Die Cyberabwehr auf dem Prüfstand

Mit Red-Team-Services können Unternehmen ihre Cyberabwehr 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.

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 Cyberresilienz im Fokus. Für Anwender bedeutet das: Die Cyberabwehr 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 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 Zielorganisation zugeschnitten und kann jede 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.

Üblicherweise wird ein solches Projekt in drei Phasen gegliedert:

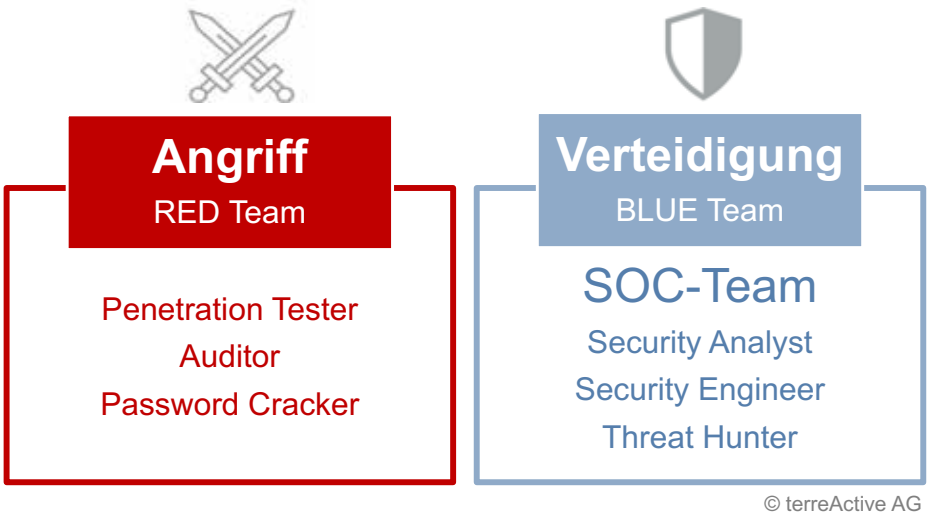
1. Vorbereitung inklusive Definition von Zielen und Regeln
2. Ausführung der Hacking-Simulation
3. Debriefing mit Massnahmenempfehlungen

Der zentrale Teil des Projekts, die Ausführung, folgt jeweils dem Muster «Get in, stay in, act». Im ersten Schritt setzt das Red Team alles daran, um unentdeckt ins Firmennetz einzudringen und in der Infrastruktur Fuss zu fassen. Dazu werden sowohl echte Hacking-Methoden wie Social Engineering eingesetzt als auch direkte Angriffe auf Anwendungen oder Dienste ausgeführt, die dem Internet ausgesetzt sind. Gelingt das unbemerkte Eindringen ins Netzwerk, 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 auch 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 Cyberabwehr stärken zu können. In welcher Phase wurde die Cyberattacke 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 (vgl. Kasten). Die Prüfung umfasst alle beteiligten Rollen und technischen Komponenten. Man untersucht dabei:

- 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



Beim Red und Blue Team zeigt sich, wie viele unterschiedliche Jobprofile allein in diesem Bereich der Cybersecurity benötigt werden. Know-how-Austausch zwischen den Jobprofilen ist dabei ein Muss.
Quelle: Red-Blue-Team/terreActive

- und wie es allgemein um die Cyberresilienz des Unternehmens steht.

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

Red-Team-Service versus Penetrationstest

Auf den ersten Blick ähnelt die Methodik des Red-Team-Services stark jener des Penetrationstests. Bei genauerem Hinschauen offenbaren sich 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. Anders beim Red-Team-Service: Hier versuchen die Security-Profis zunächst, sich Zugang zum Firmennetz zu verschaffen. Gelingt dies, bewegen sie sich seitlich durch die Infrastruktur, um auf die interessantesten Daten zugreifen zu können. Im Zentrum steht dabei stets 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 damit besonders für mittlere und grosse Unternehmen, die über ein eigenes 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.

Fazit

Zusammenfassend lässt sich sagen: Das Red Team hilft CISOs und Sicherheitsverantwortlichen dabei, ihre Sicherheitslage gesamtheitlich besser verstehen zu können. Und die Verbesserungsmassnahmen geben ihnen die Möglichkeit, die Cyber Defense ihres Unternehmens langfristig zu stärken und zu erhöhen. Nicht zuletzt sind solche Projekte auch eine gute Gelegenheit, um den Prozess des Krisenmanagements mal wieder oder vielleicht sogar erstmalig durchzuspielen. In der Schweiz verfügen übrigens nur wenige Security-Anbieter über ein Red wie auch ein 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. ■

TerreActive AG, CH-5001 Aarau
✆ +41 (0)62 834 00 55
info@terreActive.ch, www.security.ch