The SymBCS-Security Newsletter

From the Business Critical Services Team

SONDERAUSGABE ZUM TOI MAI, 2013

Sehr geehrte Damen und Herren,

wie bereits während des TOI in Berlin angekündigt, übersende ich Ihnen den Sondernewsletter zu dieser Veranstaltung. Ich bedanke mich für das Feedback zu der Veranstaltung und hoffe ich konnte in Zusammenarbeit mit dem Symantec Team Ihre Fragen vor Ort und hier als Hilfestellung in Form von Technotes, HowTo's und Best Practise beantworten. Gern stehe ich Ihnen im Nachgang für weitere Fragen zur Verfügung. Besonders wichtige Informationen wurden „grün" hervorgehoben, damit diese leichter im Text zu finden sind.

CONTENTS

TOI - PRÄSENTATIONSFOLIEN

Anbei finden Sie den aktuellen Download-Link für die Präsentationen der Redner in Form eines kompakten ZIP-File Archives.
Dieser Link ist temporär bis zum 01.07.2013 gültig.

https://www.nortonzone.com/pickup/22307?key=TXSQWBShGhW9PWzdwwoDkx0lD_HLcR0e61R8NAz-r5VgqbLYoW8villh6woA2SIf&src=url

SEP 12.1.2 (RU2) – VORBEREITUNG & INSTALLATION

DOC4322	Symantec™ Endpoint Protection 12.1.2 Getting Started Guide
DOC6153	Symantec™ Endpoint Protection and Symantec Network Access Control 12.1.2 Installation and Administration Guide
DOC3719	Symantec™ Endpoint Protection and Symantec Network Access Control 12.1.2 Client Guide
HOWTO81153	About Symantec Endpoint Protection 12.1.2 product guide locations
HOWTO81091	What's new in Symantec Endpoint Protection 12.1.2
TECH195325	System Requirements for Symantec Endpoint Protection, Enterprise and Small Business Editions, and Network Access Control 12.1.2
HOWTO81069	Supported upgrade paths for Symantec Endpoint Protection Manager
HOWTO81070	Supported upgrade paths for the Symantec Endpoint Protection client
TECH197426	Upgrading or migrating to Symantec Endpoint Protection 12.1.2 (RU2)
HOWTO80791	Migrating from Symantec AntiVirus or Symantec Client Security to Symantec Endpoint Protection 12.1 or later
HOWTO80759	Upgrading to a new release of Symantec Endpoint Protection
TECH197344	Best practices for virtualization with Symantec Endpoint Protection 12.1.2
TECH134203	Symantec Endpoint Protection for Macintosh Frequently Asked Questions
HOWTO81261	Why do I need to replace the client-server communications file on the client computer?
HOWTO81455	Restoring client-server communications by using a client installation package
HOWTO81337	Managing the client-server connection
HOWTO54706	How to prepare a Symantec Endpoint Protection 12.1 client for cloning
TECH163349	How to repair duplicate IDs on cloned Symantec Endpoint Protection 12.1 clients
TECH90936	**How to add or remove features to existing Symantec Endpoint Protection (SEP) client installations**

LIVE UPDATE ADMINISTRATOR 2.3.X

TECH93409	Best Practices for LiveUpdate Administrator (LUA) 2.x
TECH102701	Installing and Configuring LiveUpdate Administrator (LUA)
TECH131177	How To Determine the Corresponding Product for a LiveUpdate Administrator 2.x File
TECH152817	About Installing LiveUpdate Administrator 2.x on a Windows XP, Windows Vista or Windows 7 Operating System
TECH132545	How to configure a Windows Server 2008 as a Distribution Center for LiveUpdate Administrator 2.x content

TECH159239	How to backup and restore LiveUpdate Administrator (LUA) configuration in LUA 2.3
TECH103198	Using the LiveUpdate Administrator 2.x to download updates for Symantec Endpoint Protection for Macintosh
TECH103249	How to set up Macintosh clients to download updates from an internal LiveUpdate server
HOWTO61146	How to Export the LiveUpdate Administrator 2.x Server Event Log

GROUP UPDATE PROVIDER

HOWTO80957	About the types of Group Update Providers
TECH198640	Understanding "Explicit Group Update Providers (GUPs) for Roaming Clients" in Symantec Endpoint Protection (SEP) 12.1.2
TECH196741	What is the processing order of an Explicit GUP list within version 12.1.2 of Symantec Endpoint Protection?
Endpoint SWAT	**SEP Content Distribution Monitor (for GUP health-checking)**
Endpoint SWAT	**SEP Content Distribution Monitor - Introduction**

FEHLERSUCHE (TROUBLESHOOTING)

TECH198977	After upgrading to version 12.1.2 of the Symantec Endpoint Protection Manager, an error is displayed when trying to launch the SEPM's Java remote console
TECH194754	Creating a network scan password with SHA-256 hashing after upgrading to Symantec Endpoint Protection 12.1.2
TECH196253	The Symantec Endpoint Protection (SEP) 12.1.2 Host-Integrity Custom Requirement for Checking Symantec Antivirus-Infected is Not Backwards Compatible to Previous Versions
TECH104314	Compatibility between Symantec Endpoint Protection/Symantec AntiVirus for Macintosh and HFS Extended, case-sensitive formatted volumes
TECH195152	Navigation to the next page of the Audit report saved from the Symantec Endpoint Protection Manager shows the error "A Runtime Error has occured. Line:9579 Error:Object expected"
TECH93564	Symantec Endpoint Protection reports "No Symantec Protection technologies are Installed"
TECH103176	How to clear out corrupted definitions for a Symantec Endpoint Protection client manually
TECH104539	Troubleshooting the Group Update Provider (GUP) in Symantec Endpoint Protection (SEP)
TECH163787	Which Communications Ports does Symantec Endpoint Protection use?
TECH97190	How to confirm if SEP Clients are receiving LiveUpdate content from Group Update Providers (GUPs)
CONNECT FORUM	"scan for viruses" in the context menu is missing

VIRTUALISIERUNG

TECH197344	**Best practices for virtualization with Symantec Endpoint Protection 12.1.2**
TECH91070	Best Practices for Symantec Endpoint Protection on Citrix and Terminal Servers
TECH123419	How to prepare Symantec Endpoint Protection clients on virtual disks for use with Citrix Provisioning Server
CONNECT FORUM	SEP launching on a new XenClient deployment
HOWTO55311	About the Symantec Endpoint Protection Shared Insight Cache tool
HOWTO55318	How Shared Insight Cache works
TECH174123	Network-based Shared Insight Cache - Best Practices and Sizing guide
TECH172806	System requirements for network-based Symantec Shared Insight Cache Server
HOWTO55313	Installing Shared Insight Cache
HOWTO55321	Configuring your clients to communicate with Shared Insight Cache
CONNECT FORUM	Installation and Configuration of Shared Insight Cache

NÜTZLICHE LINKS

In diesem Bereich finden Links rund um das Thema Case-Eröffnung sowie um die Themen Malware und False-Positive Meldungen. Weitergehende Informationen entnehmen Sie bitte der TOI Präsentation „SYM_BSI_Support_Prozesse“

CONNECT FORUM	https://www-secure.symantec.com/connect/ Dies ist eine Plattform, wo Kunden sich praxisorientiert untereinander und mit dem Produktmanagement austuaschen können.
Knowledge Base	http://www.symantec.com/business/support/index?page=home&locale=de_de Sammlung von technischen Dokumenten, die durch den technischen Support von Symantec erstellt und gepflegt werden.
SEP 12.1 FAQ	http://www.symantec.com/docs/HOWTO59095 Die am häufigsten gestellten Kundenanfragen für SEP 12.1.
BCS PORTAL	https://www-secure.symantec.com/platinum/login_de.html Alles rund um BCS.
MySymantec	https://my.symantec.com Zugangsportal zum technischen Support.
BCS MALWARE UPLOAD	https://submit.symantec.com/websubmit/bcs.cgi Portal zum einsenden von verdächtigen Dateien an Symantec.
FALSE POSITIVE	https://submit.symantec.com/false_positive/ Portal zum melden von Falscherkennunge

Für Entwickler von Software stellt Symantec für BCS Kunden das „Customer Whitelisting Program“ zur Verfügung. Mithilfe dieses Programmes können Sie die Interferenzen zwischen der Sicherheitssoftware und Ihrer Software auf ein minimum reduzieren. Mehr Informationen dazu enthält das Dokument „Customer White List Program Detail“ welches sich als PDF Dokument unter folgenden Link downloaden können:

https://www.nortonzone.com/pickup/23405?key=R_FofGYKc2EHMpw9Cavdn_pfTqLbu0OkB3c8fG86ODT9SwDXSsC3qIv0IkSANTVp&src=url

Dieser Link ist temporär bis zum 01.07.2013 gültig.

BEST PRACTICES SEP	http://www.symantec.com/business/support/index?page=content&key=54619&channel=TECHNICAL_SOLUTION&basecat=BEST_PRACTICES&sort=recent
ENDPOINT SWAT	http://www.symantec.com/connect/endpointswat

MÖGLICHE VORGEHENSWEISE BEI VIRENBEFALL

TECH122466	Best Practices for Troubleshooting Viruses on a Network
SECURITY RESPONSE	Security Best Practise – Stopping malware and other threats
ENDPOINT SWAT	http://www.symantec.com/connect/articles/outbreak
TECH102539	What is Risk Tracer?
TECH94526	How to use Risk Tracer to locate the source of a threat in Symantec Endpoint Protection

Wir möchten Sie hier auf zwei weitere Interressante Artikel zum Thema “ Stoppen eines Malwareausbruches in Ihrem Netzwerk“ hinweisen. Diese Artikel sind im Connect Forum erschienen und werden in kürze fortgeschrieben.

CONNECT FORUM	Using SEPM Alerts and Reports to Combat a Malware Outbreak
CONNECT FORUM	How to utilize SEP 12.1 for Incident Response - PART 1

SAV FOR LINUX

Das Thema AV für Linux ist wie bereits auch während des TOI angesprochen sehr anspruchsvoll und bedarf von Ihrer Seite her tiefgreifende Linux Kenntnisse. Aufgrund der Vielzahl an Distributionen auf dem Mark, hat sich Symantec für den Support der Distributionen entschieden, die erstens einen Long Time Support und zweitens eine Roadmap haben.

TECH103599	Release notes for Symantec AntiVirus for Linux 1.0x
TECH101598	**System requirements for Symantec AntiVirus for Linux 1.0**
TECH102882	How to configure scanning of compressed files in Symantec AntiVirus for Linux
TECH95274	Symantec AntiVirus for Linux: How to Configure Scan Exclusions from the Command Line Interface

TECH123497	How to add Folder Exclusion for autoprotect, manual and weekly scans in Symantec Antivirus for Linux

Wir möchten Sie hier auf vier weitere Interressante Artikel zum Umgang mit SAVfL hinweisen.

CONNECT FORUM	SAV for Linux Scanning Best Practices: A (Somewhat) Illustrated Guide
CONNECT FORUM	SAV for Linux: A (Somewhat) Illustrated Guide Part 2
CONNECT FORUM	SAV for Linux: A (Somewhat) Illustrated Guide Part 3
CONNECT FORUM	SAV for Linux: A (Somewhat) Illustrated Guide Part 4: SAVFL Reporter
CONNECT FORUM	How to Install SAV for Linux (SAVFL) and Update It Using LUA 2.x (2.3.0.71)

HÄUFIG GESTELLTE FRAGEN UND IHRE ANTWORTEN

Q:
Nach der Installation neuer Clients tauchen diese in der Übersicht des SEPM zwar auf, verschwinden aber wieder. Diese Phenomen betrifft sowohl neue als auch ältere Clients. Vor Ort kontrolliert sind diese Clients topaktuell. Dadurch sind die Dashboardanzeigen des SEPM irreführend.

A:
Dies ist ein A-Typisches Phänomen und sollte dringend durch einen „Support Case“ geklärt werden.

Q:
Läßt sich die Anzeige-Größe im SEPM anpassen? Bei meiner verwendeten Auflösung wird nur knapp 2/3 der Anzeige verwendet, statt dessen muß man scrollen? Gibt es dafür Tips?

A:
Derzeit noch nicht, es ist geplant dieses mit der nächsten Revision der SEPM GUI zu beheben.

Q:
Welche Möglichkeiten gibt es, von Sonar und Risikoerkennung beanstandete Software allgemein als gutartig einstufen zu lassen?

A:
Bitte nutzen Sie dazu das „Customer Whitelisting Program“ und sofern möglich lassen Sie Ihre Software digital signieren.

COMPUTACENTER

Wie bereits während des TOI vorgestellt, steht Ihnen die Firma ComputaCenter als Rahmenverrtragspartner des BSI mit Ihren Schulungs- und Beratungsangeboten zur Verfügung. Diese können Sie nutzen um Ihr bereits vorhandenes Wissen zu festigen und auszubauen.

Oliver Kunert
Consultant
Consulting Services - Secure Information

Computacenter AG & Co oHG
Services & Solutions

Mariendorfer Damm 1, 12099 Berlin, Germany
E-Mail: oliver.kunert@computacenter.com

Für tiefergreifende Schulungen, jedoch außerhalb des Rahmenvertrages, steht Ihnen auch die Firma Symantec zur Verfügung. Falls Sie Interresse an einer solchen Schulung haben, nehmen Sie bitte Kontakt mit Ihrem BCAM auf, zur Koordination des weiteren Vorgehens.

BCS ALLGEMEINE INFORMATIONEN

Fragen oder weiterführende Hilfe wird benötigt?

Woher bekomme ich die Symantec Reference Card?

Ich möchte den BCS Security Nerwsletter erhalten?

Nehmen Sie Kontakt zur Ihren Business Critcal Account Manager Team auf

Lothar Schmitz Business Critical Account Manager Mobile: +49 175 407 5620 **lothar_schmitz@symantec.com**	**Torsten Knorr** Business Critical Account Manager Mobile: +49 174 186 8096 **torsten_knorr@symantec.com**