Michael Muncan, Sebastian Schreiber

Interne Penetrationstests

Sicherheitstests im Firmennetz

Penetrationstests im internen Firmennetz sind eine besondere Form von Sicherheitstests. Häufig wähnen IT-Entscheider und Sicherheitsbeauftragte die größten Gefahren außerhalb ihres Unternehmens und übersehen dabei gerne, dass es auch innerhalb der Firma und ihrer Netze nicht unerhebliche Sicherheitsrisiken gibt.

Einleitung

Sicherheitsrisiken von innen sind häufiger als oftmals vermutet. Während viele Sicherheitsexperten und IT-Entscheider befürchten, dass die Hauptgefahr für Firmennetzwerke von außen kommt, gibt es von innen zahlreiche Wege, Netze zu kompromittieren. Dabei wird oft übersehen, wie leicht oftmals in Firmen eingedrungen und Firmennetze bedroht werden können. In diesem Beitrag sollen diese Sicherheitsrisiken beleuchtet und mögliche Bedrohungsszenarien aufgezeigt werden. Anschließend wird dargelegt, wie Penetrationstests Firmen helfen können, Sicherheitslücken aufzuspüren und zu schließen und so einen entscheidenden Beitrag zur firmeneigenen IT-Sicherheit zu leisten.

Michael Muncan M.Sc., Dipl.-Wirtschaftsinformatiker (FH)

SySS GmbH, Tübingen, Security Consultant bei der SySS GmbH und erfahrener Penetrationstester.
E-Mail: michael.muncan@syss.de

Dipl.-Inform. Sebastian Schreiber

SySS GmbH, Tübingen, Gründer und Geschäftsführer der SySS GmbH. Expertise bei Penetrationstests, bekannt durch Vorträge und Live Hacking-Präsentationen im In- und Ausland und in den Medien.
E-Mail: sebastian.schreiber@syss.de

1 Unerkannte Personen im Unternehmen

Ein nicht zu unterschätzendes Gefahrenpotenzial birgt die Größe einer Firma. Während kleinere Firmen normalerweise überschaubar sind und die Mitarbeiter sich untereinander kennen, ist dies in Unternehmen etwa ab einer Mitarbeiterstärke von 80-100 Personen nicht mehr der Fall. Dort kennen Mitarbeiter in der Regel die Kollegen ihrer eigenen Abteilung, wissen aber oft nicht, wer zu anderen Abteilungen gehört. Daher sind sie es gewohnt, immer wieder ihnen unbekannte Gesichter zu sehen. Aus diesem Grund fällt in diesen Unternehmen auch seltener auf, wenn sich unternehmensfremde Personen in den Gängen der Firma bewegen. Zu diesem Personenkreis gehören vor allem Mitarbeiter externer Dienstleister oder Praktikanten, die nicht allen Firmenangehörigen bekannt sind, aber durchaus ihre Daseinsberechtigung im Unternehmen haben.

Unerwünschte Personen, die sich unter einem Vorwand Zugang zum Unternehmen verschaffen, haben somit gute Chancen, unerkannt zu bleiben. Daher ist auch die Gefahr eines Sicherheitsvorfalls von innen bei größeren Unternehmen höher und verstärkt die Bedeutung interner Penetrationstests in Firmennetzwerken.

2 Burggrabenprinzip

Computernetze in Unternehmen sind häufig nach dem Burggrabenprinzip[1] konzipiert. Unternehmen gehen dabei implizit davon aus, dass sich innerhalb ‚der Mauern' ihres Firmennetzwerks (Corporate Network) ausschließlich vertrauenswürdige Mitarbeiter befinden, die es durch wirksame Firewalls vor Angriffen von außen, sprich dem Internet, zu schützen gilt. Die eingesetzten Firewalls sind hierbei immer nur so gut wie ihre Konfiguration, und eine besondere Bedeutung kommt daher den Firewallregeln sowie in diesem Zusammenhang dem Change Management zu. Somit kann eine Firewall einen guten Schutz bieten, wenn die Firma an diesem Burggrabenprinzip festhält.

Im Laufe der Weiterentwicklung der Firmennetzwerke wurde meist irgendwann damit begonnen, gegen dieses Prinzip zu verstoßen: Mitarbeiter und externe Partner durften sich von außen über Remote Access Service (RAS) oder Virtual Private Network (VPN) mit dem Unternehmensnetz verbinden. Das Privileg, Zugriff auf das Firmennetz zu erhalten, wurde nicht mehr nur Mitarbeitern im Inneren der Firma gewährt, sondern auch Personen außerhalb, womit das Burggrabenprinzip aufgeweicht wurde. Moderne Schutzkonzepte müssen dieser Entwicklung Rechnung tragen, um Firmennetze auch weiterhin wirksam und ausreichend vor Bedrohungen schützen zu können.

1 Das Burggrabenparadigma sieht die Firewall als einen nahezu unüberwindbaren Burggraben.

3 Bedrohungen des Firmennetzwerks

Die veränderte Ausgangslage schafft eine neue Bedrohungssituation. Der Burggraben, um bei diesem Bild zu bleiben, bietet keinen vollständigen Schutz mehr, denn er hat neben dem vormals einzigen Zugangstor weitere Nebentüren und Schlupflöcher bekommen, durch die Eindringlinge ins Innere gelangen könnten.

In den folgenden Abschnitten werden mehrere konkrete Beispiele für derartige Bedrohungen interner Firmennetze vorgestellt. Diese sollten auch bei Penetrationstests analysiert werden, um eine Aussage über den Stand der firmeneigenen IT-Sicherheit treffen zu können.

3.1 Frei liegende Netzwerkzugänge

Der direkte Netzwerkzugang zum Firmennetzwerk stellt ein primäres Problem dar. Meist gibt es in Unternehmen eine Reihe von Möglichkeiten, auf das Firmennetzwerk zuzugreifen, wenn kein Schutz gegen Unbefugte besteht. Zum einen sollten alle Rechner selbst vor Zugriffen durch nicht berechtigte Personen geschützt sein. Zum anderen besteht in vielen Firmen die Möglichkeit, über frei zugängliche Netzwerkkabel, ungesicherte Patchdosen, Bodentanks, von Geräten im Netzwerk, wie beispielsweise (Thin-)Clients, VoIP-Telefonen oder Kiosk-Systemen auf die Hardware eines Unternehmensnetzwerks zuzugreifen.

3.2 Innentäter

Auch wenn diese Perspektive etwas heikel ist, weil sie davon ausgeht, dass sich vor allem in größeren Unternehmen auch Mitarbeiter befinden könnten, die als Innentäter Schaden anrichten könnten, sollte dieser Gedanke nicht gänzlich außer Acht gelassen werden. Daher ist es ratsam, darauf zu achten, dass unterschiedliche Bereiche im Firmennetz von einander abgeschottet sind und Mitarbeiter grundsätzlich nur Zugang zu den Bereichen erhalten, die für ihre Arbeit relevant sind.

3.3 Ungenügend geschützte WLANs

Wireless LANs hebeln das Burggrabenparadigma völlig aus, falls Unternehmen ein schlecht geschütztes WLAN betreiben. In solchen Fällen kann jeder, der sich in Reichweite des WLANs befindet, ins Firmennetz gelangen. Mit der zunehmenden Verbreitung drahtloser Netze gewinnt auch dieser Aspekt bei der Analyse der eigenen internen Sicherheit an Bedeutung. Eine Überprüfung der WLAN-Sicherheit stellt eine spezielle Form des Penetrationstests dar und ist aufgrund seiner Komplexität ein eigener Test, der aber als Ergänzung zu einem internen Penetrationstest in Erwägung gezogen werden kann.

3.4 Notebooks

Auch Notebooks, die von Mitarbeitern in nicht vertrauenswürdigen Netzen verwendet werden und daraufhin wieder zurück in das Firmennetzwerk gelangen, bilden ein großes Gefahrenpotenzial und können zur Bedrohung für die IT-Sicherheit werden. Aktuelle Notebooks sind zudem mit Technologien wie WLAN, UMTS und Bluetooth ausgestattet, die sich potenziell als Firewall-Bypass oder zur Koppelung verschiedener Netze missbrauchen lassen.

4 Neuere Bedrohungen des Firmennetzes

4.1 USB-Sticks

In letzter Zeit sind weitere Bedrohungen zu den oben genannten hinzugekommen. Seit der Markteinführung von U3-USB-Sticks tauchen diese immer öfter auch als Werbegeschenke auf. Diese USB-Sticks bieten je nach Konfiguration des Systems die Möglichkeit, beim Einstecken automatisch Software auszuführen. Ein Mitarbeiter könnte somit Opfer eines zufälligen oder gezielten Angriffs werden, indem er einen präparierten U3-USB-Stick erhält und diesen an einem System im Firmennetz anschließt. Hierdurch gefährdet er nicht nur dieses eine System, sondern möglicherweise das gesamte Netzwerk.

4.2 Multifunktionsgeräte

Hinzu kommen Geräte wie Beamer oder Multifunktionsgeräte, deren voller Funktionsumfang auf den ersten Blick nicht erkennbar ist. Beamer sind teilweise mit WLAN ausgestattet und Multifunktionsgeräte vereinen Drucker, Scanner und Fax und erlauben den Zugriff über Netzwerkdienste, USB-Schnittstellen, Speicherkartenlesegeräte und das integrierte Faxmodem.

4.3 Push E-Mail

Ein besonderes Augenmerk sollte auf Push-E-Mail-Dienste gerichtet werden. Über ihre ursprüngliche Funktion hinaus, das automatisierte Versenden von eingehenden E-Mails auf mobile Endgeräte wie beispielsweise Smartphones, bieten diese weitere Möglichkeiten wie den Zugriff auf zentrale Kalender, Instant Messaging und den Zugriff auf Applikationen im Firmennetz. Dabei sind sie zusätzlichen Bedrohungen ausgesetzt, wie zum Beispiel Verlust oder Diebstahl, und werden somit ebenso zur potenziellen Bedrohung für das Firmennetz.

5 Ziel und Perspektive des Penetrationstests

Aufgrund der geschilderten Bedrohungen verfolgen Penetrationstests im Firmennetzwerk das Ziel, konkrete Sicherheitslücken aufzuspüren und die Schwere der von ihnen ausgehenden Risiken zu bewerten. Im Rahmen der Dokumentation wird ein Katalog mit Maßnahmen zur Beseitigung der erkannten Schwachstellen erstellt. Auf diese Weise kann eine Firma anhand der Testergebnisse zügig agieren und etwaige Sicherheitsschwächen schnell beheben.

Schwerpunkt bei internen Penetrationstests ist dabei die Feststellung von Sicherheitslücken, die ein hohes Innentäter-Potenzial haben. Bei einem internen Penetrationstest gibt es grundsätzlich zwei mögliche Perspektiven, die eingenommen werden können:

- Entweder wird die Perspektive eines Benutzers gewählt, der mit dem eigenen Notebook Zugang zum Firmennetz hat. Aus diesem Blickwinkel heraus werden alle erreichbaren Systeme auf Sicherheitslücken hin untersucht.
- Oder es wird die Position eines bestimmten Systems (beispielsweise die Situation, dass ein Praktikant einen Standard-PC erhält) eingenommen. In diesem Fall wird geprüft, inwieweit das System gegen Manipulationen geschützt ist und ob es für Angriffe verwendet werden kann.

Darüber hinaus ist das Netzwerk selbst Gegenstand der Untersuchung, wobei sich das Augenmerk vor allem auf die vorhan-

dene Struktur richtet. Die Erfahrung bei der Durchführung solcher Tests zeigt, dass häufig sehr flache Netze angetroffen werden, in denen kaum oder gar keine Segmentierung existiert. Solche Netze bieten oft aus Bereichen wie Besprechungsräumen mit geschalteten Netzwerkdosen Zugang zu wichtigen Diensten, wie beispielsweise Datenbanken auf zentralen Servern, auf die eigentlich kein direkter Zugriff bestehen sollte.

6 Testvorbereitung

Sowohl die technische als auch die organisatorische Testvorbereitung sind von großer Bedeutung. Mit der Vorbereitung des Tests werden die Voraussetzungen für einen optimalen Testverlauf geschaffen.

Bereits bei der Vorbereitung eines Penetrationstests im Firmennetz ist es ratsam, Meetings mit allen Beteiligten zu planen. Diese sind wichtig, denn sie dienen der optimalen Vorbereitung des Tests und vor allem auch dazu, vorhandene Vorbehalte und Bedenken auszuräumen. Da ein Penetrationstest von Mitarbeitern nicht immer als positive Maßnahme aufgefasst wird, muss vor allem die interne Kommunikation sorgfältig geplant werden, damit der Test dann sowohl von den Testverantwortlichen im Unternehmen als auch von den Mitarbeitern selbst als positive, die innere Sicherheit stärkende Maßnahme aufgefasst wird. Auch unmittelbar vor Testbeginn sollte noch einmal eine Besprechung mit allen Projektbeteiligten stattfinden, damit der Test reibungslos verlaufen kann.

Die organisatorische Testvorbereitung umfasst auch den Zugang zum Unternehmen und den entsprechenden Räumlichkeiten. Falls ein Zutrittskontrollsystem existiert, ist eine Freischaltung oder ein Gastzugang für die Tester erforderlich. Wenn der Test in einem Bereich mit besonderen Sicherheitsanforderungen stattfindet, sind möglicherweise entsprechende Überprüfungen im Vorfeld nötig, oder der Tester muss in ständiger Begleitung eines Mitarbeiters sein.

Für den Test im Firmennetz sollte ein entsprechender Arbeitsplatz mit Netzwerkzugang und Stromversorgung bereitgestellt werden. Der Zugang zum Netzwerk muss funktionsfähig sein; falls kein DHCP genutzt wird, müssen die benötigten Informationen wie IP-Adressen, Netzmaske usw. vorhanden sein, ebenso ein zu testender PC, der gegebenenfalls mit einem gültigen Benutzerkonto für Testzwecke versehen sein sollte.

Alle von einem Sicherheitstest betroffenen Personen sollten vorab über diesen informiert werden. Für die Dauer des Tests sollten die Verantwortlichen und die Betroffenen stets gut erreichbar sein.

7 Auswahl der zu testenden Systeme

Zielsysteme eines internen Penetrationstests sind alle über das Netzwerk erreichbaren Systeme wie beispielsweise Server, Clients, Netzwerkkomponenten, Drucker, Multifunktionsgeräte, Telefone, Telefonanlagen, Kameras und Steuerungsrechner.

Aufgrund der meist großen Zahl erreichbarer Systeme und infolgedessen der enormen Anzahl an testbaren Diensten, kommt der Auswahl sinnvoller Stichproben eine sehr hohe Bedeutung zu. Eine Clusterbildung ist dabei sehr hilfreich.

Ziel ist dabei üblicherweise, einen Überblick über die Gesamtsituation zu erhalten, und nicht der erschöpfende Test eines einzelnen Systems. Hierbei werden vor allem bei einem ersten Test die „low hanging fruits" gesammelt, also auf bekannte Schwachstellen geachtet, die typischerweise häufig vorkommen.

Bei sehr großen oder sehr komplexen internen Netzen kann ein erfahrener Tester bei der Auswahl geeigneter Stichproben behilflich sein und gegebenenfalls auch eine Inventarisierung durchführen, die grob der Perimetererkennung[2] entspricht.

8 Risiken durch den Penetrationstest

Das Risiko unbeabsichtigter Schäden ist bei internen Penetrationstests höher, da im Unternehmensnetz zumeist keine Abschottung einzelner Systeme vorgenommen wird und eine Vielzahl von Diensten erreichbar ist. Für gewöhnlich gibt es keine Testsysteme, sodass die Penetrationstests meistens in Produktivumgebungen durchgeführt werden.

Zudem werden in internen Netzen häufig Systeme eingesetzt, die entweder nicht für den Einsatz im Internet vorgesehen sind oder sehr lange, teilweise weit über ihren Product Lifecycle hinaus, genutzt werden. Das Risiko, dass es beim Test solcher Systeme zu Abstürzen kommt, ist sehr hoch. Daher ist seitens des Testers eine erhöhte Vorsicht bei der Durchführung interner Tests angebracht.

9 Testablauf

Im Prinzip beginnt ein interner Penetrationstest immer mit der Prüfung der Systeme auf erreichbare Dienste. Diese Dienste wiederum werden gezielt mit automatischen Schwachstellenscannern getestet. Ein verantwortungsvoller Tester führt mit Rücksicht auf das zuvor beschriebene Risiko keine unbeaufsichtigten automatisierten Tests durch. Somit ist im Falle von Problemen jederzeit eine Unterbrechung oder gar ein Abbruch des Scans möglich.

Bei den zuvor genannten Tests kommen Tools wie Portscanner und Schwachstellenscanner zum Einsatz. Mit einem Portscanner wird versucht, alle erreichbaren Dienste auf einem System zu identifizieren. Dabei kann unter Umständen die eingesetzte Software und deren Version ermittelt werden. Diese Ergebnisse werden im weiteren Verlauf einem Schwachstellenscanner übergeben, der nach bekannten Schwächen für die identifizierten Dienste sucht.

Im Verlauf der automatisierten Scans wird sehr viel Wert auf die Protokollierung gelegt, um einzelne Schwachstellen manuell verifizieren zu können oder aufgetretene Probleme nachzustellen. Sobald die Ergebnisse der automatisierten Tests vorliegen, werden diese einer manuellen Verifizierung unterzogen. Zusätzlich gibt es manuelle Prüfungen mit dem Ziel, einzelne Schwachstellen auszunutzen, um sie auf diese Weise deutlich zu machen.

Bei den Tests wird immer auch die Eindringwahrscheinlichkeit bewertet, wobei hier zwischen Produktiv- und Testsystemen zu unterscheiden ist. Diese Wahrscheinlichkeit kann über den Einsatz von Exploits verifiziert werden. Hierbei spielt zunächst eine Rolle, ob ein Exploit (oder auch nur *Proof-of-Concept-Code*) frei verfügbar ist, oder im Rahmen von kommerziellen Exploit-Sammlungen existiert. Dabei gibt es oft Unklarheiten, ob das Testen

2 Unter einer Perimetererkennung versteht man die Identifizierung von Netzwerksegmenten an der Schnittstelle zweier Netzwerke (beispielsweise die DMZ eines Unternehmens).

von Exploits im Rahmen eines Penetrationstests unter den Paragraphen § 202c StGB (umgangssprachlich „Hackerparagraph" genannt) fällt und eine Straftat darstellt. Der Rechtsausschuss des Deutschen Bundestages hat hierzu 2007 in einem Bericht darauf hingewiesen, dass der gutwillige Umgang mit Hackertools durch IT-Sicherheitsexperten nicht von §202c StGB erfasst werde [1].

10 Weitere Tests

Zusätzlich zum zuvor beschriebenen Testablauf können bei Bedarf die eingesetzten Protokolle auf deren potenzielle Verwundbarkeit für *Man-in-the-Middle*-Angriffe untersucht werden. Um in einem internen Netz eine *Man-in-the-Middle*-Position erlangen zu können, ist ARP-Spoofing[3] eine zwingende Voraussetzung. Hierbei wird überprüft, ob die eingesetzte Netzwerkinfrastruktur solche Angriffe zulässt. Mit dem zunehmenden Einsatz von VLANs gehören auch deren Analyse sowie der nicht autorisierte Zugang zu einem VLAN zum Testumfang.

Des Weiteren sind VoIP-Tests sehr aufschlussreich, wenn ein Unternehmen die Telefoninfrastruktur entsprechend umgestellt hat. Hierbei wird überprüft, ob die Telefonanlage und die Endgeräte über das Netzwerk erreichbar sind, ob sich Datenverkehr mitlesen lässt und sich Gespräche abhören lassen.

In vielen Unternehmen kommt inzwischen eine Port Security zum Einsatz, beispielsweise in Form eines *Network Access Control (NAC)*-Systems, das die zuvor beschriebenen Angriffe unterbinden soll. Bei derartigen Systemen bietet sich eine Überprüfung an, ob die komplexe Konfiguration korrekt durchgeführt wurde. Somit wird vermieden, dass sich Firmen mit einer Port Security in falscher Sicherheit wiegen, die möglicherweise ihre Funktion nicht oder nur teilweise erfüllt.

Eine Sonderform des internen Penetrationstests ist die umfassende Prüfung eines Arbeitsplatzes. Hierbei wird getestet, ob direkte Manipulationen an der Hardware möglich sind, etwa das Booten von externen Medien wie USB-Sticks oder CD-ROMs oder ob das Betriebssystem selbst die Option bietet, eigene Installationen auszuführen.

Ziel dieser Tests sind die auf den Systemen gespeicherten Passwort-Hashes. Werden schlechte Passwörter oder schwache Hashing-Algorithmen verwendet, so können Angriffe mit Wörterbüchern oder sogenannten Rainbow-Tables innerhalb kurzer Zeit zum Erfolg führen. Ein Tester zielt bei seiner Arbeit immer auch auf den potenziellen Angriff gegen das Benutzerkonto des Windows-Domänen-Administrators ab. Wenn solche Angriffe erfolgreich sind, hat das weitreichende Konsequenzen für das Firmennetz.

Fazit

Bei einer guten Vorbereitung und einem sorgsamen Vorgehen können Penetrationstests im Firmennetz dazu beitragen, das Sicherheitsniveau der firmeneigenen IT-Umgebung nachhaltig zu erhöhen, indem Sicherheitsschwächen konkret aufgezeigt und Maßnahmen zu ihrer Behebung vorgeschlagen werden.

Sie sind für die innere Sicherheit insofern aufschlussreich, da sie aus der Perspektive eines Innentäters durchgeführt werden. Da Firmen in der Regel nicht mit internen Angreifern rechnen, werden solche Schwachstellen in firmeninternen Netzen nämlich eher übersehen, als Schwachstellen an den Zugangsstellen von außen. Ein solcher Test bedarf einer sorgfältigen Vorbereitung, damit seine Durchführung der Firma Nutzen bringt und im Endeffekt sein Ziel erfüllt, die IT-Sicherheit des geprüften Unternehmens zu steigern.

Referenzen

[1] Bundestag: *Beschlussempfehlung und Bericht des Rechtsausschusses*, Bundestags-Drucksache 16/5449, 2007,http://dip.bundestag.de/btd/16/054/ 1605449.pdf

[2] Markus a Campo: *Penetration Testing*, 2003, mitp Verlag.

[3] S. Schreiber: *Drahtlose Netze – neue Gefahren zwingen zum Paradigmenwechsel*, White Paper, 2009, http://www.syss.de/fileadmin/downloads/artikel/Artikel_Drahtlose_Netze.pdf

[4] S. Schreiber und S. Arbeiter: *Durchführung und Gestaltungsmöglichkeiten von Penetrationstests*, White Paper, 2008, http://www.syss.de/fileadmin/ressources/010_aktuell/dokumente/WhitePaper_160209.pdf

3 Siehe Fox, ARP Poisoning, Gateway, DuD 10/2005, S. 614.