consectra
mIT-Sicherheit ein guter Partner

PENETRATIONSTEST

Whitepaper zur Durchführung von Penetrationstests durch die consectra GmbH

Autoren: Anselm Rohrer
Dirk Haag

consectra GmbH
Im Unteren Angel 13
77652 Offenburg
http://www.consectra.de

Inhalt

Der Penetrationstest

Was ist ein Penetrationstest?

Ein Penetrationstest ist die Simulation eines realen Hackerangriffs auf IT-Infrastrukturen oder Teile davon. Er ist eine der effektivsten Maßnahmen zur Ermittlung und Optimierung des aktuellen Niveaus der IT-Sicherheit.

Welchen Mehrwert bringt ein Penetrationstest?

Ein Penetrationstest soll Sicherheitslücken finden, bevor es einem Hacker gelingt, diese auszunutzen. Die eingesetzten Werkzeuge sind hierbei einem realen Angriff nicht unähnlich. Allerdings wird die Vorgehensweise abgestimmt und Prüfungen behutsam durchgeführt, um Schäden möglichst zu vermeiden.

Vorgehensweise

Um das bestmögliche Ergebnis zu erzielen, bedarf es einer engen Absprache zwischen dem technischen und organisatorischen Ansprechpartner Ihrerseits und unseren verantwortlichen Mitarbeitern. Um die Rahmenbedingungen festzulegen, müssen folgende Punkte geklärt werden:

Scope – Festlegung des Prüfungsgegenstandes

Welches System soll auf Sicherheitslücken geprüft werden? Die Website, Produktionssysteme, Dateiserver, ein WLAN oder gar das ganze Unternehmensnetzwerk? Je nach Größe Ihres Unternehmens kann es sinnvoll sein, sich gezielt auf bestimmte Systeme zu konzentrieren. Aus der Anzahl der zu prüfenden Systeme und Systemkomponenten ergibt sich die Testbreite, welche die Grundlage zur Bestimmung der Testdauer bildet.
Es kann vorkommen, dass durch neue Erkenntnisse während eines laufenden Testverfahrens eine Anpassung des Scopes sinnvoll wird. Derartige Änderungen können auf Wunsch jederzeit berücksichtigt werden.

Die Testtiefe

Die Testtiefe ist abhängig vom Prüfungsgegenstand und dem vereinbarten zeitlichen Rahmen. Sollen wenige Systeme in einem langen Zeitraum getestet werden, so ist es unseren Testern möglich, nicht nur auf erhebliche Sicherheitsmängel hin zu testen, sondern auch geringfügigere Gefahrenquellen zu ermitteln. Auch falsche Konfigurationen, die die Performance beeinträchtigen, können so erkannt werden. Sollen dagegen viele Systeme in einem geringen Zeitraum getestet werden, legen unsere Tester den Fokus auf kritische Sicherheitsmängel.

Es ist unerlässlich, gemeinsam festzulegen, wie weit unsere Tester bei der Durchführung gehen sollen. Oberflächentests können offene Schnittstellen, wie z. B. nach außen offene Ports ermitteln und potentielle Gefahren dokumentieren. Je nach Anforderung kann durch weiterführende Angriffe eine größere Testtiefe erreicht werden. Viele Lücken lassen sich erst dadurch sicher nachweisen, dass sie auch tatsächlich ausgenutzt werden. Dabei kann es jedoch zu Beeinträchtigungen, Ausfällen oder im schlimmsten Fall auch zu Schäden kommen. Daher sind klare Absprachen und entsprechende Vorkehrungen unerlässlich.

Vorabinformationen für den Tester (Black-, White-, Greybox)

Auf Basis der Informationslage der Personen, welche die eigentlichen Tests durchführen, werden drei Szenarien unterschieden.

Blackbox-Test

Bei einem Blackbox-Test stehen unseren Mitarbeitern nur wenig Vorabinformationen über den zu testenden Prüfungsgegenstand zur Verfügung. Die Testziele werden weitgehend selbstständig identifiziert. Diese Art des Penetrationstests ist sehr realitätsnah, allerdings auch sehr zeitaufwändig, da sich die Tester alle notwendigen Informationen zur Durchführung des Tests selbst beschaffen müssen.

Nachdem das Testteam Ziele ermittelt und definiert hat, bedarf es der Freigabe und Erlaubnis des tatsächlichen Anbieters oder Betreiber eines Dienstes, um mit dem Test zu beginnen (siehe Kapitel 2.4.2). Auf diese Weise werden Angriffe auf fremde Systeme oder auf solche, die nicht mit einbezogen werden sollen, verhindert.

Nachdem in Zusammenarbeit mit Ihnen die Ergebnisse der Informationsbeschaffung besprochen wurden und die notwendigen Genehmigungen vorliegen, kann der eigentliche Penetrationstest beginnen.

Whitebox-Test

Bei dieser Art von Test werden alle notwendigen Informationen bereits im Vorfeld zur Verfügung gestellt. Ein Whitebox-Test ist somit das Gegenstück zu einem Blackbox-Test.

Greybox-Test

Der Greybox-Test stellt eine Mischform aus den beiden vorher genannten Verfahren dar. Ein Teil der Informationsgewinnung, welche im Rahmen eines Blackbox-Tests durchgeführt werden muss, ist sehr zeitaufwändig. Dies kann dazu führen, dass einem geringen Informationsmehrwert immense Kosten gegenüber stehen. Bei einem Greybox-Test werden derartige Informationen vorab übermittelt. Detailinformationen zu Systemen, wie sie im Whitebox-Test mitgeteilt werden, muss der Tester jedoch selbst herausfinden.

Dieses Verfahren wird von der consectra GmbH bevorzugt eingesetzt. In einem Großteil der Fälle stellt dieses Verfahren aus ökonomischer Sicht die effizienteste Vorgehensweise dar.

Prüfung organisatorischer Voraussetzungen

Testfenster

Damit es durch den Penetrationstest nicht zu unnötigen Behinderungen Ihres Geschäftsbetriebes kommt, kann die Festlegung eines oder mehrerer Zeitfenster sinnvoll sein. Es werden also vorab Zeiten festgelegt, in welchen Ihre Systeme und Systemkomponenten penetriert werden. Dies ist zum Beispiel für Kunden entscheidend, die internetgestützte Services betreiben und prüfen lassen möchten. Auch eine Anpassung an interne Vorgänge, wie z. B. die Datensicherung, sollte berücksichtigt werden. So können Beeinträchtigungen Ihres Geschäftsbetriebes durch Störungen oder Ausfall vermieden bzw. reduziert werden.

Genehmigungen

Um alle gesetzlichen Bestimmungen zur Durchführung eines Penetrationstests einhalten zu können, bedarf es der Genehmigung des Tests Ihrerseits. Diese Genehmigung muss alle in Betracht kommenden Systeme umfassen. Werden Systeme oder Komponenten von einem Dritten gehostet oder gar betrieben, bedarf es auch dessen Genehmigung.

Alle Genehmigungen, auch die Dritter, müssen schriftlich vor Beginn des Penetrationstests vorliegen.

Risiken

Während des Testverfahrens kann es zu einem erhöhten Datenverkehr auf Servern und Netzwerken kommen. Es ist nicht auszuschließen, dass hierdurch Systeme überfordert werden. Dies gilt vor allem dann, wenn die eingesetzte Hard- und Software nur geringe Leistungsreserven aufweist. Allerdings ist die durch den Test aufkommende Datenmenge in der Regel deutlich geringer als die, welche durch einen realen Hackerangriff verursacht werden kann.

Tests von Webservices können zu Beeinträchtigungen der Funktionalität und der Stabilität eines Webservices führen.

Sollten Systeme ausfallen, kann ein manueller Eingriff vor Ort nötig werden.

Auf Grund detaillierter Absprachen zum Ablauf und der professionellen Vorgehensweise unserer Penetrationstester, konnte die consectra GmbH bislang nennenswerte Schäden an Kundensystemen vermeiden.

Durchführung der Tests

Module

Der Testgegenstand kann von Ihnen individuell abgegrenzt werden. Die nachfolgend aufgeführten Module stellen typische, standardisierte Pakete dar, welche die Auswahl vereinfachen.

Modul 1: Perimetererkennung

Ein Perimeter stellt die Umschließung eines Areals dar. In der IT besteht er aus der Summe der von außen erreichbaren Schnittstellen bzw. Schnittstellennetzwerken. Dazu zählt nicht nur der Internetzugang selbst, sondern auch Dienste, die in eigenen oder auch fremden Rechenzentren betrieben werden. In diesem Modul findet in erster Linie Recherchearbeit statt, deren Ergebnis in Folge für weitere Tests freigegeben werden kann oder auch einfach die eigene Inventarisierung unterstützt.

Modul 2: Off-Site-Test (Internet)

Systeme, welche aus dem Internet erreichbar sind, werden verschiedenen Prüfungen unterzogen. Es werden Schwachstellen analysiert, welche Angreifer ausnutzen könnten, um Systeme lahm zu legen, vertrauliche Informationen zu sammeln, Daten gezielt zu manipulieren, Systeme zum Versand von Spam oder Schadsoftware zu missbrauchen, Datenspeicher als Zwischenspeicher illegaler Informationen zu nutzen oder einfach Informationen zu sammeln, welche für spätere Angriffe dienlich sein können.

Unsere Penetrationstester agieren hierbei ausschließlich aus dem Internet mit der Ausgangslage eines Außentäters.

Modul 3: On-Site-Test (LAN / WLAN / WAN)

Welchen Schaden kann eigentlich ein Gast aus dem Besprechungszimmer heraus, ein externer Dienstleister, eine Reinigungskraft, ein Auszubildender oder gar ein Mitarbeiter von seinem Arbeitsplatz aus anrichten? Was kann aus dem WLAN alles erreicht werden?

Dieser Frage geht unser Test-Team bei einem On-Site-Szenario nach. Sie rüsten unsere Mitarbeiter mit den Möglichkeiten der Zielgruppe aus. Diese analysieren dann die Abhör- und Angriffsmöglichkeiten auf Netzwerke, Server, Arbeitsplätze, Telefonanlagen, administrative Werkzeuge und weitere Systeme.

Modul 4: Web-Applikation & Webservices

Web-Applikationen und Webservices sind überwiegend über das Internet erreichbar und somit stetigen Angriffen ausgesetzt. Aber auch im Intranet lauern Gefahren. Häufig werden beim Start des produktiven Betriebs die wichtigsten Sicherheitsaspekte berücksichtigt. Hält nach einigen Wartungsarbeiten die Applikation noch immer Angriffen Stand?

Darüber hinaus bestehen derartige Systeme häufig aus vielen Einzelkomponenten mit diversen Schnittstellen, die alle potentiellen Angriffsflächen bieten.

Webserver, welche stetig aus dem Internet heraus erreichbar sind und über eine gute Anbindung verfügen, ziehen schnell die Aufmerksamkeit von Angreifern auf sich. Sie werden gerne als Dropzone für erbeutete Bankdaten, als Downloadplattform illegaler Inhalte, zum Versand von Spam E-Mails oder Schadsoftware sowie zu Angriffszwecken auf andere Systeme verwendet.

Modul 5: Mobile (Android, iOS, Windows Phone)

Smartphones sehen sich im Alltag verschiedenen Angriffen ausgesetzt. Die lokal gespeicherten Daten können interessant sein, die Kommunikationsdaten und Telefongespräche, die Ortung und Nachverfolgung, aber auch der Zugriff über das Gerät auf das interne Unternehmensnetzwerk.

Der Penetrationstest eines Mobiltelefons verfolgt mehrere Ansätze. Hierbei nehmen unsere Mitarbeiter verschiedene Rollen ein:

- Ein Fremder befindet sich in der Nähe des Geräts, erlangt jedoch keinen physischen Zugriff.
- Ein Fremder erlangt temporär oder dauerhaft physischen Besitz.
- Das Gerät kommt ungesperrt in den Besitz eines Angreifers, z. B. durch die Bitte, kurz telefonieren zu dürfen. Hierbei stehen Modifikationsversuche im Vordergrund, welche ein Ausspähen des Gerätes, aber auch Angriffe auf andere Teile der Infrastruktur ermöglichen.

Modul 6: Social Engineering

Die Lageberichte zur Informationssicherheit in Deutschland des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zeigen seit Jahren, dass die erfolgreichsten Angriffe meist mit Unterstützung von Social Engineering durchgeführt wurden. Hierbei werden typische soziale Verhaltensweisen ausgenutzt, um an Informationen zu gelangen oder Schadsoftware einzuschleusen.

Unsere Mitarbeiter versuchen, über verschiedene Wege an vertrauliche Informationen zu gelangen, Mitarbeiter zur Herausgabe von Anmeldedaten zu bewegen oder sie dazu zu bewegen, Software auf Rechnern oder Smartphones auszuführen. Derartige Angriffe laufen selbstverständlich unangekündigt über einen längeren Zeitraum.

Beachten Sie, dass die betroffenen internen Mitarbeiter sich entweder freiwillig derartigen Tests unterziehen oder wenigstens über die Durchführung informiert sein sollten. Dies verhindert einen negativen Einfluss auf das Verhältnis zwischen Arbeitgeber und Mitarbeiter.

Werkzeuge

Zur Durchführung eines Penetrationstests nutzen unsere Mitarbeiter vielfältige Werkzeuge, die auftragsangepasst zum Einsatz kommen können. Nachfolgend listen wir eine Auswahl dieser Werkzeuge auf. Um Kriminelle nicht in ihren Aktivitäten zu unterstützen, verzichten wir darauf, Hard- und Software vorzustellen, deren Zweck die Begehung einer Straftat nach den §§ 202 a, 202 b und 202 c StGB darstellt. Da Angreifer derartige Mittel einsetzen nutzen, wir diese auch, um eine möglichst realistische Situation herzustellen.

- Internetbrowser
  Dieser dient in erster Linie zur Informationsbeschaffung, kann aber auch zum Manipulieren von Zugriffen eingesetzt werden.
- Whois, nslookup, telnet/telcat, ping, traceroute
  Über diese Protokolle werden Informationen zu Servern und –diensten, sowie zur Domain ermittelt und ggf. versucht, diese Informationen zu manipulieren.
- nmap
  nmap ist ein Portscanner, mit dessen Hilfe Informationen über das Zielsystem ermittelt werden können. Verschiedene Voreinstellungen ermöglichen hierbei aktive Intrusion Prevention Systeme zu umgehen.
- Nessus
  Ein Skriptbasiertes Werkzeug zur Schwachstellenanalyse.
- Wireshark
  Mit Wireshark lässt sich der Datenverkehr auf einem Netzwerk mitschneiden und analysieren. Dies kann besonders interessant sein, wenn zeitgleich bestimmte Informationen angefordert werden oder Systeme durch Befehle etwas „gesprächiger“ gemacht werden.

- Ettercap
  Durch einen Man-in-the-Middle-Angriff bieten sich Möglichkeiten, Daten aus verschlüsselten Verbindungen mitzulesen.
- Metasploit
  Ein Werkzeug zur vereinfachten Ausführung tausender Exploits auf Fremdsystemen.
- BurpSuite / OWASP
  Beide Tools dienen der Analyse von Webapplikationen.
- WEPCrack
  WEPCrack verschafft Zugang zu WEP-verschlüsselten Netzwerken, welche aus historischen oder Kompatibilitätsgründen noch immer zum Einsatz kommen.
- Diverse kleine, spezialisierte Werkzeuge
  Je nach Situation finden sich eine Vielzahl kleiner spezialisierter Werkzeuge im Fundus unserer Penetrationstester.

Alle angegebenen Produkte stehen stellvertretend für weitere Tools ihrer Art, eine vollständige Aufzählung der eingesetzten Werkzeuge findet sich in der kundenspezifischen Abschlussdokumentation des jeweiligen Penetrationstests.

Abschluss

Abschlussdokumentation

Nach Abschluss aller Maßnahmen des Penetrationstests wird durch unseren verantwortlichen Testleiter und dessen Team eine ausführliche Dokumentation der Methoden und Ergebnisse erstellt. Sie beinhaltet unter anderem:

- Eine Zusammenfassung der Ergebnisse und eine Einschätzung des vorhandenen Sicherheitsniveaus.
- Eine detaillierte Übersicht der festgestellten Sicherheitsmängel sowie Vorschläge zu deren Behebung.
- Den Nachweis des jeweiligen Sicherheitsmangels sowie dessen Bewertung.
- Auszüge der erlangten Daten durch die eingesetzten Verfahren und Tools.
- Berichte über mögliche besondere Vorkommnisse während des Tests.
- Schriftverkehr und Kommunikationsnachweise zwischen dem Verantwortlichen Ihres Unternehmens und unserem verantwortlichen Mitarbeiter.
- Auf Wunsch erstellen wir eine Auflistung aller eingesetzten Werkzeuge und übergeben die damit gesammelten Rohdaten.

Präsentation der Ergebnisse

Die Ergebnisse werden im Rahmen einer Präsentation dargelegt und gemeinsam mit Ihnen erörtert. Dabei anonymisieren wir alle personenbezogenen Daten, um die Bloßstellung einzelner Mitarbeiter zu vermeiden. Es empfiehlt sich erfahrungsgemäß, die Präsentation der Ergebnisse zielgruppenspezifisch für die Unternehmensleitung bzw. den Kreis der Administratoren aufzuteilen.