Security Audit

Die Cyber-Abwehr auf dem Prüfstand

Mit Red-Team-Services können Unternehmen ihre Cyber-Abwehr auf die Probe stellen. Solche Hacking-Simulationen helfen in der Praxis nicht nur bei der Erkennung und Bewältigung von Angriffen, sondern stärken langfristig auch die Resilienz.

→ VON CHRISTIAN FICHERA

DER AUTOR

Christian Fichera ist Senior Cyber Security Consultant bei terreActive und Leiter des Teams Audit, Risk & Compliance. Seine Abteilung verfügt über langjähriges Security-Know-how, das unter anderem auf Projekten zu Penetrationstests, Red-Team-Services und Secure Code Review für Unternehmen verschiedener Branchen in der Schweiz basiert.
→ www.security.ch

Dass Unternehmen, Bundesämter oder auch Gemeindeverwaltungen von Hackern attackiert werden und dabei heikle Informationen verloren gehen, ist heutzutage keine Seltenheit mehr – im Gegenteil. Solche Schlagzeilen sind mittlerweile regelmässig in der Presse zu lesen. Ein zuverlässiger Schutz ist deshalb wichtiger denn je und in der modernen Arbeitswelt mit verteilten Infrastrukturen steht zunehmend die Cyber-Resilienz im Fokus. Für Anwender bedeutet das: Die Cyber-Abwehr sollte proaktiv auf den Prüfstand gestellt, bewertet und trainiert werden.

Und genau dafür gibt es in der IT-Security das sogenannte Red Team. Ihm steht das Blue Team gegenüber – in Unternehmen ist das meist das Cyber-Defense-Team oder auch das Security Operations Center (SOC). Das Red Team übernimmt im Rahmen von konkreten Hacking-Simulationen die Rolle eines fingierten Angreifers. Aus dieser Perspektive heraus werden die Abwehrkräfte der entsprechenden Organisation beurteilt. Mit den gewonnenen Erkenntnissen lässt sich diese entsprechend trainieren, damit sie in Zukunft auch einem echten Angriff standhalten kann.

«GET IN, STAY IN, ACT»

Beim Red-Team-Service gibt es keinen «One size fits all»-Ansatz. Er wird immer individuell auf die jeweilige Zielorganisation zugeschnitten und kann sämtliche Ressource einschliessen, die unter ihrer Kontrolle steht – beispielsweise verschiedene Security-Technologien und -Werkzeuge, Personen aller Abteilungen inklusive SOC oder auch Prozesse wie die Alarmierung sowie das Krisenmanagement. Es werden sowohl echte Hacking-Methoden wie Social Engineering eingesetzt, als auch direkte Angriffe auf Anwendungen ausgeführt, die dem Internet ausgesetzt sind.

Ein solches Red-Team-Projekt wird üblicherweise in drei Phasen gegliedert:

1. Vorbereitung inklusive Definition von Zielen und Regeln
2. Ausführung der Hacking-Simulation
3. Debriefing mit Massnahmenempfehlungen

Der zentrale Teil des Projekts, die Ausführung, folgt dem Muster «Get in, stay in, act». Im ersten Schritt setzt das Red Team alles daran, unentdeckt ins Firmennetz einzudringen und in der Infrastruktur Fuss zu fassen.

Gelingt das unbemerkte Eindringen, bewegt sich das Red Team darin und stärkt seine Position innerhalb der Infrastruktur. So findet es die optimale Ausgangslage für seinen Angriff auf die gewünschten Ziele. Das können zum Beispiel Personendaten, Kontonummern oder Konstruktionspläne sein. Schliesslich führt das Red Team seine Operationen durch, etwa indem es Daten entwendet.

UMFASSENDE ÜBERSICHT FÜR CISOS

Wie bei so manchem Service stellt sich möglicherweise auch hier für Unternehmen zuerst einmal die Frage: «Warum brauchen wir das überhaupt?» Nun, CISOs sind auf eine ganze Reihe an Informationen angewiesen, um die Cyber-Abwehr stärken zu können. In welcher Phase wurde die Cyber-Attacke entdeckt? Welche Tools halfen dabei? Wie gut funktionierten die Abwehrmassnahmen?

Auf diese Fragen und noch viel mehr liefert der Red-Team-Service Antworten. Denn bei diesem Service handelt es sich um eine ganzheitliche Analyse, die CISOs und Sicherheitsverantwortlichen eine umfangreiche Übersicht gibt (vergleiche Kasten). Die Prüfung umfasst alle betei-

Bild: iStock/Tommy Lee Walker

Gut gegen Böse: Das Blue Team verteidigt die Firmen-IT während das Red Team den Hacker mimt

ligten Rollen und technischen Komponenten. So wird getestet:

- wo Schwachstellen existieren
- wie gut die Angriffserkennung funktioniert und welche Tools Alarm schlagen
- inwiefern das Blue Team auf den Angriff reagiert
- wie gut die Gegenmassnahmen des Blue Teams greifen
- und wie es allgemein um die Cyber-Resilienz steht.

Bleibt der Angriff unentdeckt, gilt es herauszufinden, welche Technologien dem Blue Team für den zukünftigen Erfolg fehlen oder welche Use Cases eingebunden werden müssen. Letzteres sind Angriffsszenarien, die seitens des SOC gemäss einer Risikobeurteilung erstellt wurden. In einem Playbook – also einer Arbeitsanleitung für das SOC – wird definiert, wie bei den verschiedenen Use Cases zu reagieren ist. Auch dazu können aus der Analyse Rückschlüsse gezogen werden.

FAZIT

Das Red Team hilft den CISOs und Sicherheitsverantwortlichen dabei, ihre Sicherheitslage besser zu verstehen. Und die Verbesserungsmassnahmen geben ihnen die Möglichkeit, ihre Cyber Defense langfristig zu stärken. Nicht zuletzt sind solche Projekte eine gute Gelegenheit, den Prozess des Krisenmanagements mal wieder oder vielleicht sogar erstmalig durchzuspielen. In der Schweiz verfügen nur wenige Security-Anbieter über ein Red und Blue Team zugleich. Dabei sind gerade die Erkenntnisse aus beiden Welten – Angriff und Verteidigung – für die kontinuierliche Prozessoptimierung und den Know-how-Aufbau sehr wichtig. ←

Red-Team-Service versus Penetrationstest

Auf den ersten Blick ähnelt die Methodik von Red-Teams stark jener des Penetrationstests. Es gibt jedoch deutliche Unterschiede – besonders in Bezug auf die Absicht. Der Penetrationstest hat zum Ziel, so viele Sicherheitslücken wie möglich zu finden, sie auszunutzen und den Risikograd jeder Schwachstelle zu beurteilen. Beim Red-Team-Service versuchen die Security-Profis zunächst, sich Zugang zum Firmennetz zu verschaffen. Gelingt dies, bewegen sie sich seitlich durch die Infrastruktur, um auf interessante Daten zugreifen zu können. Im Zentrum steht dabei die Frage, ob und wie schnell die interne IT den Angriff erkennen kann, um im Nachgang die Cyber Defense nachhaltig zu stärken.

Der Red-Team-Service eignet sich für mittlere und grosse Unternehmen, die über ein internes oder externes Blue Team verfügen und ihre Cyber-Abwehrkräfte überprüfen und verbessern möchten. Für eine seriöse Vorbereitung, Durchführung und Analyse rechnet ein Security-Dienstleister, der das Red Team aufbietet, mit mindestens 15 Arbeitstagen.