GreSec
IT CONSULTING

Whitepaper Penetrationstest

Der Weg zur erfolgreichen Planung und Umsetzung

Ein Penetrationstest stellt die Simulation eines gezielten Angriffs auf Komponenten Ihrer IT-Infrastruktur dar. Grundlegendes Ziel ist es hierbei, IT-Schwachstellen aufzudecken und in der Folge den Zugriff von Dritten auf firmeninterne Daten rechtzeitig zu verhindern.
Die Methoden und Werkzeuge, die sich dabei zunutze gemacht werden, entsprechen grundsätzlich denen, die auch bei Hackern Anwendung finden.
Im Rahmen der Durchführung wird, je nach Kundenwunsch, zwischen verschiedenen Formen des Penetrationstests sowie Intensitätsgrads der IT-Sicherheitsüberprüfung gewählt.
Zwingend notwendig ist ein vorab geführtes Briefing-Gespräch zwischen auftraggebendem Unternehmen und GreSec, in dem der Testgegenstand spezifiziert sowie die Rahmenbedingungen festgelegt werden.
Nur so stellen Sie sicher, dass Ihre eigenen Erwartungen mit den generierten Ergebnissen übereinstimmen oder gar übertroffen werden.

Nachfolgend habe ich Ihnen zusammengefasst, worauf es bei der Planung und Durchführung eines Penetrationstests im Wesentlichen ankommt. Die aufgeführten Details zur Vorgehensweise resultieren aus Erfahrungswerten, die bis heute mit den unterschiedlichsten Kundengruppen generiert wurden.

1. ZIELDEFINITION

Als erster Schritt sollte die Definition des Prüfungsgegenstandes erfolgen:
Auf welche Fragen möchte welche Zielgruppe in Ihrem Unternehmen eine Antwort erhalten? Welches System soll auf Sicherheitslücken überprüft werden ? Beispielsweise die unternehmenseigene Website, Dateiserver (wie regelmäßig werden diese gewartet?), das WLAN oder gar das gesamte Unternehmensnetzwerk? Oder aber möchten Sie wissen, ob bestimmte Compliance-Vorgaben eingehalten werden? Funktioniert Ihr Patch-Management?
Die Zielvorgaben können in die unterschiedlichsten Richtungen gehen und müssen aus diesem Grund exakt geplant und formuliert werden.

2. ZEITLICHE PROJEKTPLANUNG

Die Kalkulation des Timings darf nicht nur auf der eigentlichen zeitlichen Durchführung des Penetrationstests basieren. Vielmehr muss auch genügend Vorlauf für die Bearbeitung notwendiger Vertragsunterlagen sowie Vereinbarungen eingeplant werden. Hierzu gehören beispielsweise Datenschutzerklärungen, Haftungs- und Vertragsvereinbarungen, die geprüft und unterzeichnet werden müssen. Hier sind in der Regel die Rechtsabteilung sowie die Geschäftsleitung beteiligt. Als Richtwert empfehlen wir, ein Zeitfenster von 4 Wochen bis zum Beginn des Audits für diesen Prozess einzuplanen.

3. ENGE ZUSAMMENARBEIT ZWISCHEN KUNDEN UND PENETRATIONSTESTER

Mit der Planung des Penetrationstests müssen feste Ansprechpartner auf beiden Seiten benannt und deren Erreichbarkeit während der Testphasen sichergestellt werden. Nur so ist z.B. im Falle der Identifizierung kritischer Schwachstellen gewährleistet, dass Informationen mit schnellstmöglichen Reaktionszeiten ausgetauscht werden.

4. WAHL DES TESTSZENARIOS

Im Rahmen der Durchführung eines Penetrationstests werden – je nach Grad an Informationen, die dem verantwortlichen IT-Sicherheitsspezialisten zur Verfügung stehen – zwischen White Box-, Black Box- und Grey Box-Ansatz unterschieden. Darüber hinaus wird der Faktor Mensch beim Testverfahren „Social Engineering“ in den Mittelpunkt gestellt.

WHITE BOX TEST:

Alle notwendigen Informationen über IT-Systeme und interne Strukturen des zu überprüfenden Unternehmens werden dem IT-Sicherheitsspezialisten bereits vorab zur Verfügung gestellt.

BLACK BOX TEST:

Hier liegen dem durchführendem Testteam kaum Vorabinformationen über die zu prüfenden IT-Systeme vor. Analog zum Vorgehen eines externen Angreifers sollen Möglichkeiten und Wege für einen realen Angriff identifiziert werden – die Testziele werden weitgehend selbstständig vom Prüfer ausgespäht. Damit ist diese Art des Penetrationstests sehr realitätsnah, aber auch sehr viel zeitaufwändiger und damit kostspieliger als der White Box Test.

GREY BOX TEST:

Diese Art des Penetrationstests kombiniert beide oben genannten Verfahren und wird von unseren IT-Sicherheitsexperten oft empfohlen, da diese Variante aus ökonomischer Sicht eine sehr effiziente Vorgehensweise darstellt. Ein Teil der notwendigen Informationen, die besonders zeitintensiv zu generieren sind, werden vorab zur Verfügung gestellt, Detailinformationen von zu prüfenden Systemen müssen jedoch selbstständig herausgefunden werden.

SOCIAL ENGINEERING:

Eines der größten Risiken für die Stabilität der Sicherheit Ihrer IT-Umgebung ist noch immer der Faktor Mensch. IT-Sicherheitsspezialisten legen daher nahe, das „Social Engineering“ Audit als eine wesentliche Komponente zu berücksichtigen. Es umfasst die Überprüfung Ihres Unternehmens auf physische und „menschliche“ Schwachstellen und berücksichtigt zum Beispiel die Räumlichkeiten des Gebäudes, die Hotline Ihres PC-Helpdesks oder den Mitarbeiter, der „zufällig“ einen USB-Stick auf Ihrem Firmenparkplatz findet.

Wenn Sie ein Bewusstsein bezüglich der Gefahren schaffen, die von Sicherheitslücken ausgehen, erreichen Sie ein verantwortungsbewussteres Handeln der Mitarbeiter im Interesse Ihres Unternehmens.

5. DEFINITION DER HANDLUNGSGRENZEN

An dieser Stelle wird die Testtiefe des Penetrationstests festgelegt. Darf eine aufgedeckte Schwachstelle ausgenutzt oder soll sie nur theoretisch bewertet werden? Die Definition der Handlungsgrenzen ist abhängig von Punkt 1. Zieldefinition sowie dem vereinbarten zeitlichen Rahmen. An dieser Stelle sei angemerkt, dass sich bestimmte Sicherheitslücken nur dann sicher nachweisen lassen, wenn sie auch aktiv ausgenutzt werden. Geben Sie daher konkrete Zeitrahmen für die aktiven Tests vor, um sicherzustellen, dass die Fachabteilungen bzw. Ressourcen effizient besetzt sind und so bei einem Systemausfall umgehend reagieren können.

6. MELDUNG KRITISCHER SCHWACHSTELLEN

Informationen, die über kritische Schwachstellen im Rahmen des Pen-Tests aufgedeckt wurden, müssen sofort an den unter Punkt 3. definierten Ansprechpartner weitergegeben werden. Nur so wird gewährleistet, dass identifizierte Sicherheitslücken ohne Verzögerungen geschlossen werden.

7. INVOLVIEREN UNTERNEHMENSZUGEHÖRIGER DIENSTLEISTER

Beziehen Sie auch Ihre Dienstleister in die Durchführung des Penetrationstests mit ein und lassen Sie deren IT-Infrastruktur ebenfalls überprüfen. So können Sie nachvollziehen, ob bestimmte Sicherheitsdienstleistungen, für die Sie bezahlen, auch richtig umgesetzt und wirksam sind. Bedenken Sie hierbei, dass es für die Systeme oder Komponenten, die von einem Dritten gehostet bzw. betrieben werden, auch dessen Genehmigung bedarf.

8. ERGEBNISPRÄSENTATION VOR ORT

Im Anschluss an die Durchführung des Penetrationstests wird eine ausführliche Dokumentation der Ergebnisse erstellt. Diese beinhaltet eine detaillierte Übersicht der identifizierten Sicherheitsmängel sowie Handlungsempfehlungen zu deren Beseitigung. Das vorhandene Sicherheitsniveau wird übergreifend bewertet. GreSec empfiehlt eine Ergebnispräsentation vor Ort, die sowohl die Administratoren als auch das Management mit einbezieht.
So findet ein Know-How Transfer zwischen beiden Zielgruppen statt.

9. BESEITIGTE SCHWACHSTELLEN

Bereits gemeldete und beseitigte Schwachstellen sollten im Audit-Bericht entsprechend deklariert sein. Nur so kann das Management die Dringlichkeit der betreffenden Maßnahmen einschätzen. Des Weiteren wird die Arbeit der IT-Verantwortlichen positiv hervorgehoben.

10. REGELMÄSSIGES RE-AUDIT

Generell ist zu beachten, dass sich die Ist-Situation hinsichtlich bestehender und neuer Schwachstellen ständig ändert. Regelmäßige Re-Audits, z.B. alle 6 Monate, stellen sicher, dass regelmäßig auf den jeweiligen Ist-Zustand reagiert wird. Hier zeigt sich, ob die beschlossenen Maßnahmen erfolgreich durchgeführt wurden oder ob Nachbesserungen erforderlich sind.

Verantwortlich für den Inhalt:

GreSec IT Consulting

Michael Greco

Unnaer Landstrasse 75

58708 Menden

Telefon: 02373 9707512

E-Mail: info@gresec.com

Internet: www.gresec.com