Fidelis Cybersecurity

Datenblatt

Fidelis Deception Modul

Eine erfolgreiche Strategie - mit geringem Aufwand - für jedes Unternehmen geeignet
Angreifer ködern, locken, binden und abwehren, denn Prävention alleine reicht nicht

Die Chance, Angreifer zu erkennen, ohne nach ihnen zu suchen

Prävention alleine reicht nicht mehr aus, Angreifer werden irgendwann in jedes Netz eindringen. Die Aufgabe lautet also, diese zu erkennen, bevor sie Schaden anrichten können. Cyberkriminelle sind auf der Jagd nach Passwörtern und Anmeldedaten, mit denen sie weiter eindringen, Prozesse ausspionieren und Daten stehlen können. Aus Erfahrung wissen wir, dass menschliche Angreifer eher in E-Mails, Dateien, Dokumenten und unstrukturierten Daten nach Anmeldeinformationen suchen, wohingegen automatisierte Malware sich auf strukturierte Daten in Web-Browsern und Anwendungen konzentriert. Dabei geht es den Hackern vor allem um Passwörter, die ihnen die Bewegung im Netzwerk ermöglichen. Mit jedem erfolgreich ausgeführten Schritt können Angreifer weiter unbemerkt agieren und digitale Spuren vermeiden, die sie verraten könnten. ***In dem Wissen, worauf es die Angreifer abgesehen haben, liegt die Chance für eine aktive Verteidigung: Angreifer anlocken, binden und abwehren.***

Die Anforderungen

- Angreifer und Malware im Netzwerk automatisiert und sicher erkennen
- Valide, zuverlässige Alarme mit wenigen oder gar keinen Fehlalarmen generieren
- Erkennung & Untersuchung, dabei Abwehrmaßnahmen automatisieren
- Die Wirksamkeit und Effizienz von Sicherheitsmaßnahmen steigern
- Maßnahmenketten für eine weiterhin verbesserte Abwehr entwickeln

Die Lösung: Deception

- Eine umfangreiche Auswahl an realistischen Ködern, glaubhaften Brotkrumen und Lockvögeln
- Klone von echten Daten, Diensten und Betriebssystemen, emuliert und alles automatisch aktualisiert
- Köder mit speziellen Anwendungen, die Hacker beschäftigen, binden und deren Zeit kosten
- Erkennung von Angreifern anhand ihrer Zugriffe auf Brotkrumen und Ködern sowie Man-in-the-Middle Überwachung und Analyse des Datenverkehrs
- Köder vor legitimen Nutzern verbergen, um unbeabsichtigte Zugriffe und somit False-Positives zu verhindern

Inventarisierung

- Erfasst fortlaufend das Netzwerk und vorhandene Ressourcen
- Erstellung und Aktualisierung von Profilen für Standort, Nutzung, Typ usw. von Ressourcen

Ergebnis: Eine individuelle Grundlage für jeden ausgelegten Köder

Köderdesign

- Entwicklung von Täuschungsmaßnahmen ausgehend von der realen Umgebung im Unternehmen
- Automatischer Aufbau eines Ködernetzes basierend auf echten Ressourcen, Diensten und Prozessen

Ergebnis: Ein realistisches und attraktives Ködernetz und Täuschungsmanöver

Verteilung

- Automatische Platzierung von Ködern in Netzwerken
- Ausstreuen von Brotkrumen in echten Ressourcen und Active-Directory-Inhalten

Ergebnis: Eine schnelle Bereitstellung und hohe Effizienz

Erkennung

- Alarmierung beim Zugriff auf Köder und deren Nutzung
- Analyse bei Nutzung der Köderdaten (z. B. hinsichtlich Anmeldedaten)

Ergebnis: Eine zuverlässige Erkennung von humanen und Script-Angreifern, Insider-Threats und ähnlichen Gefahren

Anpassung

- Erkennung neuer Ressourcen und Netzwerkstrukturen
- Automatische Updates des Netzwerkzustands und der ausgelegten Köder

Ergebnis: Eine Abwehr durch intelligente und anpassungsfähige Täuschungsmanöver

„Fidelis Deception hat sich als sehr effizient erwiesen. Die Köder waren ein hervorragendes Mittel zur Erkennung von Auffälligkeiten, ohne wie bei anderen Verfahren Datenmassen durchsuchen zu müssen."

Weston Nicolls, SVP, Information Security Manager, First Midwest Bank

Wie Täuschungsmaßnahmen funktionieren

Intelligente Deception findet Angreifer mit Hilfe von Brotkrumen, Ködern und Attrappen, um menschliche Hacker und automatisierte Malware zu locken und zu binden, von welchen bekannt ist, dass sie Hunderte von Anwendungen scannen. Deception verändert das Spielfeld in der Sicherheit. Anstatt vergeblich nach dem bösen Akteur in einem „Ozean" guter Daten zu suchen, liefert Deception aussagekräftige Alarme und Ereignisse von Ködern, MITM-Verhalten und Verkehrsanalysen. Diese haben eine extrem hohe Zuverlässigkeit und wenige False Positives. Fidelis Deception geht noch einen Schritt weiter und bietet verfälschte Zugangsdaten einschließlich Active Directory-Einträgen und simulierten Zugriffen auf Unternehmensressourcen. Diese so nachgebildeten Zugangsdaten bilden ein überzeugendes Scheinnetzwerk, das Geräte, Daten und Verhaltensweisen enthält, die alle dazu dienen, den Angreifern den Spieß umzudrehen. Sie verfolgen die Köder, damit die Verteidiger sie erkennen, daraus lernen und sich erfolgreich verteidigen können.

Köderprofile

- **Hardware:** Laptops, Server, Router, Switches, Kameras, Drucker, IoT-Geräte im Unternehmen usw.
- **Software:** Betriebssysteme, Apps, Ports, Services, Anwendungen und ähnliche Daten
- Die Köder sind nicht direkt sichtbare und gut verborgene Informationshappen. Die Mitarbeiter des Unternehmens haben keinen Anlass, darauf zuzugreifen oder sie zu nutzen.
- Köder halten Angreifer beschäftigt und lenken sie weg von den wirklich wertvollen Ressourcen.

Brotkrumen, Fallen und Lockvögel

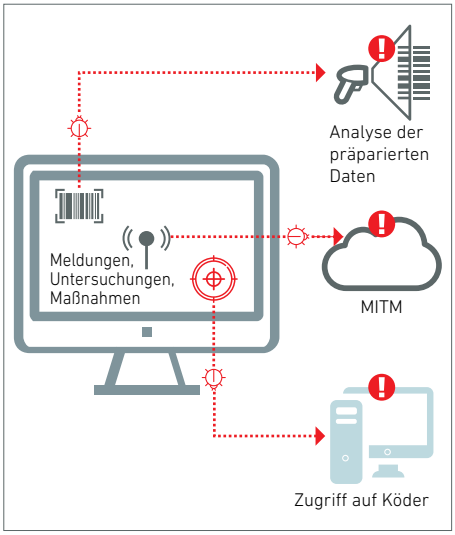
- **Fallen:** Dateien, Anwendungen und Zugangsberechtigungen
- **Brotkrumen:** Dateien, Dokumente, E-Mails, Systemressourcen usw.
- **Lockvögel:** Präparierte Daten, oft in Form von Anmeldedaten oder von Angreifern genutzten Profilen

Erkennung von Angreifern nach dem Eindringen

- Zugriff auf unbekannte Ressourcen, die als Köder dienen (z. B. durch Angreifer oder Betriebsangehörige)
- Datenanalysen zeigen die Verwendung der präparierten Daten (z. B. spezielle, nachgebildete Anmeldedaten)
- Beobachtung der Nutzung der Köder und Brotkrumen durch die Angreifer
- Analyse des Netzwerks in der Umgebung der Köder, Warnung bei Datenzugriff

Intelligente Täuschung

- Automatisierte und angepasste Bereitstellung von Ködern und Brotkrumen
- Erkennt laterale Ausbreitung, Command-and-Control-Datenverkehr und die Ausschleusung von Daten
- Transparenz und Forensik, um die Taktiken, Techniken, Verfahren und die gewünschten Assets zu erlernen.
- Zentrale Konsole mit umfassendem Überblick über Analysen, Aufspüren und Abwehrmaßnahmen
- Keine Beeinträchtigung des Geschäftsbetriebs, kein Risiko für Daten oder Ressourcen



Zuverlässige Meldungen mit sehr wenigen Fehlalarmen

„DDPs [Distributed Deception Platforms] bieten eine neue Art von Erkennungsmöglichkeiten, indem sie Täuschung nutzen, um Erkennung und Reaktion zu beschleunigen und zu verbessern, unabhängig davon, ob ein fortgeschrittener Angreifer ausweichend agiert."

Gartner: „Competitive Landscape: Distributed Deception Platforms, 2016", Lawrence Pingree, Aktualisierung: 26. Dezember 2017 | Erstveröffentlichung: 04. August 2016, G00310123

Warum Fidelis Deception?

Fidelis Deception geht weit über Honeypots und klassische Täuschungsmanöver hinaus, indem es intelligente Deception betreibt, die Angreifer und Malware anlockt, verwirrt und ausbremst. Fidelis Deception hilft Sicherheitsteams bei der Erkennung verborgener Angreifer, beim Erlernen neuer Angriffstechniken und beim Schutz kritischer Datenbestände. Das Fidelis Deception Modul analysiert den internen Ost-West-Verkehr, während Fidelis Network eine unübertroffene Analyse des Nord-Süd-Verkehrs liefert. Fidelis automatisiert die Erkennung und Reaktion auf Cyberangriffe über Netzwerke und Endpunkte hinweg mit Hilfe unserer innovativen, speziell entwickelten und durchgängigen Technologien. Fidelis stärkt First-Level-Responder und hilft auch fortgeschrittenen Incident Response Spezialisten bei der Identifizierung, Untersuchung, Validierung und Reaktion auf Bedrohungen.

Nehmen Sie Kontakt mit uns auf, wenn Sie mehr über Fidelis erfahren möchten

Fidelis Cybersecurity | +49 30 4081 73 210 | dach@fidelissecurity.com

Fidelis ist die einzige integrierte, automatisierte Plattform für die Erkennung und Bekämpfung von Cyberangriffen in Netzwerken und auf Endpunkten. Die Elevate™-Plattform von Fidelis steigert die Wirksamkeit und Effizienz von Sicherheitsteams, indem sie Warnmeldungen zu rasch auswertbaren Bedrohungszusammenfassungen bündelt und die erforderlichen Analyse- und Abwehrmaßnahmen automatisiert. Fidelis bestätigt, analysiert und vereitelt Angriffe automatisiert, sorgt für Netzwerk- und Endpunkttransparenz und zeichnet sich durch die schnelle Reaktion auf sicherheitsrelevante Bedrohungen aus. Deshalb vertrauen einige der renommiertesten Unternehmen der Welt auf Fidelis.

