20

Red Teaming: Angriff ist die beste Verteidigung

Dipl. Ing. Knut Schönfelder – Manager Cyber Risk Services; Deloitte

- Red Teaming ist eine ursprünglich militärische Methode, um Schwachstellen einer Organisation aus Sicht eines Gegners zu analysieren.
- Red Teaming hilft Unternehmen, mögliche Cyber-Angriffe zu identifizieren, ihre Abwehrfähigkeit zu bewerten und sich so besser gegen Angriffe zu schützen.
- Kritisch ist, dass das Red Team an das Führungsgremium eines Unternehmens berichtet und so aus den gewonnenen Erkenntnissen geeignete Maßnahmen abgeleitet werden.

Wer verstehen will, wie gut das eigene Unternehmen auf Cyber-Angriffe vorbereitet ist, muss die möglichen Angriffsarten und deren Auswirkungen kennen. Für bestimmte Branchen gibt es bereits entsprechende gesetzliche Verpflichtungen und wahrscheinlich kommen weitere hinzu. Durch Red Teaming – einer ursprünglich militärischen Methode – identifizieren Unternehmen ihnen bisher unbekannte Risiken und erfahren, wie gut die Schutzmechanismen wirklich funktionieren.

Am Tag nach den Anschlägen des 11. September machte George Tenet, Leiter des US-Auslandsgeheimdienstes CIA, eine ebenso kurze, wie ungewöhnliche Vorgabe: Tenet ordnete die Aufstellung einer CIA Red Cell genannten Einheit an. Deren Auftrag: Das liefern von Informationen, die sonst niemand liefert und die Entscheidungsträgern Sorgen bereiten.

Warum das ungewöhnlich ist? Weil Tenet an sich eine Behörde leitete, deren Hauptaufgabe ohnehin der Gewinn

und die Auswertung von Informationen zur nationalen Sicherheit ist. Nach den verheerenden Anschlägen wollte er jetzt ein Team, dass die bisherige konventionelle Denkweise ebenso radikal wie systematisch in Frage stellt und so die Gefahr weiterer überraschender Terror-Angriffe minimieren sollte.

Diesen ungewöhnlichen Ansatz können sich auch Unternehmen zum Schutz ihrer Datenbestände und Netzwerke zunutze machen. Und zwar durch Planspiele, wie sie schon lange integraler Bestandteil der militärischen Planung sind und in diesem Umfeld als „War Games" bezeichnet werden. Innerhalb eines War Games wird der militärische Gegner – oder die Gruppe, die diese Rolle einnimmt - als Red Team bezeichnet, die Verteidiger sind das Blue Team. George Tenet wollte also ein solches Red Team, um an Einsichten zu gelangen, die ihm die bisherigen Prozesse nicht liefern konnten.

„Tell me things others don´t, and make senior officials feel uncomfortable."[1]
George Tenet, ehemaliger Leiter des CIA

Ausgehend von der zeitlich begrenzten Analyse eines vorher ausgewählten Szenarios im Rahmen eines War Games ist die Praxis des Red Teamings entstanden: Es ist das systematische Anwenden von Analysetechniken aus der Sicht eines Wettbewerbers oder Gegners. Organisationen – neben dem Militär heute auch zivile Unternehmen – prüfen durch Red Teams ihre Annahmen und Pläne kritisch, identifizieren Schwachstellen und erlangen ein besseres Verständnis ihres operativen Umfeldes, insbesondere im Cyber-Umfeld.

Das ist angesichts der zunehmenden Digitalisierung von Geschäftsprozessen dringend nötig, da die Anfälligkeit und der Schutzbedarf der IT-Systeme steigen. Die Herausforderung ist es, mögliche Schwachstellen in den Systemen und Auswirkungen von Angriffen auf diese hochgradig vernetzten IT-Systeme zu erkennen. Neben technischen und organisatorischen Schwachstellen hängt der Erfolg eines Angriffs – genau wie im militärischen Konflikt – von der Vorgehensweise des Angreifer und der Reaktion des Angegriffenen ab.

1 Tenet, George; At the Center of the Storm, o.O., harper Perennial, 2008, S. 185.

„One thing a person cannot do, no matter how rigorous his analysis or heroic his imagination, is to draw up a list of the things that would never occur to him."[2]
Thomas Schelling

Angriff ist die beste Verteidigung

Durch Red Teaming erkennen Organisationen Probleme und gewinnen Erkenntnisse, die im Rahmen einer klassischen, vom Schreibtisch aus angefertigten Analyse unentdeckt bleiben. Der Wirtschaftswissenschaftler und Nobel-Preisträger Thomas Schelling unterstreicht mit seinem „impossibility theorem" das zugrunde liegende Dilemma: Niemand kann eine vollständige Liste derjenigen Ereignisse erstellen, die einem nie wiederfahren werden. Dieser Gedanke trieb – höchst wahrscheinlich – auch George Tenet an, als er die Red Cells formte.

Im Kontext IT-Sicherheit stellt sich die Frage, welchen Angriffen eine Organisation zukünftig ausgesetzt sein könnte, welche Auswirkungen ein erfolgreicher Angriff hätte und wie die Organisation sich wirksam gegen diese Angriffe schützen könnte.

Um diese Fragen angesichts unvollständiger Informationen beantworten zu können, müssen Führungskräfte zwangsläufige Annahmen zu Motivation und Möglichkeiten der Angreifer und eigener Fähigkeiten treffen. Dabei bewerten sie die Situation unweigerlich subjektiv – beeinflusst durch individuelle, organisatorische und kulturelle Einflussfaktoren (Englisch „bias"). Das Grundprinzip des Red Teamings ist es, diese Faktoren offen zu legen. Dazu betrachtet das Red Team Annahmen, Pläne und Konzepte der eigenen Organisation aus der Perspektive eines Gegenspielers, mit dem Ziel, systematisch Schwachstellen und falsche Annahmen zu finden. Die Ausgangsfrage des Red Teams lautet: Was wäre wenn… ? Galten bisher die eigenen Annahmen und Maßnahmen zur Abwehr potentieller Angriffe bis zum Beweis des Gegenteils als angemessen und ausreichend, zwingt das Red Team die eigene Organisation zum Gegenteil: Angesichts eines simulierten Angriffes müssen die

2 Schelling Thomas; The role of war games and exercises, in: Managing Nuclear Operations; A. Carter, J. Steinbrunner und C. Zraket (Hrsg.), o.O., Brookings Institution Press, 1986, S. 436.

eigenen Entscheidungen validiert werden.

Die Auswirkungen von Angriffen verstehen

Den Führungsgremien in Unternehmen kommt dabei eine besondere Bedeutung zu, da sie letztlich Security-Strategien verantworten und das Budget zuteilen. Beim Red Teaming liegt im Gegensatz zu Penetrationstests der Fokus nicht auf der systematischen Identifikation technischer Schwachstellen, sondern vielmehr auf der Analyse von Auswirkungen von Angriffen. Red Teaming eignet sich daher besonders gut, um das Verständnis von Führungskräften für Cyber-Security, also die „Cyber Board Awareness", zu verbessern.

Schwachstellen in den Komponenten und Prozessen zum Schutz der eigenen Datenbestände finden sich nicht vom Schreibtisch aus. Unternehmenslenker sind gut beraten, sich des Konzepts des Red Teamings zu bedienen – und sich selbst anzugreifen.

So wie für einen Angreifer die Schwachstelle nur ein geeignetes Mittel zum Zweck ist, beurteilen Führungskräfte eine Schwachstelle danach, welche negativen Auswirkungen eine Cyber-Attacke auf die Geschäftsprozesse hat, welcher monetäre Schaden droht, wie gefährdet vertrauliche Unternehmensinformationen sind, welche rechtlichen Sanktionen drohen und welchen negativen Einfluss auf die Reputation des Unternehmens ein Angriff haben kann. All diese Aspekte lassen sich schwerlich analysieren ohne die Motivation und Taktik eines Angreifers, aber auch die eigenen Fähigkeiten bei der Abwehr des Angriffes, einzubeziehen.

Durch die Simulation von Angriffen – im Rahmen von War Games - wird deutlich, wie gut die eigene Organisation auf möglicher Angriff vorbereitet ist, das heißt:

- einen Angriff frühzeitig erkennt und das Ausmaß richtig abschätzt
- schnell und wirkungsvoll reagiert, um die Auswirkungen einzugrenzen
- rechtzeitig wichtige Stakeholder (Mitarbeiter, Kunden, Partner, Sicherheitsbehörden) informiert
- geeignete Maßnahmen zur Aufrechterhaltung des Betriebes einleitet und
- rasch zum Normalbetrieb zurückkehren kann

Red Teaming hilft einer Organisation durch die Konfrontation mit möglichen, simulierten Angriffen beim Verbessern der Fähigkeiten ihrer Mitarbeiter und Prozesse (Kontinuitätsmanagement / Krisenmanagement). Letztendlich ist die Organisation dadurch besser auf zukünftige, reale Angriffen vorbereitet.

Aus dem im Jahr 2015 in Kraft getretenen IT-Sicherheitsgesetz ergeben sich für ausgewählte Unternehmen, insbesondere für Betreiber sogenannter Kritischer Infrastruktur (beispielsweise Strom- und Wasserversorgung, Finanzen und Ernährung) besondere Verpflichtungen. Neben dem Umgang mit relevanten Bedrohungen, Schwachstellen und Risiken sowie dem Berücksichtigen einer geänderten Gefährdungslage, sind konkret das Einrichten eines Business Continuity Managements und Maßnahmen zum Steigern der Abwehrfähigkeit der IT-Architektur gefordert.

Die 2016 in Kraft getretene europäische NIS-Richtlinie (Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit) muss von den europäischen Staaten bis Mai 2018 in nationales Recht umgesetzt werden und gilt als zentrale Rechtsverordnung zum Stärken der Sicherheit von IT-Systemen. Mit Blick auf die Vorgaben der Europäischen Kommission und Empfehlungen anderer Gremien entwickelt Eurosystem (die Organisationseinheit der Europäischen Zentralbank und den nationalen Zentralbanken derjenigen EU-Staaten, die den Euro als Zahlungsmittel eingeführt haben) aktuell ein Europäisches „Red Team Testing Framework". Ziel ist es, Red Teaming als geeignete Methode zum Überprüfen der Cyber Resilience zu etablieren und zu standardisieren. Es ist davon auszugehen, dass es vergleichbare Initiativen in anderen Branchen geben wird. Daher ist es ratsam, sich frühzeitig mit dieser Art der Vorbereitung vertraut zu machen.

Grundsätze und Erfolgsfaktoren beim Red Teaming

Für das Red Teaming gilt der Grundsatz

"adverse advice", also die Beratung aus der Perspektive des Gegenspielers. War Games zum Überprüfen vorher entwickelter Szenarien folgen einem interaktiven Ansatz: Jede Reaktion des Angegriffenen beeinflusst die folgende Aktion des Angreifers und umgekehrt. Im fortgesetzten Wechselspiel beider Seiten werden bisher unbekannte oder unbedachte Schwachstellen und die unerwünschten Auswirkungen eines Angriffs deutlich.

Das Ziel sind „actionable intelligence", also Schlussfolgerungen, abgeleitet aus systematisch gewonnenen und bewerteten Informationen, die dann konkrete Führungsentscheidungen ermöglichen. Ein Red Team nutzt dazu ausgewählte Analysetechniken und ein dreistufiges Vorgehen:

- Zunächst werden in einer Diagnosephase die grundlegenden Informationen und Annahmen überprüft.
- In der folgenden Kreativphase werden der Analysegegenstand umfassend betrachtet, mögliche Einflussfaktoren und Auswirkungen bewertet sowie Alternativen identifiziert.
- In der abschließenden Testphase werden die entwickelten Szenarien kritisch und umfassend überprüft.

Bei der Analyse von Cyber Risiken für eine Organisation werden in der Diagnosephase die bereits existierenden Risikoanalysen, Sicherheitskonzepte und Schutzmaßnahmen auf Konsistenz geprüft. Im Fokus steht die Frage: Was möchte das Unternehmen schützen und wogegen?

In der zweiten Kreativphase beschäftigt sich das Red Team mit Fragen wie: Welche Akteure könnten ein Motiv haben das Unternehmen anzugreifen? Welche Fähigkeiten haben sie und welche Schwachstellen könnten sie ausnutzen? Welche kurz-, mittel- und langfristigen Folgeschäden könnten sich aus einem Angriff ergeben? In dieser Phase untersucht es zudem, wie ein Angreifer die Erfolgswahrscheinlichkeit eines Cyber-Angriffs durch Kombination mit anderen Angriffsvektoren erhöhen kann. Mögliche Vektoren sind hier beispielsweise die gezielte Kontaktaufnahme mit Mitarbeitern des Unternehmens, die dann zur Preisgabe vertraulicher Informationen verleitet werden sollen (social engineering) oder das unbemerkte Eindringen in Unternehmensgebäude, um einen physischen Zugriff auf das IT-System zu bekommen (physical penetration test).

Ausgangspunkt der Testphase sind ausgewählte Szenarien, die systematisch hinterfragt werden: Welche möglichen Änderungen der Rahmenbedingungen haben einen entscheidenden Einfluss auf die zugrunde liegenden Risiken und Bedrohungen? Auf welchen Prämissen beruhen die eigenen Annahmen? Welchen Einfluss haben Handlungen einer Partei auf die Möglichkeiten der anderen Partei? In dieser Phase kommt das War Gaming zum Einsatz.

Blick hinter die Kulissen: War Gaming und Red Teaming in der Praxis

Ein international führender Logistikkonzern wollte im Rahmen eines War Games die Gefahren und möglichen Auswirkungen kombinierter

Die Geschichte des War Gamings

Eine disruptive Innovation befeuerte Red Teaming am Anfang des 19. Jahrhunderts: Der Transport von Militärtruppen mit der Eisenbahn. Mit der Eisenbahn konnten Truppen schnell über große Strecken verlegt werden, anstatt sich in beschwerlichen und langsamen Fußmärschen dem Schlachtfeld nähern zu müssen. Damit wuchsen die Möglichkeiten sprunghaft, wann und wo es zwischen den gegnerischen Truppen zum Gefecht kam; die Komplexität der militärischen Planung stieg.
Das preußische Militär begann in dieser Zeit, systematisch Gefechtsszenarien zu simulieren, um die eigenen Operationspläne auf Eignung und Vollständigkeit zu überprüfen und Offiziere in der Strategie zu schulen. Dieser streng reglementierte Prozess, bei dem im Rollenspiel zwei Parteien Zug um Zug ihre Operationspläne umsetzten und dabei auf die Aktionen des Gegners reagieren mussten, wurde als Kriegsspiel (War Gaming) bezeichnet.

Von Hackern und Modelleisenbahnen

Der heute inflationsartig verwendete Begriff „Hacker" ist an und für sich zweckentfremdet. Denn am Anfang des Hacking stand – genau wie beim War Gaming – ebenfalls die Eisenbahn, genauer der Modeleisenbahnclub der amerikanischen Elite-Uni Massachusetts Institute of Technology (MIT). Studenten des MIT erbauten in den 1950er Jahren eine komplexe Modelleisenbahnanlage und entwickelten diese stetig weiter.
Neben der modellbauerischen Gestaltung stand das Automatisieren der Anlagensteuerung von Anfang an im Fokus der Club-Mitglieder. In seinem Buch „Hackers" beschreibt der Journalisten Stephen Levy die Kreativität und das Improvisationstalent der Studenten bei der Beschaffung von Bauteilen und der Manipulation von Anlagenteilen. Er formulierte so erstmals eine in sechs Grundsätzen zusammengefasste Hacker-Ethik. Der MIT Tech Model Railroad Club gilt als Geburtsstätte der Hacker-Kultur.
Heute wird der Begriff Hacking eher mit dem verbotenen Zugriff auf IT-Systeme aus sozialen, kriminellen oder politischen Motiven in Verbindung gebracht. In aller Regel wäre „krimineller Hacker" daher treffender.

Cyber- und physischer Angriffe erkennen und bewerten. Das vierstündige War Game wurde in einem Zeitraum von drei Monaten geplant, Teilnehmer war der erweiterte Vorstand des Unternehmens. Das Projekt bestand aus fünf Phasen: Initiation, Design, Production, Delivery und Evaluation. In der Initiation-Phase wurden zunächst die Rahmenbedingungen (Teilnehmer, Zeitpunkt und Dauer der Simulation) und ein generisches Szenario abgestimmt. Das Szenario wurde in der folgenden Design-Phase weiter strukturiert und in einer ‚Master Event List' – einem Drehbuch für den genauen Ablauf der Simulation – dokumentiert.

Die Production-Phase dient dem Entwickeln vorgeplanter Handlungselemente, sogenannter Injects. Diese Injects wurden in der Simulation vom Red Team genutzt, um das vorgeplante Angriffsszenario schrittweise darzustellen. Nach einer umfangreichen Einweisung aller Beteiligten in das Ausgansszenario und die Rahmenbedingungen begann in der Delivery Phase das eigentliche War Game: Das Blue Team (bestehende aus dem Vorstand des Kunden) wurde in mehreren Schritten durch das Red Team mit dem Angriffsszenario konfrontiert. Aus dem Wechselspiel vorgeplanter Aktionen des roten Teams und situativer Reaktion des blauen Teams ergab sich bereits im zweiten Zug eine unerwartete neue Lage, die wiederum zu angepassten Aktionen beider Seiten führte.

Nach je fünf Zügen beider Seiten endete die Simulation Aus dem Verlauf und der Endsituation ergaben sich unmittelbare Erkenntnisse über die Erfolgswahrscheinlichkeit und Folgen eines komplexen Angriffs sowie der Wirksamkeit von Abwehrmaßnahmen. Der Ablauf des War Games wurde durch einen Moderator geleitet und eine Kontrollgruppe gesteuert. Beobachter dokumentierten alle Aktionen, die dann in der abschließenden Evaluationsphase gemeinsam ausgewertet wurden. Das Unternehmen nutze die Erkenntnisse des War Games zu einer grundlegenden Neubewertung der Bedrohungslage und umfangreichen Anpassung der eigenen Sicherheitsorganisation für eine verbesserte Abwehr möglicher Angriffen.

Red Teaming bei einem Finanzdienstleister

Unabhängig von ausgewachsenen War Games kann ein Red Team laufend für Verbesserung der Abwehrkräfte sorgen. So überprüft ein multinationaler Finanzdienstleister durch Red Teaming regelmäßig die Sicherheit der eigenen Mitarbeiter, der Unternehmensgebäude und des IT-Netzwerkes. Das Red Team entwickelt dazu kontinuierlich Angriffsszenarien, abgeleitet aus bekannten aktuellen Angriffstaktiken oder als Ergebnis einer gezielten Suche nach Schwachstellen. Hierbei wird vorher vereinbart, ob das Red Team nur selbst beschaffte Informationen nutzen kann, oder auch auf interne Informationen zurückgreift.

Die identifizierten Szenarien werden dem Sicherheitsverantwortlichen des Unternehmens in regelmäßigen Abständen vorgestellt und gemeinsam bewertet. Ausgewählte Angriffsszenarien werden dann in sogenannten Red-Team-Audits praktisch simuliert. Das Red Team versucht also beispielsweise tatsächlich unbemerkt in einen gesicherten Unternehmensbereich einzudringen, sich dort einen unberechtigten Zugang zum IT-Netzwerk zu verschaffen und Schadsoftware zu installieren oder vertrauliche Daten zu entwenden. Die Red-Team-Audits verlaufen immer mit klaren Handlungsanweisungen, im Rahmen eines vorher freigegebenen Konzepts und mit einem bekannten Verfahren zur Deeskalation, sollt das Red Team entdeckt werden. Das Vorgehen wird detailliert dokumentiert und ausgewertet. Darauf basierend werden konkrete Maßnahmen zum Verbessern der Sicherheit abgeleitet. Die Ergebnisse der Audits und das Umsetzen der folgenden Maßnahmen wie bauliche Veränderungen oder Schulungskampagnen, werden an die Unternehmensführung berichtet und sind ein fester Bestandteil des Sicherheitskonzeptes.

Red Teaming „as a service"

Neben der strukturierten Analyse haben weitere organisatorische Faktoren Einfluss auf den Erfolg eines Red Teams. So ist zunächst zu entscheiden, ob ein externer Dienstleister oder eigene Mitarbeiter das Red Team stellen. Beide Möglichkeiten haben ihre Vorteile: Ein externes Red Team kann unabhängig agieren und ist in der Analyse nicht durch Erfahrung im oder Wissen aus dem Unternehmen in der Urteilsfindung vorbelastet. Ein internes Red Team hingegen profitiert von der Expertise über Struktur, Kultur und Prozessen im eigenen Unternehmen. Bewährt hat sich die Zusammenarbeit von externen Red-Teaming-Experten mit internen Spezialisten. So ergänzen Methodenkompetenz und eine unabhängige Sichtweise unternehmensspezifisches Wissen.

Da Red Teaming letztlich immer der verbesserten Vorbereitung auf zukünftige Angriffe dient, ist der Wissenstransfer vom Red Team hin zu den verantwortlichen Mitarbeitern in der eigenen Organisation (Blue Team) ein entscheidender Erfolgsfaktor, der ausreichend berücksichtigt und geplant werden muss. In der Praxis hat sich für die Zusammenarbeit zwischen roter und blauer Mannschaft der Begriff „Purple Teaming" etabliert.

Beim Zusammenstellen eines Red Teams können Unternehmen wiederum von den eingangs erwähnten Red Cells des CIA lernen: Bei der Mitgliederauswahl der Red Teams des Geheimdienstes wurde auf ein möglichst weites Spektrum an fachlicher Expertise und Erfahrung im Team geachtet. Um die kritische, unkonventionellen Vorgehensweise der Red Cell aufrecht zu erhalten und den Red-Teaming-Ansatz innerhalb der CIA generell bekannt zu machen, kehren die Team-Mitglieder in der Regel nach spätestens zwei Jahren wieder in andere – gewöhnliche – Funktionen zurück. Bemerkenswert ist, dass die CIA Red Cell in der Regel den Fokus ihrer Analysen sowie deren Agenda eigenständig bestimmt und ihre Analyseprodukte ungefragt vorlegt.

Sicherheit – ein dauerhafter Prozess

Führungskräfte, die Red Teams einsetzen wollen, müssen sich über eines im Klaren sein: Die gewonnenen Erkenntnisse eines Red Teams sind zwar sinnvoll für die eigene Organisation. Sie basieren dabei aber auf Schwachstellen oder falschen Annahmen, die zuvor nicht bekannt waren. Das Red Team sollte daher immer von einer Stelle beauftragt werden und auch an diese berichten, die sowohl die notwendige Kompetenz als auch Verantwortung hat, ausreichend begründete Empfehlungen des Red Teams umzusetzen.

„Security is a process not a product."[3]
Bruce Schneier

Der bekannte Kryptologe und Sicherheitsexperte Bruce Schneier bemerkte: Sicherheit ist ein Prozess, kein Produkt. Von ihm stammt auch die Aussage, dass Angriffe mit der Zeit immer besser werden aber niemals schlechter. Was hat das mit der passenden Dauer und Frequenz des Red Teamings zu tun? Grundsätzlich kann Red Teaming anlassbezogen, regelmäßig oder kontinuierlich erfolgen. Ein anlassbezogener Einsatz könnte beispielsweise durch den Wunsch zur Überprüfung einer neuen Sicherheitsstrategie oder Organisation begründet sein.

Ein regelmäßiger Einsatz könnte hingegen durch gesetzlichen oder geschäftlichen Ver-

3 Schneier, Bruce; The Process of Security, https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html, 08.08.2017

pflichtungen (Sicherheits-Audits, Erneuerung von Versicherungspolicen, Geschäftsberichte) gerechtfertigt sein. Mit Blick auf die stetige Veränderung der Gefährdungslage und oben genanntem Verständnis von Sicherheit als einem nie endenden Prozess sollte ein Unternehmen immer ein kontinuierliches Red Teaming anstreben.

Vier Schritte zur Einführung von Red Teaming

Das Einführen von Red Teaming kann sinnvollerweise in vier Schritten erfolgen:

- Am Anfang steht eine kritische Überprüfung der Risikoanalyse mit Fokus auf der Neubewertung möglicher Angreifer und Angriffsziele.
- Dem folgt die Identifikation und Detaillierung möglicher Angriffsszenarien. Dabei werden neben den ausgenutzten Schwachstellen auch Motivation und Fähigkeiten des Angreifers berücksichtigt. Zudem sollt das fiktive Angriffsziel auch mit vorgenannten Faktoren übereinstimmen.
- Daran anschließend werden mögliche Auswirkungen der zuvor ausgewählten Angriffsszenarien im Rahmen von War Games analysiert. Das Red Team konfrontiert dazu das Blue Team mit dem möglichen Angriff, auf den das Blue Team reagiert. In der wiederum folgenden Gegenreaktion berücksichtigt das Red Team das Verhalten der Verteidiger und die neue, geänderte Situation. Während dieses Wechselspiels werden systematisch beiden Parteien zur Verfügung stehende Informationen und Handlungsoptionen ausgewertet. Als Ergebnis kann die Erfolgswahrscheinlichkeit eines Angriffs bewertet werden. Solassen sich Maßnahmen zur Verbesserung des Schutzniveaus ableiten.
- Als wichtigste Aufgabe erscheint die Verstetigung und Institutionalisierung des Red Teamings. Wird das Verfahren richtig angewendet, ist es eine sinnvolle und notwendige Maßnahme klassische Ansätze des Cyber-Risikomanagements zu ergänzen und Organisationen eine realistische Einschätzung ihrer Resilienz zu geben. Es hat sich jedoch gezeigt, dass beim Etablieren eines Red Teams die organisatorische Verortung ein kritischer Erfolgsfaktor ist. Es gilt daher rechtzeitig zu klären, wer zukünftige Red Teaming Einsätze initiiert und über Fokus und Frequenz entscheidet. Wer nimmt die gewonnenen Erkenntnisse auf und reagiert entsprechend? Wie erfolgt der Wissenstransfer vom Red Team zum Blue Team?

Per se gibt es keinen Grund, warum nicht jedes Unternehmen einen für die jeweilige Organisation und Situation passenden Red-Teaming-Ansatz finden sollte – um das Konzept regelmäßig in der Praxis zu nutzen. Richtig angewandt und konsequent genutzt, unterstützt Red Teaming das Bewusstsein für gängige und außergewöhnliche Risiken sowie den Umgang mit Cyber-Risiken.