunächst von der Mersive-Website auf Ihrem Windows-Host-PC oder -Server herunterladen, installieren und anschließend den Windows-Host mit dem eigenständigen Netzwerk verbinden.

5. Importieren Sie Ihre Pods in das Dashboard. Sobald die Pods im lokalen Netzwerk (einzeln oder alle gleichzeitig) bereitgestellt wurden, klicken Sie auf die Schaltfläche "discover", um die Pods in Ihr Dashboard zu importieren. Sollten nicht alle Pods angezeigt werden, befinden diese sich in einem Netzwerk, das UDP / Broadcast-Datenverkehr nicht unterstützt. Verwenden Sie in diesem Fall die Importoption "CSV", zum Import oder geben Sie die Pods manuell ein.

   Informationen und Anleitungen zum Import der Pods finden Sie im Solstice Dashboard-Benutzerhandbuch.

Sichere Konfigurationsoptionen
Sichern Sie den Zugriff auf die Konfigurationsoptionen, um unbefugte Änderungen zu vermeiden. Deaktivieren Sie hierzu im Solstice Dashboard die Zugangsmöglichkeit auf die Konfigurationsoptionen für nicht authentifizierte Benutzer.

1. Wählen Sie im Solstice Dashboard alle Pods in der Bereitstellung aus und rufen Sie die Registerkarte "Sicherheit" auf.

2. Geben Sie ein Administratorkennwort ein. Für den Zugriff auf die Konfigurationsoptionen für Pods muss nun ein Administratorkennwort über das Dashboard geändert werden. „Enforce password validation rules" sollte aktiviert sein.

   Passwörter, die im Dashboard in das Feld „admin" eingegeben werden, unterliegen den Regeln der Unternehmensrichtlinie, um sicherzustellen, dass sie kein Sicherheitsrisiko darstellen: Kennwörter müssen mindestens 8 Zeichen lang sein, mindestens einen Großbuchstaben und einen Kleinbuchstaben enthalten, keine Wörterbuchwörter enthalten und mindestens eine Zahl oder ein Symbol enthalten. Passwörter mit drei aufeinanderfolgenden Zeichen werden nicht akzeptiert. Diese Regeln werden vom Dashboard erzwungen, Passwörter, die diesen Einstellungen nicht entsprechen, werden abgelehnt.

3. Deaktivieren Sie "Allow Local Configuration", um sicherzustellen, dass Benutzer nicht physisch auf Konfigurationseinstellungen zugreifen können, indem Sie eine Tastatur oder Maus an das Gerät im Raum anschließen. Hinweis: Administratoren, die einen Pod im Dual-Network-Modus konfigurieren, können den Konfigurationsdatenverkehr von einem der Netzwerke vollständig deaktivieren. Hiermit wird sichergestellt, dass Gast-Netzwerke oder nicht authentifizierte Netzwerke durch die Konfiguration des Pods eingeschränkt

werden können.

4. Deaktivieren Sie "Allow Browsers to Configure Pod". Danach können nur authentifizierte Benutzer aus dem Solstice Dashboard die Pod-Einstellungen ändern.

Konfiguration der Netzwerkeinstellungen
Der Solstice Pod unterstützt den sicheren Zugriff auf zwei unabhängige Onboard-Netzwerkschnittstellen. Beide sind unabhängig voneinander konfiguriert und verwenden jeweils eine eigene Routing-Tabelle, die den sicheren gleichzeitigen Zugriff auf den Pod aus zwei segmentierten Netzwerken unterstützt (z. B. Firmen- und Gastnetzwerke). Wenn diese Konfiguration ausgewählt wird, sollte die Firewall-Funktion aktiviert werden.

1. Wählen Sie alle Pods im Dashboard aus und rufen Sie die Registerkarte "Netzwerk" auf.

2. Konfigurieren Sie entweder die Ethernet-Schnittstelle (empfohlen) oder die Einstellungen für die drahtlose Schnittstelle, um die Verbindung zu Ihrem Unternehmensnetzwerk herzustellen. Weitere Informationen zum Auswählen und Konfigurieren der Konfiguration, die Ihre Netzwerktopologie unterstützt, finden Sie im Network Deployment Guide.

3. (Optional) Konfigurieren Sie bei einer Konfiguration mit zwei Netzwerken die zweite Netzwerkschnittstelle (entweder Ethernet oder Wireless), um eine Verbindung mit dem zweiten Netzwerk herzustellen. Wählen Sie dann "Firewall-Einstellungen" und wählen Sie "Alle Zugriffe zwischen kabelgebundenen und drahtlosen Netzwerken blockieren", um den Netzwerkverkehr zu den zwei unabhängigen Netzwerkschnittstellen zu isolieren.

Standortoptionen
Da der Pod keine Benutzeranmeldeinformationen, unverschlüsselte Kennwörter oder Benutzerdaten speichert, die für die Anzeige freigegeben wurden, müssen sich die Pods nicht an sicheren Speicherorten befinden. Andere Überlegungen bezüglich Diebstahlsicherung und Umgebungsbedingungen sollten jedoch in Betracht gezogen werden.

1. Wählen Sie eine geeignete physische Montage für den Pod, die nicht gelöst werden kann. Berücksichtigen Sie die Verwendung von Montageschlössern und / oder versteckten VESA-Montagesystemen hinter dem Display.

2. Die spezifische Montageausrichtung ist kein wichtiger Faktor, da der Pod in jeder Ausrichtung betrieben werden kann.

3. Bitte berücksichtigen Sie, dass das Gerät in einem Umgebungstemperaturbereich von 0 ° C bis 35 ° C betrieben werden sollte.

4. Der Pod sollte nicht in direktem Kontakt mit einer Oberfläche montiert werden, deren Temperatur 30 ° C überschreitet.

Laufende Grundschutzmaßnahmen
Überwachen Sie nach der Bereitstellung Ihrer Pods die Gewährleistung der Datensicherheit

1. Stellen Sie sicher, dass kompetentes Sicherheits- oder Verwaltungspersonal ihre E-Mail-Adressen bei Mersive registriert hat. Sicherheitsbenachrichtigungen werden bei Bedarf per E-Mail an diese Benutzer gesendet.

2. Wir empfehlen eine regelmäßige, planvolle Überwachung der verfügbaren Updates. Rufen Sie den Tab "Lizenzierung" auf und wählen Sie "Nach Updates suchen". Lesen Sie die Update-Versionshinweise, um sicherzustellen, dass durch Updates keine Sicherheitslücken entstehen. Eventuelle Probleme werden in den Versionshinweisen mit einem fett gedruckten Sicherheitsmarker gekennzeichnet. Wenn ein Sicherheitsupdate gefunden wird, wenden Sie es an. (Siehe Solstice Dashboard Reference Guide).

3. Die Standardüberwachung der Sicherheitskonfigurationsrichtlinie wird empfohlen. Führen Sie die Sicherheitsüberprüfungen regelmäßig über das OpenControl-Protokoll durch, damit der Prüfer eine Verbindung zu einem Pod herstellen, die Einstellungen erfassen und diese mit der Konfigurationsrichtlinie vergleichen kann.