

### Es ist doch alles sicher? - Oder?

Es gibt faktisch kein Unternehmen, das keine IT-Sicherheitsvorrichtungen zum Schutz der eigenen Infrastruktur und der darin gespeicherten Daten einsetzt. Wenn sich auch Unternehmen mittlerweile neuen Risiken stellen müssen, sind die bisherigen Schutzmechanismen am Perimeter des lokalen Netzwerks nicht überflüssig geworden. Ganz im Gegenteil müssen sich auch etablierte Schutzvorrichtungen den sich ständig ändernden Angriffen stellen.

Viele Unternehmensverantwortliche vertrauen darauf, daß man ja (seinerzeit) viel Geld in den Schutz des LAN investiert hat. Doch verlassen sich dabei nicht viele auf eine Art Scheinsicherheit? Nicht jede Firewall ist auf dem aktuellen Stand, nicht alle Einrichtungen sind fehlerfrei gepflegt und es wurden doch ständig neue Services in der IT hinzugefügt. Sind keine neuen Risiken durch diese neuen Dienste entstanden?

Doch wie kann die Wirksamkeit des Schutzes geprüft und gemessen werden?

Nur, wenn man die Bedrohung, die mit dem modernen IT-Betrieb einhergeht, simuliert und die Infrastruktur Scheinangriffen aussetzt, kann festgestellt werden, ob die getroffenen Sicherheitsmaßnahmen greifen und ob es nicht doch unentdeckte Lücken im Schutzschild der IT gibt. Dazu ist es notwendig auf das Wissen und die Erfahrung von IT-Sicherheitsexperten zurück zu greifen, die nicht im eigenen Unternehmen eingebunden sind. Neutrale, vertrauenswürdige Dritte, die mit dem Know-how von negativ motivierten Angreifern den IT-Schutz auf die Probe stellen.

Aus diesem Grund lassen Sie als professioneller IT-Verantwortlicher turnusmäßige Sicherheitsprüfungen, sog. Penetrationstest durchführen.

Ist es denn notwendig, jedes Jahr diesen großen Aufwand zu treiben, zumal solche Prüfungen nicht immer als billig zu bezeichnen sind? Kann man denn nicht größere Zeitabstände zwischen den Prüfungen lassen? Kann man denn feststellen, daß es nach einer größeren Zeitspanne wieder einmal nötig sein könnte, einen vollständigen Sicherheitscheck durchführen zu lassen? Oft fragt man: „Reicht es nicht aus, wenn da mal jemand drüberschaut?“

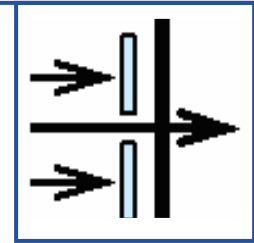
### Die Antwort ist JA und NEIN!

So unterschiedlich wie die Unternehmen ist auch deren Informationstechnologie. Unterliegt das eine Unternehmen vielen IT-technischen Änderungen, so bleibt eine andere Firma relativ stabil, was den Bedarf an Neuerungen in der IT angeht. So auch die Sicherheitssysteme. Muß das eine Unternehmen seine Einrichtungen sehr schnell auf neue Risiken anpassen, so bleibt in einem anderen Unternehmen das Risikopotential relativ gleich. Und so unterschiedlich ist auch der Bedarf eine komplexe Sicherheitsüberprüfung durchführen zu müssen.

Jedoch ein Fakt bleibt:

**Nur geprüfte Sicherheit ist  
verlässliche Sicherheit.**

Schließlich sehen viele auch nicht die unzähligen, permanent stattfindenden Versuche, Informationen über die netzwerktechnische Seite Ihres Unternehmens herauszubekommen. Man kann das als Angriffs-grundrauschen bezeichnen, und diesem sind alle an öffentliche Netze wie das Internet angeschlossene Teilnehmer ausgeliefert - ob sie das „sehen“ oder nicht - Ihre IT-Sicherheit schützt Sie davor.



### Oberflächliche Prüfung

Daß die CareForce One™ der Bristol Group professionelle strukturierte Sicherheitsprüfungen für Netze und Server anbietet, ist fast als selbstverständlich anzusehen. Was ist aber mit gerade den Unternehmen, die den Aufwand einer umfangreichen Prüfung nicht möchten oder nicht für notwendig halten? Die Antwort der CareForce One™ ist **Overscan** - eine minimalistische Sicherheitsprüfung, die Ihrem Unternehmen bei der Entscheidung hilft, sich wieder einmal einer vollständigen Sicherheitsprüfung zu unterziehen.

**Overscan** benutzt einen Teil der zum BASIC-Modul der CareForce One™ gehörenden Tests, der zur ersten Informationsbeschaffung bei der Vorbereitung einer Penetrationsprüfung dient. Also genau das, was Kunden so oft formulieren: „Kann man da nicht einmal so drüberschauen?“

Sogenannte Scanner-Programme prüfen automatisch alle 65356 Service-Ports einer IP-Adresse. Dieses wird für alle 255 Protokolltypen durchgeführt, ob diese verbindungsbehaftet oder verbindungslos sind. Ebenso wie im BASIC-Modul, werden diese Tests stark randomisiert, d.h. die Ports werden nicht sequentiell und immer mit dem gleichen Zeittakt abgescannt, die Herkunftsadresse wechselt, damit Intrusion-Detection-Systeme/Funktionen keine Regelmäßigkeiten leicht erkennen können.

### Eine einfache Sicherheitsüberprüfung professionell

Wichtige Voraussetzungen für ordentliche Sicherheitsüberprüfungen sind:

- ★ Kompetenter, vertrauenswürdiger Auditor
- ★ Saubere, juristisch klare Abmachungen
- ★ Strukturierte Planung und Ablauf der Prüfung
- ★ ordentliche Dokumentation der Ergebnisse

Ein guter Auditor muß über langjährig aufgebaute Erfahrungen in der IT-Sicherheit verfügen und sollte nicht zum zu prüfenden Unternehmen gehören, um eine kritische, neutrale Betrachtungsweise mitzubringen. Es ist in aller Regel erforderlich und hilfreich, wenn Kunde und Prüfungsunternehmen ein passendes, gegenseitiges Verschwiegenheitsabkommen unterzeichnen.

Der Kunde gibt eine eindeutige Einverständniserklärung gegenüber dem Prüfunternehmen ab, um die Legalität der Prüfung zu bestätigen. Eine Festlegung der Rahmenbedingungen des Audits über das Prüfungsziel und die Penetrationsprägnanz sind für **Overscan** nicht nötig, da der Umfang von vornherein feststeht.

Nur die zu prüfende IP-Adresse ist auf dem Formular der Einverständniserklärung zu vermerken. Ebenso befindet sich auf diesem Formblatt auch die Möglichkeit die Optionen eines kostenpflichtigen, erweiterten **Overscan** zu wählen. Als Prüfungsabschluß erhält der Kunde einen Prüfbericht über den vorgefundenen Zustand.

Umfang der enthaltenen Leistungen:

- **Overscan** ist eine kostenlose Leistung
- Ist begrenzt auf eine öffentliche IP-Adresse
- Ist ein automatischer Scan aller 65365 Ports mit 255 Protokollen
- Wird automatisch bei Auffinden einer nachweisbaren Schwachstelle beendet
- Erhebt keinen Anspruch auf Vollständigkeit
- Liefert einen Kurzbericht mittels E-Mail inkl. Verbesserungsvorschlag
- Bedarf einer Einverständniserklärung des Kunden

Selbstverständlich kann man **Overscan** vervollständigen, oder es lassen sich die vollständigen Sicherheitsprüfungen für Netze und Server der CareForce One™ buchen. Als Folge, daß der **Overscan** etwas aufdecken konnte, was Ihnen bisher verborgen war, werden oft weitere Informationen gewünscht. Daher sind zu **Overscan** zwei kostenpflichtige Optionen erhältlich. Einige Kunden möchten nicht, daß **Overscan** nach einer gefundenen Schwachstelle beendet wird, sondern bis zum Ende des Durchlaufs über alle 65356 Ports nach weiteren Risikopunkten sucht. Dann kann der volle Scanumfang als Option (Fullscan) hinzugenommen werden.

Andere Kunden möchten, daß durch den Einsatz von Software, die eine Ausnutzung der gefundenen Schwachstelle durchführt (sog. Exploits) auch eine Art Beweis für die Gefährlichkeit der Schwachstelle, ein sog. Proof of Concept erzeugt wird, um gegebenenfalls auch nicht technisch versierte Mitarbeiter von einem gegebenen Handlungsbedarf zu überzeugen.

**Overscan** Optionen:

- a) Voller Umfang über alle Ports - **Fullscan**
  - Vollständiger Scan (kein Abbruch bei Schwachstelle)
  - Bericht mit Einstufung des Risikos der gefundenen Schwachpunkte (jedoch keine CVE-Referenzen)
- b) Proof of Concept - **Exploit**
  - Proof of Concept für die eine gefundene Schwachstelle
  - Bericht mit genauer Darstellung der Schwachstelle und den erreichten Zielen (z.B. Passwörter ausgelesen oder vollständige Systemübernahme)

Den beiden Optionen ist die Anrechnung bei Beauftragung eines vollständigen BASIC-Tests gemeinsam, da erfahrungsgemäß Kunden, bei denen mittels **Overscan** ein Schwachpunkt aufgedeckt wurde, mehr über den Sicherheitszustand und ihren Risikostatus in Erfahrung bringen möchten. Der Leistungsumfang der vollumfänglichen Sicherheitsprüfungen für Netze und Server ist in einem anderen Datenblatt und einer detaillierten Leistungsbeschreibung erklärt.

## Kompetenz

THE BRISTOL GROUP beschäftigt sich seit mehr als 15 Jahren mit IT-Security. In dieser Zeit wurden Hunderte von Beratungen zum Thema Netzwerksicherheit durchgeführt. Als unabhängiger IT-Security Provider auf die Optimierung der Sicherheit in der Informations-Technologie spezialisiert, wurden Tausende Lösungen jeglicher Größe implementiert. Durch die Erfahrung konnte ein enormer Bestand an Wissen aufgebaut werden. Alle BRISTOL Consultants verfügen über mehrere Herstellerzertifizierungen und sind als Ausbildungstrainer tätig. Mit der „Akademie für Netzwerksicherheit“, einem Unternehmen der BRISTOL GROUP, wird ein wesentlicher Beitrag zur Ausbildung von Fachkräften für IT-Sicherheit in Deutschland geleistet. Mit dem Wissen über die Denkweise und Methoden von Angreifern und unter Einsatz ähnlicher oder gleicher Softwarewerkzeuge, wird die Schwachstellenanalyse der Kundensysteme vorgenommen. Tiefe Kenntnisse der Kommunikationsverfahren und das Wissen über die üblichen Fehler von Administratoren befähigen zu qualitativ hochwertigen Überprüfungen mit äußerst realistischen Aussagen.

Der Situation und dem Kundenbedürfnis angepaßt, werden auch über **Overscan** hinausreichende Sicherheitsüberprüfungen für Netze und Server angeboten. Von automatisierten Scans aus dem Internet über den Einsatz von ethischem Hacking bis zu Sicherheits-Audits großer LANs sind verschiedene Leistungen skalierbar. Hierfür stehen dem Kunden von der CareForce One™ eine ganze Palette beschriebener Module zur Verfügung. Zusätzlich lassen sich eine Reihe offener Parameter, wie „geheimer Test“ festlegen.

Verschaffen Sie sich einen ersten Überblick mit **Overscan**



## Verschwiegenheit ist oberstes Gebot!

THE BRISTOL GROUP sichert verbindlich zu, daß alle Informationen über die Prüfung und deren Resultate streng vertraulich behandelt werden. Keinerlei Aufzeichnungen des Tests werden länger als 48 Stunden nach Abgabe des Berichts gespeichert.

Schenken Sie uns Ihr Vertrauen,  
die **CareForce One™** der Bristol Group.

### THE BRISTOL GROUP Deutschland GmbH

#### Niederlassung Berlin

Fasanenstraße 81  
D 10623 Berlin  
Tel +49 (0) 30 – 31 00 76 10  
Fax +49 (0) 30 – 31 00 76 20

#### Zentrale Rhein/Main

Robert-Bosch-Straße 11  
D 63225 Langen  
Tel +49 (0) 61 03 – 20 55 300  
Fax +49 (0) 61 03 – 70 27 87

#### Niederlassung München

Lilienthalstraße 25  
D 85399 Hallbergmoos  
Tel +49 (0) 8 11 – 99 86 110  
Fax +49 (0) 8 11 – 99 86 129