IT-ON.NET
IT-Online-Services Partnernetzwerk

AUDIT-ON.NET
Präsentation und Live Hacking

Einführung

Einführung

IT-ON.NET
IT-Online-Services Partnernetzwerk

- Was ist AUDIT-ON.NET
  - Modular aufgebautes Paket zum Gesamtschutz ihrer IT Landschaft
    - Warum Modular?
      - Nicht jedes Unternehmen ist gleich
      - Anforderungen sind unterschiedlich implementiert

Einführung

IT-ON.NET
IT-Online-Services Partnernetzwerk

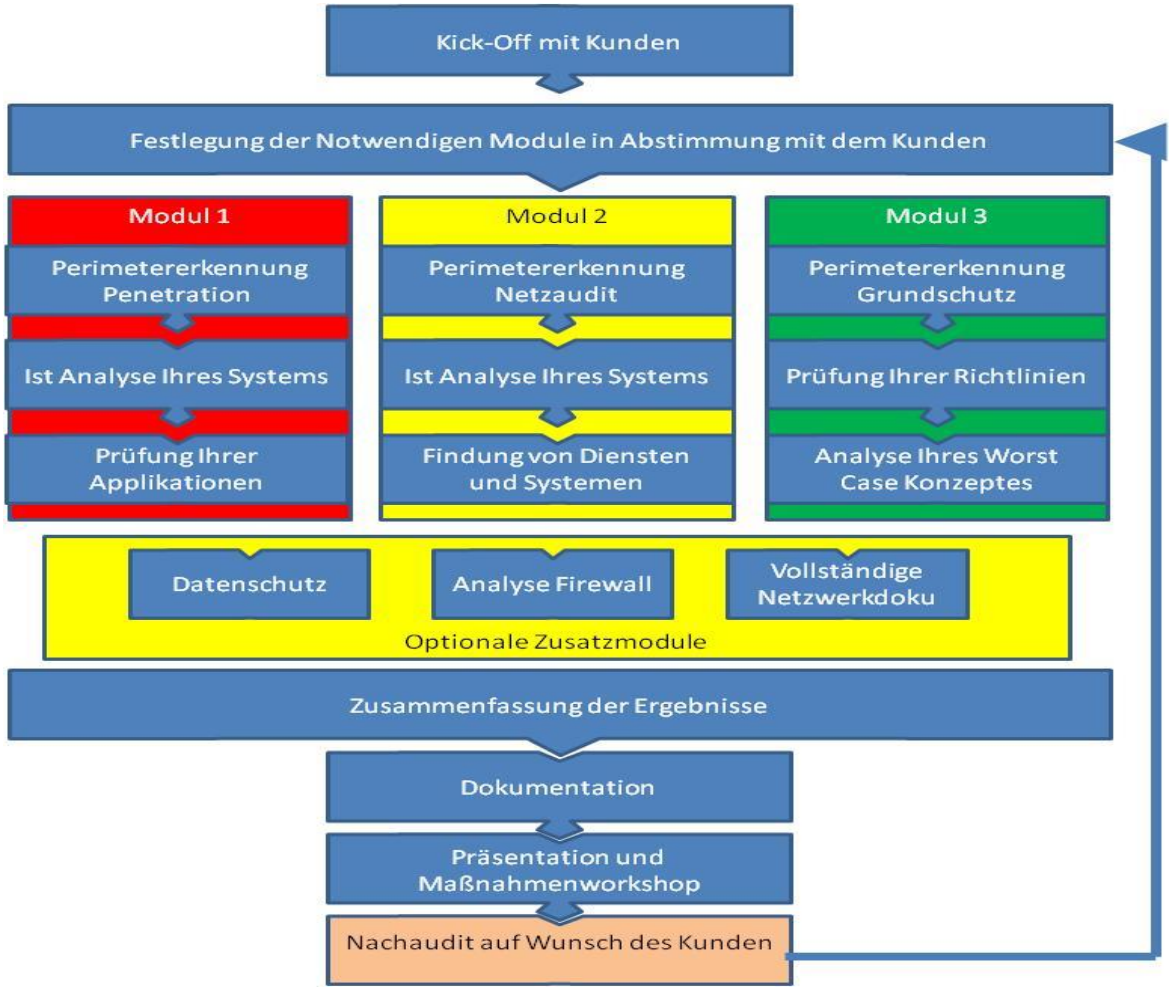
- Warum AUDIT-ON.NET
  - Praxis zeigt erheblichen Bedarf
  - Sicherheitsrelevante Vorfälle nehmen wieder zu
  - Mehr Schutz für unsere Kunden

  - http://www.computerwoche.de/security/2365238/
  - http://www.gulli.com/news/studie-cyber-angriffe-auf-kritische-infrastrukturen-nehmen-zu-2011-04-19

Einführung

IT-ON.NET
IT-Online-Services Partnernetzwerk

- Inhalt von AUDIT-ON.NET
  - 3 Hauptmodule
    - Grundschutz IT
    - Netzwerkaudit
    - Penetrationstest
  - 3 Optionale Module
    - Datenschutz
    - Firewall Analyse
    - Vollständige Netzwerkdokumentation


Kick-Off mit Kunden
Festlegung der Notwendigen Module in Abstimmung mit dem Kunden
Modul 1
Perimetererkennung Penetration
Ist Analyse Ihres Systems
Prüfung Ihrer Applikationen
Modul 2
Perimetererkennung Netzaudit
Ist Analyse Ihres Systems
Findung von Diensten und Systemen
Modul 3
Perimetererkennung Grundschutz
Prüfung Ihrer Richtlinien
Analyse Ihres Worst Case Konzeptes
Datenschutz
Analyse Firewall
Vollständige Netzwerkdoku
Optionale Zusatzmodule
Zusammenfassung der Ergebnisse
Dokumentation
Präsentation und Maßnahmenworkshop
Nachaudit auf Wunsch des Kunden

Einführung

IT-ON.NET
IT-Online-Services Partnernetzwerk

- Erfahrungen mit AUDIT-ON.NET
  - Live Vorstellung einiger Erfahrungen, die mit AUDIT-ON.NET gemacht werden konnten.
  - Schwachstellen, die immer wieder gefunden werden.
  - Automatisierter Scan oder doch besser von Hand?
  - Ist der Bundestrojaner wirklich neu?
  - Daten Lauschangriff – wirklich neu?

Der erste Angriff mit arpspoof

arpspoof

IT-ON.NET
IT-Online-Services Partnernetzwerk

- Vorbereiten des Systems als Router.
- Starten eines Scans auf das Netzwerk nmap –F –O –sV Ziel
- Auswählen des Opfers.
- Starten von arpspoof über die Console.

Aufzeichnung der Daten

Aufzeichnung der Daten

IT-ON.NET
IT-Online-Services Partnernetzwerk

- Um die Daten aufzuzeichnen wird das Programm Wireshark gestartet der Datenverkehr mitgeschnitten.
- Dies kann man live mitverfolgen.
- Es können durch Filter schon erste Ergebnisse sichtbar gemacht werden.

Aufzeichnung der Daten

IT-ON.NET
IT-Online-Services Partnernetzwerk

Vielleicht ist es Ihnen egal, das jemand weiß welche Seiten Sie im Internet besuchen, aber wenn jemand das Kennwort zu Ihrem privaten Mail Account bekommt, das ist dann bestimmt nicht in Ihrem Interesse.

Er könnte ja jetzt lustige Mails in Ihrem Namen schreiben.

PPTP Verbindung

PPTP Verbindung

IT-ON.NET
IT-Online-Services Partnernetzwerk

Da Sie sich ja sicher fühlen, bauen Sie schnell noch eine VPN Verbindung über PPTP in das Firmennetz auf. Über eine VPN Verbindung kann ja nichts passieren.

Nur leider handelt es sich bei PPTP nicht um eine wirklich sichere VPN Verbindung. Sie ist lediglich einfach zu konfigurieren und gehört zum Windows Betriebssystem dazu.

Schön dass PPTP auch von Ihrem iPad und Ihrem iPhone unterstützt werden, mit dem Sie ja auch im Hotel WLAN unterwegs sind.

PPTP Verbindung

IT-ON.NET
IT-Online-Services Partnernetzwerk

- Der Hacker schneidet nun den Netzwerkverkehr über PPTP mit und mit etwas Glück hat er in ein paar Minuten Ihr Passwort und kann sich dann in Ihrem Namen in der Firma anmelden.

- Eine nette Mail an Ihre Sekretärin, in der Sie Ihr erklären, dass sie nun wirklich zu viel zugenommen hat, und schon beginnt der Spaß, leider nicht für Sie.

PPTP Verbindung

IT-ON.NET
IT-Online-Services Partnernetzwerk

Ach ja, wenn er kein Glück hat, kann er sich das für 200$ kaufen, so kann er jedes PPTP Kennwort knacken.

•Wireshark Filter auf das CHAP Protokoll einstellen.

•Warten bis die Anmeldung erfolgt.

•Cracken des Passworts mittels asleap.

- Hier dient ein Wörterbuch als Hilfe.

- Ach ja, wenn man kein Glück hat, kann man sich das für 200$ kaufen, so kann man jedes PPTP Kennwort knacken.

Social Engineering

Social Engineering

IT-ON.NET
IT-Online-Services Partnernetzwerk

- Was ist Social Engineering und wie geht der Hacker vor?
  - Bundesamt für Sicherheit in der Informationstechnik: [BSI] Social Engineering ist eine Methode, um unberechtigten Zugang zu Informationen oder IT-Systemen durch Aushorchen zu erlangen. Beim Social Engineering werden menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt. Dadurch können Mitarbeiter so manipuliert werden, dass sie unzulässig handeln.
    - Albert Einstein sagte einmal: Zwei Dinge sind unendlich: das Universum und die menschliche Dummheit. Aber beim Universum bin ich mir nicht ganz sicher

Social Engineering

IT-ON.NET
IT-Online-Services Partnernetzwerk

- Methoden
  - Phishing, Direktangriff mit falscher Identität,
  - Angriff auf Firmenneulinge,
  - Hilfe anbieten,
  - um Hilfe bitten,
  - der Einsatz von Sympathie, Schuld und Einschüchterung,
  - Dumpster Diving,
  - Shoulder Surfing

Social Engineering

IT-ON.NET
IT-Online-Services Partnernetzwerk

- Wie komme ich an Passworddaten oder Wörterbücher
  - Diese gibt es zu tausenden im Internet
- Beispiel: Infos aus Xing
  - IT Leiter ist begeisterter Motorradfahrer und BMW Fan
  - Passendes Wörterbuch suchen und Hackangriff starten
  - Facebook
- Einschüchterung per Telefon – Einfach mal fragen
- Der nette Vertreter
- Hilfsbereitet Techniker

Immer verbunden

Verbindung mit User PC

IT-ON.NET
IT-Online-Services Partnernetzwerk

- Immer mit der Firma verbunden – Hintertür mit Folgen
  - Starten von SET
    - Erstellung eines Exploits
    - Einspielen des Exploits in das Unternehmen
  - Starten von msf3
    - Einrichtung und warten auf Verbindung
    - Remote Shell starten
    - Was kann ich nun alles machen – ALLES!

USB Stick Angriff

IT-ON.NET
IT-Online-Services Partnernetzwerk

- Bundestrojaner – Einspielen z.B. beim Zoll
- Einfach mal liegenlassen und schon ist alles vorbei
  - USB Stick mittels SET vorbereiten
  - USB Stick interessant für die Mitarbeiter machen
    - Lohnkosten Berechnung
    - Gehaltsentwicklung
    - FKK Urlaub mit Ilse

Passwörter

Passwörter mal anders

IT-ON.NET
IT-Online-Services Partnernetzwerk

- Was sind sichere Passwörter
  - Mindestlänge,
  - Zahlen, Buschstaben und **Sonderzeichen**
- Bedeutung sicherer Passwörter -> siehe Webmin Hack
- Wie kann ich Kennwörter sicher machen und trotzdem behalten
  - Schlecht: PorscheGT oder MeineFirma oder Name der Frau
  - Gut: Ich liebe meine Kinder und Enkelkinder und bin dankbar, dass es ihnen gut geht! Und daraus abgeleitet **IlmKuEubd,deigg!**
  - Besser: **I1mKu3ubd,d3i66!**
    Verfremdung von Buchstaben

Schaden anrichten

Suche nach Daten

IT-ON.NET
IT-Online-Services Partnernetzwerk

- Was liegt so alles auf einem Server?
  - Beispiel Reisekostenformular
  - Webseite
  - Kundendaten
  - Buchhaltung
  - Personaldaten
  - .....

AUDIT-ON.NET

Vielen Dank für Ihre Aufmerksamkeit

IT-ON.NET
IT-Online-Services Partnernetzwerk

Ihr Ansprechpartner für Fragen und Anregungen ist:

Herr

Dirk Struwe

E-Mail : dirk.struwe@it-on.net

Telefon: 0211 95691-16