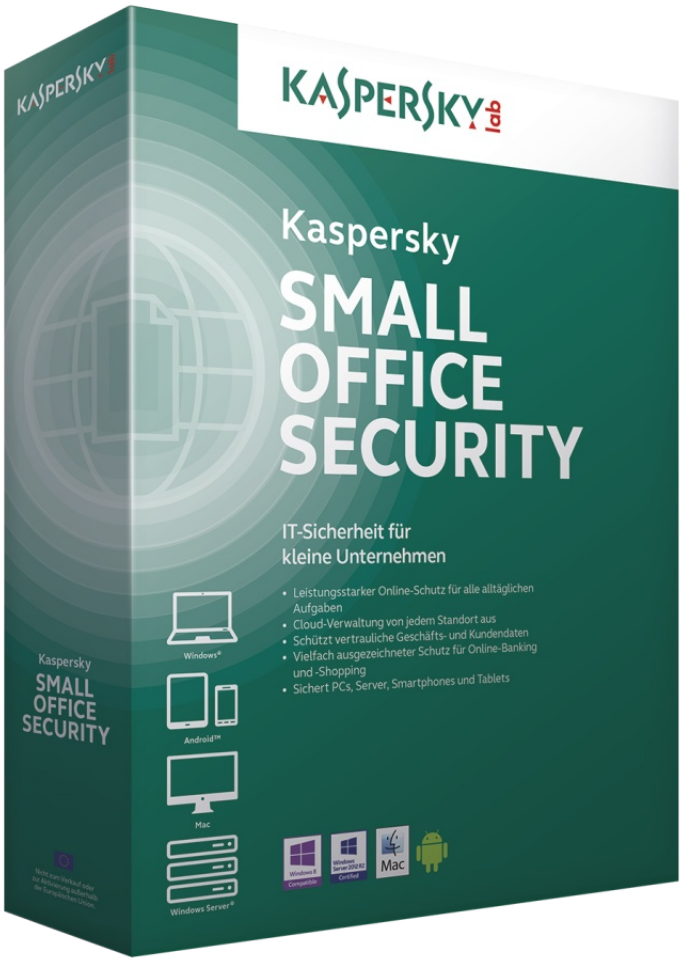
Zentral verwaltete Sicherheitslösung für kleine Umgebungen

Dr. Götz Güttich

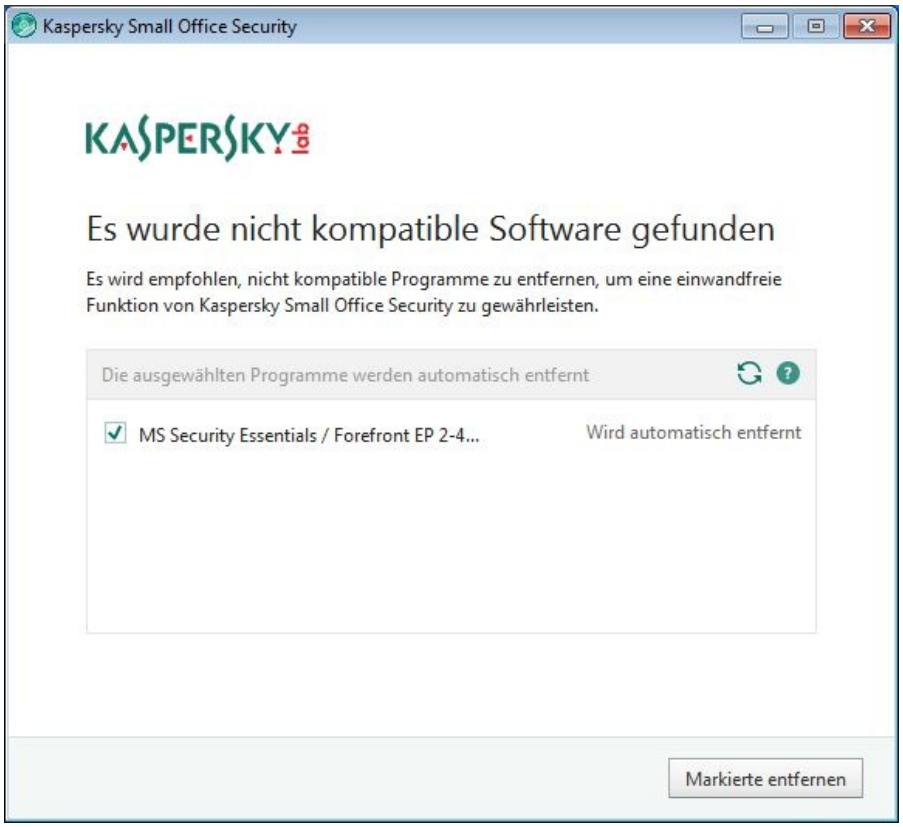
Mit der Small Office Security 4 stellt Kaspersky eine Sicherheits-Suite bereit, die sich speziell an kleinere Einrichtungen wendet. Das Produkt eignet sich für Umgebungen mit 25 Anwendern und weniger, lässt sich einfach ins Netz integrieren und bringt eine Web-Konsole für die internet-basierte Verwaltung von überall aus mit. Des Weiteren gehören zum Leistungsumfang der Small Office Security neben klassischen Antivirus-Funktionen mit mehreren Ebenen unter anderem auch ein Spam-Filter, eine automatische Datensicherung, ein Cloud-basierter Echtzeitschutz vor Bedrohungen sowie Kontrollfunktionen für das Surfen im Netz und die Nutzung sozialer Netzwerke. Wir haben die Lösung im Testlabor genau unter die Lupe genommen.



Kasperskys Small Office Security 4 soll sich von Mitarbeitern ohne tiefgehende IT-Erfahrung schnell und einfach einrichten und administrieren lassen. Die Suite wurde mit diversen Assistenten versehen, die dabei helfen, das System zu implementieren, vorhandene Malware zu entfernen, Kontrollen und Richtlinien zu definieren und Verschlüsselungen sowie Backups einzurichten. Die zentrale Verwaltungskonsole im Internet hilft dabei, später im laufenden Betrieb stets auf dem aktuellen Stand zu bleiben und die Konfiguration gleichzeitig auf mehrere Computer zu verteilen.

Zum oben erwähnten Leistungsumfang kommen noch Verschlüsselungsmöglichkeiten zum Schutz vertraulicher Daten, Anti-Phishing-Technologien, Features zum Absichern von Online-Finanztransaktionen und optional eine sichere Passwort-Verwaltung. Abgesehen davon existieren auch ein Modus für vertrauenswürdige Programme, in dem nur Software ausgeführt werden kann, die zuvor als sicher eingestuft wurde, ein Feature zum Überprüfen der Sicherheit von WLAN-Verbindungen und eine Schutzfunktion für Webcams. Die Software läuft auf Clients unter Windows XP oder neuer und Dateiservern unter Windows Server 2008 R2 oder neuer sowie mindestens dem Small Business Server 2008 mit Service Pack 2. Wird die Suite auf einem Server installiert bietet sie allerdings nicht den vollen Funktionsum-

fang, sondern beschränkt sich auf die Schutzfunktionen, die Dateiverschlüsselung sowie Backup- und Restore-Features. Außerdem unterstützt die Suite auch MacOS X 10.7 und seine Nachfolger. Für die Installationen sind mindestens 600 MByte Festplattenplatz, eine CPU mit einem GHz Taktfrequenz und ein Internet-Zugang erforderlich. Was mobile Geräte angeht, so kann die Lösung alle Android-Systeme mit Android 2.3 bis 4.4 absichern.



Bei der Installation entfernt die Kaspersky Small Office Security automatisch andere Antivirus-Lösungen

Der Test

Für den Test spielten wir die Sicherheits-Suite auf diversen Client-Systemen unter Windows 7 und Windows 8.1 sowie einem Server unter Windows Server 2012 R2 ein und verknüpften alle Rechner mit einem zuvor generierten Konto für die zentrale Managementkonsole im Internet, damit wir die Systeme remote warten konnten. Anschließend setzten wir uns mit dem Leistungsumfang der Lösung auseinander und legten dabei ein besonderes Augenmerk auf die einfache Bedienung, da diese ja eines der wichtigsten Merkmale des Produkts ist. Darüber hinaus integrierten wir auch ein Android-basiertes mobiles Gerät in unsere Kaspersky-Umgebung und verwalteten dieses ebenfalls über die Management-Konsole im Internet. Da bei der Software die Kaspersky-Engine zum Einsatz kommt und die Usability im Zentrum des Tests steht, untersuchten wir die Virenerkennungsrate an dieser Stelle nicht, sondern verweisen statt dessen auf die entsprechenden Tests von AV-Test und AV-Comparatives.

Nachdem die Suite auf allen Devices zufriedenstellend arbeitete, wandten wir uns der Dateiverschlüsselung, den Funktionen für Backup und Restore, dem sicheren Zahlungsverkehr und dem Passwort Manager zu. Letzteren testeten wir nicht nur unter Windows und Android sondern auch unter iOS 8.3.

Installation und Inbetriebnahme

Für den Test stellte uns Kaspersky eine Setup-Datei zur Verfügung. Es genügte, diese auf den Zielsystemen auszuführen und die Lizenz und ähnliches anzunehmen. Danach installierte der Setup-Assistent die Software ohne weitere Rückfragen. Sollte sich zum Zeitpunkt der Installation bereits ein anderes Antivirus-Programm – beispielsweise die Security Essentials von Microsoft – auf dem jeweiligen Rechner befinden, so entfernt die Kaspersky Setup-Routine diese automatisch.

Nach dem Abschluss des Setups können die Benutzer die Small Office Security-Software über ein auf dem Desktop hinterlegtes Icon aufrufen. Danach landen sie in einem übersichtlich gestalteten Interface, in dem sich die wichtigsten Funktionen über große Buttons aufrufen lassen. Der erste Button verzweigt auf die Statusübersicht. Diese informiert den Anwender über durchgeführte Updates, gefundene Bedrohungen und ähnliches. Mit dem nächsten Button lassen sich Virus-Scans starten. Hierbei unterscheidet Kaspersky zwischen vollständigen, schnellen und benutzerdefinierten Scans. Auf Wunsch untersucht die Software auch Wechselmedien und führt Scans automatisch per Zeitplan durch.

Unter "Update" laden die Benutzer Aktualisierungen für die Sicherheitslösung herunter. Nor-

malerweise funktioniert das automatisch, sollte es aber einmal erforderlich sein, die Virus-Datenbank auf die Schnelle manuell auf den neuesten Stand zu bringen, so lassen sich an dieser Stelle jederzeit Aktualisierungen anstoßen. Zusätzlich steht den Anwendern auch ein Überblick über die aktuelle weltweite Virenaktivität zur Verfügung, die auf die Seite www.viruslist.com/de verweist, die von Kaspersky betrieben wird.

Die Oberfläche der Kaspersky Small Office Security

Ebenfalls von Interesse: der "Verwalten"-Button. Hier haben die User die Option, ihren Client mit dem bereits erwähnten Web-Verwaltungsportal zu verbinden. Dazu müssen sie zunächst einmal einen Account generieren. Das funktioniert über die Angabe einer Mail-Adresse und eines Passworts sowie das Akzeptieren der AGB. Sobald diese Schritte erledigt sind, erhalten die Anwender eine Mail, in der sie auf einen Link klicken müssen, um das Konto zu aktivieren. Danach ist es möglich, das Portal im Browser zu öffnen. Auf die Funktionalität dieser Web-Konsole gehen wir später noch genauer ein.

Der Button "Passwort Manager" verweist auf eine Web-Seite, über die die Benutzer die genannte Software, die als Stand-Alone-Produkt erhältlich ist, von der Kaspersky-Webseite herunterladen können. Für die Verwaltung von bis zu 15 Passwörtern bleibt der Einsatz der Lösung kostenlos.

Auch die Installation des Passwort Managers erfolgt nach dem Aufruf der Setup-Datei und dem Akzeptieren der Lizenz ohne weitere Rückfragen. Um den Passwort Manager zu nutzen, müssen sich die User nach dem Start der Software zunächst mit dem Web-Interface verbinden und ein Master-Passwort vergeben, das den Zugriff auf die Passwort-Datenbank absichert. Wenn die Anwender mit dem Passwort Manager arbeiten möchten, so öffnen sie das Programm später entweder über den Button innerhalb der Small Office Security oder separat als getrennte Software. Die Arbeit mit dem Passwort Manager im laufenden Betrieb wird ebenfalls noch ein Thema dieses Testberichts sein.

Der "Virtuelle Speicher" stellt verschlüsselte Container-Dateien zum Absichern wichtiger Unternehmensinformationen bereit während "Sichern und Wiederherstellen" Backup und Restore von Dateien im Netz oder in der Cloud übernimmt. Auf diese Funktionen gehen wir im weiteren Verlauf des Tests auch noch genauer ein, ebenso wie auf den sicheren Zahlungsverkehr und die Web-Kontrolle.

Unter "Zusätzliche Tools anzeigen" hat Kaspersky schließlich den Zugriff auf die restlichen Funktionen der Sicherheits-Suite zusammengefasst. Dabei liefert dieser Punkt zunächst einmal eine Übersichtsseite, die Daten über die System- und Netzlast präsentiert und Informationen über die letzten Malware-Funde bereitstellt. Außerdem haben die User hier Zugriff auf eine virtuelle Tastatur, die Quarantäne, eine Funktion zum Löschen von Aktivitätsspuren (wie Browser-Journal oder Temp-Ordner), eine Option zum Erstellen einer sicheren Browser-Konfiguration und einen Link zum Download der kostenlosen Kaspersky Notfall-CD 10. Darüber hinaus sind die Benutzer unter anderem dazu in der Lage, eine Schwachstellensuche nach unbenutzten Programmcode-Fragmenten durchzuführen, das System nach einer Infektion wieder herzustellen und Daten unwiderruflich zu löschen (mit verschiedenen Algorithmen wie zum Beispiel Bruce Schneier, VSITR, NAVSO oder auch GOST R 50739-95).

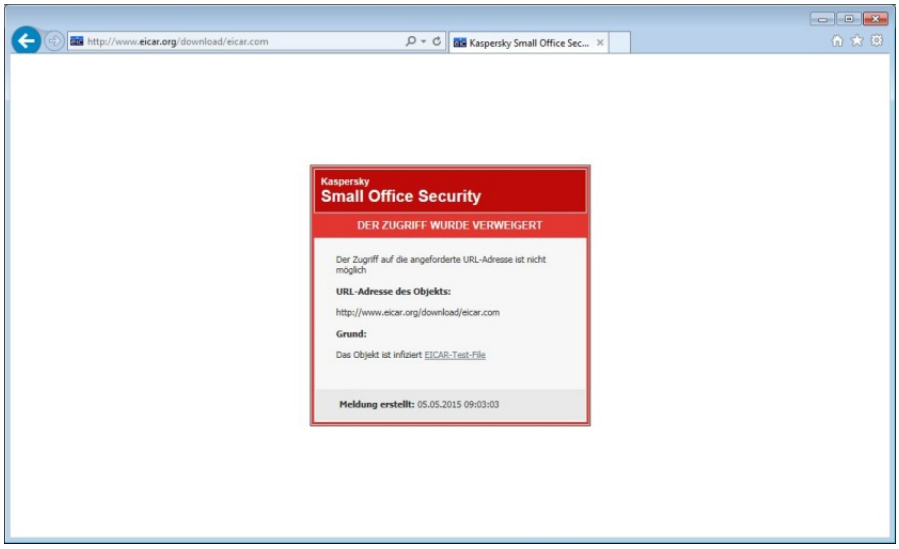
Die Konfiguration der Software

Bevor wir uns im Detail der Funktionalität des Produkts zuwenden, ergibt es Sinn, zuerst einmal auf seine Konfiguration einzugehen. Ruft der Benutzer das Einstellungs-Menü auf, so erhält er zunächst die Möglichkeit, den Schutz ein- und auszuschalten. Außerdem kann er ein Kennwort vergeben, dass den Zugriff auf die Settings und Funktionen wie das Backup oder den sicheren Zahlungsverkehr einschränkt und festlegen, ob die Sicherheitslösung beim Hochfahren des Computers automatisch starten soll. Darüber hinaus hat er die Option, den interaktiven Schutz zu konfigurieren und dabei festzulegen, ob die Kaspersky-Lösung empfohlene Aktionen automatisch ausführen oder möglicherweise infizierte Objekte nicht löschen soll.

Im Untermenü "Schutz" besteht die Möglichkeit, die einzelnen Sicherheitsfunktionen ein- und auszuschalten. Konkret handelt es sich dabei im den Datei-Antivirus, die Programmkontrolle, den Schutz vor Netzwerkangriffen, den Instant-Messaging-Antivirus, den Mail-Antivirus, den Zugriffsschutz für die Webcam, den Web-Antivirus, die Firewall, den Aktivitätsmonitor (für Rollbacks), den sicheren Zahlungsverkehr und die Anti Spam- beziehungsweise Anti Banner-Features.

Unter "Leistung" sorgen die Mitarbeiter dafür, dass bei Akkubetrieb geplante Aufgaben nicht durchgeführt werden um Strom zu sparen und dass die Suche nach Viren bei hoher Last pausiert, um Ressourcen für andere Programme freizumachen. Außerdem ist es auch möglich, den Präsentationsmodus zu verwenden (dieser verhindert beispielsweise beim Vorführen von Powerpoint-Slides das Einblenden von Meldungen) und beim Hochfahren Ressourcen für das Betriebssystem freizugeben. Das funktioniert dadurch, dass die Software beim Systemstart erst einmal nur die wichtigsten Programmfunktionen aktiviert. Alternativ lässt sich die Sicherheits-Suite auch so konfigurieren, dass sie ihre Tätigkeiten nur bei Leerlauf des PCs ausführt und den Datei-Antivirus nach definierten Zeitplänen anhält.

Interessanter wird es im Bereich "Untersuchung". Hier definieren die Benutzer die zu verwendende Sicherheitsstufe. Dabei stehen die Optionen "hoch", "empfohlen" oder "niedrig" zur Verfügung, letzteres als ressourcenschonender Modus für eine hohe PC-Leistung. Auch die bei Malware-Funden durchzuführende Aktion lässt sich an dieser Stelle festlegen: "Informieren", "Desinfizieren", "Desinfizieren mit Löschen irreparabler Dateien", "Löschen" und "Automatisch". Letzteres bedeutet, dass die Software anhand von Vorgaben selbst entscheidet, was zu tun ist und beispielsweise erkannte Viren sofort entfernt. Die auszuwählenden Einträge wurden folglich relativ einfach gehalten und sollten auch für technisch unerfahrene Nutzer verständlich sein. Bei Bedarf können die Anwender bei der Konfiguration der Scan-Durchläufe auch das Durchsuchen von Wechselmedien aktivieren und Zeitpläne für automatische Scans festlegen. Außerdem ist es möglich, die Untersuchungen selbst anzupassen, mit dem für die Schwachstellensuche zu verwendenden Bereich und den dabei einzusetzenden Benutzerrechten. Generell gilt, dass das Einstellungsmenü keine Anwender vor unüberwindliche Schwierigkeiten stellen sollte, außerdem wurden die Default-Settings so gewählt, dass sie für die meisten kleineren Umgebungen völlig ausreichen dürften. Abgeschlossen werden die Settings durch den Bereich "Erweitert", den die Benutzer wohl nur in Sonderfällen manuell anpassen müssen. Hier lassen sich Einstellungen für die Updates der Malware-Datenbank vornehmen, zum Beispiel durch Angabe einer alternativen Update-



Die Lösung verhindert im Betrieb den Zugriff auf gefährliche Elemente

Quelle. Zudem ist es auch möglich, eine sichere Dateneingabe zu aktivieren, die mit einem virtuellen Keyboard arbeitet und vor Keyloggern schützt. Sie lässt sich beispielsweise für Kennwort-Eingabefelder oder für das Online-Banking sowie für E-Mail-Dienste, soziale Netze und ähnliches verwenden.

Darüber hinaus besteht die Option, die Erkennung von Remote-Control-Programmen als Malware ein- und auszuschalten beziehungsweise Ausnahmen und vertrauenswürdige Programme festzulegen, deren Aktivität das System nicht überwacht. Dazu kommt noch eine aktive Desinfektion für Schadprogramme, die ihre Prozesse bereits im OS des Rechners gestartet haben.

Die Sicherheitsfunktionen für den Selbstschutz der Kaspersky-Software sperren alle Änderungs- und Löschversuche in Bezug auf Dateien, Prozesse oder Registrierungseinträge der Sicherheits-Suite selbst. Dieser Schutz lässt sich bei Bedarf deaktivieren.

Unter "Netzwerk" legen die User die zu überwachenden Ports fest und geben an, ob auch sichere Verbindungen untersucht werden sollen. Die Einstellungen unter "Erweitert" erfordern also durchaus gewisse Fachkenntnisse über Netzwerkprotokolle und ähnliches. Sie eignen sich folglich eher für IT-Fachleute.

Abgeschlossen werden die erweiterten Einstellungen durch die Konfiguration der Meldungen, der Berichte, der Verbindung zu den Kaspersky Webdiensten und der Quarantäne. Meldungen lassen sich mit einem Warnton unterlegen und es besteht die Option, das Anzeigen von Kaspersky-Nachrichten und von Sonderangeboten zu deaktivieren.

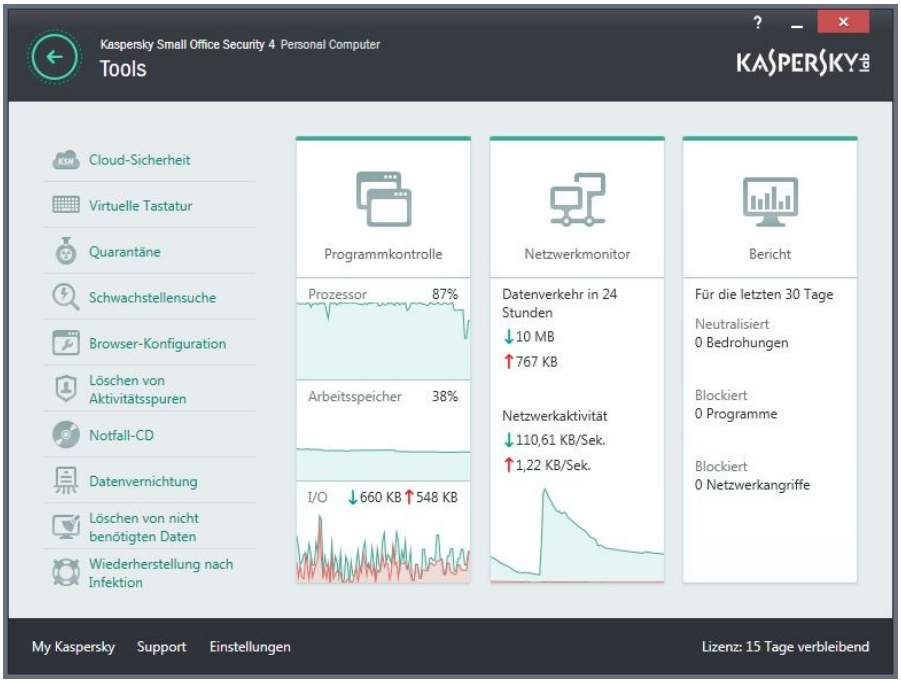
Was die Berichte und die Quarantäne angeht so, haben die Verantwortlichen die Option, Berichte und Objekte für bestimmte, definierte Zeiträume zu speichern, maximale Dateigrößen festzulegen und zu definieren, was protokolliert werden soll. Die Kaspersky Webdienste umfassen wiederum eine Reputations-Datenbank für Dateien, Internet Ressourcen und Software. Die Teilnahme der Small Office Security an diesen Services ist standardmäßig aktiv.

Zusammenfassend lässt sich sagen, dass die Small Office Security im Test schnell in Betrieb genommen war und sich einfach konfigurieren ließ. Alle Features sind leicht zugänglich und auch die Einstellungen wurden im Großen und Ganzen einfach gehalten und klar gegliedert, so dass Anwender in keinen Unternehmen keine Schwierigkeiten mit dem Produkt haben sollten.

Die Arbeit mit der Web-Konsole

Loggt sich der Anwender im laufenden Betrieb bei dem Web-Interface ein, so landet er in einer Übersicht, die ihm alle mit seinem Konto verbundenen Geräte anzeigt. Im Test installierten wir neben unseren Windows-Systemen und dem Passwort-Manager für iOS auch die Kaspersky Internet Security und den Passwort Manager für Android auf einem unserer Smartphones, dieses erschien daraufhin ebenfalls im Web-Interface. So genannte Gruppenaufgaben ermöglichen schnelle und vollständige Untersuchungen der verwalteten Devices und den Anstoß von Datenbankaktualisierungen auf den verbundenen Computern.

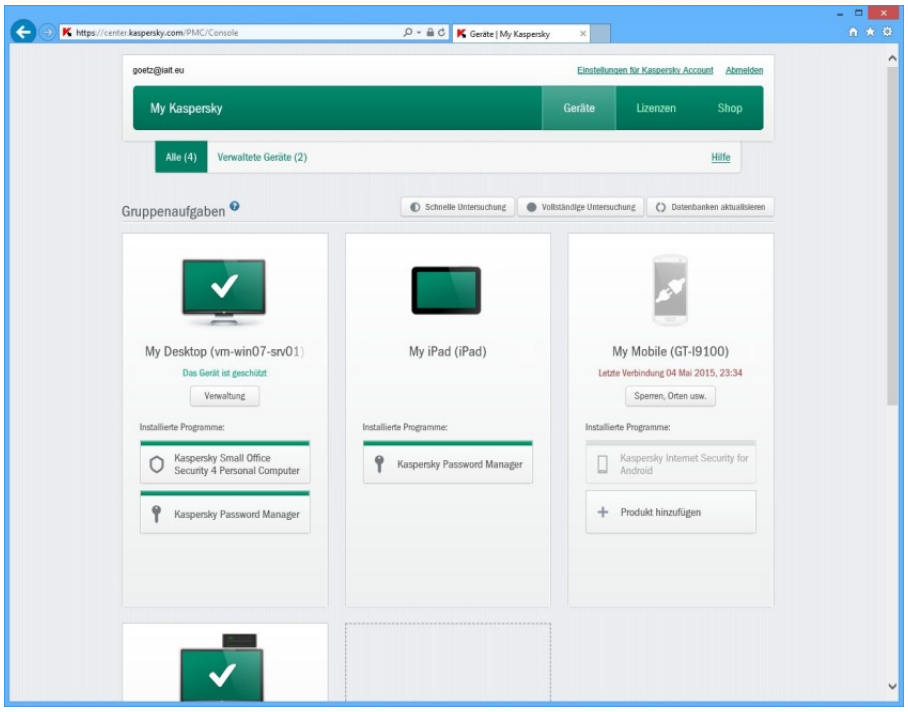
Zu den Geräten stehen darüber hinaus noch diverse Informationen zur Verfügung. Dazu gehören die jeweils installierten Kaspersky-Programme wie Small Office Security oder Passwort Manager und der Sicherheitszustand der Systeme. Abgesehen davon las-



Eine große Zahl von Werkzeugen hilft den Benutzern beim Sichern ihrer Unternehmensumgebungen

sen sich über das Web-Interface auch einzelne Programmkomponenten aktivieren beziehungsweise deaktivieren. Dabei handelt es sich im Wesentlichen um die gleichen Sicherheitsfunktionen, die der Anwender auch im Konfigurationsmenü der Software selbst steuern kann.

Neben der Geräteübersicht existiert auch eine Lizenzübersicht, über die die Anwender die auf den Geräten vorhandenen Lizenzen mit Informationen wie dem Aktivierungsdatum und ähnlichem anzeigen lassen. An der gleichen Stelle besteht auch die Option, Lizenzcodes hinzuzufügen. Darüber hinaus bietet das Web Interface noch einen Link zum Kaspersky Online Shop und ein Einstellungsmenü, in dem die Benutzer die für den Account verwendete Mail-Adresse und



Die Web-basierte Management-Konsole mit den verwalteten Clients

das Kennwort ändern können. Außerdem umfasst der Einstellungsbereich noch die Möglichkeit, Kreditkarteninformationen zu hinterlegen sowie Übersichten über die früheren Bestellungen und die vorhandenen Aktivierungscodes. Eine Hilfefunktion unterstützt die User bei Bedarf beim Anbinden von Geräten an das Web-Interface.

Die Web-Kontrolle

Die Web-Kontrolle stellt eine der leistungsfähigsten Funktionen der Kaspersky Security Suite dar. Diese ist nach der Installation inaktiv, kann aber über die Verwaltungskonsole in Betrieb genommen werden.

Mit der Web-Kontrolle haben die Benutzer ein Werkzeug in der Hand, das ihnen hilft, wenn es darum geht, die Internet-Zugriffe der Unternehmensmitarbeiter zu beschränken. So lassen sich zum Beispiel Zugriffsbeschränkungen unter der Woche oder am Wochenende zu bestimmten Uhrzeiten einrichten. Es ist außerdem auch möglich, eine sichere Suche zu aktivieren und diverse Webseiten zu sperren. Dazu gehören Karrierenetzwerke und Seiten die bestimmte Themen behandeln, wie Alkohol, Gewalt, Glücksspiel, Konfessionen, Seiten für Erwachsene und so weiter. Darüber hinaus ermöglicht das System den Einsatz von White Lists, woraufhin es ausschließlich den Verkehr zu den in diesen White Lists aufgeführten Web-Seiten zulässt. Bei Bedarf unterdrückt die Software auch den Download bestimmter Dateien, nämlich Programmfiles, Audiodateien, Archive und Videos.

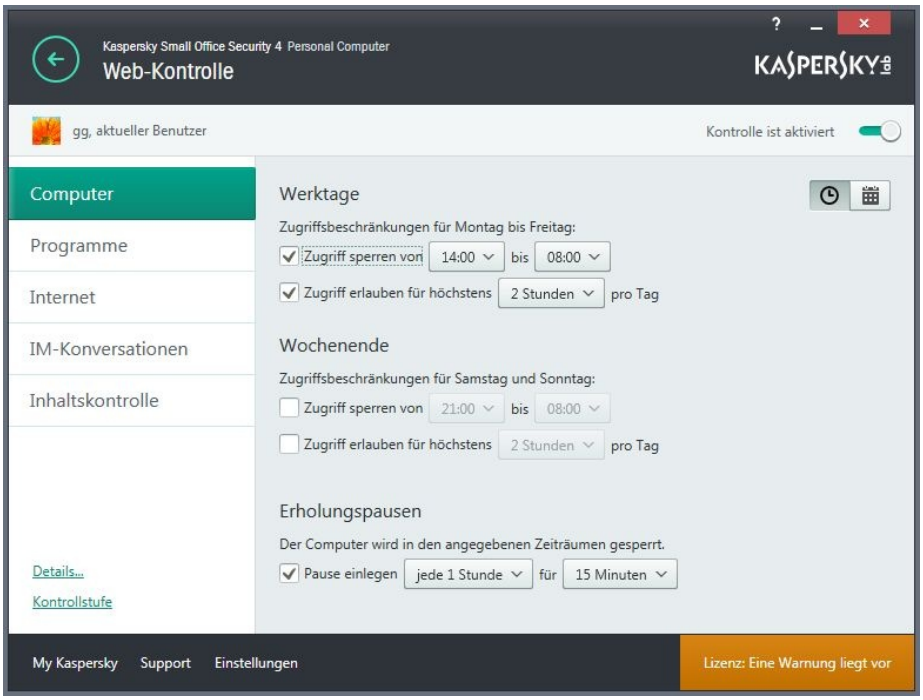
Damit nicht genug, lässt sich auf Wunsch auch der Zugriff auf die Computer selbst einschränken. Auch dazu können die Verantwortlichen wieder Zeitpläne für die Arbeitswoche und das Wochenende festlegen. Sie sind aber auch dazu in der Lage, den Zugriff nur für eine bestimmte Zeitdauer, zum Beispiel zwei Stunden pro Tag, zu erlauben. Es ist sogar möglich, zwangsweise Erholungspausen vorzugeben, beispielsweise jede Stunde 15 Minuten. Im Test funktionierte das einwandfrei.

Abgesehen davon unterstützt die Web-Kontrolle auch das Sperren von Programmen, zum Beispiel Instant Messaging-Lösungen, Spielen, Downloadprogrammen oder auch Bittorrent-Clients. Die Verantwortlichen haben jederzeit die Option, Programme zu der Liste hinzuzufügen oder auch den Start von Spielen einer bestimmten Altersstufe von vornherein zu unterbinden.

Eine Steuerungsfunktion für Konversationen in sozialen Netzen (diese lassen sich auf bestimmte Kontakte beschränken) und eine Inhaltskontrolle runden den Leistungsumfang der Web-Kontrolle ab. Wenn es um das Sichern der Inhalte geht, so überwacht die Security Suite das

Senden persönliche Daten wie Kreditkartennummern und Anschriften und unterbindet bei Bedarf die Übertragung dieser Informationen an Dritte. Es lässt sich sogar der Einsatz diverser Schlüsselwörter kontrollieren. Legen die Anwender eine Liste mit solchen Wörtern an, so überwacht die Software den Gebrauch dieser Begriffe in Konversationen, Nachrichten und Eingabefeldern auf Webseiten. Im Test funktionierte das auf Anhieb.

Zusätzlich lassen sich im Menü der Web-Kontrolle noch Berichte über die Aktionen eben dieser Kontrollfunktion einsehen und eine so genannte Kontrollstufe festlegen. Dabei kann es sich um eine starke Beschränkung des Verkehrs handeln, bei der das System sowohl Webseiten als auch Downloads blockiert, oder eine schwache Beschränkung, bei der nur der Webseitenverkehr eingeschränkt wird. Die Regeln sind jederzeit an die Benutzerwünsche anpassbar und es ist auch möglich, die Kontrollfunktion lediglich zur Datenerfassung zu nutzen.



Die Web-Kontrolle der Kaspersky Small Office Security

Virtuelle Datenspeicher

Im nächsten Schritt des Tests nahmen wir die Funktion zum Verschlüsseln kritischer Unternehmensdaten genauer unter die Lupe. Zu diesem Zweck legt die Kaspersky Small Office Security Containerdateien an, die als virtuelle Laufwerke in das Betriebssystem eingebunden werden und auf die sich dann die zu sichernden Informationen verschieben oder kopieren lassen. Die Konfiguration erfolgt über einen Wizard und stellt niemanden vor besondere Anforderungen. Die verschlüsselten Container können im Betrieb sowohl über das Management-Interface der Sicherheitslösung als auch über das Betriebssystem selbst verwaltet werden, es ist also zum Zugriff auf die verschlüsselten Daten nicht nötig, immer zuerst die Small Office Security zu starten, obwohl die Encryption-Lösung nahtlos in die Sicherheits-Suite integriert wurde. Die Verschlüsselung erfolgt mit AES und einer effektiven Schlüssellänge von 56 Bit.

Backups und Wiederherstellungen von Daten

Über die Backup-Funktion sichern die Anwender ihre Daten auf eine lokale Festplatte, ein Windows-Share, ein Wechselmedium, einen FTP-Server oder via Dropbox in die Cloud. Die Datensicherung wird wie die Verschlüsselung über einen Wizard konfiguriert.

Dieser bietet an, alles aus dem Ordner "Eigene Dateien" und dem Desktop zu sichern. Alternativ erstellt er auch Sicherheitskopien der auf dem jeweiligen Rechner vorhandenen Fotos und Bilder, der Filme und Videos und der Musikdateien. Falls nötig, lassen sich auch weitere Ordner als Sicherungsquelle angeben.

Die Backup-Vorgänge starten entweder manuell oder automatisch nach einem Zeitplan. Bei Bedarf können die Benutzer die Backup-Dateien mit einem Passwort schützen und die Zahl sowie die Speicherdauer der vorgehaltenen Daten begrenzen. Sowohl das Sichern, als auch die Wiederherstellung der Daten ließen sich im Test mit den von Kaspersky bereitgestellten Funktionen sehr einfach realisieren.

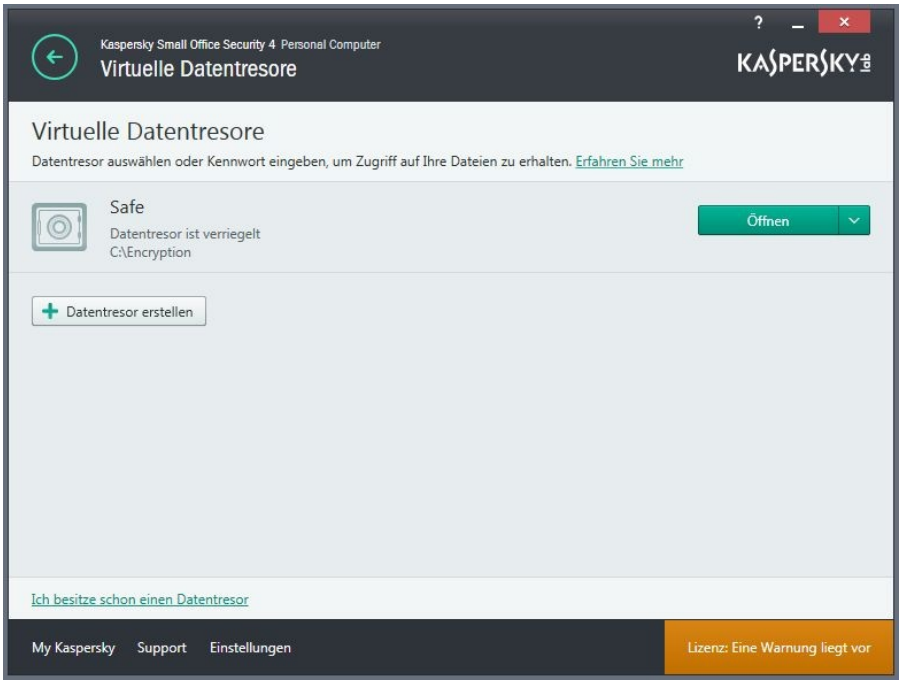
Der sichere Zahlungsverkehr

Zum Sichern des Zahlungsverkehrs über das Netz verwendet Kaspersky die Safe Money-Technologie. Um diese Funktion zu nutzen, müssen die Anwender zunächst die abzusichernden Webseiten mit ihrer URL in eine Liste eintragen und die Option "Sicherer Browser aktivieren" einschalten. Gehen sie danach auf eine der genannten Webseiten, so

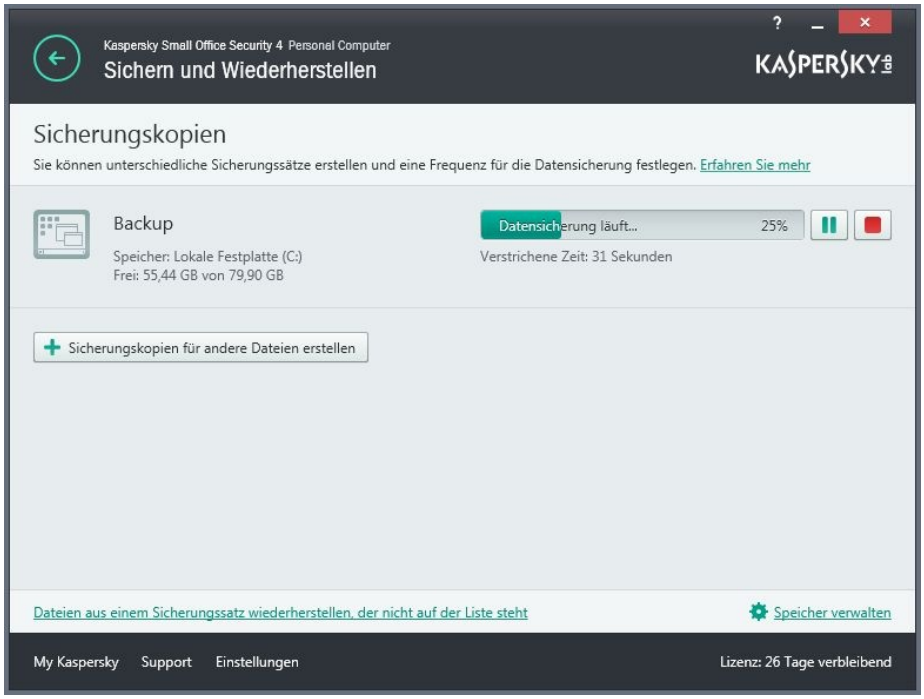
öffnet sich der "Sichere Browser" automatisch. Bei Bedarf steht auch eine virtuelle Tastatur zur Verfügung.

Konkret sieht die Benutzung des sicheren Zahlungsverkehrs folgendermaßen aus: Ruft der Benutzer im Betrieb mit seinem Browser eine der in der Liste erfassten Webseiten auf, so überprüft Kaspersky während des Ladens der Seite automatisch anhand einer Datenbank mit vertrauenswürdigen Adressen (die vom Hersteller oder vom Benutzer selbst zur Verfügung gestellt wird) ob die Seite in Ordnung ist. Trifft das zu, so wechselt der Browser in den "Safe Mode", der ihn vor Injections und Angriffen von verdächtigem Code schützt.

Taucht die Webseite nicht in der eben genannten Datenbank auf, so untersucht die Security Suite die Site mit einer heuristischen Analysefunktion, um Phishing-Scams auszumachen. Stellt sich heraus, dass die Seite unsicher ist, so blockt das System den Zugriff. Außerdem kommt der digitale Zertifikatsverifikationsdienst von Kaspersky zum Einsatz, um die Authentizität der Site zu garantieren. Gleichzeitig sorgt die Security-Lösung dafür, dass der Rechner, von dem aus die Transaktion durchgeführt werden soll, als sicher gelten kann. Im Betrieb traten bei der Arbeit mit der Funktion zum Absichern des Zahlungsverkehrs keine Schwierigkeiten auf.



Die Funktion zum Erstellen verschlüsselter Container

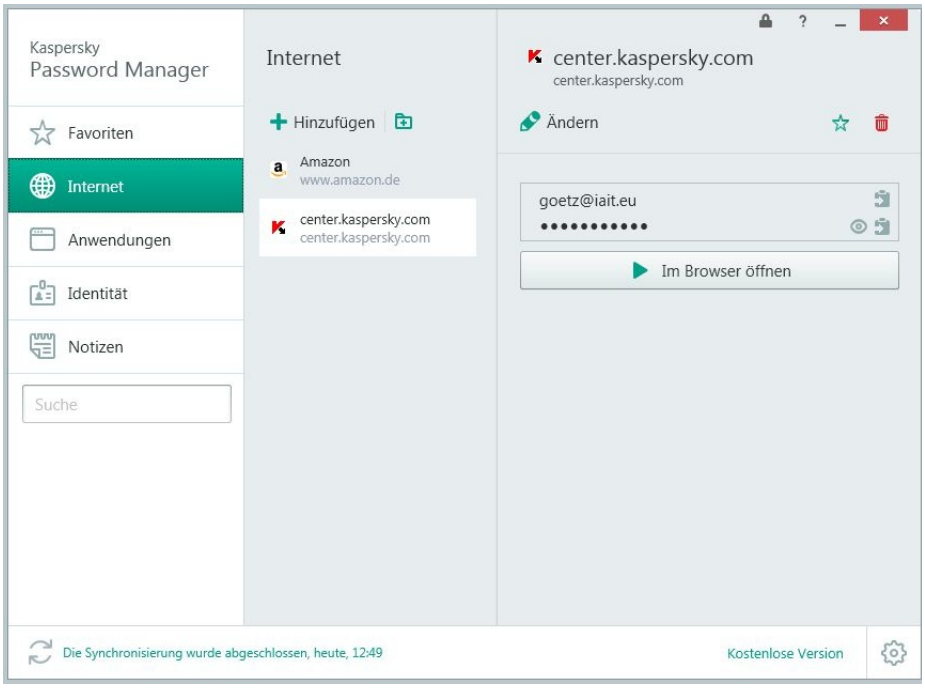


Die Backup-Funktion im laufenden Betrieb

Der Passwort-Manager

Zum Schutz der von den Anwendern benutzten Passwörter stellt Kaspersky als optionale Lösung einen Passwort Manager bereit. Bis zu 15 Passwörter lassen sich kostenlos damit verwalten, ansonsten wird eine zusätzliche Gebühr fällig. Der Passwort-Manager steht für Windows, Android und iOS zur Verfügung und die Einträge werden über das Web-Portal synchronisiert, so dass mobile Nutzer auch unterwegs den gleichen Zugriff auf ihre Passwörter haben, wie an ihrem Windows-Rechner. Nach der Installation des Produkts und der Definition eines Master-Passworts, das den Zugriff auf die gespeicherten Credentials ermöglicht, sind die Benutzer dazu in der Lage, Internet-Zugangsdaten einzutragen, die der Passwort Manager dann im Betrieb automatisch beim Öffnen der dazugehörigen Webseiten in diese einfügt. Das gleiche gilt auch für Zugangsdaten für Anwendungen. Abgesehen davon ermöglicht der

Passwort Manager auch das Sichern von Bankkonten und Kreditkartendaten und das Speichern so genannter Notizen, die Informationen enthalten, die nicht in fremde Hände gelangen sollen. Credentials in Webseiten und Anwendungsloginfenster – das im Test auf Anhieb funktionierte – nimmt den Usern viel lästige Tipparbeit ab und verhindert gleichzeitig frustrierende Tippfehler.



Die Oberfläche der Windows-Version des Passwort-Managers

Die Benutzer haben die Option, besonders wichtige Einträge zu favorisieren. Diese landen dann in einer Favoritenübersicht, in der sie besonders schnell auffindbar sind. Eine Suchfunktion steht ebenfalls bereit.

Die Android- und die iOS-Varianten der Software verfügen praktisch über den gleichen Leistungsumfang, ermöglichen aber zusätzlich den manuellen Anstoß der Datensynchronisierung mit dem Web-Interface und das Einrichten einer automatischen Sperre nach einer bestimmten Minutenzahl. Die Zwischenablage der Geräte leert die Software auf Wunsch nach ein paar Sekunden.

Im Betrieb gefiel uns der Passwort Manager sehr gut. Es ist praktisch, die Passwörter auch unterwegs dabei zu haben und das automatische Eintragen der

Fazit

Die Kaspersky Small Office Security 4 bietet den Anwendern mit den Anti Malware-Funktionen, dem Web-Filter, dem Internet-basierten Konfigurationstool, der Verschlüsselungsfunktion, dem Backup, dem sicheren Zahlungsverkehr und dem optionalen Passwort Manager alles, was ein kleines Unternehmen für den Schutz seiner Daten braucht. Da alle Funktionen nahtlos in die Software integriert wurden, müssen die Anwender lediglich auf ein Programm zugreifen, wenn sie ihre Sicherheitsfeatures nutzen wollen. Das macht die Arbeit mit der Suite einfach, spart Schulungskosten und ermöglicht es jedem User, seine Daten selbst zu schützen. Gleichzeitig hilft das Web-Interface dabei, das Sicherheitsniveau des ganzen Netzes auf einem konsistenten Stand zu halten.

Installation und Inbetriebnahme des Produkts brachten im Test keine Schwierigkeiten mit sich und die Software ließ sich auch im laufenden Betrieb einfach nutzen. Kaspersky hat das durch sinnvoll zusammengefasste und größtenteils selbsterklärende Einstellungsoptionen und diverse hilfreiche Assistenten realisiert, so dass komplizierte Konfigurationsparameter unter der Haube bleiben und die Benutzer nicht verwirren. Die große Zahl zusätzlicher Tools – an dieser Stelle seien nur die virtuelle Tastatur, die Funktionen zum Löschen von Aktivitätsspuren und Daten sowie die Suche nach Programmcode-Fragmenten genannt – macht den Leistungsumfang der Lösung vollends rund. Das Produkt eignet sich damit sehr gut für den Einsatz in kleineren Umgebungen.

Dr. Götz Güttich leitet das Institut zur Analyse von IT-Komponenten (IAIT) in Korschenbroich.

Kaspersky Small Office Security 4

Sicherheitssuite für kleinere Umgebungen mit Anti-Virus, Spam Filter, Backup, zentralem Administrationsinterface im Internet, Datenverschlüsselung und Funktionen zum Absichern von Online-Finanztransaktionen.

Vorteile:
- Einfache Installation
- Übersichtliche Konfiguration
- Viele nützliche Assistenten
- Großer Funktionsumfang

Hersteller:
Kaspersky Lab
www.kaspersky.com/de