"All warfare is based on deception."

(Nach: Sun Tzu in „Die Kunst des Krieges")

mVISE erklärt: Deception Technologie

Der Mornellregenpfeifer [1]

Der Mornellregenpfeifer ist ein Vogel aus der Gattung der Regenpfeifer und hat sein Hauptbrutgebiet in den Tundren Eurasiens am und nördlich des Polarkreises. Besonders an ihm ist sein „Verleite-Verhalten" zum Schutz seines Nestes und seiner Nachkommen.

So verfügt er über situationsangepasstes Verhalten zur Ablenkung und Täuschung seiner Fressfeinde. Die niedrigste Stufe wird als „Wegsehen" gedeutet. Dabei wendet sich der Mornellregenpfeifer von dem erkannten Eindringling ab, fixiert aber trotzdem diesen potenziellen Feind.

Die nächste Stufe wird als „auffälliges Weglaufen" bezeichnet. Hierbei humpelt der Mornellregenpfeifer mit hängenden Flügeln, welches in raschen Laufen übergeht, sobald er sich von seinem Feind oder dem eigenen Nest abwendet. Dieses Verhalten wird durch klagende Rufreihen begleitet.

Reicht dies nicht, um den Feind vom eigenen Nest abzulenken, so wird die „sterbende" Phase begonnen. Hierbei präsentiert er sich mit krampfhaften Flügel-, Bein- und Schwanzzittern.

Bei jeder dieser drei Phasen zeigt der Mornell dem potentiellen Feind, dass er ein leichtes Ziel ist, sodass der Feind ihn und nicht das Nest bzw. die Brut als Ziel ausmacht. Geht der Feind zum Angriff über, stellt der Mornell sein Verhalten ein und fliegt gesund und munter davon.

Kunst der Täuschung und Ablenkung

Die Kunst der Täuschung und Ablenkung ist eine Technik, um angemessen auf unberechenbare Feinde zu reagieren. So wird sie nicht nur in der Natur durch den beschriebenen Mornellregenpfeifer eingesetzt, sondern auch in der klassischen und modernen Kriegsführung, wie auch bei diversen Sportarten. Diese gelten dann als ausgemachte Finten und Taktiken.

Aber auch Angreifer auf moderne IT-Systeme setzen bewusst auf Täuschung und Ablenkung, um Systeme zu infiltrieren. Dabei geht es nicht nur um Social Engineering, sondern auch um getarnte Datenpakete und das bewusste Verschleiern von Mustern.

Daher müssen sich IT-Verantwortliche die Frage stellen, ob Täuschung und Ablenkung auch elementare Bestandteile der eigenen IT-Sicherheitsstrategie darstellen sollten.

Vorteile einer Deception Lösung:

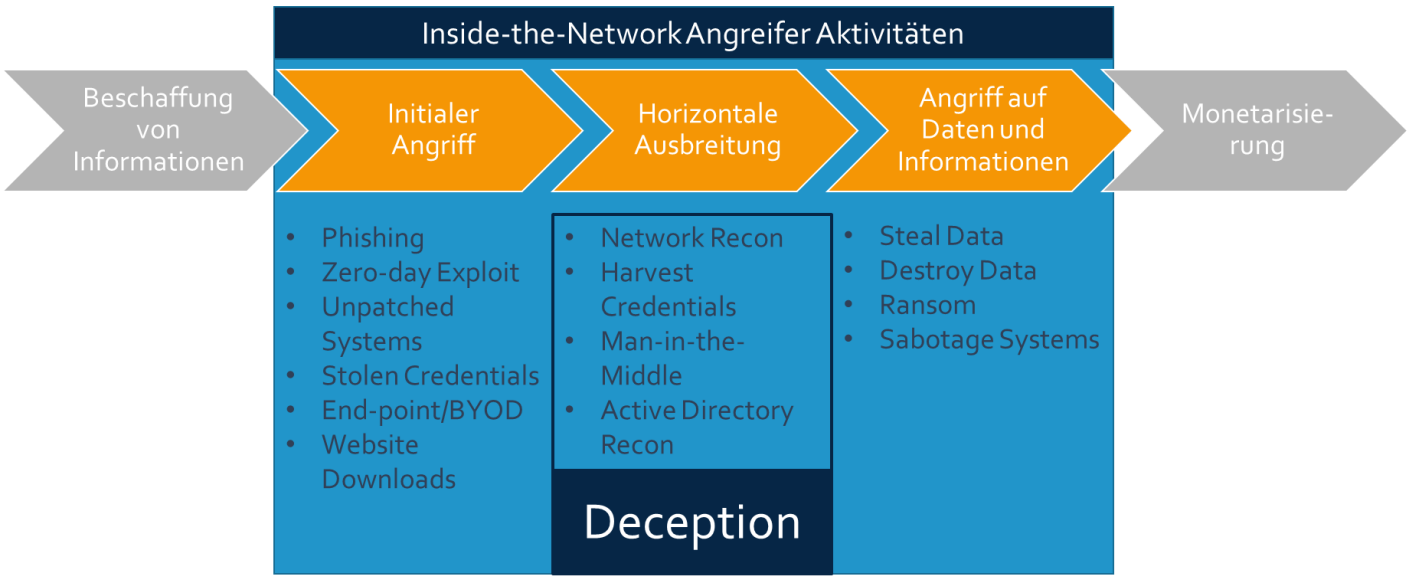
- ✓ Absolute Sichtbarkeit bei Angriffen
- ✓ Schnelle Reaktion bei Angriffen (Mean Time To Detect – MTTD & Mean Time To Recover – MTTR)
- ✓ Eliminierung von False-Positive Ereignissen
- ✓ Skalierbarkeit und Automatisierung
- ✓ KI gestützte Generierung von präparierten Systemen
- ✓ Erkennung von OT als auch IT-Gefährdern

[1])Foto taken by Helwig Brunner Unter CC license 2.5 gestellt von Dr. Peter

mVISE AG | Wanheimer Straße 66 | 40472 Düsseldorf | security@mvise.de | +49 211 781 780 0 | www.mvise.de

Setzen klassische IT-Sicherheitsmechanismen auf eine klare Perimeter-Verteidigung mit gut kontrollierten Zugängen, kann man diese mit einer Festung aus dem Mittelalter gleichsetzen. So ist die unüberwindbare Festungsmauer die Next-Gen Firewall, die Zugbrücke mit ihren Wachen kann mit IPS/IDS, Anti-Virus und DLP gleichgesetzt werden.

Die Erkennung von Bedrohungen kann im Verhältnis zur klassischen IT-Sicherheit ohne eine Vielzahl von komplexem und ausgefeiltem Regelwerk realisiert werden. Es lässt sich folgern, dass der legitime Nutzer Ressourcen nur innerhalb seines Aufgabenspektrums verwendet und andere Ressourcen unbeachtet lässt.



Deception Technologie erkennt und lenkt die Inside-the-Network Angreifer Aktivitäten

Das Bild einer Festung zeigt auch, dass diese durchaus überdacht werden muss, wenn moderne IT-Systeme betrieben werden sollen. Denn zu jeder Festung gehören neben den Angreifern von außen, auch Spione und Saboteure. Letztere sind umso vernichtender, je länger sie unentdeckt schalten und walten können. Auch kann eine Burg nicht einfach skalieren, um mehr Platz zu schaffen. Der Umbau ist aufwendig und nicht ohne Risiko durchzuführen.

Säulen der Deception Technologie

Um diese Risiken eines Angreifers im Inneren begegnen zu können, bedarf es der Aufklärung und Sichtbarkeit. Eine gute Deception Technologie basiert also auf drei Säulen: Der Erkennung (Detect), der Ablenkung (Deceive) und den Umgang (Defeat) mit Bedrohungen.

Somit muss nun ein Angreifer lediglich in Versuchung geführt werden, präparierte Systeme anzugreifen und nicht die echten Assets. Hierzu macht man sich zu nutzen, wie Angreifer vorgehen:

1. Beschaffung von Informationen
2. Initialer Angriff
3. Horizontale Ausbreitung
4. Angriff auf Daten und Informationen
5. Monetarisierung

Ein aktiver Admin-Account wird wohl interessanter sein für jemanden, der sich ohne Legitimation ausbreiten möchte, als ein deaktivierter Gast-Account. Wichtig dabei ist, dass der Angreifer die ihm zugeworfenen Informationen – auch Brotkrümel und im englischen Breadcrumbs genannt – als legitime Informationen annimmt. Mit diesen Brotkrümeln wird der Angreifer dann versuchen, das nächste

Ziel anzugreifen. Deception-Lösungen schaffen es, dass der Angreifer auch nach dem Ausnutzen der Brotkrümel nicht feststellen kann, dass er sich in die Falle begeben hat. Dies ist Aufgabe der geschickten Ablenkung (Deceive).

Ist der Angreifer identifiziert und in einen Bereich gelenkt worden, wo er kein Unheil anrichten kann, bleibt die Frage, wie man mit der Bedrohung umgehen soll (Defeat). Je nach Typ des Angreifers kann man diesen beobachten, um seine Methodik zu studieren, bevor man den Angreifer aussperrt, denn sein Angriff ist so oder so bereits erfolgreich abgewehrt.

Deception Technologie ist somit ein wichtiger Baustein in jeder IT-Sicherheitsstrategie, um Angreifer, die bereits Perimetersysteme überwunden haben, zu erkennen, abzulenken und schließlich zu neutralisieren.

Was bietet mVISE an?

Die mVISE AG bietet ein umfassendes Leistungsspektrum rund um das Thema Informationssicherheit. Kunden profitieren von einem ganzheitlichen Lösungsansatz.

mVISE unterstützt, berät und realisiert IT-Security-Projekte in allen Phasen: von der Konzeption bis zur Umsetzung. Die Herausforderungen der Digitalisierung löst mVISE gemeinsam mit den Kunden.

Mit der Deception Technologie wird das mVISE Beratungsportfolio um diesen innovativen Baustein erweitert. Bereits in mehreren Kundenprojekten hat sich gezeigt, dass diese Technologie ein wichtiger Bestandteil der Absicherung von IT-Systemen darstellt.

Über den Autor:

Bernhard Borsch ist als Manager IT-Security bei der mVISE AG tätig. Zu seinen Kernkompetenzen gehört neben PKI und Kryptographie auch das Themenfeld Cloud & Enterprise Security.

Derzeit unterstützt er mit seinem Team Kunden bei der Absicherung ihrer Enterprise Serverlandschaft.

Bernhard Borsch
Manager IT-Security
Mail: Bernhard.Borsch@mvise.de
Mobil: +49 152 341 512 36