Computerworld **Dossier IT-Sicherheit**

Hacken im Dienste der Systemsicherheit

Sicherheit Mit simulierten Hackerangriffen können Sicherheitssysteme auf deren Wirksamkeit hin überprüft werden. Wer einen Auftragshacker bestellt, sollte klare Zielvorgaben festlegen und eine kontrollierte Umgebung bieten.

Christoph Baumgartner*

Vor Hackern ist niemand gefeit. Sie suchen oder bauen sich ein Hintertürchen in nahezu jedes Computersystem. Illustration:thü

Die Bezeichnung «Ethical Hacking» weist auf die ethische Vertretbarkeit dieser Form des Hackings hin – was impliziert, dass Hacking per se unethisch ist. Ethical Hacking gilt als Königsdisziplin der informationstechnischen Sicherheitsüberprüfungen. Wie bei allen Sicherheitschecks geht es dabei darum, Sicherheitslücken aufzudecken, bevor dies Unberechtigte tun. Üblicherweise werden anschliessend Massnahmen zur Schliessung allfällig gefundener Lücken vorgeschlagen. Die Umsetzung dieser Massnahmen erhöht das Sicherheitsniveau.

Problematik

Im Gegensatz zu Vulnerability-Scans, Security-Scans und traditionellen Penetrationtests, welche nur nach Sicherheitslücken suchen und diese dokumentieren, werden beim Ethical Hacking Sicherheitslücken gezielt ausgenutzt und das Untersuchungsobjekt manipuliert oder modifiziert. Ausserdem ist der manuell zu erbringende Anteil an den Projektarbeiten (Engineering und Durchführung der eigentlichen Attacke) massiv höher, weil für den eigentlichen «Hackerangriff» normalerweise nur bedingt Standardtools wie Security-Scanner oder Testskripts eingesetzt werden können. Besonders bei komplexen Zielvorgaben müssen vom Tester oftmals massgeschneiderte Tools programmiert werden. Dies wirkt sich auf den Projektpreis aus und setzt entsprechende Fachkenntnisse des Testers voraus. Wenn der Auftraggeber nur das Ziel – beispielsweise das Löschen oder Abspeichern einer bestimmten Datei auf einem FTP-Server – nicht aber die Methode definiert, genügt dem Tester eine einzige Sicherheitslücke, welche er für seine Zwecke ausnutzen kann. Nach allfälligen weiteren Sicherheitslücken mit möglicherweise weit höherem Gefährdungspotenzial wird vom Tester nicht gesucht.

Um die Wirksamkeit von kombinierten Systemen wie Anti-Viren-System, IDS (Intrusion Detection Systems) und Firewall unter realistischen Bedingungen zu testen, kommt man um Ethical Hacking nicht herum.

Direkt oder indirekt

Die Methoden des Ethical Hacking lassen sich grundsätzlich in zwei Kategorien einordnen. Die erste Kategorie verfolgt einen direkten Ansatz und kommt zum Zug, wenn das Untersuchungsobjekt Sicherheitslücken aufweist, welche es dem Tester direkt ermöglichen, die vordefinierten Ziele wie Speicherung oder Löschung einer bestimmten Datei auf dem Zielsystem als Beweis der gelungenen Attacke zu erreichen. In diese Kategorie fallen alle «Buffer Overflow»-, «Brute Force»-, «Denial of Service»-Attacken und das «Sniffing». Im Gegensatz dazu wird beim indirekten Ansatz die (un)freiwillige, aktive Hilfe eines «Komplizen», welcher autorisierten Zugriff auf das Untersuchungsobjekt hat, benötigt. Dies kann ein normaler PC-User beim Auftraggeber sein. Auf diese Hilfe muss zurückgegriffen werden, wenn zur Zielerreichung Systeme genutzt werden müssen, welche vom Tester nicht direkt wegen einer Firewall, eines Medienbruchs oder nur mittels grossem Aufwand erreicht und manipuliert werden können.

Ein Praxisbeispiel: Es soll die Wirksamkeit von kombinierten Sicherheitssystemen überprüft werden. Zu diesem Zweck soll versucht werden, einen PC im LAN (Local Area Network) des Auftraggebers via Internet aus der Ferne zu administrieren. Der Erfolgsnachweis muss live gemäss telefonischen Instruktionen erfolgen. Um ans Ziel zu kommen, muss als erstes der Ziel-Computer mit der Serverkomponente eines sogenannten «RAT» (Remote Administration Tool; Trojaner, Back Door) unbemerkt vom Anti-Viren-System, welches die üblichen RATs erkennt und eliminiert, infiziert werden. Bei Erfolg versucht das infizierte System als nächstes durch die Firewall hindurch Kontakt mit der zugehörigen Steuerkomponente auf dem System des Testers aufzunehmen. Es bricht aus dem Netzwerk durch die Firewall aus. Falls dies gelingt und die Verbindung steht, kann der Ziel-Rechner vom Tester administriert werden und das Ziel wurde erreicht. Die Arbeit des Sicherheitsexperten ist damit getan. Im Anschluss daran dokumentiert er das Vorgehen und schlägt der Auftraggeberin entsprechende Gegenmassnahmen vor.

Nutzenoptimierung

Wer das Kosten-Nutzen-Verhältnis optimieren will, sollte die Stärken der verschiedenen Testtypen kombinieren. Vulnerability- und Security-Scans durchforsten das Untersuchungsobjekt mit Hilfe von spezialisierten Tools voll- oder teilautomatisch auf Sicherheitslücken. Dank dieser Automatisierung können in relativ kurzer Zeit verschiedenste Tests auf sämtliche Komponenten des Untersuchungsobjekts durchgeführt werden. Leider finden diese Tools in der Regel nur allgemein bekannte Sicherheitslücken und generieren auch Falschmeldungen – vermeintliche Sicherheitslücken. Ausserdem fehlt diesen Tools die Intelligenz, Sicherheitslücken kontextorientiert zu bewerten. Sofern detektierte Sicherheitslücken manuell verifiziert werden – Definition Security Scan – eignen sich diese Tests dennoch gut für einen ersten Überblick bezüglich des generellen Sicherheitsniveaus des Untersuchungsobjekts.

Schutzmassnahmen

Basierend auf den Ergebnissen des Vulnerability- oder Security-Scans kann nun mittels eines Penetrationtests gezielt nach Sicherheitslücken gesucht werden. Die daraus resultierenden Ergebnisse zeigen vorhandene mögliche Angriffspunkte im Untersuchungsobjekt auf. Mit anderen Worten: Der Auftraggeber weiss, welche Sicherheitslücken von Hackern in welcher Form ausgenutzt werden könnten, um bestimmte Ziele beziehungsweise Effekte zu erreichen. Falls die Wirksamkeit von kombinierten Sicherheitssystemen überprüft werden soll und noch Projektbudget zur Verfügung steht, ist Ethical Hacking im Anschluss daran sinnvoll. Die Vorgehensweise nach diesen drei Schritten – Vulnerability- oder Security-Scans, Penetrationtests und Ethical Hacking – stellt sicher, dass monetäre und personelle Ressourcen und Tools optimal eingesetzt werden. Der Auftraggeber kann gezielt IT Risk Management betreiben und bestimmen, wie er welchen Risiken zu begegnen gedenkt.

Das perfide an Hackerattacken ist, dass Hacker sich im Normalfall sehr viel Zeit nehmen, um in der Vorbereitungsphase passiv oder aktiv Informationen zu sammeln. Dies kann mittels Information Gathering oder Social Engineering geschehen und wird vom Opfer oftmals nicht bemerkt. Diese Phase kann sich über Wochen, Monate oder sogar Jahre hinziehen. Nachdem der Hacker alle für den eigentlichen Hackerangriff benötigten Informationen wie Netzwerkplan, Betriebssysteme, Firewall- und IDS-Typen und -Konfigurationen, mögliche Zielpersonen, Arbeitszeiten der Sicherheitsadministratoren gesammelt hat, schlägt er für das Opfer unvermittelt zu. Aus diesem Grund sollten die Abwehr- und Schutzmassnahmen im Sinne des IT-Riskmanagements ganzheitlich betrachtet werden. Da der Mensch nach wie vor die grösste Sicherheitslücke darstellt, sind die Prävention sowie widerspruchsfreie Sicherheitskonzepte und -Policies bei Unternehmen die wirkungsvollsten organisatorischen Massnahmen. Das Sicherheitsbewusstsein der Mitarbeiter muss gezielt gefördert werden. Bei den technischen Massnahmen nützen die besten und teuersten Firewalls, Anti-Viren-Systeme, IDS und IPS (Intrusion Prevention Systems), Proxies und gehärteten Systeme nichts, wenn kein aktives Update- und Patchmanagement betrieben wird. Ausserdem nützt es wenig, wenn Hackerattacken erst im Nachhinein an Hand von ausgewerteten Logfiles erkannt werden. Bei laufenden Angriffen zählt jede Minute. Aus diesem Grund ist ein Notfallhandbuch, ein gut ausgebildetes, eingespieltes und gut trainiertes Abwehrteam mitsamt den nötigen Handlungskompetenzen bei grösseren Organisationen und Unternehmen heutzutage eine Selbstverständlichkeit. Kleinere Betriebe müssen dabei nicht hinten anstehen: Diese Dienstleistungen können sie bei spezialisierten Outsourcern einkaufen.

Rechtlicher Exkurs

Jegliche Ausführung von «Sicherheitsüberprüfungen» ohne die ausdrückliche Genehmigung des Eigentümers und des Betreibers des zu untersuchenden Systems sind strafbar. Da beim Ethical Hacking sogar das Untersuchungsobjekt willentlich manipuliert und modifiziert wird, sollte Projektauftrag, Projektteam, Untersuchungsobjekt, Ziele, Methodik, Zeitfenster, Form und Granularität der Dokumentation sowie sämtliche Eventualitäten vertraglich zwischen Auftraggeber und Tester genauestens festgehalten werden. Falls der indirekte Ansatz gewählt wird, sollte der «Komplize» vor der Durchführung des «Hackerangriffs» genannt und vor den rechtlichen Folgen wie Ahndung des Verstosses gegen die geltende Security Policy seiner Tat – aktives Einschleppen von bösartigem Code – geschützt werden. Oft ist es sinnvoll, wenn ein Mitglied des Managements den «Komplizen» mimt.

Info/http://www.oneconsult.com
http://www.cdcit.ch

*Christoph Baumgartner ist Geschäftsführer der auf IT-Riskmanagement (IT-Security) spezialisierten Oneconsult und Head of IT Consulting bei der CDC IT.

Dossier: IT-Sicherheit

Sicherheitschecks in der Grauzone

Fredy Haag

Ethical Hacking wird mit Fug und Recht die Königsdisziplin der IT-Sicherheitsüberprüfungen genannt, denn es geht ans Eingemachte. Im Gegensatz zu Hackern und Crackern, die sich unbefugt an elektronischen Systemen zu schaffen machen und zum Teil gezielt Informationen klauen oder manipulieren, wird der Ethical Hacker von Unternehmen beauftragt, Informationslecks aufzuspüren und zu dokumentieren. Dabei bedient er sich der gleichen Kanäle, wie sie auch von unerwünschten Eindringlingen genutzt werden – Web, Telefon und Hacking-Tools.

Der Eigentümer als auch der Betreiber des zu untersuchenden Systems müssen explizit ihren Segen dazu geben. Ansonsten macht sich auch ein sogenannter ethischer Hacker strafbar. Grundsätzlich unterscheidet man beim Ethical Hacking zwei Ansätze. Beim direkten Ansatz wird mit allerlei Werkzeugen versucht, ins System einzubrechen. Im Gegensatz dazu werden beim indirekten Ansatz menschliche Schwächen ausgenutzt, um ans Ziel zu gelangen. Bei dieser perfiden Art der Informationsbeschaffung empfiehlt es sich, einen Projektmitarbeiter oder ein Mitglied der Geschäftsleitung als Zuträger zu bestimmen. Vor allem muss der Betreffende vor den rechtlichen Folgen, die ein Verstoss gegen die geltende Security Policy vorsieht, geschützt werden. Das Projektziel sollte ja sein, auswertbare Informationen und Schwachstellen aufzudecken und nicht für die Entlassung von Mitarbeitern zu sorgen.

In dieser Ausgabe: Hacken im Dienste der Systemsicherheit, Seite 7; Das höchste Ziel bleibt die Sicherheit und Rechtliches bei Sicherheitschecks, Seite 9.