



**Marktplatz für Kurzentschlossene**  
Sparen Sie 15% bei Ihrer Akademie Schulungsbuchung. Wie?  
Lesen Sie weiter ... Seite 2

**Software oder Appliance?**  
Eine spannende Frage auf der Suche nach der besten Lösung für Ihre Unternehmenssicherheit ... Seite 3

**Check Point Support läuft aus**  
Der Support für Ihre Check Point VPN-1 und Provider-1 NGX R65 läuft am 31.03.11 aus. Lesen Sie mehr ... Seite 4

**Tufin SecureTrack 5.2**  
Die neue Version wurde veröffentlicht. Auf einen Blick präsentieren wir Ihnen wesentliche Neuerungen ... Seite 4

**Technology Day**  
Vorankündigung! Reservieren Sie sich heute schon einmal den 26.05.2011. Es wird spannend... Seite 2

**Kolumne: Problem trifft Lösung**  
Ein bisher unbekannter Angriffsvektor!  
Lesen Sie weiter ... Seite 5

### Einer wie Keiner! Ihr Newsletter ...

Liebe Freunde, liebe Leser,  
ein ereignisreiches Jahr liegt hinter uns - mit zahlreichen Sternstunden! Sternstunden, die wir auch unseren Lesern zu verdanken haben. Denn Ihre Gedanken und Meinungen zu unseren Beiträgen waren und sind für uns Anregung und Herausforderung zugleich. Sie wissen ja, ein Newsletter lebt vom Dialog mit seinen Lesern. Weiter so: Ihre Meinung ist uns wichtig!

Weitere Sternstunden, die wir unseren Kunden und Partnern verdanken, liegen vor uns. Sie gehören den unterschiedlichsten Branchen an. Sie kommen aus mittelständischen Unternehmen oder Fachabteilungen großer Konzerne. Sie arbeiten mit verschiedenen Methoden und leben individuelle Unternehmenskulturen. So unterschiedlich wie unsere Auftraggeber sind auch unsere Lösungen. Eines jedoch haben sie gemeinsam: Alles, was wir tun, ist auf die jeweiligen Bedürfnisse unserer Kunden zugeschnitten. Daher sind sie uns über Jahre treu. DANKE!

Wir freuen uns auf die Zukunft mit vielen Sternstunden, auf eine weiterhin partnerschaftliche, vertrauensvolle Zusammenarbeit und gemeinsame Erfolge.

Ihr Team der BRISTOL GROUP und der Akademie für Netzwerksicherheit

... mit technischem Mehrwert

### •Aus II wird I3:

#### THE BRISTOL GROUP Langen in neuen Räumen

Zum 01.01.2011 haben wir unsere neuen Räume in Langen bezogen. Wir freuen uns besonders darauf, Sie, unsere geschätzten Kunden und Schulungsteilnehmer bei uns begrüßen zu dürfen. Bitte beachten Sie ab dem 01.01.2011 folgende Adresse:

THE BRISTOL GROUP Deutschland GmbH  
Robert-Bosch-Straße 13  
63225 Langen

### Unsere Highlights in dieser Ausgabe

<b>BRISTOL NEWS</b> .....	Seite 2
Neues aus der Wartung Akademie für Netzwerksicherheit – Check Point Workshops in der Version R75 Begegnen Sie uns - Vorankündigungen	
<b>Thema des Monats</b> .....	Seite 3
Software oder Appliance	
<b>Wir wissen nicht, ob Sie's schon wussten</b> .....	Seite 4
Tufin – SecureTrack in der Version 5.2 Check Point R75 – jetzt neu	
<b>Kolumne: Problem trifft Lösung</b> .....	Seite 5
DLL Hijacking	
<b>Spielraum</b> .....	Seite 6

**Neues aus der Wartung:**

**Haus der  
Dienstleistung:  
flexibel und individuell**

Wartung ohne Wartungsvertrag - auch das gibt es bei der BRISTOL GROUP in Form von Bristol On Demand, kurz BonD.

BonD stellt Ihnen qualitativ hochwertigen Support durch zertifizierte Security-Consultants der Bristol Group auch dann zur Verfügung, wenn Sie keine Wartung oder nur eine reine Subskription für Ihr Produkt erworben haben. Auch wenn Ihr regulärer Dienstleister außerhalb Ihrer vertraglichen Supportzeiten nicht für Sie ansprechbar ist, gleich aus welchem Grund, können Sie BonD jederzeit in Anspruch nehmen.

Mit BonD ergänzen Sie optimal Ihren Bristol-Wartungsvertrag. Wenn nämlich eine Krisensituation außerhalb Ihres Support-Zeitrahmens (oft 5x10) eintritt, kann es im Einzelfall für Sie wirtschaftlicher sein, zusätzlich zum vertraglichen Support sofort einen kostenpflichtigen Call zu eröffnen. So sparen Sie wertvolle Ausfallzeit. Sie erreichen das BonD-Team über eine Mehrwertdienste-Rufnummer rund um die Uhr.

Weitere Informationen zu unseren BonD-Dienstleistungen finden Sie auch unter "CareForce One" auf der Bristol-Website.

Sprechen Sie uns an:  
wartung@bristol.de

**Neues aus der Akademie für  
Netzwerksicherheit:**

**Wir haben unser Portfolio für Sie  
ausgebaut**



Zum Beginn dieses Jahres haben wir für Sie unser Portfolio weiter optimiert und ausgebaut. Wir freuen uns, Ihnen heute die folgenden neuen Check Point Workshops Ihrer Akademie präsentieren zu können – und als besonderes Highlight, unsere Check Point Workshops in der Version R75:

**Check Point Essentials R70/R71  
(CCSA/CCSE Kompakt Workshop)**

In diesem Kurs werden die grundlegenden Elemente aus dem Seminaren zum CCSA und CCSE, die zum Betrieb eines Firewall Gateways/Management erforderlich sind, vermittelt. Dies geschieht unter Zuhilfenahme der original Kursunterlagen, so dass Sie sich nach der Schulung die restlichen Kenntnisse erarbeiten können, um die Zertifizierungstests abzulegen.

Lesen Sie mehr ...

**Check Point Workshop – Upgrade  
Sicheres Upgrade von R65 auf R75**

Während diesem Kurs wird ein Upgrade auf Check Point R75 in kompakter Form durchgenommen und gemeinsam durchgeführt - darüber hinaus sieht die Agenda das Thema Backup vor.

Lesen Sie mehr ...

**Check Point Workshop - Hands-On the  
Blades R75**

In diesem Kurs wird ein Kurz-Update auf Check Point R75 vorgenommen und dann dediziert auf die einzelnen neuen Blades und deren spezielle Funktionen eingegangen.

Lesen Sie mehr ...

**Marktplatz für Kurzentzuschlossene:**

Der erste Marktplatz für Kurzentzuschlossene im Jahr 2011. Buchen Sie eines der nachfolgend genannten Seminare und Sie erhalten 15% Preisnachlass auf den Listenpreis:

Hacker-Angriffe-Sicherheitslücken  
Extended + WLAN

Termin: 15.02. - 17.02.11 in Langen  
Preis: statt 1.950,00 € nur 1.657,50 €

Weitere Informationen ...

Check Point Security Administrator R70  
Termin: 14.02. - 18.02.11 in Berlin

Preis: statt 2.990,00 € nur 2.541,50 €

Weitere Informationen ...

Check Point Workshop – Operating R75  
Termin: 22.02. - 24.02.11 in

Hallbergmoos

Preis: statt 1.890,00 € nur 1.606,50 €

Weitere Informationen ...

**BEGEGNEN SIE UNS**

Die BRISTOL GROUP ist immer auf der Suche nach den aktuellen Trends in der IT-Security. Mit unseren Events - die Wissen vermitteln - freuen wir uns immer wieder auf's Neue Sie begeistern zu können!

**Vorankündigung:  
Technology Day**

Halten Sie sich schon heute den Termin frei. Während unserem Technology Day werden wir Sie über spannende Themen rund um die IT-Sicherheit informieren und Ihnen interessante Lösungsansätze und Gäste präsentieren. Seien Sie mit dabei!

Termin:

**26. Mai 2011 – Rhein/Main Gebiet**

# Thema des Monats

## Software oder Appliance?

### Lösung: eine individuelle Mischung

Auf der Suche nach der besten Lösung für Ihre Unternehmenssicherheit stellen uns Kunden immer wieder die Frage, ob die Gateway Firewall als klassische Software oder aber als Appliance aufgesetzt werden soll.

Auf dem Markt stehen sich Soft- und Hardware basierende Lösungen in Form von Appliances gegenüber. Die Vorteile von Appliance Lösungen liegen auf der Hand. Hard – und Software sind aufeinander abgestimmt und sowohl Patches und neue Versionsupgrades werden vollumfänglich unterstützt. Eine separate Installation der Software mit den daraus möglichen Risiken entfällt. Die Auswahl erfolgt anhand des nötigen Durchsatzes und nicht basierend auf Userzahl oder IP-Adressen. Der Anwender kann für sich das optimale Gerät wählen. Des Weiteren wird bei den Appliance Lösungen auch immer häufiger der UTM Ansatz gefahren. Dies

bedeutet Firewall, VPN-Funktionalität, IPS, AntiVirus und mehr befinden sich auf dem Gerät. Das spart natürlich Kosten bei der Beschaffung, aber auch bei der Betreuung der Systeme. Eine Managementoberfläche für alles erleichtert den Administratoren ihre Arbeit und spart Zeit.

Allerdings bedeutet dies auch eine hohe Verwundbarkeit des Netzwerkes beim Ausfall der Hardware. Deshalb ist bei dieser Lösungsvariante eine redundante Auslegung und ein schneller Hardwareaustausch unabdingbar.

Eine Alternative dazu ist natürlich die Software basierende Variante.

Auch dem Konsolidierungsansatz kann bei der Software Variante Rechnung getragen werden. Viele Kunden haben sich für einen Hardware Lieferanten im Serverbereich entschieden. Durch die Auswahl eines Herstellers und Lieferanten für die Serverhardware ergeben sich Einsparungsmöglichkeiten. Hardwareaustauschlevel können durch den Einsatz von Spareparts auf kostengünstige Varianten heruntergefahren werden. Bei Erweiterungen oder Erneuerungen der Geräte offenbart sich ein weiterer Vorteil der Trennung von Hard- und Software:

Unabhängig von den Software Lizenzen können die Server ausgetauscht werden. Bei den Appliances hingegen muss die gesamte Lösung erneuert werden.

Auch das Thema Virtualisierung kann nur mit einer Softwarelösung umgesetzt werden. Bei Appliances werden die Gateways per SSH über eine WebGui administriert. Wenn darüber hinaus die

Möglichkeit besteht, ein abgesetztes zentrales Management zu implementieren, so handelt es sich hierbei in der Regel um eine separate Appliance. Bei den Software basierenden Lösungen ergeben sich hingegen die Optionen eines normalen Management Servers oder den Einsatz auf einer Vmware.

Hersteller wie Check Point und Stonesoft bieten sowohl Software als auch Appliances an. Diese beiden Hersteller zeichnet besonders ein möglicher Mischbetrieb aus beiden Varianten aus. So kann man mit einem zentralen Management verschiedene Standorte zentral administrieren.

Eine Mischung beider Lösungsansätze ist diesen Herstellern möglich, da sie seit langem auf dem Markt vertreten sind und sich somit auch die notwendige Erfahrung und Logistik aufbauen konnten.

Als Quintessenz kann also kein eindeutiges Urteil abgegeben werden, welches die bessere Lösung ist. Dies bedeutet, dass eine solche Entscheidung im Einzelfall auf den Kunden abgestimmt getroffen werden und als individuelles kundenorientiertes Konzept umgesetzt werden muss.

Sprechen Sie uns an, gerne beraten wir Sie zu diesem Thema: 06103/20 55 300

### Sprechen Sie uns an, gerne sind unsere Experten für Sie da:



#### Thorsten Metzger

Ihr technischer Spezialist ganz besonders wenn es um Check Point geht. Mit Rat und Tat steht er Ihnen zur Seite und auch bei Schulungen ist er Ihr Mann.



#### Erik Goransch

Ihr technischer Experte für Stonesoft. Egal ob ausführliche Beratung vorab, Implementierung des Systems oder Support im nachhinein.

# Wir wissen nicht, ob Sie's schon wussten ...

## Tufin SecureTrack Version 5.2

### What's new?

Die neue Tufin SecureTrack Version 5.2 wurde zum Ende des letzten Jahres released. Auf einen Blick einige der neuen Features:

- Verbessertes Reporting in Bezug auf Gruppen, Netzwerke, Services, Objekte und auch ungenutzte Objekte
- auch nicht-SecureTrack Nutzer können per eMail über Reports informiert werden

- Die Reports können automatisiert im PDF Format gespeichert werden, z.B. via SCP
- in der neuen Version besteht die Möglichkeit, die Reports mit einem Firmenlogo zu versehen
- Verbesserung der Policy Analyse und des Policy Management
- Stark verbesserter Fortinet Support

Sprechen Sie uns an, gerne beraten wir Sie: 06103/20 55 300

## Horoskop für IT-Wassermänner

Wassermann 21.01. - 19.02.



Das Jahr 2011 wird Ihr Jahr. Der richtige Moment, um Ihre Pläne zu verwirklichen ist gekommen. Ihre neuen Ideen und kreativen Einflüsse im Team, machen die Geschäftsleitung auf Sie aufmerksam. Teilen Sie Ihre Kreativität im Unternehmen mit Ihren Kollegen und klettern Sie die Karriereleiter hinauf. Nutzen Sie die Möglichkeiten der modernen Technik und Fortbildungsmaßnahmen, die Sterne hierfür stehen sehr gut. Jedoch neigen Sie gelegentlich zu Übereifer. Erledigen Sie eine Aufgabe nach der anderen, damit Ihre Power auch gut ankommt und nicht ins Gegenteilige verläuft. In Hinsicht auf Ihre Gesundheit sieht es in diesem Jahr ebenso gut aus, wie im beruflichen Bereich. Ihre Vitalität und Ihre Leistungskurve sind überdurchschnittlich hoch. Halten Sie sich weiterhin so fit und gesund.

## Support endet

Wichtig für alle Check Point Kunden



**Check Point**  
SOFTWARE TECHNOLOGIES LTD.

Der Support für Ihre Check Point VPN-1 und Provider-1 NGX R65 läuft am **31.03.2011** aus.

Wann planen Sie das Upgrade auf R75?

Um das Upgrade für Sie so unkompliziert wie möglich zu gestalten, hat unser CareForce One Team bereits alles nötige für Sie zusammengestellt: unser **Total Intelligence Package 7 – Check Point R75**.

Wir haben an alles gedacht, von der Analyse der Ist-Situation über die Planung des Upgrades, die Durchführung, den anschließenden Support bis hin zur Schulung Ihrer technischen Mitarbeiter.

Erfahren Sie mehr ...

Gerne beraten wir Sie auch telefonisch: 06103/20 55 300

## Jetzt da – Check Point R75 Wann realisieren Sie das Upgrade?



Seit Beginn dieses Jahres ist die neue Version Check Point R75 verfügbar. Diese bietet Ihnen die folgenden Features:

- Neuartige Application Control
- Verbesserte Benutzererkennung (Captive Portal)
- DLP on the Gateway
- Vollständige Unterstützung "Secure Client Next Generation"

Sehr gerne senden wir Ihnen nähere Informationen – wir sind immer für Sie da [sales@bristol.de](mailto:sales@bristol.de).

## Horoskop für IT-Fische

Fische 20.02. – 20.03.



Es könnte sein, dass dieses Jahr anfängt wie das letzte aufhört, zumindest hat es den Anschein. Nutzen Sie die vielen ups and downs für sich und für Ihren Erfahrungsschatz. Es kann nicht immer alles glatt laufen. Ab Mitte des Jahres ergibt sich eine gute Gelegenheit, Ihr Können unter Beweis zu stellen, ergreifen Sie diese und bauen Sie darauf auf. Wichtig ist es, an sich selbst und an Ihre Fähigkeiten zu glauben, zeigen Sie Ihren Mitmenschen ruhig Ihr Selbstbewusstsein. Denn Selbstbewusstsein wird Ihnen einige Türen öffnen. Gesundheitlich geht es Ihnen dieses Jahr besser denn je. Achten Sie auf ausgewogene Ernährung und auf reichlich Sport.

# Kolumne: Problem trifft Lösung

## Vom Wert der Lösung

Ein Problem muss nichts negatives sein. Es bedeutet eine Chance für uns, Neues zu lernen, in unseren Fähigkeiten und Fertigkeiten zu wachsen. Wie erfolgreich wir ein Problem lösen, hängt auch von unserer inneren Einstellung und den Fragestellungen ab, mit denen wir an das Aufgabenlösen gehen.

Das gilt generell im Leben und speziell im Beruf. Probleme bieten uns eine Chance. Jede Aufgabe, mit der wir uns auseinandersetzen und beschärfen, macht uns ein wenig mehr zum Spezialisten auf ihrem Gebiet. Dieses Wissen und die Erfahrung, kurz unser Know-how, wenn es darum geht Lösungen zu finden, die Ihrer IT-Sicherheit dienen, möchten wir Ihnen hier weitergeben und vermitteln. Problemlösungen mit Mehrwert!

Unser Consultant-Ihr  
Redakteur der Kolumne.  
Wie stellen vor:  
**Michael Schimpf**



## DLL Hijacking

### Nicht ganz ohne Ecken und Kanten

Microsoft Windows wird immer wieder gerne in der Öffentlichkeit wegen seiner vielen Sicherheitslücken belächelt. Zwischen den regulären Patchdays finden sich vermehrt kritische Hotfixes, die irregulär eingespielt werden sollen, um sein System möglichst sicher zu halten. Häufig werden Lücken publik, die Tage und sogar Wochen ungepatcht bleiben.

Nun erschüttert ein neu entdeckter Angriffsvektor die Sicherheit der Microsoft Welt – DLL Hijacking.

Eine slovenisches Sicherheitsunternehmen veröffentlichte im letzten Jahr Details zu dieser Lücke. Unabhängig davon haben zwei Studenten der University of California bereits Anfang des Jahres ein Dokument veröffentlicht, welches ziemlich genau dieses Problem adressiert.

DLL Hijacking ist eigentlich sehr simpel. Es folgt grob diesem Prinzip: Öffnet man über eine Netzwerkfreigabe eine Datei, die mit iTunes verknüpft ist, so lädt iTunes auch eine oder mehrere DLL Dateien aus der Freigabe nach. Selbst wenn die eigentlich geladene Datei sauber ist, können bösartige DLL Dateien platziert werden, die schließlich zur Ausführung des Schadcodes führen. Die erwähnten DLL Dateien werden "on-the-fly" generiert, wenn sie von der betroffenen Applikation angefragt werden. Sie liegen also nicht im Verzeichnis und sind daher auch nicht sichtbar.

Nach dem selben Prinzip wie iTunes arbeiten viele andere Anwendungen unter Windows und sind dementsprechend auch davon betroffen.

Wichtig dabei ist, dass das aktuelle Verzeichnis geladen werden muss, um das Verhalten zu provozieren. Ein direkter Link auf eine Datei (z.B. `\\dateiserver\2010\bilanz.pdf`) löst das Problem nicht aus. Man müsste vorher das Verzeichnis `\\dateiserver\2010\` öffnen und dann die Datei öffnen.

Für gewöhnlich trifft diese Grundsatzregel zu. Es gibt allerdings einige Ausnahmen. Das hängt aber von der einzelnen Anwendung ab.

Wie schützt man sich nun vor DLL Hijacking? Jeder Hersteller jeder

verwundbaren Anwendung muss einen Patch schreiben und veröffentlichen. Bis dies geschehen ist, bleiben nur einige Workarounds.

- SMB nur dort erlauben, wo es wirklich gebraucht wird (an der Internet Firewall auf jeden Fall blocken)

- WebDAV nach außen blocken, entweder über einen HTTP Proxy oder die "PROPFIND HTTP Methode" verbieten

- WebDAV bereits auf den Clients über eine Group Policy deaktivieren, dadurch entfällt auch der PROPFIND Filter

Weitere Informationen und Schutzmöglichkeiten von Microsoft selbst sind unter anderem im Internet bereitgestellt und zu finden.

Sehr gerne senden wir Ihnen weitere Informationen zu diesem Thema zu. Sprechen Sie uns an: 06103/20 55 300

Auch wenn sich dieser Beitrag eher auf der Netzwerkebene bewegt, es sind nicht nur WebDAV und SMB betroffen. Das dynamische Laden der DLLs findet auch in jedem anderen Verzeichnis statt, wie z.B. auf USB Sticks oder anderen Wechseldatenträgern. Der Angreifer muss nur Zugriff auf das entsprechende Verzeichnis haben, aus dem die Datei geöffnet wird.

# Spielraum

## Rezept des Monats: Rosenkohl-Maronen-Gratin

Zutaten für 4 Personen

500 g Esskastanien  
1 l Wasser  
500 g Rosenkohl  
2 Zwiebeln  
40 g Butter (1)  
Salz  
1 Prise Muskat  
Butter  
150 g Parmesan  
100 g saure Sahne  
40 g Butter (2)

Die Maronen mit spitzem Messer kreuzweise einschneiden und in kochendem Wasser in etwa 20 Minuten weich kochen. Kalt abschrecken, Schale und das innere Häutchen entfernen. Rosenkohl waschen, Deckblätter entfernen. Die Zwiebeln schälen, kalt abspülen, dann halbieren und würfeln. In heißer Butter (1) goldbraun braten. Rosenkohl, Salz sowie Muskatnuss beifügen, zugedeckt bei mittlerer Hitze ca. 10 Minuten dünsten. Die Kochbrühe abgießen und aufheben. Eine hohe Auflaufform leicht fetten, abwechselnd Rosenkohl, Maronen und geriebenen Parmesan schichten. Saure Sahne mit einigen Löffeln der Rosenkohlbrühe verrühren und die Mischung über die obere Schicht verteilen, die Butter (2) in Flocken darüber setzen. Im Backofen, auf der mittleren Schiene bei 200° C in 25-30 Minuten gratinieren.

## Impressum

THE BRISTOL GROUP  
Deutschland GmbH  
Zentrale Rhein Main  
Robert-Bosch-Straße 13  
63225 Langen

Telefon +49 (0) 61 03 / 20 55 - 300  
Telefax +49 (0) 61 03 / 70 27 87  
[info@bristol.de](mailto:info@bristol.de) - [www.bristol.de](http://www.bristol.de)

Geschäftsführung:  
Ruth Townsend  
Susanne Daum

Anregungen zur Gestaltung oder  
Fragen zum Inhalt dieses Newsletters  
senden Sie bitte an:  
[marketing@bristol.de](mailto:marketing@bristol.de)

## Das Alte zurücklassen

Das Alte zurücklassen,  
um begeistert zu leben,  
sich an das Gute erinnern  
und Unrecht vergeben.

Lösen, was uns gefangen nimmt,  
im Blick auf das Jahr, das nun zerrinnt.

Die Kraft aufbringen, nichts festzuhalten,  
was sich nicht lohnt aus den Zeiten, den alten.

Im Vertrauen auf Gott den Aufbruch wagen  
an der Schwelle zu den neuen Tagen.

Dem Menschen am Straßenrand ohne Hast  
aufhelfen und mittragen seine Last.

Die eigenen Gaben der Welt gerne schenken,  
und mit Zuversicht den Blick  
auf das neue Jahr lenken.

Mit einem herzlichen Dankeschön für ein erfolgreiches  
vergangenes Jahr wünschen wir Ihnen und Ihren  
Lieben alles Gute für das Jahr 2011, viel Glück, Erfolg  
und vor allem Gesundheit.

Ihr Team der BRISTOL GROUP