Der ultimative Pentest

Red-Team-Assessments – „echte" Angriffe für mehr Sicherheit

Beim Versuch, sich ein vollständiges Bild über alle möglichen Schwachstellen zu machen, bleiben bisweilen blinde Flecke. Red-Team-Assessments begnügen sich mit der Suche nach dem Übersehenen, dem leichtesten Weg zu sensiblen Unternehmensdaten – ganz so, wie es ein wirklicher Angreifer täte.

Von Michael Brügge, Heilbronn

Kein typischer Arbeitsbeginn für die IT-Sicherheit: Draußen dämmert es noch und leichter Nebel liegt über den umliegenden Feldern. Mein Kollege und ich sind mit dem Auto vom Hotel zu unserem Zielobjekt unterwegs – eine halbe Stunde später parken wir das Auto etwas entfernt auf einem Parkplatz. Ausgestattet mit Anzug und einer Aktentasche voller nützlicher Gadgets gehen wir die letzten paar Meter zu Fuß. Der einzige Weg führt uns vorbei an einem Mitarbeiter des Sicherheitspersonals; er schaut flüchtig auf unsere gefälschten Mitarbeiterausweise und lässt uns aufs Gelände.

Das Hauptgebäude unseres Kunden liegt direkt vor uns. Doch anstatt geradeaus hineinzugehen, biegen wir nach rechts ab und betreten das Treppenhaus der Tiefgarage. Ein Stockwerk tiefer drückt der Kollege den Nottaster des Fluchtwegsicherungssystems und die daneben liegende Tür lässt sich öffnen. Als die schwere Sicherheitstür hinter uns ins Schloss fällt, ist der schrille Alarm nur noch leise zu hören. Wir betreten den nächsten Fahrstuhl, mischen uns unter die Mitarbeiter und lassen unsere Blicke schweifen. Das anwesende Sicherheitspersonal verhält sich ruhig und alles läuft normal. Jetzt kann es so richtig losgehen ...

Was sich wie der Anfang eines Krimis liest, ist Teil der Durchführung eines Red-Team-Assessments. Bereits aus dieser ersten Beschreibung lässt sich erahnen, dass die Durchführung eines solchen Projekts sich nicht für jedes Unternehmen eignet. Dennoch häufen sich die Anfragen nach Prüfungen dieser Art bei spezialisierten Dienstleistern in den letzten zwei Jahren merklich.

In gewisser Weise kann der Eindruck entstehen, dass Red-Teaming zu einer Art Modeerscheinung geworden ist. Bei vielen Anfragen nach Red-Teaming lässt sich allerdings bereits in einem ersten Abstimmungstelefonat feststellen, dass es weniger um die Durchführung eines wirklichen Red-Team-Assessments als um eine Sicherheitsüberprüfung geht. Doch worin liegen die Unterschiede?

Abgrenzung zur Sicherheitsüberprüfung

Ein Red-Team-Assessment zielt auf die Simulation realer Angriffe, sprich die Abbildung einer möglichst realistischen Bedrohungslage ab. Das bedeutet, dass beim Red-Teaming der Rahmen (Scope) nicht oder nur sehr begrenzt eingeschränkt wird: Das sogenannte Red-Team bereitet Angriffe vor und führt sie auch durch.

Bei einer Sicherheitsüberprüfung wird der Gegenstand der Betrachtung hingegen meist stark beschränkt, beispielsweise auf eine konkrete Webanwendung oder auf ein bestimmtes Netzwerksegment. Zudem verfolgt die Sicherheitsüberprüfung in der Regel das Ziel, ein möglichst vollständiges Bild über die Schwachstellen des Betrachtungsgegenstands zu liefern – ein aktives Ausnutzen der Schwachstellen erfolgt in diesem Rahmen meist aber nicht. Klassische Sicherheitsüberprüfungen berücksichtigen zudem in der Regel weder die physische Sicherheit noch das Thema Social-Engineering.

Ein Red-Team-Assessment sucht stattdessen bewusst nach relevanten Schwachstellen, um diese anschließend sinnvoll zu verketten und auszunutzen. Dabei geht es gerade *nicht* darum, ein vollständiges Schwachstellenbild zu erzeugen, sondern den Weg des geringsten Widerstands zu gehen. Oder mit anderen Worten: Es geht darum, den ersten Dominostein zu Fall zu bringen und so den Zugriff auf sensible interne Ressourcen zu ermöglichen. Dabei ist es egal, ob es sich um eine technische Schwachstelle in angebotenen Diensten handelt oder der

Zugriff durch Lücken in der physischen Sicherheit oder fehlende Sensibilisierung der Mitarbeiter möglich wird. Ein weiteres Ziel eines Red-Team-Assessments ist zudem meist, auch die Fähigkeiten der Verteidiger (Blue Team) zu prüfen beziehungsweise zu trainieren.

Letztlich ermöglicht es ein Red-Team-Assessment, den Sicherheitsstatus eines Unternehmens oder einer anderen Organisation unter realistischen Bedingungen zu evaluieren und Probleme in Prozessen oder getroffenen Schutzmaßnamen zu entdecken. Besonders durch die verkettete Ausnutzung von Schwachstellen erlangt man häufig erst eine neue Sicht auf den aktuellen Sicherheitszustand, der möglichweise durch eine zu enge Einzelbetrachtung von Systemen zuvor nur unvollständig wahrgenommen wurde.

Zielgruppe für Red-Teaming

Bedingt durch den offenen Scope und die offene Herangehensweise eignet sich die Durchführung eines Red-Teamings nicht für jede Organisation. So ist es beispielsweise wenig sinnvoll, ein Red-Team-Assessment durchzuführen, wenn einem die sprichwörtlich offenen Scheunentore zu seinem Unternehmen bereits bekannt sind. Diese würden für das Red-Team den Weg des geringsten Widerstands bedeuten und der Erkenntnisgewinn wäre dementsprechend gering.

Die Zielgruppe für Red-Teaming sollte vielmehr einen hohen und umfassenden Reifegrad in der Informations- und IT-Sicherheit aufweisen – das umfasst besonders auch die folgenden Punkte:

- physische Sicherheit
- Netz- und Infrastruktursicherheit
- Endgerätesicherheit
- Awareness für Social-Engineering bei allen Mitarbeitern

Abhängig von Reifegrad und Größe eines Unternehmens können simulierte Angriffe eines Red-Team-Assessments nicht nur durch einen externen Dienstleister, sondern auch durch ein unternehmenseigenes Team durchgeführt werden. Heute erfolgen jedoch die meisten Red-Team-Assessments zumindest mit externer Unterstützung.

Ablauf eines Red-Team-Assessments

Ein Red-Team-Assessment lässt sich in vier wesentliche Projektphasen unterteilen:

- Vorbereitung und Kick-off
- Informationsbeschaffung und Angriffsplanung
- Schrittweise Durchführung des Red-Team-Assessments
- Nachbereitung, Dokumentation und „Lessons Learned"

Phase 1 – Vorbereitung und Kick-off

Alles beginnt mit einem gemeinsamen Kick-off, an dem alle relevanten Personen teilnehmen. Dazu zählen neben den Red-Team-Mitgliedern in der Regel der Projektleiter, der Leiter der physischen Sicherheit, Leiter der Corporate-Security sowie der CISO (o. Ä.) des beauftragenden Unternehmens. Grundsätzlich gilt: Der eingeweihte Personenkreis sollte möglichst klein gehalten werden, um die Ergebnisse durch unnatürliches Verhalten nicht zu verfälschen. Es sollte also kein Zettel mit dem Inhalt „Heute Red-Teaming: Bitte seien Sie wachsam und sensibel!" am schwarzen Brett hängen.

Der Kick-off dient vor allem auch der Festlegung grundsätzlicher Rahmenbedingungen:

- Ansprechpartner für das Projekt
- Projektlaufzeiten
- Welche Standorte/Partner/Systeme sind tabu?
- Welche Vorgehensweisen sind nicht erlaubt?

Ansprechpartner des Projekts sollten laufend über den Stand der Durchführung sowie die nächsten Schritte informiert werden. Zum einen, damit sie einen Überblick behalten, zum anderen aber auch eingreifen können, sofern etwas schieflaufen sollte – zum Beispiel wenn ein durchführender Red-Teamer vor Ort vom Sicherheitspersonal erwischt wird.

Die Projektlaufzeiten werden ebenfalls in diesem Meeting fixiert und sollten großzügig bemessen sein: Idealerweise veranschlagt man eine Laufzeit von ungefähr sechs Monaten, um die Angriffsfläche nicht künstlich zu beschränken. Denn einige Angriffe brauchen lange Vorbereitungszeit, beispielsweise zum Einschleusen von Mitarbeitern über den Bewerbungsprozess oder die Beschaffung spezieller Werkzeuge. Zudem dürfen etwa gezielt registrierte Domains für Phishing-E-Mails nicht zu neu sein, damit versendete E-Mails nicht schon am Gateway abgelehnt werden. Auch öffentliche Firmenveranstaltungen können so in diesen Zeitraum fallen und dafür sorgen, den Zutritt zum Betriebsgelände zu erleichtern.

Obwohl ein Red-Team-Assessment einen sehr offenen Scope hat, ist es dennoch sinnvoll, bestimmte Grenzen festzulegen, die nicht überschritten werden dürfen. Aber Achtung: Zu starke Einschränkungen schieben den Red-Team-Ansatz schnell in Richtung Sicherheitsüberprüfung und das eigentliche Ziel wird verfehlt! Typischerweise

wird für ein Red-Team-Assessment auch kein detaillierter Testplan erstellt, da sich die konkreten Angriffe erst in der folgenden Phase entwickeln und somit nicht im Vorfeld zu benennen sind.

Phase 2 – Informationsbeschaffung und Angriffsplanung

In der zweiten Projektphase holt das Red-Team zunächst umfassende Informationen über die zu testende Organisation beziehungsweise das Unternehmen ein. Dazu zählen allem voran:

_____ Standorte und ihre Absicherung
_____ IP-Adressbereiche
_____ eingesetzte Technik
_____ Organisationsstrukturen und Mitarbeiter
_____ Partner und Dienstleister
_____ Veranstaltungen und Termine

Für die Informationsbeschaffung werden unterschiedliche öffentliche Quellen herangezogen und zu einem Gesamtbild kombiniert: Detaillierte Informationen finden sich dabei häufig bereits auf der Unternehmenswebsite – und dienen dann als Ansatzpunkte für Recherchen in Social-Media-Netzwerken, Kartendiensten und beispielsweise Projektreferenzlisten von Dienstleistern.

Identifizierte IP-Adressbereiche sollten dabei mit einem Projektansprechpartner abgeglichen werden, um versehentliche Angriffe auf Unbeteiligte auszuschließen und möglichen rechtlichen Konsequenzen entgegenzuwirken.

Neben der passiven Informationsbeschaffung über öffentliche Quellen erfolgt zudem ein aktives Sammeln von Informationen durch Netz- und Schwachstellenscans und in der Regel auch E-Mail-Anfragen, Telefonanrufe oder Begehungen von Standorten. Bereits in dieser Phase werden in der Regel Social-Engineering-Techniken eingesetzt, denn mit einer guten Geschichte geben Menschen schneller interessante Informationen preis. Die gesammelten Informationen bilden die Grundlage für die Planung des weiteren Vorgehens.

Phase 3 – Schrittweise Durchführung des Red-Team-Assessments

Basierend auf den gesammelten Informationen und der bisherigen Angriffsplanung geht es anschließend an die Durchführung. Dabei gilt es, in einem ersten Schritt den sprichwörtlichen Fuß in die Tür zu bekommen: Das kann wie zu Beginn des Artikels beschrieben durch das Ausnutzen von Schwachstellen in der physischen Sicherheit erfolgen, aber auch durch den Einsatz von Social-Engineering-Techniken oder einen Angriff auf externe Systeme und Dienste geschehen.

Ziel ist regelmäßig das Einschleusen eines eigenen Geräts in das interne Netzwerk oder die erfolgreiche Kompromittierung eines ersten Systems, das anschließend als Ausgangspunkt für weitere Angriffe und die Ausbreitung im Netzwerk dient, um so letztlich Zugriff auf sensible Daten des Unternehmens zu erlangen.

Zum Umgehen der Zutrittskontrolle kommen verschiedenste Techniken und Werkzeuge zum Einsatz. Im simpelsten Fall wird eine Tür von einem Keil offen gehalten und der Weg ist frei, aber auch das Klonen von RFID-Karten oder der Einsatz von Lock-Picking-Werkzeugen ist situationsbedingt sinnvoll. Hat man Zutritt zu einem Gebäude erlangt, ist der nächste Schritt in der Regel das Platzieren eines eigenen Geräts im Netzwerk oder die Kompromittierung eines Mitarbeiter-PCs. Damit fremde Geräte nicht auffallen, können diese beispielsweise als Netzteile getarnt in einem Bodentank oder im Kabelgewirr unter einem Schreibtisch versteckt werden.

Abbildung 1 zeigt beispielhaft ein umgebautes Netzteil, das statt eines Ladesteckers einen RJ45-Stecker zum Anschluss an die Netzwerkdose besitzt. Über die Stromversorgung werden dann der enthaltene Raspberry Pi Zero sowie ein LTE-Modem mit Energie versorgt. Mit diesen Komponenten können die Angreifer aus dem Internet auf dieses unauffällige Gerät zugreifen.

Aber interne Systeme lassen sich auch durch den Einsatz von Social-Engineering-Techniken kompromittieren, beispielsweise indem man Mitarbeiter unter dem Vorwand, „etwas drucken zu müssen", bittet, einen USB-Stick in ihren PC zu stecken. Dass es sich dabei nicht um einen regulären USB-Massenspeicher, sondern um ein spezielles USB-Gerät zur Kompromittierung des Systems handelt, fällt vielen Personen erfahrungsgemäß nicht auf. Auch der Einsatz von WiFi-Keyloggern ist möglich: Diese zeichnen – sind sie erst einmal zwischen PC und Tastatur gesteckt – alle Tastendrücke auf und können über WLAN ausgelesen werden.

In vielen Fällen sind Angriffe vor Ort jedoch gar nicht nötig, denn oft führen bereits gezielte Phishing-E-Mails zur erfolgreichen Kompromittierung eines internen Clients. Dass extern erreichbare Systeme schwerwiegende Schwachstellen aufweisen, die sich im Rahmen eines Red-Team-Assessments ausnutzen lassen, kommt hingegen seltener vor – denn häufig werden genau diese Systeme regelmäßigen Sicherheitsüberprüfungen unterzogen. Unabhängig davon, über welchen Weg ein internes System kompromittiert wurde, erfolgt anschließend

– sofern nötig – die Erweiterung der Rechte und die Suche nach weiteren Zielen im Netzwerk.

So wie bei unserem Kunden aus der eingangs beschriebenen Szene: Nachdem mein Kollege und ich uns unter die Mitarbeiter gemischt haben, machen wir uns auf die Suche nach einem VoIP-Telefon – schnell werden wir fündig. Wir notieren uns seine MAC-Adresse und konfigurieren den Raspberry Pi im mitgebrachten umgebauten Netzteil (vgl. Abb. 1) mit der MAC-Adresse des Telefons. Mein Kollege zieht das Netzwerkkabel des Telefons aus der Wanddose und steckt stattdessen unser Gerät an. Über das eingebaute LTE-Modem prüfen wir, ob sich unser Gerät erfolgreich mit dem Netzwerk verbunden hat. Jetzt nur noch einen Zettel mit „Defekt. Techniker ist informiert" auf das Telefon kleben und das umgebaute Netzteil im Kabelgewirr verstecken. Der vom eingeschleusten Gerät durchgeführte Netzwerkscan servierte uns anschließend einen internen Tomcat-Server mit aktiver Management-Oberfläche und Standardpasswörtern. Ab da war alles ein Kinderspiel ...

So einfach läuft es zwar nicht immer, aber genau dieses Beispiel zeigt die Vorzüge eines Red-Team-Assessments, da man häufig Schwachstellen genau dort entdeckt, wo sich vorher ein blinder Fleck befand (siehe unten).

Phase 4 – Nachbereitung, Dokumentation und „Lessons Learned"

Da Red-Team-Assessments in produktiven Umgebungen erfolgen, sind nach der Durchführung der Angriffe alle Änderungen an Systemen rückgängig zu machen. Dazu ist es wichtig, alle durchgeführten Schritte entsprechend detailliert zu dokumentieren – ein entsprechendes Protokoll sollte dem Kunden zusammen mit der Dokumentation ausgehändigt werden.

Um in Zukunft Angriffe besser erkennen und verhindern sowie Schwachstellen beheben zu können, sollten im Nachgang die Ergebnisse des durchgeführten Red-Team-Assessments gemeinsam detailliert besprochen werden. An diesem Workshop sollte das Blue Team ebenfalls teilnehmen, um einen direkten Wissenstransfer zu ermöglichen.

Beim Kunden aus dem eingangs beschriebenen Szenario standen wir drei Wochen später vor etwa 15 Personen in einem großen Besprechungsraum – auf der Folie hinter uns sind das umgebaute Netzteil sowie die Ergebnisse des Netzwerkscans zu sehen. Ein Klick auf den Presenter und die nächste Folie skizziert den Weg zum Tomcat, der mit Systemrechten auf einem veralteten Windows-Server läuft. „Das Testsystem hatten wir nicht auf dem Schirm", berichtet ein Mitarbeiter aus dem Infrastruktur-Team seinen Kollegen. Die Verwendung von Standardpasswörtern ermöglichte den Zugriff auf den aktiven Tomcat-Manager zur Verwaltung des Servers, erklärt mein Kollege und fährt mit der Erläuterung des Vorgehens fort. Über eine neu ausgerollte Webanwendung konnten beliebige Dateien auf den Server kopiert, dank der weitreichenden Berechtigungen des Tomcat-Servers jegliche Betriebssystemkommandos abgesetzt werden. Dadurch war es möglich, die Anmeldeinformationen der Benutzer auszulesen – darunter auch die Zugangsdaten eines Mitarbeiters mit administrativen Berechtigungen für die Windows-Domäne. Damit konnten wir das Kartenhaus vollends zum Einsturz bringen.

Als mein Kollege und ich nach dem Abschlussworkshop mit dem Auto vom Gelände fahren, liegt kein Nebel mehr über den Feldern. Und auch das getestete Unternehmen sieht nun klarer. ■

Michael Brügge ist Senior Berater bei cirosec.

Abbildung 1: In dem vielfach üblichen Kabelgewirr unter oder auf Schreibtischen fällt ein eingeschleustes zusätzliches „Netzteil" meist nicht auf – hier ein Spionagesystem mit Minicomputer Raspberry Pi Zero (1), LTE-Modem (2), USB-Netzwerkadapter (3) und Spannungsversorgung (4).