Herausforderungen im Rahmen von Red Team Assessments

Angriffspläne

Joshua Tiago

Bevor die Sicherheitsverantwortlichen in einem Unternehmen eine Angriffssimulation durch ein Red Team veranlassen, gilt es, deren Ziele und Prüftiefe möglichst detailliert festzulegen. Sinnvoll kann es auch sein, das verteidigende Blue Team gleich mitzuschulen.

Um die Wehrhaftigkeit eines Unternehmens gegen Angriffe zu prüfen, haben sich in den letzten Jahren sogenannte Red Team Assessments etabliert – also Angriffssimulationen durch ein externes Expertenteam. Bevor die Verantwortlichen ein solches Red Team Assessment veranlassen, gilt es, einige Aspekte zu berücksichtigen und in die Planung einzubeziehen (siehe Kasten „Fragen vor Beginn ...“). Planungs- und Entscheidungsphase bergen sowohl für den Auftraggeber als auch für den Dienstleister einige Herausforderungen. Am Anfang steht immer die Frage, warum ein Red Team Assessment stattfinden soll. Die Antwort „Wir möchten die Sicherheit unseres Unternehmens erhöhen“ ist in diesem Kontext nicht immer zielführend. Ohne Frage, Red Team Assessments erfreuen sich immer größerer Beliebtheit. Dennoch sind manchen Sicherheitsverantwortlichen die relevanten Unterschiede zwischen einem Red Team Assessment und einem Penetrationstest nicht klar.

Erschwerend kommt hinzu, dass inzwischen viele IT-Sicherheitsfirmen Red Team Assessments anbieten. Ein genauer Blick offenbart oftmals, dass die angebotenen Leistungen nur bedingt als Red Team Assessment bezeichnet werden können. In einigen Fällen werden umfangreiche Penetrationstests, die zum Ziel haben, möglichst viele Schwachstellen in der Breite aufzudecken, fälschlicherweise als Red Team Assessment angeboten. Daher sollte man solche Dienstleistungen stets kritisch hinterfragen und darauf achten, dass der Dienstleister für diese Art der Prüfung Erfahrung und Sachkenntnis vorweisen kann. Doch wann ist es angebracht, ein Red Team Assessment zu beauftragen, und wann reicht ein Penetrationstest aus? Eine Gegenüberstellung beider Prüfungsarten liefert eine erste Antwort.

Zwei verschiedene Verfahren

Penetrationstests sind zielgerichtete Prüfungen zum Feststellen der aktuellen Sicherheit einer Anwendung, eines Systems oder einer Netzwerkumgebung. Der konkrete Prüfgegenstand ist sehr unterschiedlich, angefangen von Webapplikationen (siehe Artikel „Automatisch sicher“, Seite 46) und mobilen Apps über Netzwerkprotokolle bis hin zu IoT-Geräten. Dabei sucht ein erfahrener Penetrationstester Schwachstellen und nutzt sie aus, um die Verantwortlichen bei der Risikoeinschätzung ihrer Systeme oder Applikationen zu unterstützen. Abschließend empfiehlt er Maßnahmen, mit denen sich die Schwachstellen beheben lassen oder die zumindest ihr Gefährdungspotenzial minimieren.

Ein Beispiel dafür könnte sein, dass eine Bank ihre Onlinebanking-Anwendung überprüfen lassen möchte. Ein Penetrationstest würde sich in diesem Fall ausschließlich auf die Webapplikation beschränken und der Prüfer nach potenziellen Schwachstellen suchen, die ein Angreifer ausnutzen kann. Für die Gesamtsicherheit der Bank ist diese Anwendung sicherlich eine wichtige Komponente, aber eben nicht die einzige. Dennoch sind Penetrationstests sinnvoll. Wenn zum Beispiel eine neue Version der Webapplikation entwickelt wurde oder sich der Aufbau der Architektur des Onlinebankings gravierend verändert hat, lohnt sich eine solche Überprüfung.

Ein Red Team Assessment unterscheidet sich von einem Penetrationstest in mehreren Punkten. Der größte Unterschied besteht darin, dass nicht eine Anwendung oder ein System, sondern alle Entitäten eines Unternehmens gleichermaßen im Visier sind. Dabei spielt es keine Rolle, ob es sich um ein IT-System, einen Mitarbeiter, einen Standort oder auch ein Un-

Fragen vor Beginn eines Red-Team-Assessment-Projekts

- Was sind die konkreten Ziele des Red Team Assessments?
- Können die Ziele auch mit einem im Umfang beschränkten Penetrationstest erreicht werden?
- Sollen festgelegte Szenarien im Rahmen des Projekts simuliert werden? Wenn ja, welche?
- Sollen bestimmte Angriffstechniken, Methoden oder Personenkreise aus dem Prüfungsumfang ausgeschlossen werden?
- Falls einige Methoden und Szenarien ausgeschlossen werden sollen, ist die Aussagekraft der Ergebnisse ausreichend relevant?
- Wer soll über die geplante Prüfung unterrichtet werden?
- Wurden bereits Erkennungstechnologien und Prozesse eingeführt, um die zu simulierenden Angriffe zu erkennen und zu unterbinden?
- Welche Angriffe sollten definitiv erkannt werden?
- Falls das Blue Team informiert werden soll, welche Informationen über Art, Umfang und Zeitraum der Angriffe sollen bekannt gegeben werden?
- Soll die Reaktion des Blue Teams auf die Angriffe beobachtet und bewertet werden? Über welchen Zeitraum soll sich die Prüfung erstrecken?

ternehmen in der Holding-Struktur handelt. Es werden nicht nur die technischen Systeme auf eine Möglichkeit zur Kompromittierung untersucht. Vielmehr handelt es sich um einen ganzheitlichen Ansatz, der alle möglichen Einfallstore eines modernen Unternehmens berücksichtigt.

Dazu zählt unter anderem auch das physische Eindringen in die Räumlichkeiten, das es einem Angreifer erlaubt, einen besseren Zugriff auf die IT-Systeme zu erhalten. Erfolgreiche Angriffe auf die Mitarbeiter erleichtern ebenfalls den Zugriff auf die Infrastruktur, Systeme oder sensible Daten. Daher gibt es auch nur wenige Einschränkungen, wie weit ein Red Team Assessment gehen darf. Während der Tester bei einem Sicherheitsaudit lediglich auf Schwachstellen hinweist und sie meist nicht ausnutzt, steht gerade Letzteres bei einem Red Team Assessment im Vordergrund.

Hier werden Schwachstellen geschickt kombiniert und aktiv ausgenutzt, um sich einen Vorteil für einen Angriff zu verschaffen. Diese Art von Prüfung dient nicht dazu, möglichst viele Schwachstellen zu identifizieren. Es reicht in der Regel, nur die eine schwerwiegende Schwachstelle oder die Kombination aus mehreren Schwachstellen zu finden, die es erlaubt, einen Teil der Infrastruktur zu übernehmen. Ein weiterer Unterschied liegt in der Dauer und dem zeitlichen Ablauf des Projekts. Während ein Penetrationstest über einen bestimmten Zeitraum stattfindet, meist ein bis zwei Wochen, läuft ein Red Team Assessment weniger linear ab. In der Regel erstreckt es sich über einen längeren Zeitraum, in dem immer wieder einzelne Angriffssimulationen oder -schritte stattfinden.

Welche Prüfung für wen?

Wenn man diese Unterschiede betrachtet, wird nachvollziehbar, warum ein Red Team Assessment nicht für alle Unternehmen und in allen Situationen die bessere Variante ist. Da dabei alle relevanten Sicherheitsmechanismen und Prozesse abgeklopft werden, um ein Eindringen zu erreichen, ist eine solche Prüfung nur dann sinnvoll, wenn das betreffende Unternehmen bereits die grundlegenden Aufgaben im Bereich IT-Sicherheit erledigt hat und hoher Schutzbedarf besteht.

Um beim Beispiel der fiktiven Bank zu bleiben, folgendes Szenario: Die Bank hat in den vergangenen Jahren viel Zeit, Personal und Geld in das Thema IT-Sicherheit investiert. Es kommen diverse Schutzmechanismen zum Einsatz, Erkennungstechniken wurden eingeführt und Prozesse definiert. Nun möchte die Bank einschätzen, wie es um die Gesamtsicherheit bestellt ist. Gibt es Einfallstore, die nicht berücksichtigt wurden? Sind die Mitarbeiter ausreichend sensibilisiert worden? Gibt es Angriffsketten, die nicht bekannt sind? All diese Fragen lassen sich im Rahmen eines Red Team Assessments beantworten.

Obwohl nur bedingt Einschränkungen für solche Prüfungen bestehen, wird das zu erreichende Ziel im Vorfeld definiert. Konkrete Fragestellungen und Szenarien sind hierbei sehr hilfreich. Am Beispiel der fiktiven Bank wäre eine konkrete Fragestellung, ob ein Angreifer, der in das Gebäude der Bank gelangt, in der Lage ist, unberechtigt eine Zahlung zu veranlassen oder zu manipulieren. Ein weiteres Ziel könnte darin bestehen, die existierenden Erkennungsmechanismen zu überprüfen. Werden Anomalien im Netzwerk entdeckt? Kann sich Malware unbemerkt ausbreiten? Kann sich ein Angreifer dauerhaft im Netzwerk der Bank einnisten?

Schutz der „Kronjuwelen“

Die Ziele sind je nach Unternehmen und Branche sehr unterschiedlich. Ein weltweit führendes Maschinenbauunternehmen muss andere „Kronjuwelen“ schützen als eine Bank oder Versicherung. Doch Red Team Assessments bieten weitere Vorteile. So kann eine solche Prüfung einen hervorragenden Einblick in die Leistungsfähigkeit und Arbeitsweise eines vorhandenen Blue Teams bieten. Blue Teams stellen den Gegenpart zum Red Team dar (siehe Artikel „Rot gegen Blau“, Seite 54). Sie bestehen aus Mitarbeitern der IT-Sicherheitsabteilung und verteidigen das Unternehmen gegen reale Angriffe oder eben die simulierten Angriffe des Red Teams. Große Unternehmen setzen Blue Teams in ihren Security Operations Centern (SOC) ein (siehe Abbildung).

X-TRACT

- Vor einem sogenannten Red Team Assessment gilt es abzuwägen, ob ein solches Projekt überhaupt das Richtige ist oder ein Penetrationstest eventuell sinnvoller wäre.
- Nach Auswahl der geeigneten Testform für das eigene Unternehmen sind das genaue Ziel des Tests, aber auch die Rahmenbedingungen festzulegen.
- Je nach Situation und Umfang des Assessments können Blue Teams, die firmeninternen „Verteidiger“, auf der Gegenseite mitwirken und so gleich mitgeschult werden.

Im Rahmen eines Red Team Assessments können zum Beispiel folgende Aspekte betrachtet werden: Welche Angriffe werden tatsächlich entdeckt? Welche Aktionen des Angreifers bleiben unbemerkt? Wie reagiert das Blue Team auf Stresssituationen, die bei einem Red Team Assessment immer wieder auftreten? Die Erkenntnisse sind für die Verbesserung und Weiterentwicklung der Arbeitsweise und Prozesse eines Blue Team beziehungsweise eines SOC-Teams sehr wertvoll.

Frustration bei den Teams vermeiden

Wenn das Training des Blue Teams im Vordergrund steht, ist es empfehlenswert, einen Mitarbeiter des IT-Sicherheitsunternehmens, der das Red Team Assessment durchführt, für den Zeitraum der Prüfung im Blue Team oder im SOC zu platzieren. In diesem Fall spricht man von einer War-Gaming-Übung. Dadurch ist der Mitarbeiter des Dienstleisters in der Lage, in Echtzeit das Reaktionsverhalten des Blue Teams auf die ihm bekannten Angriffe zu beobachten, um das Blue Team später entsprechend zu beraten. Die Herausforderung des Auftraggebers besteht unter anderem darin, Szenarien festzulegen, die im Alltag relevant sind und für die bekanntermaßen Erkennungstechniken und Prozesse vorliegen.

Andernfalls droht dem Blue Team Frustration, wenn Angriffe nicht erkannt werden, weil zum Beispiel keine Metriken oder Erkennungstechniken dafür vorhanden sind oder weil der simulierte Angriff im „Security Playbook“ des SOC nicht definiert wurde. Ziel einer solchen Maßnahme ist es nicht, dem Blue Team Versagen vorzuwerfen, sondern konstruktiv an der Optimierung der Arbeitsweise, der Prozesse und der Erkennungstechniken des Teams mitzuwirken. Eine weitere Herausforderung besteht darin, festzulegen, wie viele Informationen man dem Blue Team bekannt geben soll.

Dazu zählen beispielsweise der Zeitraum, in dem die Angriffe zu erwarten sind, die Art der Angriffe sowie die verwendeten Angriffstools. Wie viele Informationen bereitgestellt werden, hängt unter anderem davon ab, wie erfahren das Blue Team ist oder ob es weniger um ein Training des Blue Teams geht, sondern vielmehr darum, ein möglichst realistisches Angriffsszenario nachzustellen. Um den größtmöglichen Lerneffekt zu erreichen, ist es sinnvoll, nach Abschluss des Projekts im Rahmen eines Workshops mit dem Blue oder SOC-Team die daraus gewonnenen Erkenntnisse vorzustellen und gemeinsam Verbesserungen auszuarbeiten. Dabei sollte man auf die vorhandenen Prozesse und Werkzeuge des Blue Teams eingehen.

Neben dem Auftraggeber muss sich auch der Dienstleister vor Beginn eines solchen Projekts einigen Herausforderungen stellen. Während viele Penetrationstests sehr ähnlich verlaufen, sieht das bei Red-Team-Assessment-Projekten ganz anders aus. Jedes dieser Projekte ist sehr unterschiedlich und spezifisch auf den jeweiligen Auftraggeber zugeschnitten. Bei solchen Prüfungen lässt sich kein Standardvorgehen von Projekt zu Projekt übertragen. Daher muss man viel Zeit für die Vorbereitung und das laufende Projektmanagement einplanen.

Die Hauptakteure auf Dienstleisterseite sind die Mitglieder des Red Teams. Ein solches besteht typischerweise aus erfahrenen Penetrationstestern. Jedes Mitglied ist Experte auf seinem Fachgebiet. Dadurch wird gewährleistet, dass im Team Kompetenz zu Webschwachstellen, Netzwerken, Windows- und Linux-/Unix-Betriebssystemen, Social Engineering, Malware, Lateral Movement, Reversing, Exploiting und vielem mehr vorhanden ist (siehe Tabelle „Anforderungen an das Red Team“). In speziellen Fällen stehen dem Red Team weitere Kollegen im Büro des Dienstleisters zur Verfügung, wenn es die Situation erfordert oder Fachwissen zu sehr speziellen Themengebieten benötigt wird.

Quelle: Telekom

In den SOCs großer Unternehmen helfen Blue Teams bei der Verteidigung gegen Internetangriffe. Hier das SOC der Telekom, dessen Dienste auch von kleinen Unternehmen beansprucht werden.

Schnelles Anpassen ist gefragt

Somit ist sichergestellt, dass das Red Team stets alle vorhandenen Möglichkeiten und Ressourcen nutzen kann, um sein Ziel zu erreichen. Doch die fachlichen Kenntnisse sind nur eine von vielen Anforderung an die Red-Team-Mitglieder. Sie müssen zudem in der Lage sein, flexibel auf Änderungen – die sich immer wieder im Rahmen solcher Projekte ergeben – zu reagieren und gegebenenfalls ihr Vorgehen anzupassen. Erfolgreiche Red Team Assessments sind nie Ergebnis der Leistung eines Einzelkämpfers. Vielmehr ist eine enge Zusammenarbeit im Team Voraussetzung für den Erfolg.

Wie in jedem Team ist es sinnvoll, einen Leiter für das Red Team zu benennen. Eine seiner Hauptaufgaben besteht darin, das

Projektziel im Auge zu behalten und die Red-Team-Mitglieder entsprechend ihren Fähigkeiten einzusetzen. So lässt sich sicherstellen, dass die Mitglieder des Teams nicht die Orientierung verlieren, wenn die Anzahl an entdeckten Schwachstellen sehr hoch ist und der Weg zum Ziel nicht immer klar definiert werden kann. Der Leiter des Teams muss gegebenenfalls entscheiden, ob das ursprünglich geplante Vorgehen weiterhin Erfolg versprechend ist oder ob eine andere Herangehensweise zum Erreichen des vorgegebenen Ziels lohnender ist. Hierzu sollte eine kontinuierliche Abstimmung mit dem restlichen Team stattfinden.

Vor dem eigentlichen Red Team Assessment ist eine klare Definition der Ziele und des Rahmens notwendig, in dem die Prüfung stattfinden soll. Die Ziele definiert nicht der Dienstleister, sondern der Auftraggeber. Allerdings kann und sollte der Dienstleister seine Erfahrung einbringen und Vorschläge bezüglich sinnvoller Ziele, Szenarien und Vorgehensweisen unterbreiten. Typischerweise beginnt ein solches Projekt daher mit einem Workshop, in dem die grundsätzlichen Rahmenbedienungen für das Red Team Assessment besprochen und die Ziele definiert werden.

Zudem werden ein oder mehrere Ansprechpartner auf Auftraggeberseite benannt, die eingeweiht sind und im Ernstfall eingreifen können sowie für etwaige Rückfragen zur Verfügung stehen. In diesem Kreis wird die in einem früheren Red-Teaming-Artikel genannte „Du kommst aus dem Gefängnis frei“-Karte für den Dienstleister vorbereitet und ausgestellt. Gerade bei Prüfungen für Unternehmen im Bereich kritische Infrastrukturen ist es wichtig, eine solche schriftliche Vereinbarung bei sich zu führen, um die Situation bei Entdeckung mit den Mitarbeitern für den Objektschutz schnell klären zu können.

Der Vorbereitungsworkshop: Rahmen festlegen

Des Weiteren sollte der Auftraggeber der Prüfung im Workshop Bereiche benennen, die vom Assessment ausdrücklich auszuschließen sind: etwa Örtlichkeiten, die nicht betreten werden dürfen, Personen, die im Rahmen von Social Engineering nicht angegriffen werden dürfen, oder bestimmte Tochterunternehmen und Systeme, die unbedingt auszuschließen sind. Darüber hinaus kann während des Workshops festgelegt werden, welches Vorgehen und welche Angriffstechniken nicht infrage kommen. Hierbei gilt es, zusammen mit dem Auftraggeber mit viel Fingerspitzengefühl einen Rahmen zu definieren, der das Ergebnis der Prüfung nicht verwässert – was durch zu viele Einschränkungen der Fall sein könnte.

Solche Workshops erstrecken sich typischerweise über ein bis zwei Tage und werden oftmals in mehreren Terminen durchgeführt, da manche Aspekte erst nach interner Rücksprache auf Seite des Auftraggebers abschließend festgelegt werden können. Am Ende des Workshops hat der Dienstleister in Abstimmung mit dem Auftraggeber einen „Schlachtplan“ entworfen, der grob die Szenarien und Angriffspfade benennt.

Ein wichtiger Aspekt, der zu diesem Zeitpunkt berücksichtigt werden sollte, ist der zeitliche Ablauf der Prüfung. Natürlich hat der Auftraggeber ein Interesse daran, das Projekt möglichst schnell abschließen zu können. Allerdings spielt der

Anforderungen an das Red Team	
Hohe Expertise	**Soft Skills**
Webschwachstellen	Teamfähigkeit
Angriffe auf Netzwerkebene	Kommunikationsfähigkeit
Informationsgewinnung	analytische Fähigkeiten
Spear-Phishing	Problemlösungskompetenz
Social Engineering	Flexibilität
Angriffe auf die physische Sicherheit	
Angriffe mit dem Ziel der Rechteerweiterung	
Lateral Movement in komplexen Umgebungen	
Exfiltration der gewonnenen Daten	
Anpassen und Entwickeln von Malware und Backdoors	
Reverse Engineering von Applikationen	

Zeitraum, über den sich eine solche Prüfung erstreckt, eine wichtige Rolle. In der Vergangenheit hat es sich bewährt, das Assessment über mehrere Monate zu verteilen. Innerhalb dieses vorab abgestimmten Zeitraums werden immer wieder Angriffe vorbereitet und durchgeführt. Der große Zeitraum ist notwendig, da bestimmte Angriffe eine längere Vorlaufzeit benötigen.

Beispielsweise kann es sein, dass eine Phishingkampagne mittels E-Mails erst nach mehreren Wochen erfolgreich ist oder unter Umständen auch mehrere Anläufe erfordert. Zudem ist es von Vorteil, die dafür verwendeten Internetdomänen mehrere Wochen bis Monate im Voraus zu beantragen, da manche Sicherheitsprodukte auf Eigenschaften wie das Alter einer Internetdomäne prüfen. Darüber hinaus ergeben sich im Laufe eines Jahres immer wieder gute Gelegenheiten für einen Angriff, zum Beispiel bei öffentlichen Ausstellungen an den Standorten des Auftraggebers, die einen besonders einfachen Zugang zu dessen Gebäude ermöglichen. Je länger der Zeitraum bemessen wird, umso höher ist die Chance, dass auch solche Veranstaltungen berücksichtigt werden können.

Nach dem Workshop ist vor dem Assessment

In der Phase nach dem Workshop beginnt die eigentliche Arbeit für das Red Team. Durch gemeinsames Brainstorming arbeitet das Team Ideen und Vorschläge aus, um die mit dem Auftraggeber definierten Ziele und Angriffsszenarien umzusetzen. Hierbei kristallisiert sich oftmals heraus, welche speziellen Fertigkeiten das Red Team benötigt und welche Werkzeuge, Methoden und Verfahren zum Einsatz kommen sollen. Je nach Auftraggeber und Projekt kann der Fokus eher auf der technischen Seite liegen, auf der physischen Sicherheit oder eben sehr stark auf Social Engineering.

Während des Assessments steht das Red Team immer wieder vor ähnlichen Herausforderungen. Oft stellt sich heraus, dass der ausgearbeitete „Schlachtplan" nicht eingehalten werden kann. Auf technischer Seite kann es viele Gründe dafür geben. Zum Beispiel trifft das Red Team auf robuste Sicherheitsmaßnahmen, die vorher nicht bekannt waren und aufwendig umgangen werden müssen. Oder die Malware, die vor zwei Monaten bei einem anderen Projekt zum Einsatz kam, wird inzwischen von vielen AV-Lösungen erkannt. Das Red Team muss auf diese Änderungen entsprechend reagieren und gegebenenfalls die Methoden und Werkzeuge anpassen oder ersetzen. Im Fall der erkannten Malware kann es notwendig sein, dass das Red Team diese so anpasst, dass das eingesetzte AV-Produkt sie anhand von Signaturen oder Verhaltensanalyse nicht mehr erkennt.

Es kann jedoch auch erforderlich sein, eigene Tools zu programmieren oder sogar spezielle Hacking-Hardware zu entwickeln, um ans Ziel zu gelangen. Zwar gibt es eine Fülle von Angriffswerkzeugen und Hardware für Pentester, allerdings müssen diese teilweise modifiziert werden, um sie im Rahmen eines Red Team Assessments zielgerichtet einsetzen zu können. Dies trifft insbesondere dann zu, wenn die Aktionen des Red Teams so lange wie möglich unentdeckt bleiben sollen.

Des Weiteren kann es sein, dass der geplante Angriffspfad zum Erreichen des Ziels nicht optimal ist. Beispielsweise könnte das Red Team versuchen, mittels Lateral Movement schnell seine Rechte in der Umgebung zu erweitern und so in wenigen Schritten das Zielsystem zu kompromittieren. Dabei könnte sich dann herausstellen, dass das eigentliche Ziel so gar nicht erreicht werden kann, weil andere Schutzmaßnahmen wirken oder sich das Zielsystem isoliert in einem eigenen Segment befindet, zu dem es keine direkte Verbindung gibt. In solchen Fällen ist die langjährige Erfahrung und Kreativität des gesamten Red Teams gefordert, um die Herangehensweise anzupassen und andere Wege und Möglichkeiten zu wählen. Je erfahrener das Red Team ist und je öfter ähnliche Hürden in der Vergangenheit umgangen werden mussten, desto wahrscheinlicher ist es, dass das Team das vorgegebene Ziel erreicht.

Fazit

Neben den technischen Herausforderungen, die im Rahmen eines Red Team Assessments auftreten, ist auch eine Reihe an organisatorischen Aspekten zu berücksichtigen. Beginnend mit der Frage, warum und ob tatsächlich ein Red Team Assessment beauftragt werden soll, bis hin zur Definition von Zielen und Angriffsszenarien eines solches Projekts. Nicht unerheblich sind im Zusammenhang mit vertraulichen Daten und Mitarbeiterrechten auch Compliance- und Datenschutzaspekte, die es ebenfalls im Vorfeld einzuplanen gilt (siehe dazu Artikel „Rahmenwerk", Seite 58).

Unternehmen mit einem sehr hohen Schutzbedarf, die bereits die grundlegenden Aufgaben im Bereich IT-Sicherheit erledigt haben, profitieren enorm von einem Red Team Assessment. Es vermittelt ein sehr gutes Bild über die Sicherheitslage – insbesondere wenn möglichst realistische Szenarien gewählt werden, bei denen ein potenzieller Angreifer einen erheblichen Schaden herbeiführen könnte. Dadurch ist es möglich, das eigene Unternehmen, die eigenen Mitarbeiter und die Sicherheitsarchitektur aus dem Blickwinkel eines versierten Angreifers zu betrachten und geeignete Maßnahmen zum Beheben der aufgedeckten Schwachstellen zu ergreifen. Die Möglichkeit, das Blue Team dabei zu schulen und seine Arbeitsweise und Prozesse zu optimieren, schlägt als weiterer Vorteil für diese Art von Prüfungen zu Buche.

Wer tiefer in die Praxis des Red Teaming einsteigen möchte, findet in den zwischen Februar 2019 und April 2019 in loser Folge erschienenen *iX*-Artikeln zu „Red Team Assessments" eine umfangreiche Übersicht über Methoden, Techniken und Werkzeuge der einzelnen Projektphasen.

(ur@ix.de)

Joshua Tiago

ist Leitender Berater bei der cirosec GmbH und verantwortet Red-Team-Assessment-Projekte für große Kunden.