

Vertrauen ist gut - Kontrolle ist viel besser

Unternehmen müssen sich zunehmend um die Konformität mit Gesetzen und Regelung bemühen, um deren Einhaltung sicherzustellen. Die Dokumentation zur konformen Richtlinieneinhaltung wird mehr und mehr durch Geschäftsbeziehungen, Zugehörigkeit zu Firmenzusammenschlüssen oder Verbänden sowie neuen Gesetzesauflagen gefordert. Einen wichtigen Teil spielt dabei die Einschätzung der Risikolage eines Unternehmens. Dieses Risiko setzt sich aus betriebsbedingten und organisatorischen Risiken zusammen. Zu den organisatorischen Risiken zählen heutzutage auch die Risiken, die beim Betrieb von Informationstechnologie (IT) entstehen. Unternehmen sind von der Verfügbarkeit, Integrität und Vertraulichkeit Ihrer IT-Systeme und der darin gespeicherten Daten mittlerweile überlebenswichtig abhängig, was landläufig mit dem Wort „unternehmenskritisch“ bezeichnet wird.

Zu diesem Zweck setzen Unternehmen einen Teil ihrer IT-Budgets gezielt für den Schutz der unternehmenskritischen IT-Ressourcen ein. Doch wie kann die Wirksamkeit dieses Schutzes geprüft und gemessen werden?

Nur, wenn man die Bedrohung, die mit dem modernen IT-Betrieb einhergeht, simuliert und die Infrastruktur diesen Scheinangriffen aussetzt, kann festgestellt werden, ob die getroffenen Sicherheitsmaßnahmen greifen und ob es noch weitere, unentdeckte Lücken im Schutz 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.

Strukturierte Prüfung

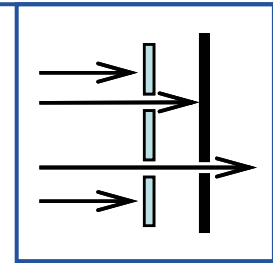
Um IT-Infrastrukturen professionell auf Sicherheitschwachstellen und die damit verbundenen Risiken überprüfen zu können, bedarf es nicht nur exzellenter Kenntnis der IP-Protokolle und der sie verarbeitenden Geräte, sondern auch breites Wissen über die Unzulänglichkeiten einiger genutzter Verfahren, Einstellungen und Programmiersprachen. Ebenso ist es erforderlich, eine strukturierte, projektartige Vorgehensweise zu verwenden, um am Ende zu einer aussagefähigen Risikoeinschätzung zu gelangen.

Eine IT-Sicherheitsprüfung ist immer in mehreren Schritten unterteilt, die sich zeitlich als Auditierungstiefe oder Prägnanz skaliert. Vom oberflächlichen Abtasten aller möglichen Angriffsstellen über das Testen von üblichen Nachlässigkeiten, bis zum penetranten Prüfen bekannter Angriffsmethoden wird Schritt für Schritt jede sich bietende Möglichkeit getestet. Die manchmal umfangreichen Ergebnisse müssen danach fachlich bewertet werden und in einer übersichtlich strukturierten Dokumentation aufbereitet den Verantwortlichen zur Verfügung gestellt werden. Die Resultate einer Sicherheitsprüfung fügen sich unkompliziert in das Konformitätsmanagement (Compliance-Management) eines Unternehmens ein, indem die gefundenen Schwachpunkte eine an die Klassifizierung des Risiko-Managements anlehende Einstufung erhalten.

Sicherheitsüberprüfungen für Dienste & Netze

Wichtige Voraussetzungen für ordentliche Sicherheitsüberprüfungen sind:

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



Ein guter Auditor muß über langjährig aufgebaute Erfahrungen in der IT-Sicherheit verfügen und darf nicht zum eigenen Unternehmen gehören, um eine kritische, neutrale Betrachtungsweise zu haben. 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 Prüfungsunternehmen, um die Legalität der Prüfung zu bestätigen. Nach der Festlegung der Rahmenbedingungen des Audits über zu prüfende IP-Adressen (z.B. Internetanschluß oder Webserveradresse) und die Penetrationsprägnanz werden die Tests termingerecht durchgeführt. Das Unternehmen erhält eine sauber aufbereitete Dokumentation, die auch die Möglichkeit von Nachfragen beim Auditor oder eine Präsentation beim Kunden beinhaltet.

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. Der Situation und dem Kundenbedürfnis angepaßt, werden verschiedene Sicherheitsüberprüfungen angeboten: Von automatisierten Scans aus dem Internet über den Einsatz von ethischem Hacking bis zu Sicherheits-Audits großer LANs sind verschiedene Leistungen skalierbar.

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.

Projektablauf der CareForce One™ Assessments

Um der Forderung einer strukturierten, projektartigen Vorgehensweise bei Sicherheitsüberprüfungen gerecht zu werden hat die CareForce One™ der Bristol Group die Erfahrungen aus vielen durchgeführten Sicherheitsprüfungen in ein sauber definiertes Prüfungskonzept umgesetzt. Aus einem Katalog von über 60 Einzelprüfungen werden in Absprache mit dem Kunden die Penetrationsprüfungen, die zur individuellen Kundensituation passen, ausgewählt. Durch die Gliederung in Modulgruppen wird die Auswahl auf die zu überprüfende Einrichtung erleichtert. Es stehen folgende Modul Gruppen zur Verfügung:

- **BASIC** - ist Grundlage aller Penetrationstests
- **MAIL** - Überprüfungen am E-Mail System
- **DNS** - Domain Name Service Überprüfungen
- **HTTP** - Webservertest in den Untergruppen
 - Information Discovery
 - Application Testing
 - Filehandling
 - Logic Testing
 - Authentication Testing
 - Classic Webattacks
 - Advanced Webattacks*
 - Webservice DoS
- **DDoS** - Denial of Service (dynamic)
- **Social** - Social Engineering

Damit Kunden feststellen lassen können, welche Informationen über Ihr Unternehmen netzwerktechnisch gefunden werden können, steht optional ein vorgelagerter BlackBox-Test zur Verfügung. Dieser Test legt alle am Internet verfügbaren Daten, wie beispielsweise E-Mail-, IP-Adressen oder Domainnamen offen, die potentiellen Angreifern zusätzliche Informationen über das Angriffsziel geben könnten.

Jede der obigen Gruppen widmet sich neben den klassischen und teilweise bekannten Schwachpunkten auch neu aufgetauchten Angriffsmethoden und wird ständig erweitert. Ein vollständiger Katalog mit weiteren Erklärungen zu jedem Test kann bei der CareForce One™ eingesehen werden. Dieser Katalog dient ebenfalls als Besprechungsgrundlage bei der Vorbesprechung zur Definition des Prüfungsumfangs.

Projektablauf

Der Projektablauf einer CareForce One™ Sicherheitsüberprüfung ist grob in drei Phasen gegliedert:

- **Vorbereitungsphase mit ersten Tests und Vorbesprechung**
- **Haupt-Prüfungsphase zum vereinbarten Termin**
- **Auswertungsphase mit Berichterstellung**

Bei Kunden, die eine Sicherheitsüberprüfung durch die CareForce One™ durchführen lassen, wird bereits in der Vorbereitungsphase mit den ersten Tests des BASIC-Moduls kostenlos begonnen, um für die Vorbesprechung die nötigen Informationen bereit zu haben. Beim Vorgespräch tauschen sich die Teilnehmer über Penetrationsziel und Penetrationstiefe aus und legen die zu verwendeten Testgruppen sowie den Prüftermin fest. Anschließend erhält der Kunde eine Projektbeschreibung mit diesen Rahmenbedingungen und einem integrierten Warenwirtschaftsangebot.

Hier lassen sich mögliche Feinkorrekturen vornehmen. Nach Beauftragung der CareForce One™ beginnen die Test des BASIC-Moduls und liefern die Informationen über ansprechbare Services oder die Oberfläche des Webserver. Es werden die geplanten Prüfungen entsprechend Ihrer Ausprägung über den Prüfzeitraum durchgeführt.

Je nach individueller Sachlage und Prüfziel erfolgen diese Tests vor Ort oder remote über das Internet.

Wird während der Durchführung der Penetrationstests eine schwerwiegende, kritische Schwachstelle entdeckt, wird direkt, noch während der Prüfungsphase, der Kunde über diesen bedrohlichen Zustand alarmiert.

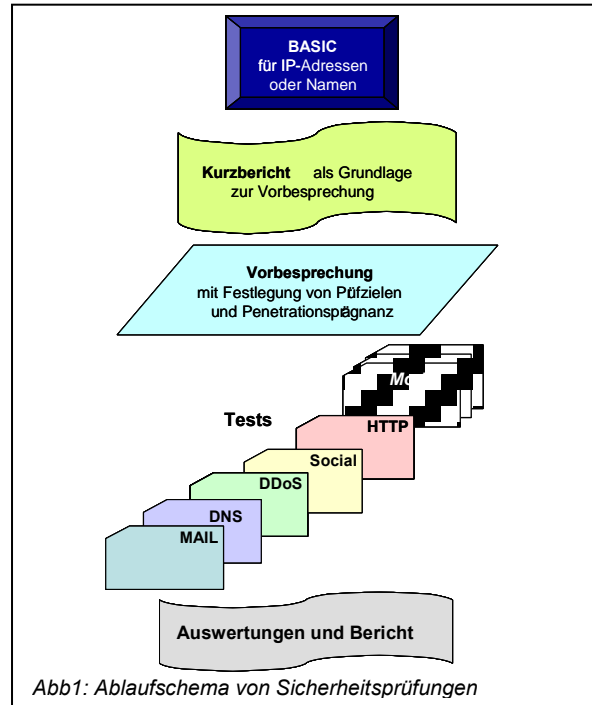


Abb1: Ablaufschema von Sicherheitsprüfungen

Nach Abschluß aller Prüfungen werden die Ergebnisse im Büro der Bristol Group ausgewertet und der Bericht erstellt. Über jede gefundene Schwachstelle wird eine Risikobewertung in Anlehnung an die vom BSI (Bundesamt für die Sicherheit in der IT) benutzten Stufen vorgenommen. Berichte werden in Form von PDF-Dateien, Excel-Dateien sowie optionalen PowerPoint Präsentationen dem Kunden geliefert.

Klare Leistungen - klare Kosten

Da eine Sicherheitsüberprüfung mit klaren Projektparametern zusammen mit dem Kunden abgestimmt wird, ist auch die Preisermittlung, wie bei anderen Projekten der CareForce One™ klar und transparent definiert. Die Kosten des BASIC-Moduls staffeln sich entsprechend der Menge an zu prüfenden IP-Adressen, andere Module kalkulieren sich nach Zeitaufwand. Es kommen unterschiedliche Sätze für die Tests, die Auswerte- und Berichtsarbeitszeiten zur Anwendung. Reisekosten werden gemäß der aktuell gültigen Bristol Zonenpauschale ausgewiesen.

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.