Mobile-Sicherheit – Sicheres arbeiten von unterwegs mit Check Point Abra

Stefan Schurtz

Check Point Software Technologies Ltd. ist weltweit für seine Firewall- und VPN-Produkte bekannt und stellt mit Abra, einen USB-Stick für sicheres mobiles Arbeiten zur Verfügung

IN DIESEM ARTIKEL ERFAHREN SIE...

• Wie man mit Check Point Abra sichere Mobile-Arbeitsplätze für Mitarbeiter oder externe Dienstleister zur Verfügung stellen kann

WAS SIE VORHER WISSEN SOLLTEN...

- Kenntnisse in der System- und Netzwerk-Sicherheit
- Kenntnisse in der Konfiguration von Check Point Produkten
- Kenntnisse in der TCP/IP Netzwerktechnik

eimarbeitsplätze bzw. Arbeiten von unterwegs ist seit Jahren eine wichtige Anforderung von Firmen an die IT und stellt nach wie vor eine große Herausforderung für die IT-Sicherheit dar.

Etabliert für den Zugriff von fremden/unsicheren Netzen und Systemen in ein Firmennetzwerk, haben sich Virtuelle Private Netzwerke per IPSec oder SSL-VPN. Der sichere Zugriff bzw. eine gesicherte Verbindung von Privat-/Fremdsystemen in das Unternehmensnetzwerk sind damit weitestgehend gewährleistet. Problematisch ist jedoch, dass kaum die Möglichkeit der Kontrolle besteht, beispielsweise bei externen Dienstleistern, was auf diesen Systemen installiert ist und/oder welche Verbindungen noch vorhanden sind. Auch die allgemeine Sicherheit (Patches usw.) dieser Systeme kann wohl kaum garantiert werden. Sicher wäre es ebenso nicht von Vorteil, wenn interne, womöglich vertrauliche Dokumente auf solchen Systemen abgespeichert und dann von Unbefugten gelesen oder gar kopiert werden.

Auf einem firmeneigenen Host-PC, lässt sich dem Problem der Sicherheit, der Systemupdates und aktivierter Virenscanner, möglicherweise noch mit einer Endpoint-Security entgegenwirken, doch den Anwender soweit Einzuschränken, dass ein Arbeiten von unterwegs kaum mehr möglich ist, wird früher oder später wohl eher problematisch und zu hitzigen Diskussionen führen.

Abra

Check Point stellt mit Abra, einen (**SanDisk**) FIPS 140-2 Level 2 zertifizierten USB-Stick zur Verfügung, welcher zum einem die Sicherheit der Daten auf dem Stick durch moderne Kryptographie (AES 256-bit hardware

Check Point Gateway - cfw	-sb-utm	<u>?</u> ×
General Properties Topology NAT SecurePlatform IPSec VPN Legacy Authentication SmartDirectory (LDAP) Dos and Masters	IPSec VPN This Security Gateway participates in the following VPN Communities:	
Capacity Optimization Cooperative Enforcem Advanced	Add Remove	

Abbildung 1. Konfiguration der VPN-Community für RemoteAccess

Haking

- General Properties	VPN Clients			
⊡ Topology ⊡ NAT	VPN clients allowed to connect to this gateway			
- SecurePlatrorm	Selecting a client will enable Visitor Mode.			
- Authentication	SSL Network Extender			
VPN Advanced Link Selection	🔲 SecureClient Mobile			
- Remote Access	🔽 Abra			
Office Mode Clientless VPN	Note: Abra configuration is only relevant for secur	ity gateways that support	t the device.	
	The gateway authenticates with this certificate:	defaultCert	•	
 Legacy Authentication 		8		
SmartDirectory (LDAP)				
E Logs and Masters				
Capacity Optimization				
- Advanced				

Ξ	Abra Connect (R	ule 2)									_
2	Abra Connectivity	* Any	👫 cfw-sb-utm	* Any Traffic	TCP https	💮 accept	Log	🔐 cfw-sb-utm	* Any	Abra Connectivity	
۸b	hildung 3 E	irowall_Pa	aal für Abra Zu	ariff							

Abbildung 3. Firewall-Regel für Abra Zugriff

encryption), z. B. gegen Verlust oder Diebstahl sicherstellt und der zum anderen, einen passwortgeschützten "virtuellen", vom Host-PC getrennten, Arbeitsbereich (ohne Installation) zur Verfügung stellt.

Darüber hinaus, ist es durch das Einbinden in ein Check Point Management möglich, Einfluss auf den Import/Export von Dateien und auf die in der virtuellen Umgebung nutzbaren Anwendungen, zu nehmen. Diese konfigurierbare, so genannte "*Secure Workspace Policy*", bewirkt letztlich mehr Sicherheit für den Zugriff von Fremdsystemen und lässt dem Anwender trotzdem noch die Möglichkeit komfortabel von unterwegs zu arbeiten.

Secure Workspace Policy

Folgende Secure Workspace bzw. Endpoint Policy wird in diesem Artikel mit Hilfe von Abra umgesetzt:

Der Import bzw. Export von Dateien wird nur von und zu vertrauenswürdigen Systemen (Trusted Hosts – Host im internen Netz bzw. ein Host der sich einmal dort befunden hat) zugelassen. Das Drucken von Dokumenten sowie das Kopieren über die Zwischenablage wird nicht erlaubt. Ein Umschalten zwischen dem "Host-Desktop" und dem "Abra-Desktop" soll möglich sein. Darüber hinaus soll nach 60 Minuten Inaktivität ein automatischer Logout erfolgen.

Auf dem Host-PC wird geprüft ob Virenscanner, Anti-Spyware-Tools, Personal Firewalls, aktuelle Windows Service Packs und Windows Update vorhanden bzw. aktiviert sind. Entspricht der Host-PC diesen Sicherheitsanforderungen wird der Zugriff gestattet bzw. erhält der Anwender eine Warnung welche Anforderungen nicht erfüllt sind. Sind bestimmte Kriterien nicht erfüllt, wird der Zugriff verweigert. So sind zum Beispiel eine fehlende Personal Firewall bzw. ein fehlendes Anti-Spyware-Programm, zwar ein Grund zur Warnung, der Zugriff wird dennoch gestattet. Bei fehlendem AntiVirus Programm, fehlendem aktuellen Windows Service Pack und/oder deaktiviertem Windows Update wird der Zugriff jedoch komplett verweigert.

Security Management

Damit überhaupt mit Abra gearbeitet bzw. eine VPN-Verbindung hergestellt werden kann, müssen auf dem Security Management folgende Vorbereitungen getroffen sein.



Abbildung 4. Benutzer Konfiguration

ABWEHR

obal Properties			ļ
	Abra		
NAT - Network Addres Authentication	Security Policy		
	Secure Workspace Policy		
⊕ Remote Access	Scan endpoint for spyware and com	ipliance Configure () Wide Impact	
SmartDirectory (LDAP) QoS	User Authentication —		
 Management High Ava ConnectControl 	Support certificate based user authe	ntication () Wide Impact	
- OSE - Open Security E	Connectivity Settings		
 Stateful Inspection Log and Alert 	Connect mode:	Configured on endpoint client	
Reporting Tools OPSEC	Location Aware Connectivity:	Configured on endpoint client Configure.	
- Security Management .	Disconnect when device is idle:	Configured on endpoint client	
Non Unique IP Addres Proxy	Route all traffic to gateway:	No	

Abbildung 5. Global Proberties – Abra

VPN

Im Check Point Gateway Objekt muss unter "Network Objects -> Check Point -> Gateway Object → General Properties → Network Security, der Punkt "IPSec VPN" aktiviert sein und das Objekt "RemoteAccess" muss der VPN-Community angehören. Dies wird über "Network



Objects -> Check Point -> Gateway Object -> IPSec VPN["] konfiguriert (Abbildung1).

Zum Abschluss der VPN Konfiguration auf dem Management, muss Abra als VPN-Client erst noch erlaubt werden, diese Einstellung nimmt man unter "*Network Objects -> Check Point -> Gateway Object -> IPSec VPN -> VPN Clients*" vor (Abbildung2).

Firewall-Rule

Eine Firewall-Regel, welche HTTPS-Verbindungen auf das Security Gateway zulässt, muss ebenfalls

Genera	Application Control	Outbo	und Firewall Rules			
Applic	ation Control					
	ou all applications					
LI Aut	se the Applications Table	helow to c	letermine which shorts	uts are place	ed on th	e Abra desktop
✓ En	able Program Advisor to	validate th	e integrity of allowed a	applications in	n Applic	cations Table *
6	Allow Trusted only					
0	Allow Trusted and Un	known				
* 1	These settings apply only	when 'Allo	w all applications' is d	sabled		
Approv	ved Vendors					
Selectin	ng a Vendor allows all app	olications	igned by that Vendor	to run within	the Ab	ra secured workspace.
Allaur	Mandar Name		Comment			
Allow	A Jaba		Cineral Lu Adab			
	Adobe		Signed by AdoL	e		
-	Charle Dates		Cierced by Apple	n Li Ducas		
M	Check Point		Signed by Chec	K Point		
	Computer Associates		Signed by Comp	Juter Associa	1(62	
	Loogie		Signed by Goog	lie		
	IBM		Signed by IBM			
	Intel		Signed by Intel			
Applic	ations Table					
Define	which applications will be	placed or	n the Abra desktop.	2 P. 1 1		and the second
when t	ne Allow all applications	setting ac	ove is disabled then ti	his list determ	nines wi	nich applications are allowed to fun within
Allow	Display Name	Shortcut	Executable File		MD5	Comment
	InstallFree		\IFInterConn.exe			InstallFree
	Windows Media Player		\wmsetsdk.exe			Microsoft Windows Media Player
V	Microsoft Office IME 2010		VIMECMNT.EXE			Microsoft Office IME 2010
~	Internet Explorer		\ie4unit.exe			Microsoft Internet Explorer web browser
ব	Microsoft Office IME 2010 Internet Explorer		\IMECMNT.EXE			Microsoft Office IME 2010 Microsoft Internet Explorer web bro

Abbildung 6. General Abra Settings

Abbildung 7. Abra - Application Control

Mobile-Sicherheit – Sicheres arbeiten von unterwegs mit Check Point Abra

eneral	Application Con	trol Outbound Firewall Rules	£		
ily conn	ections that match	one of the applied rules in the table b	elow are accepted. <i>i</i>	W other connections are dropped.	
Apply	Rule Name	IP Address	Port	Comment	Remove
~	Default rule	0.0.0.0-255.255.255.255	0-65535	Allow all connections by default.	Remove
Add Rule Na	I Rule				
Add Iule Na P Addre 'ort:	I Rule me: ess: e.g. 1.2.3.4, port number,	1.2.3.4-10.20.30.40 or a.b.c.com group of ports or range of ports e.g. 2:	34 or 234, 236 or 20	0-300	

Abbildung 8. Abra - Outbound Firewall Rules

Anti-Spyware-Rule

Name:

existieren, da diese von Abra genutzt werden (Abbildung 3).

Benutzer anlegen

Damit sich ein Benutzer mit Abra per VPN zum Security Gateway verbinden kann, muss dieser auf dem Management angelegt sein. Die Konfiguration erfolgt über den Menüpunkt "Users and Administrators -> Users

Description: Anti-Spyware-Rule	Name: Anti-Virus-Rule
Windows	Description: Anti-Virus-Rule
Windows Anti-Spyware Application Properties	Windows
Application Name	Windows Anti-Virus Application Properties
ACC. INCOMENDATION OF A CONTRACT	Application Name Conditions
🗖 Kaspersky AntiSpyware	Kaspersky antivirus Enforce minimum engine version : Enforce DAT file :
TrendMicro AntiSpyware	AVG antivirus Enforce minimum engine version : Enforce DAT file :
Symantec AntiSpyware	
Add Edit Delete	
Windows Rule Action	Add Edit Delete
C Restrict endpoints that don't comply	Windows Rule Action
 Warn endpoints that don't comply 	 Restrict endpoints that don't comply
C Log Only endpoints that don't comply	C Warn endpoints that don't comply
	C Log Only endpoints that don't comply

Abbildung 9. Anti-Spyware Regel

Abbildung 10. Anti-Virus Regel

-> Rechte Maustaste -> New User -> Default" (Abbildung4).

Damit sind die Voraussetzungen für eine erfolgreiche VPN-Verbindung gegeben und es kann mit der Konfiguration der Secure Workspace Policy begonnen werden.

Secure Workspace Policy

Die Einstellungen der Secure Workspace Policy erfolgen im Check Point Management unter "*Policy -> Global Properties -> Abra -> Secure Workspace Policy*" (Abbildung5).

General

Unter General werden die beiden Punkte "File transfer from host PC to secure workspace (Import)" und "File transfer from secured workspace to host PC (Export) auf "Allow from trusted hosts only" gestellt. Unter "Data Protection" wird "Prevent host PC from printing secure documents" und "Prevent copying clipboard content to host PC" aktiviert. Der Punkt "Log out idle users after", unter "User Experience" wird auf 60 Minuten eingestellt. Alle weiteren Punkte werden deaktiviert. (Abbildung 6)

Application Control

Unter Application Control wird der "Program Advisor" aktiviert und auf "Allow Trusted only" eingestellt. Des Weiteren wird unter den "Approved Vendors" nur Check Point zugelassen. In der Liste "Applications Table" wer-

Security Scan Results			
Security Requirements	Security Status	Solutions	
Anti-Virus Rule	😢 Restricted	NO antivirus	
Firewall Rule	🕜 Pass		
Anti-Spyware Rule	O Caution	Anti-Spyware-Rule	
Windows Security Rule	Pass		



sscription: [Firewall Application-Rule] Windows Windows	tion
Application Name	Conditions
Windows Built-in Firewall	Windows Built-in Firewall installed, enabled and running
McAfee Firewall	McAfee Firewall installed, enabled and running
🔲 Windows Live OneCare	Windows Live OneCare installed, enabled and running
🗖 Trend Micro Firewall	Trend Micro Firewall installed, enabled and running
🗖 Kaspersky IS Firewall	Kaspersky IS Firewall installed, enabled and running
Add Edit Delete	
Windows Rule Action	
C Restrict endpoints that don't comply	
Warn endpoints that don't comply	
C Log Only endpoints that don't comply	

den, alle Anwendungen, außer Office- und Browser-Anwendungen, deaktiviert (Abbildung7).

Outbound Firewall Rules

Mit den *Outbound Firewall Rules* werden (ausgehend) erlaubte Verbindungen zu IP-Adressen und Ports konfiguriert, welche von den Anwendungen im Secure Workspace genutzt werden dürfen, alle anderen werden verworfen (Abbildung8).

Scan Endpoint for spyware and Compliance

Die Regeln zur Prüfung des Host-PC, unter anderem, nach installierten Virenscannern, Personal Firewall und Windows-Update werden unter dem, zuvor aktivierten, Menüpunkt "Scan endpoint for spyware and compliance \rightarrow Configure" eingerichtet.

Specify the c	riteria for this rule	
Name:	Windows-Security-Rule	
Description:	Windows-Security-Rule	
Operating Syste	m: All	-
Rule Conditio	ns	
Require the	a latest Service Pack to be installed	
🗹 Require Au	tomatic Updates to be turned on	
Hot Fixes		
	Keyword	
2		
Add	Edit Delete	
Rule Action -		
• Restrict end	dpoints that don't comply	
C Warn endp	oints that don't comply	
C Log Only er	ndpoints that don't comply	

Abbildung 12. Firewall-Application Regel

Abbildung 13. Windows-Security Regel

Hakina

Anti-Spyware-Rule

Zur Konfiguration der Anti-Spyware Rule wählt man den Punkt "Scan endpoint for spyware and compliance -> Configure -> New Rule -> Anti-Spyware Application" aus. Neben dem Namen für die Regel, werden unter dem Punkt "Windows Anti-Spyware Application Properties" nun alle zur Verfügung stehenden Anwendungen ausgewählt und der Punkt "*Windows Rule Action*" auf "*Warn endpoints that don't comply*" gestellt (Abbildung9). Damit wird nun bei fehlenden Anti-Spyware-Anwendungen, im Compliance Report, eine Warnung an den Benutzer ausgegeben, der Zugriff aber trotzdem gestattet.

Abra	2
SanDisk Enterprise	Check Point Abra®
Welcome to the Abra Firs	t Time Configuration Wizard
The first time configuration wizard will help you se device. This password is used to protect the dev	elect a strong password for the Abra vice and encrypt all your private data.
You will need to enter this password ear	ch time you start Abra.
Note: an automatic Abra launcher can be installe	ed using the button available on the Advanced tab.

Abbildung 14. Abra - First Time Configuration Wizard



Abbildung 15. Abra - Lizenzbestimmungen

Hakina

ABWEHR

	Samisk ENTERPRISE Check Point Abra®	2
	Create a password for your Abra device: Create Password: Confirm Password:	
	The password must contain at least 8 characters. The password must contain characters from at least 2 of the following groups: Lowercase (a-z), Uppercase (A-Z), Digits (0-9), Special characters (!@#\$%^&* etc.)	
Abra V	firtual Keyboard	
Esc	F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 Print. 1 2 3 4 5 6 7 8 9 0 - = Backspace Inset	Scroll Paus Lock Breat Home PgD
Tab		Jumeric Keypa
Caps	q w e r t y u i o p []] \ \ Show M	

Abbildung 16. Abra - Passwort Eingabe

Anti-Virus-Rule

Die Anti-Virus Regel wird per "Scan endpoint for spyware and compliance -> Configure -> New Rule -> Anti-Virus Application" angelegt. Diese wird auf die beiden Virescanner "Kaspersky antivirus" und "AVG antivirus" eingeschränkt. Im Gegensatz zur Anti-Spyware-Rule wird diese Regel allerdings auf "Restrict



Abbildung 17. Abra - Secure Workspacce

endpoints that don't comply["] gestellt (Abbildung10). Damit wird, ist keiner der beiden Virenscanner auf dem Host-PC installiert, der Zugriff verweigert (Abbildung11).

🗿 Site	Wizard	×
A	Welcome to the Site Wizard A site is your gateway to network resources.	
	Obtain the IP address or name of the site from your system administrator	
	Server address or Name:	
	Display name:	
	Back Next Cancel He	lp

Abbildung 18. Site Wizard – IP / Hostname Konfiguration

7 Haring



Abbildung 19. *Site Wizard – Fingerprint*



Abbildung 20. Site Wizard – Authentication Method

Firewall-Application-Rule

Analog zu den beiden oben erstellten, wird als vorletztes, eine Regel für Firewall-Applications über "Scan endpoint for spyware and compliance -> Configure -> New *Rule -> Firewall Application*" erstellt. Bei dieser Regel werden ebenfalls alle vorhandenen Anwendungen hinzugefügt und die Windows Rule Action auf "Warn endpoints that don't comply gestellt (Abbildung12).

Windows-Security-Rule

Als letzte Regel wird die Windows-Security-Rule über "Scan endpoint for spyware and compliance -> Configure -> New Rule -> Windows Security" erstellt und lediglich die beiden Punkte "Require the latest Service Pack to be installed" und "Require Automatic Updates to be turned on" aktviert. Die Rule Action wird auf "Restrict endpoints that don't comply" gestellt (Abbildung13).

Da nun die zuvor definierte Secure Workspace Policy umgesetzt wurde, wird im nächsten Schritt die eigentliche Konfiguration des Abra-Stick in Angriff genommen.

Installation

Nach dem Verbinden mit dem Host-PC und dem Ausführen der "Abra.exe" auf dem USB-Stick, starte der "Abra First Time Configuration Wizard" (Abbildung14). Nach dem Bestätigen der Lizenzbestimmungen (Abbildung15) muss im nächsten Schritt das Passwort für den Abra-Stick eingegeben werden. Hierzu steht zum Schutz vor Keyloggern ein "Virtual Keyboard" zur Verfügung (Abbildung16). Nach der Eingabe eines sicheren Passwortes, wird das Device initialisiert und der Secure Workspace automatisch gestartet (Abbildung17).

VPN

Im Secure Workspace startet mit einem Klick auf "*Connect to Site*" die Konfiguration für VPN mit der Abfrage von IP bzw. Hostnamen des Security Gateways (Abbildung18). Nach der Bestätigung des Fingerprints (Abbildung19), steht zuletzt die Auswahl der "*Authentication Method*" an, in diesem Fall "*Username and Password*" (Abbildung20). Ist das VPN erfolgreich erstellt, erscheint eine entsprechende Meldung und im nächsten Fenster werden zum endgültigen Abschluss der VPN-Konfiguration, Benutzername und Passwort abgefragt (Abbildung21).



Abbildung 21. Site Wizard – Erfolgreiche Konfiguration / Login

Hakina

ABWEHR

ExmpSrv.exe	2448	54.676 K	52.840 K Application login	SanDisk
E PWClient.exe	412	5.856 K	7.456 K Check Point Abra Controller	Check Point Software Technologies
PWAccess.exe	4248	15.452 K	15.172 K Check Point Abra VPN Client	Check Point Software Technologies
VDeskSelector.exe	5568	3.824 K	672 K. Auxiliary Abra Module	Check Point Software Technologies
🖃 🏧 VDesk.exe	4656	10.312 K	14.128 K Virtual Workspace	Check Point Software Technologies
😑 💳 ISWMGR.exe	5604	24.004 K	32.544 K Abra Core	Check Point Software Technologies
🖃 💳 ISWMGR.exe	5880	24.176 K	1.076 K Abra Core	Check Point Software Technologies
👰 explorer.exe	5036	33.196 K	38.060 K Windows Explorer	Microsoft Corporation
📝 ctfmon.exe	1124	15.456 K	11.336 K CTF Loader	Microsoft Corporation
S PwViewer.exe	3652	31.072 K	34.360 K Check Point Abra VPN Client UI	Check Point Software Technologies
imapi.exe	2672	15.680 K	11.496 K. Image-Mastering-API	Microsoft Corporation
App DH.exe	5216	3.008 K	5.512 K Drive hide utility	SanDisk

Abbildung 22. Abra im ProcessExplorer

This program is not allowed	
	Check Point Abra
This program is not allowed	
The requested application is not permitted by your security policy.	
File: python.exe	
	Close

Abbildung 23. Abra verbietet die Ausführung einer Anwendung

Arbeiten im Secure Workspace

Sind alle diese Schritte erfolgreich abgeschlossen, steht der Arbeit per Abra im Secure Workspace nichts mehr im Wege. Durch das gewohnte "Look and Feel" (im Grunde wird eine Windows Explorer.exe ausgeführt - Abbildung22), kann sich der Anwender schnell mit der neuen Umgebung vertraut machen.

Dennoch müssen einige Dinge beachtet werden, so stehen einem im Windows Explorer, wie gewohnt Laufwerke, Dateien und Ordner zur Verfügung, tatsächlich ist dies aber nur ein "virtuelles Abbild" der "echten" Host-PC Umgebung! Im Secure Workspace können Dateien, wenn die Policy die entsprechende Anwendung erlaubt (Abbildung23), des Host-PC geöffnet, scheinbar sogar gelöscht bzw. verändert werden. Dies hat jedoch (hoffentlich ;D) *KEINE* Auswirkungen auf die "echte" Umgebung des Host-PC. Das bedeutet für einen Benutzer, dass Dateien *NUR* über die Funktionen Import/Export auf bzw. von dem Host-PC kopiert werden können.

Auch hängt ein vernünftiges Arbeiten natürlich davon ab, dass die erlaubten und benötigten Anwendungen auf dem Host-PC verfügbar sind, d. h. Einschränkungen sollten mit Bedacht durchgeführt werden und es

🛃 Abra - Advanced	×	👰 Abra - Advanced	×
SamDisk Enterprise	Check Point Abra®	SanDisk Enterprise	Check Point Abra®
Change Password Reset Password Device Operations	Device Information	Change Password Reset Password Device	Operations Device Information
Use this tab to change the current password for the device Old Password: New Password: Confirm New Password: The password must contain at least 8 characters. The password must contain characters from at least 2 of th Lowercase (a-z), Uppercase (A-Z), Digits (0-9), Special cha Change Password	Password Strength:	Remote Password Reset Click 'Next' to start the remote password reset	8
Close	Help	Back Next	Help

Abbildung 24. Abra Advanced – Change Password

Abbildung 25. Abra Advanced – Remote Password Reset

, Hakina

sollten ebenfalls auch mögliche Alternativen, z. B. Microsoft Office ↔ Open Office, erlaubt werden.

Abra Advanced

Unter den erweiterten Einstellungen besteht unter "*Change Password*", für den Benutzer, die Möglichkeit der "lokalen" Passwortänderung (Abbildung24). Mit dem Reiter "*Reset Password*" (Abbildung25) kann,

							Paste
te Unlock Code							
le:					Сору	Send By Mail	
k code to user. user successfully res	et the passv	vord					
					Reset Form	Close	Help
	te Uniock Code	te Unlock Code	te Unlock Code	te Unlock Code	ie Unlock Code	te Unlock Code te Unlock Code te:	te Unlock Code

Abbildung 26. Abra Advanced – Device Operations





Abra - Advanced	2
SanDisk Enterprise	Check Point Abra®
Change Password Reset Password Device Operat	tions Device Information
Device Information	
Firmware version: 6.615 SDK 1.2.14.18 CE 2.6.12 Launcher version: 83.0.0.133 Client version: 83.0.0.133 SW5 version: 1.6.153.26 ICS client version: 4.2.561.34 ICS analyzer version: 62.0.6150.10 ICS signatures version: 4.2.179.0	.80
Close	Help

Abbildung 28. xxxxxxx

Im Internet

- http://www.checkpoint.com/products/abra/
- Abra R70.1 Administration Guide http://downloads. checkpoint.com/dc/download.htm?ID=11175
- Abra R70.1 User Guide http://downloads.checkpoint. com/dc/download.htm?ID=11176

sollte das Passwort vergessen werden, mit Hilfe des Supports und dem "Abra Password Reset"-Tool (Abbildung26), dieses zurücksetzt werden .

Unter den "*Device Operations*" ist einmal mit "*Format Device*" das komplette Zurücksetzen des USB-Sticks möglich, darüber hinaus kann hier ein Logging unter "*Collect Logs*" aktiviert werden. Mit der letzten Konfigurationsmöglichkeit "*Install Automatic launcher*" ist es möglich Abra automatisch starten zu lassen (Abbildung27).

Zu guter Letzt stehen unter "*Device Information*", wie der Name vermuten lässt, Informationen unter anderem zur Firmware, Launcher und Client Version zur Verfügung (Abbildung28).

Fazit

Sicherheit bedeutet für Anwender oft Einschränkungen beim Arbeiten, dieses Problem wird auch durch Abra nicht vollständig gelöst. Jedoch kann man in Absprache mit Benutzern, Dienstleistern und einer vernünftigen durchdachten Policy einen guten Kompromiss, für einen sicheren mobilen Arbeitsplatz, schaffen.

STEFAN SCHURTZ

Der Autor arbeitet bei einem saarländischen ISP im Bereich Netzwerk-Sicherheit und beschäftigt sich auch privat mit dem Thema IT-Security

Kontakt mit dem Autor: sschurtz@t-online.de

