

Inhouse Workshop - McAfee Festplattenverschlüsselung

Der Workshop richtet sich an IT-Sicherheitsverantwortliche und IT-Sicherheitsfachkräfte sowie Mitarbeiter System/Netzwerkadministration - Datenschutz/Datensicherheit - IT-Sicherheitslösungen - Help Desk / IT-Support

Ihr Nutzen / Sie erfahren:

Sie erfahren ausführlich und in Ihrer Praxis, wie Sie Ihre Unternehmensdaten unter Nutzung der Möglichkeiten und Eigenschaften der **McAfee Endpoint Encryption for PCs** EEPC 6.0/6.1 schützen und mit Hilfe der verbesserten Funktionen des ePolicy Orchestrators 4.5/4.6 konfigurieren, integrieren und administrieren.

Inhalt / Agenda des Workshops

McAfee Endpoint Encryption EEPC Versionen 6.0 bzw. 6.1 (2 Tage)

- Einführung in die Verschlüsselung von Rechnern mit der McAfee Endpoint Encryption V6.X
- Einchecken der EEPC-Komponenten in den ePO V4.5/4.6
- Verbindung der EEPC-Verwaltung mit dem Active Directory
- Definition von Richtlinien für unterschiedliche Einsatzbereiche
 - Produktbezogene Richtlinien
 - Benutzerbezogene Richtlinien
- Single-Sign-On mit und ohne Smartcards mit der Endpoint Encryption
- Ausbringung der Verschlüsselung auf Endgeräte
 - Abfolge der Ausbringung und Verschlüsselung
 - Hinweise auf mögliche Ausbringungsmethoden für größere Rollouts
- Umgang mit der Pre-Boot-Umgebung
 - Anmeldung
 - Optionen und Recoverymöglichkeiten
- Überwachung der Ausbringung, Verschlüsselung und anderer Stati mit dem ePolicy Orchestrator V4.5
- Recoverymöglichkeiten
 - Optionen für die Selbstwiederherstellung durch den Benutzer
 - Wiederherstellung durch einen Administrator
 - Wiederherstellung durch eine Recovery-CD oder -Floppy

ePolicy Orchestrator 4.5 bzw. 4.6 (zusätzlich 1 Tag)

- ePolicy Orchestrator V4.5 und McAfee Agent V4.5
 - Installation und Grundkonfiguration bezogen auf die aktuelle Infrastruktur
 - Einrichten einer effektiven und zeitsparenden Arbeitsumgebung
 - Aktualisierungs- und Verteilkonzept für verwaltete Systeme mittels ePO-Server, verteilten Repositories und Agentensteuerungen
 - Einrichten einer angepassten Überwachung und Benachrichtigung
 - Regelmäßige Berichte
 - Einbringen und Verteilen von neuen Produkten und Patches
 - Überlegungen zur Auswahl einer Datenbank und deren Pflege
 - Fehlersuche und -Beseitigung
 - Vorkehrungen für Disaster Recovery Szenarien

Spezielle Voraussetzungen

- Active Directory Zugriff
- Test-PCs mit kleineren, zweckmäßigen Partitionen-/Plattengrößen, um den Verschlüsselungsvorgang zu beschleunigen
- Backup/Image der verwendeten Test-PCs vorher

Ihre Vorteile beim Inhouse-Workshop:

- Workshop passend zu ihrer Umgebung und an ihrer Umgebung
- Direkte Umsetzbarkeit des vermittelten Stoffes vor Ort ohne aufwändige nachträgliche Arbeiten
- Keine Firmeninterna gehen an Außenstehende
- Es kann auf dem aktuellen Wissenstand der Teilnehmer aufgebaut und erweitert bzw. vertieft werden
- Mehrere Mitarbeiter werden auf den gleichen Wissensstand gebracht
- Vermittlung von Best Practice Informationen
- Erfahrungen aus einer Vielzahl von Kundensituationen aus vielen Jahren wird vermittelt
- Nicht nur technische Fakten werden vermittelt, sondern auch effektive Arbeitsabläufe und Reaktionsmöglichkeiten bei Vorfällen und Problemen

Informationen zum Workshop:

Dauer: 2 Tage, bei Vertiefung von McAfee ePolicy Orchestrator 3 Tage. Jeweils 09.00 – 17.00 Uhr.

Termine /Ort und Registrierung:

Der Workshop findet in Ihren Räumlichkeiten statt. Vereinbaren Sie bitte einen Termin mit Ihrem eyeT secure Team. Tel. Hamburg 040 328 905 234 - Tel. München 089 189 085 700

Teilnehmerzahl:

Um die bestmögliche Effizienz des Workshops für Sie zu garantieren, ist die Teilnehmerzahl auf maximal 6 Teilnehmer beschränkt.

Gebühren/ Seminarunterlagen:

Der Teilnahmebeitrag beträgt EUR 999,- pro Tag zuzüglich gesetzlicher MwSt. Die Seminarunterlagen stellen wir Ihnen zusätzlich auf einem USB-Speicherstick gemeinsam mit Ihrem Teilnahmezertifikat am Ende der Veranstaltung zur Verfügung gestellt.

Voraussetzungen / Trainingsumgebung:

- Das Schulungsmaterial wird elektronisch zur Verfügung gestellt. Die Trainingssoftware wird in Form einer Virtuellen Umgebung für die Dauer des Trainings vorinstalliert mitgebracht und für Trainingszwecke bereitgestellt
- Benötigtes Umfeld (allgemein)
 - Ungestörtes Arbeiten im Workshop (eigener Raum)
 - Beamer, Flipchart,
 - Internet-Zugriff

Ihr Referent Top IT-Security-Experte

Ihr Senior Security Experte **Klaus G. Aringer** ist bereits seit 25 Jahren im IT-Sicherheitsmanagement tätig. Er kennt alle Facetten des McAfee Projektgeschäfts. Er verfügt über „Insider-Wissen“, wenn es um die erfolgreiche Integration und Implementierung von McAfee Security Technologien geht. Gerade im Rahmen seiner aktuellen Senior Consultant Tätigkeit hat er eine große Anzahl von Endpoint Encryption Projekten in mittelständischen und großen Unternehmen erfolgreich durchgeführt.

Fragen zu Ihrem Workshop?

Für Ihre Fragen und Wünsche steht Ihnen Ihr eyeT secure Team gerne zur Verfügung:

eyeT secure Hamburg
Tel. 040 328 905 234
Fax: 040 328 905 234 1

E-Mail: seminare@eyeTsecure.de

eyeT secure München
Tel. 089 189 085 700
Fax: 089 189 085 711

<http://eyetsecure.de/seminare/>