VIER AUGEN

Vom Selbsttest zum Pentest

Pentest: Sinn oder Unsinn?

Die Zahl der Angriffe auf Rechnersysteme, unabhängig ob in Unternehmen oder privat, steigt stetig. Verbunden mit der immer stärkeren Durchdringung der IT ist die Rolle der IT-Sicherheit so wichtig wie nie zuvor. Insbesondere bei der immer weiteren Vernetzung aller Rechnersysteme in Unternehmen stehen den durchaus zahlreich vorhandenen positiven Effekten auch zahlreiche Risiken gegenüber. Die Verbindung der Rechnersysteme führt häufig dazu, dass lokale Sicherheitsprobleme einzelner Rechnersysteme zu Risiken des Netzwerks und somit des gesamten Unternehmens werden.

In den letzten Jahren werden verstärkt sogenannte Penetrationstests (kurz: Pentest) angeboten. Bei einem Pentest betrachten externe Dienstleister die eigene IT-Infrastruktur nach dem Vier-Augen-Prinzip. Denn schnell schleicht sich eine „Betriebsblindheit" ein und man übersieht Lücken, die einem externen Pentest-Dienstleister sofort auffallen würden.

Doch sind diese Tests wirklich notwendig oder teure Spielerei? Oder können Maßnahmen innerhalb der Unternehmen ein ebenso ausreichendes oder höheres Sicherheitslevel erreichen? Dieser Artikel versucht, diese Fragen zu klären.

Interne IT-Sicherheit

Um einen Teil der Antwort schon vorwegzunehmen: Pentests sind kein Ersatz für eine gute IT-Sicherheitsstrategie, sondern ein Prüfinstrument für die Wirksamkeit dieser Strategien.

Eine gute IT-Sicherheitsstrategie besteht dabei nicht aus einer reinen Absicherung der Konfiguration von Rechnersystemen und Strukturen. Durch die tiefgehende Verflechtung von IT mit Unternehmensstrukturen besteht optimale IT-Sicherheit heute aus einer ganzheitlichen Betrachtung, die weitere Maßnahmen abseits der reinen Konfiguration und die Zusammenarbeit mit anderen Unternehmensbereichen umfasst.

Im Folgenden werden die vier Kernfelder einer guten IT-Sicherheitsstrategie kurz erläutert:

1) „Klassische" IT-Sicherheit

Auch heute ist eine sichere Konfiguration der Unternehmens-IT die Grundlage für alle anderen IT-Sicherheitsbemühungen. Sie umfasst sowohl die Software- als auch die Hardware-Sicherheit.

Sind beispielsweise die Arbeitsplatz-Rechner abgeschlossen, das Bootmenü gesperrt, nicht benötigte Schnittstellen deaktiviert und das BIOS mit einem Passwort geschützt, ist eine Kompromittierung auf Hardware-Seite, beispielsweise über einen Boot eines anderen Betriebssystems per Live-CD, relativ schwierig. Sind zusätzlich die Netzwerk-Dosen im Unternehmen durch eine Zugangskontrolle wie IEEE 802.1x geschützt, wird ein unbemerktes Einbringen unternehmensfremder Hardware erschwert.

Auf der Seite der Software-Sicherheit werden die Maßnahmen wie Patch-Management, Firewalls und Virenscanner durch weitere Maßnahmen wie eine sichere Konfiguration von Betriebssystem und Anwender-Software unterstützt. So gilt es zum Beispiel unbedingt den Autostart von Wechseldatenträgern wie USB-Sticks und CDs zu unterbinden, da dieser ein potentielles Einfallstor für Angreifer ist. An dieser Stelle wird klar, dass es einen weiteren Faktor in der IT-Sicherheit gibt, der nicht über die Konfiguration abgedeckt werden kann: der Mitarbeiter.

2) Mitarbeiter-Sensibilisierung

Fehlverhalten von Mitarbeitern, sei es unbeabsichtigt oder beabsichtigt, ist ein häufig unterschätztes Risiko. Schätzungsweise 70% der Angriffe werden innerhalb der Unternehmen durchgeführt. Mitarbeiter öffnen zum Beispiel E-Mails mit infizierten Anlagen oder wählen schwache Passwörter. Hier ist es wichtig, dass die Mitarbeiter konsequent geschult werden. Auch die sicherste Konfiguration kann nicht vor allen Angriffen schützen. Damit Rechnersysteme benutzbar bleiben, muss zwangsläufig die Nutzung von Schnittstellen und Funktionen erlaubt werden. Die Verwendung von USB-Sticks als Ersatz für Disketten und CD-ROMs und der Anschluss von Peripheriegeräten wie Drucker, Tastaturen und Mäuse verhindert beispielsweise häufig eine Deaktivierung der USB-Schnittstellen. Würde sich ein Angreifer an Ihr Firmentor stellen und verseuchte USB-Sticks verschenken, was glauben Sie, wie viele Ihrer Mitarbeiter diesen verseuchten Stick in ihren Arbeitsplatzrechner stecken würden?

Ein Schutz vor den Auswirkungen dieser Art von Angriffen lässt sich nur durch konsequente Sensibilisierung der Mitarbeiter zum Beispiel durch Schulungen durchführen. Eine gute Schulung schlägt dabei die Brücke zum privaten Bereich. Es hat sich gezeigt, dass diese Brücke das Verständnis und die Akzeptanz stark erhöht.

3) Risiken außerhalb des Unternehmens

In den letzten Jahren hat die Verbreitung und Benutzung mobiler Endgeräte stark zugenommen. Außendienstmitarbeiter nutzen ihre Firmen-Notebooks in den unterschiedlichsten Umgebungen mit unterschiedlichsten Sicherheitsleveln. Smartphones, insbesondere Blackberrys, entwickeln sich zum mobilen Arbeitsplatz, auf dem auch sensible Informationen gespeichert werden. Die größte Gefahr, die von diesen Geräten ausgeht, ist der Betrieb außerhalb der lokalen Schutzmaßnahmen. Mobile Endgeräte gehen verloren, werden gestohlen und in öffentlichen Netzwerken benutzt. Die auf den Geräten gespeicherten Informationen müssen deshalb gesondert vor diesen neuen Gefahren geschützt werden. Gleichzeitig entsteht eine neue Gefahrenquelle für das Unternehmensnetzwerk. Die Anbindung per Remote, zum Beispiel über VPNs oder über eine Reintegration in das Unternehmensnetzwerk, verwischt die klassischen Netzwerkgrenzen und umgeht klassische Sicherheitsmechanismen. Der Schutz mobiler Endgeräte ist also ein Zusammenspiel aus Konfiguration und Richtlinien, aber auch einer guten Sensibilisierung der Benutzer.

4) Unternehmensinterne Risiken außerhalb der IT

Wie bereits erwähnt, müssen heutzutage die unterschiedlichsten Unternehmensbereiche zusammenarbeiten. Dies fängt bei der Beschaffung an (Sicherheit erfordert In-

vestitionen) und hört beim Werkschutz auf, denn was nützen die besten Firewalls, wenn Besucher und Fremdfirmen ungehindert fremde Hardware mit auf das Firmengelände bringen oder Firmen-PCs herausgetragen können?

IT-Audits

Durch den immer stärkeren Einsatz von IT in Unternehmen steigt auch deren Bedeutung. Schon längst ist für viele Unternehmen ein reibungsloser Ablauf der IT überlebenswichtig. Umso wichtiger ist eine regelmäßige Überprüfung von Prozessen anhand von Richtlinien und Checklisten. Dies wurde auch durch den Gesetzgeber erkannt. Die 8. EU-Richtlinie, in Anlehnung an den in den USA gültigen „Sarbanes-Oxley-Act (SOX)" auch „Euro SOX" genannt, schreibt die Durchführung von IT-Audits vor.

Ein Baustein für einen reibungslosen Ablauf der IT ist ein funktionierender Schutz vor Angriffen und ihren Auswirkungen. Deshalb müssen IT-Audits auch eine Sicherheitsbetrachtung umfassen. Erlangt ein Angreifer beispielsweise über Schwachstellen im Firewall-Regelwerk erfolgreich Zugriff auf ein Unternehmensnetzwerk, sind sämtliche erreichbaren Rechnersysteme gefährdet und somit auch die dahinter stehenden Geschäftsprozesse.

Und wozu nun Pentests?

Kommen wir zurück zur anfangs gestellten Frage nach der Sinnhaftigkeit von Pentests:

Kurz gesagt: Penetrationstests sind eine sinnvolle Ergänzung der unternehmenseigenen Sicherheitsbemühungen.

Ein Penetrationstest erlaubt nicht nur die Überprüfung der (IT-)Sicherheit in Unternehmen nach dem Vier-Augen-Prinzip, sondern eine Betrachtung aus einem weiteren Blickwinkel, dem Blickwinkel eines Hackers, nur unter kontrollierten Bedingungen.

Mit diesem Blickwinkel werden die Sicherheitseinstellungen einer IT-Infrastruktur nicht direkt, sondern indirekt überprüft. Anstelle einer Kontrolle jeder noch so kleinen Konfigurationsoption, überprüft ein Pentest das Zusammenspiel aller Konfigurationen im Hinblick auf den erreichten Schutz vor Angriffen. Werden durch Audits meist Fragen wie: „Ist der PC abgeschlossen und das Boot-Menü deaktiviert?" überprüft, gilt beim Pentest die allgemeine Frage, ob ein Angreifer ein lokales System trotz eingeschränkter Rechte erfolgreich kompromittieren kann. Diese Fragestellung erlaubt die Betrachtung weiterer Sicherheitsaspekte wie zum Beispiel, ob Master-Passwörter um den Passwortschutz des BIOS oder Schwachstellen in der Hardware oder auf Management-Schnittstellen existieren.

Und eben diese Motivation und die Tatsache, dass sich die Spezialisten all die Informationen über das Netzwerk und die Systeme verfügbar machen müssen, fördern oft erstaunliche Dinge zu Tage, die vorher niemand beachtet hat. Ein verbreitetes Beispiel aus der Praxis, aber ein relativ unbekanntes Problem, sind unsichere Konfigurationen von Windows-Diensten. Obwohl das Problem schon vor mehreren Jahren veröffentlicht wurde, lassen sich zum Beispiel die Dienste einiger Druckertreiber für Angriffe ausnutzen.

Diese Dienste laufen mit lokalen Administrator-Rechten, sind aber von einem nicht privilegierten Nutzer konfigurierbar. So kann zum Beispiel der ausführbare Pfad des Dienstes durch eine Kommando-Shell ersetzt werden, die einen neuen Benutzer mit lokalen Administrator-Rechten anlegt. Dies führt unter Umständen durch die Erlangung weiter gehender Rechte im Netzwerk sogar zu einem globalen Angriff auf das Netzwerk. Bei den Verantwortlichen in vielen Unternehmen ist das Wissen über solche Möglichkeiten schlicht nicht vorhanden. Ein Pentest kann diese Lücke aufdecken und Anleitung zur Schließung der Lücke geben.

Ein Pentest ist dabei nicht standardisiert. Er kann und sollte immer auf die Gegebenheiten im Unternehmen angepasst werden. Es gibt zwar Richtlinien und Zertifizierungen, jedoch kann man einen Pentest nicht anhand einer Liste zum Abhaken durchführen, was in Unternehmen A richtig ist, muss nicht auch automatisch für Unternehmen B gelten.

Idealerweise werden gefundene Sicherheitslücken im Zweifelsfalle auch ausgenutzt, um die Angreifbarkeit der Systeme aufzuzeigen. Jedoch ist dies nicht immer möglich, zum Beispiel wenn dadurch Produktivsysteme in ihrer Funktion gestört werden oder gar ganz ausfallen können. Daher bedarf dies einer sorgfältigen Vorbereitung in Form von Gesprächen zwischen den Pentestern und dem Unternehmen.

Zusammenfassung

Die Rolle der IT-Sicherheit in Unternehmen wird immer wichtiger. Die Unternehmen können und müssen durch interne Maßnahmen wie Mitarbeiterschulungen und Audits die Zahl der Gefahren gering halten. Von externen Firmen durchgeführte Pentests können diese Bemühungen durch ihren speziellen Blickwinkel unterstützen und unerkannte Sicherheitslücken aufdecken. Besonders wichtig ist, dass Pentests nicht als einmalige Überprüfung gesehen werden. Jeden Tag werden neue Sicherheitslücken und beinahe wöchentlich neue Angriffsverfahren veröffentlicht. Dieses hohe Tempo macht einen erneute Überprüfung in regelmäßigen Abständen notwendig.

Autoren

Prof. Dr. Norbert Pohlmann

Marc-Aurél Ester, Marian Jungbauer und **Marco Smiatek** sind Mitarbeiter im Bereich Awareness am Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen.
Prof. Dr. Norbert Pohlmann ist Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen (www.internet-sicherheit.de)