Foto: © alphaspirit – Fotolia.com

II Der digitalen Lücke auf der Spur: Pentester untersuchen Unternehmen auf Sicherheitslecks.

Angriff auf Abruf

Wie Jens Liebchen und seine Mitarbeiter als Penetrationstester Unternehmen auf deren IT-Sicherheit überprüfen

Foto: Redfeam Pentesting GmbH

II Attackiert Unternehmen ohne Böses im Sinn: Jens Liebchen ist als Pentester unterwegs.

Eine Sicherheitslücke gibt es eigentlich immer, irgendwo. Wenn Jens Liebchen zum „Angreifer" wird, findet er sie ganz bestimmt. Manchmal spürt er sie direkt auf, manchmal dauert es Tage oder Wochen, bis er auf die richtige Fährte gerät und die Schwachstelle knackt. – Nein, Jens Liebchen, 34, ist kein „Hacker". Im Gegenteil: Er arbeitet als „Penetrationstester". Liebchen ist also vielmehr der klassische Gegenspieler des „echten" Angreifers. Mit den Kollegen seiner in Aachen ansässigen RedTeam Pentesting GmbH hat er sich darauf spezialisiert, die Sicherheit von IT-Systemen und der dort gespeicherten Daten zu überprüfen.

Die Methode dazu wird im Fachjargon als Penetrationstest – kurz: „Pentest" – bezeichnet und steht für den kontrollierten Versuch, von außen in ein IT-System einzugreifen, um mögliche Schwachstellen aufzudecken. Tester wie Jens Liebchen versetzen sich bei der Methode bewusst in die Rolle des Angreifers, um die Unternehmen so gut wie möglich vor einem Ernstfall zu bewahren.

Dieser realitätsnahe Ansatz hat anfangs Kritik geerntet. Die Gegner befürchteten, dass die Tester ihr Know-how missbrauchen könnten. Liebchen hat dazu eine klare Meinung: „Nur wer angreifen kann, kann auch verteidigen."

Der Informatiker stieß erstmals während seines Studiums an der RWTH Aachen auf die Methode. In einer Forschungsgruppe wirkte er damals an der wissenschaftlichen Weiterentwicklung von Pentests mit. Schon bald wurden die ersten Betriebe auf das Team aufmerksam. „Wir mussten so schnell wie möglich ein Unternehmen gründen, um einen rechtlichen Rahmen zu schaffen und unsere Dienstleistung anbieten zu können", erzählt er. Im Oktober 2005 wurde die Forschergruppe zunächst zur eigenständigen Abteilung der Nomis Development GmbH, bevor sie ein Jahr später die RedTeam Pentesting GmbH gründete. Von dem Konzept, sich allein auf Pentests zu konzentrieren, ist Liebchen noch immer überzeugt: „Es ist ein sehr spannendes, abwechslungsreiches Feld, bei dem wir Einblicke in viele neue Technologien bekommen." Weitere Dienstleistungen bietet RedTeam Pentesting bewusst nicht an, um den unabhängigen Charakter der Tests zu wahren: „Wir schlagen den Betrieben am Ende zwar auch Lösungen vor", sagt Liebchen, „aber die sind nicht an weitere Angebote unseres Unternehmens geknüpft."

> *„Man glaubt gar nicht, wie oft der Firmenname als Passwort verwendet wird."*
>
> *Jens Liebchen, Geschäftsführer der RedTeam Pentesting GmbH*

Die Tests des achtköpfigen Teams sind national und international gefragt. Über die Kunden schweigt Liebchen allerdings „wie ein Grab" – das sei ein wichtiger Teil der Geschäftsvereinbarung. Nur so viel verrät er: „Wir sind für keine bestimmte Branche tätig. Es kann ein Riesenkonzern sein, der uns beauftragt, oder das kleine Unternehmen von nebenan." Der Informatiker hält es für einen Mythos, dass von Industriespionage nur „die Großen" betroffen sind. „Die meisten Fälle werden gar nicht öffentlich. Sie würden einen zu großen Image-Schaden verursachen", sagt er. „Das können sich vor allem kleine Firmen nicht leisten, die sind in so einem Fall schnell weg vom Markt." Mit der technischen Weiterentwicklung steige auch die Zahl der Aufträge für Liebchen und seine Kollegen. „Mittlerweile sind Betriebe an Stellen angreifbar, die sie gar nicht erwarten", sagt der Pentester.

Welcher Bereich in einem Unternehmen getestet werden soll und über welchen Zeitraum hinweg, klären die Pentester mit den Auftraggebern im Vorfeld. Zu den klassischen Zielsystemen gehören neu entwickelte Online-Shops oder Kundendatenbanken. In der ersten Phase, der „Reconnaissance", sammeln die Mitarbeiter zunächst Informationen über das Unternehmen. Neben technischen Hinweisen auf IP-Adressbereiche, Netzwerkstrukturen, Hardware oder Passwörter können auch Örtlichkeiten sowie organisatorische und soziale Strukturen nützlich sein, um in Phase zwei zu starten: die „Enumeration". Hierbei deckt das Team mit Hilfe der Recherche-Ergebnisse mögliche Schwachstellen auf – zum Beispiel einen unsicheren Passwortschutz. „Man glaubt gar nicht, wie oft der Firmenname als Passwort verwendet wird", verrät Liebchen, der es in der Regel aber mit schwierigeren Fällen zu tun hat.

„Besonders in der zweiten Phase muss der Tester kreativ sein", sagt Liebchen. Nur mit der richtigen Idee zum richtigen Zeitpunkt könne er eine Zugriffsmöglichkeit auf das System finden. „Damit wir die Kreativität der einzelnen Pentester optimal bündeln und einsetzen können, arbeiten wir grundsätzlich in wechselnden Teams. So schleichen sich keine starren Abläufe ein." Haben die Tester mögliche Fehlerquellen ausgemacht, geht es in der dritten Phase – der „Exploitation" – darum, diese Feh-

lerquellen zu verifizieren oder zu widerlegen. Liebchen und seine Kollegen gehen jetzt zur „Attacke" über. „Der erste Einsatz ist natürlich für jeden Pentester enorm aufregend", sagt Liebchen: „Da geht der Puls nach oben." Inzwischen sind die Einsätze zur Routine geworden. Auch das Eindringen in den Serverraum gehört zum Arbeitsalltag. Den Testern ist bewusst, dass sie als Angreifer alle Sicherheitslücken ausnutzen müssen, damit ihre Kunden diese am Ende auch schließen können.

Die Angriffstechniken sind vielfältig und werden passend zur jeweiligen Schwachstelle ausgewählt. Neben technischen Angriffen auf das Netzwerk werde selten auch das „Social-Engineering" angewandt. Hierbei nutzt der Tester menschliche Schwächen aus, um Zugang zum Zielsystem zu erhalten. „Wir führen hier gerade eine Sicherheitsprüfung im Auftrag der Geschäftsleitung durch", könnte es in so einem Fall seitens des getarnten Pentesters heißen: „Ich notiere Ihren Namen, damit ich Sie lobend erwähnen kann. Bitte behalten Sie über die Prüfung Stillschweigen, damit wir weitertesten können." Indem der „Angreifer" also falsche Tatsachen vorspiegelt und so das Vertrauen des Mitarbeiters gewinnt, gelangt er an Daten, zu denen er sonst keinen Zugang hätte. „Diese Technik wenden wir in der Regel nur in Bereichen der Hochsicherheit an", sagt Liebchen, der sich bei dieser Entscheidung mit seinen Kollegen nach der Empfehlung des Bundesamts für Sicherheit in der Informationstechnik (BSI) richtet. Grund sei, dass sich nichtbetroffene Mitarbeiter meist nur schwer in die Lage des „angegriffenen" Kollegen versetzen könnten. Hinzu komme, dass sich der betroffene Mitarbeiter von der Geschäftsleitung hintergangen fühlt. „Das kann seine Einstellung zur Arbeit und das Betriebsklima nachhaltig schädigen", sagt Liebchen.

„Mittlerweile sind Betriebe an Stellen angreifbar, die sie gar nicht erwarten."

Jens Liebchen,
Geschäftsführer der RedTeam Pentesting GmbH

In der letzten Phase, der „Documentation", erstellt das Team einen Abschlussbericht und demonstriert dem untersuchten Unternehmen die Schwachstellen seines IT-Systems anhand einer Live-Performance. „Diese Vorführung ist sehr wichtig, damit die zuständigen Mitarbeiter genau nachvollziehen können, wo die Sicherheitslücken liegen", erklärt Liebchen. „Meistens sind die Auftraggeber erst mal entsetzt, wenn sie sehen, wie unsicher ihr System ist." Umso größer ist die Erleichterung nach dem ersten Schock – mit dem Wissen darüber, wie ein Angriff vermieden werden kann. Erleichtert sind am Ende solch einer verdeckten Ermittlung auch Jens Liebchen und seine Kollegen. Dann können sie ihre Angreifer-Rolle wieder ablegen. Bis zur nächsten Sicherheitslücke...

Sarah Sillius

@ www.redteam-pentesting.de

INFO

Die drei Angreifer-Typen: „Hacker", „Cracker" und „Script Kiddy"

In der medialen Berichterstattung wird der Begriff „Hacker" meist pauschal für alle Angreifer von IT-Systemen verwendet. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterscheidet in einer Studie zur Durchführung für Penetrationstests zwischen drei Täterprofilen: Der „Hacker" wird als experimentierfreudiger Programmierer betrachtet, der sich aus technischem Interesse mit Sicherheitslücken in IT-Systemen auseinandersetzt. Beim „Script Kiddy" handelt es sich um einen Täter, der ohne großes Fachwissen und eher aus Neugier weitestgehend vorgefertigte Angriffs-Tools aus dem Internet anwendet. Der „Cracker" hingegen ist eine Person, die sich aus krimineller Energie der Schwachstellen von IT-Systemen bedient, um dadurch rechtswidrige Vorteile oder gesellschaftliche Aufmerksamkeit zu erlangen. Er wird auch als „Insider" bezeichnet. Häufig handelt es sich um einen frustrierten (ehemaligen) Mitarbeiter, der seinem früheren Arbeitgeber schaden will. Der „Cracker" wird als besonders gefährlich eingestuft.

Eine ernstzunehmende Bedrohung stellt laut BSI außerdem die Wirtschaftsspionage dar: Hierbei versucht der Angreifer, von Betriebsgeheimnissen – technische Konzepte oder Strategien und Ideen, die einen Wettbewerbsvorteil bedeuten – Kenntnis zu erlangen und zum eigenen Vorteil zu verwenden.

@ https://www.bsi.bund.de