CyTRAP Labs

Roentgenstrasse 49 Street
CH-8005 Zuerich Zip Code
Switzerland Country

+41(0)44 272 1876 Voice
+41(0)76 200 7778 Cell

www.CyTRAP.eu URL
info@CyTRAP.eu E-Mail

Kurzuebersicht

Titel	CyTRAP Labs– ueber Sinn und Unsinn von Penetration-Tests
Zusammenfassung	Theoretisch gibt ein Penetration-Test ein gewisse Sicherheit, dass ein arglister Anwender keine Moeglichkeit hat unerlaubt in ein Netzwerk einzudringen. Hier diskutieren wir warum solche Tests unter Umstaenden nicht ein wirklichkeitstreues Bild des Ist-Zustandes geben. Wir presentieren uns die 'ComAnalytica Process Method' welche es einem erlaubt ein vollstaendigeres und wirklichkeitsgetreues Bild ueber Nutzerverhalten und Kommunikationsstroeme zu erhalten. Diese Methode erlaubt es den Testern nicht autorisierte Prozesse und Anwendungen wie Kazaa oder Skype software zu entdecken. Basierend auf solchen Informationen koennen diese Applikationen gestoppt werden. Die ComAnalytica Process Method ist somit ein wichtiges Instrument im internen Kontrollsystem des Unterhehmens. Es ein w strategisches is an important part of the firm's internal control system. It provides vital information needed for achieving better governance regarding the organization's information assets and assuring legal compliance.
CyTRAP ID	PenTesting-MakingSense-2007-05-18
Runterladen der neuesten Version	Checking for the latest version of this document now

CyTRAP Labs

Inhaltsverzeichnis

CyTRAP Labs

Ueber den Sinn und Unsinn von Penetrations-Tests

Als Risiko Spezialisten ist es unsere Aufgabe, quasi aus der Adlerperspektive, Informationssicherheit, Datenschutz und die Einhaltung von Standards wie auch Gesetzen zu bewerten und natuerlich zu verbessern. Auffaellig ist dabei, das fast jedes Unternehmen intensive Penetration Tests durchfuehen laesst. Die damit erhaltenen Resultate werden meistens in einem mehr oder weniger umfassenden Dokument aufgenomment. Leider sind diese Resultate jedoch nicht immer sehr aussagekraeftig. Ebenfalls sind die Kosten fuer solche Tests oftmals relativ hoch. Diese Probleme werden wir hier kurz skizzieren und effektive und oekonomisch interessante Loesungansaetze aufzeigen. Diese macht solche Tests auch interessant fuer interne Kontrollsysteme und Risikomanagement.

Warum der Penetration Test nicht alle Gefahren aufzeigen kann

Leider werden Penetration Tests oftmals als die einzige Moeglichkeit gesehen, um Schwachstellen und unakzeptable Risiken in Sachen Informationsmanagement aufzuspueren. Doch die Realitaet sieht anders aus:

- Egal wie lange Penetration Tests dauern und wie viele IP-Adressen sie umfassen, Penetration Tests sind immer eine Stichprobe. Das heisst, es koennen niemals alle IP-Adressen erfasst werden da ja niemals alle Geraete zur gleichen Zeit eingeschalted oder am Netzwerk sind. Leider ist es jedoch so, dass schon ein einziges kompromittiertes Geraet reicht, um das gesamte Sicherheitsdispositiv in Frage zu stellen.

- Malware wie z.B. Zombies werden von Penetration Tests nicht erfasst, da sie keinen Service hinter einem Port bereitstellen der vom Test erfasst wird. Sie arbeiten aktiv/aktiv, d.h. sie holen von ihrem Master z.B. von Port 80 Instruktionen ab und fuehren diese aus. Dies koennte zum Beispiel Instruktion sein Spam ueber Port 25 zu verschicken.
  Noch schlimmer wird es wenn es sich um Spionage Programme handelt, die Informationen passiv sammeln und dann per Port 80 an den Master uebertragen.

- Penetration Tests sind ein rein technischer Test. Dies bedeutet, dass das Verhalten der Mitarbeiter am Netzwerk meistens nicht in die Analyse mit einbezogen wird. Dabei sind es jedoch die Mitarbeiter welche mit den einfachsten Mitteln das Sicherheitssystem ueberrumpeln koennen.

- Die Logik eines wirklichen Angriffs bleibt beim Penetration Test ungetestet.
  Welchen Weg wuerde ein potentieller Angreifer nehmen um ins System zu gelangen?
  Vom Weg durch die Eingangstuere an der physikalischen Sicherheit vorbei, bis zum Erfolg. Ein solcher Test laesst sich gut als logischer Penetration Test beschreiben.

CyTRAP Labs

Am wichtigsten ist jedoch, dass ein sogenannter logischer Penetration Test mit sehr grosser Wahrscheinlichkeit zum Erfolg fuehrt, d.h. die Schwachstellen im Sicherheitsdispositiv schonungslos offenlegt.

Aus dieser Erfahrung muss man sich zu Recht fragen, warum Penetration Tests oft Wochen und Monate dauern. Da sie ja nur eine Stichprobe sind, muss es doch moeglich sein die gesammelten Daten schnell zu erfassen.
Schlimmer ist jedoch, dass diese Tests oftmals nicht ein umfassesendes Situationsbild generieren oder sogar ein unvollstaendiges Bild der Gefahrenpotentiale aufzeigen.

Unsere Erfahrung zeigt, dass sich in der Praxis stark gekuerzte Penetration Testphasen sehr bewaehren. Um deren Aussagekraft zu erhoehen muss jedoch noch ein sogenannter Vulnerability Scan und logische Penetration Tests mit einbezogen werden. Ebenfalls ist es notewendig, dass das Kommunikationsverhalten von Mitarbeitern und Software analysiert wird.

Je nach Unternehmensgroesse reichten manchmal schon 3 Tage vor Ort plus entsprechender Nachbearbeitung aus um zielgenaue Aussagen treffen zu koennen, wie es um die Sicherheit bestellt ist. Diese Aussagen wurden dann in einem Security Recommendation Overview Dokument praesentiert.

Was bei einem Penetration-Test passiert, soll hier nicht weiter erlaeutert werden, allerdings wird in den folgenen Abschnitten noch etwas genauer auf die logischen Penetration Test sowie das Kommunikationverhalten und dessen systematischer Analyse eingegangen.

Logischer Penetration Test

Bei einem logischen Penetration Test nimmt der Tester die Funktion eines internen Angreifers ein und versucht mit den ihm im Netzwerk verfuegbaren Mitteln und Rechten die Sicherheit zu kompromittieren. Dabei gibt es verschiedene Spielarten je nach Wunsch des Auftraggebers, wie z.B. der Angreifer bringt Hardware oder Software mit (simuliert also einen Externen) oder er bringt nichts mit und benutzt das Equipment des zu testenden Unternehmens, ausgestattet mit dem Equipment und den Rechten die ein normaler Mitarbeiter auch hat.

Dieser logische Penetration Test fuehrt meist zu erstaunlichen Ergebnissen, da die IT-Security in Unternehmen meist an komplexe Angriffsszenarien denken, aber nicht die pfiffigkeit mancher Mitarbeiter, mit einfachsten Mitteln ihr Ziel zu erreichen. Zum Beispiel muessen wir des oefteren feststellen, das Industriespionage oder Betrugsaffaeren sich dadurch kennzeichnenn, dass Daten modifiziert werden oder aber mit einfachen Mitteln aus dem Unternehmen herausgeschleust werden.

CyTRAP Labs

ComProcess Analytica Methode

Auf einem mehr technischen Niveau als der logische Penetration Test laeuft die ComProcess Analytica Methode (Protocol-Tracking-Analysis) Test ab. Hier wird aufgezeichnet, was im Netzwerk in Wirklichkeit kommuniziert um Unerwuenschtes Kommunikationsverhalten von Software zu entdecken und zu eliminieren.

Diese Analyse zeigt dem Management wo die neuralgischen Punkte zu finden sind und ermoeglicht die effektive Verbesserung der intenen Kontrollen und des Risikomanagements.

Zum Beispiel ist es oft der Fall, dass die Fuehrungskraefte ueberrascht feststellen muessen, dass eine Vielzahl von den Protokollen die im System genutzt werden weder die geplanten noch autorisierten Protokolle sind. Dies bedeutet das oftmals Anzahl von Protokollen diejenige welche eigentlich nur laufen duerfen bei weitem uebersteigt. Dies deutet natuerlich auch darauf hin, dass bessere Kontroll- und Auditmechanismen eingebaut werden muessen um dieses Risiko besser in den Griff zu bekommen. Nur dann wird es das Unternehmen schaffen, den gesetzlichen Vorschriften auch genuege zu tun.

Mit Hilfe der Protocol-Tracking-Analysis kann man die Nutzung von Kazaa aehnlichen Services, wie auch die Nutzung von Skype, illegalen Servern und Zombies im Netzwerk entdecken. In unserer Arbeit werden mit diesen Werkzeugen dann solche nicht-authorisierten Aktivitaeten entdeckt. In einigen Faellen stellte dies fuer das Unternehmen nur eine Gefahr wegen Verletzung des Urheberrechtes dar, in anderen wurde jedoch Wirschaftspionage getrieben und, noch schlimmer, auch gewerbliche Schutz- und Urheberrechte der Firma verletzt. In einigen Faellen handelte es sich sogar um illegale Inhalte auf dem Firmennetzwerke wie Kinderpornographie.

Die Protocol-Tracking-Analysis ist aus technischer Sicht einfach umzusetzten. Dazu braucht man einmal den Datenstrom wie zum Beispiel zwischen der Internet Firewall und dem internen Netzwerk anzuzapfen. Dann werden diese Daten aufgezeichnet. Allerdings bedingt die Auswertung exzellente IT Kenntnisse sowie die Faehigkeit die vielen Daten systematisch analysieren zu koennen. Ebenfalls braucht es Erfahrung mit CyberCrime. Hier muss die Expertin auch die Faehigkeit besitzen, sich in die Lage des Attackers zu versetzen, damit die Informationen korrekt ausgewertet werden koennen (z.B. was bedeutet dieser Datenfluss und was moechte der Angreifer damit erreichen).

ComProcess Analytica Methode und Risiko Management

Das oben beschriebene Vorgehen, speziell der ComProcess Analytica Methode erlaubt es dem Unternehmen die neuralgischen Punkte im Netzwerk zu identifizieren. Nicht authorisierte Prozesse am Netzwerk sind nicht nur ein Kostenproblem (z.B. Bandbreite), sie stellen jedoch auch eine grosse Gefahr fuer die Datenintegritaet und Sicherheit dar. Zum Beispiel verlangen fast alle Laender das

CyTRAP Labs

Chat Protokolle (z.B. Instant Messenger) archiviert werden. Wenn diese aber nicht autorisiert wurden und kein interner/zentraler Chat Server installiert wurde, koennen diese Kommunikationstroeme auch nicht protokolliert werden. Damit ist ein Gesetzesverstoss schon vorhanden.

Die ComProcess Analytica Methode zeigt die Datenstroeme auf welche solche nicht bewilligten Aktivitaeten zueruecklassen. Damit koennen dann diese auch gestoppt werden.

Erst nach dem schrittweisen Vorgehen wie oben beschrieben kann im Gegenzug die Firma die richtigen Schritte einleiten, welche die unerwuenschte oder sogar illegale Aktivitaet am Netz schnellstens stoppt. Wichtig ist aber auch, dass diese Aenderungen am Sicherheitsdispositiv sich auch in der Zukunft ueberprueft werden und damit das Risiko fuer das einnisten von weiteren nicht authorisierten Aktivitaeten minimiert werden kann.

CyTRAP Labs

Administrative

Author	Andreas Wagner & Urs E. Gattiker, Ph.D.
Revisionen	2007-05-23
Zugang	Level 1
Kontaktaufnahmen mit Autoren	Web: http://info.CyTRAP.eu E-mail: Intell at CyTRAP.eu Tel: +41(0)76-272-1876 oder mobil +41(0)76-200-7778 or +
Copyright	The preceding was not a legal opinion, and is not our organization's. Original portions Copyright 2007 CyTRAP Labs – Andreas Wagner and Urs E. Gattiker, all rights reserved. Our work may be copied in whole or part, with **proper attribution**, as long as the copying is not for commercial gain.
Technorati tags	Apple CASEScontact.org best practices case studies cost-benefit analysis disaster recovery plans information security regulatory compliance risk management security outsourcing offshore programming India due diligence checklist Sarbanes-Oxley
War dieses Papier hilfreich?	If yes, why not bookmark it at Del.icio.us