Cyber Polygon 2021 Trainings beschreibung

Heute entstehen unzählige digitale Ökosysteme überall um uns herum. Sie werden von Ländern erstellt, große Unternehmen und sogar kleine Unternehmen zum Zweck der Rationalisierung ihrer Operationen. Beide beinhalten eine große Anzahl von Wechselwirkungen extern und intern, wobei alle Parteien eng miteinander verbunden sind verbunden. In diesem Zusammenhang die Sicherheitslücke der Lieferketten ist zu einem wachsenden Problem geworden: Ein Angriff auf ein einzelnes Unternehmen kann eine Gefahr darstellen das gesamte Ökosystem. In den letzten Jahren sind Lieferketten häufig geworden Ziel von raffinierten Angriffen, die werden schwerer zu erkennen und zu verhindern. Allein im Jahr 2019 solche Angriffe stiegen im Vergleich um fast 80% zum Vorjahr[1]. Der Trend hielt bis 2020 an mit einer Reihe von massiven Unterbrechungen der Lieferkette das betraf Hunderte von Organisationen und Millionen von Menschen weltweit. Die Sicherheit der Lieferkette ist kein zu lösendes Problem in einem Augenblick. In diesem Sinne das zentrale Thema Das Training in diesem Jahr wird die Sicherheit des Ökosystems sein und Abschwächung von Supply-Chain-Angriffen.

[1] 'Internet Security Threat Report', *Broadcom*.

Die Teilnehmer werden ihre Fähigkeiten trainieren bei der Abwehr eines gezielten Supply-Chain-Angriffs auf einem Unternehmensökosystem

Format

Letztes Jahr übten die Teams Reaktionsmaßnahmen im Moment eines gezielten Angriffs und untersuchte den Vorfall. Ein solches Format erwies sich als effektiv und ermöglichte es den Teams, ihre praktischen Fähigkeiten zu verbessern.
Wir haben uns entschlossen, das gleiche Format mit nur wenigen Änderungen beizubehalten, um den Wünschen der Teams gerecht zu werden.
Die Schulung umfasst zwei Szenarien.

Verteidigung

Die Teilnehmer lenken einen aktiven Angriff ab auf einem Unternehmenssystem, das für das Zusammenstellen, Testen und Bereitstellen von Anwendungen verantwortlich ist. Das System verwaltet den gesamten Lebenszyklus des geschäftskritischen Service des Unternehmens.

Antwort

Die Teams werden den Vorfall untersuchen, der damit begann, dass der Host einer Tochtergesellschaft kompromittiert wurde. Der Host kommuniziert über VPN mit dem Netzwerk des Clients. Wie im letzten Jahr werden die Teilnehmer klassische Forensik- und Bedrohungsjagdtechniken anwenden.

Rollen

Red Team

Schulungsorganisatoren von BI.ZONE, simulieren Sie den Angriff.

Blue Team

Die teilnehmenden Teams schützen ihre Segmente der Trainingsinfrastruktur.

Bedingungen für die Beteiligung

1. Es können nur Organisationen teilnehmen (bitte verwenden Sie Ihre Unternehmens-E-Mail-Adresse, um sich zu bewerben).

2. Eine Organisation - ein Team. Die Nummer der Mitglieder ist nicht beschränkt.

3. Die Schulung richtet sich an Cybersicherheits- und IT-Spezialisten mit unterschiedlichem Hintergrund. Für Teams wäre es von Vorteil, Forensik-, Sicherheitsanalyse- und SOC-Spezialisten als Mitglieder zu haben.

4. Alle Aufgaben werden remote ausgeführt: Die Teams erhalten Zugriff auf eine virtuelle Cloud-Infrastruktur.

5. Neben der vorinstallierten Software
Die Teilnehmer dürfen alle Anwendungen und Dienstprogramme verwenden, die zum Schutz ihrer Segmente der Schulungsinfrastruktur beitragen.

6. Das Training ist eher als pädagogische Übung als als Wettbewerb gedacht, daher werden die Ergebnisse anonymisiert.

Szenario 1.
Verteidigung

Legende

Während eines Angriffs kann eine unbekannte Hackergruppe Netzwerkzugriff auf ein Segment der virtuellen Unternehmensinfrastruktur erhalten. Dieses Segment enthält Services, die für die kontinuierliche Integration und Bereitstellung der Webanwendung des Unternehmens verantwortlich sind.

Die Bedrohungsakteure konnten keinen Zugriff auf die virtuellen Server erhalten, stahlen jedoch große Mengen an Informationen über die zu entwickelnde Anwendung, einschließlich Teilen des Quellcodes und der Entwicklungsdokumentation.

Das Hauptziel der Gruppe sind die Benutzerdaten, die von der Anwendung verarbeitet werden. Zu diesem Zweck planen die Angreifer, die gestohlenen Informationen zu verwenden, um den Entwicklungsprozess zu manipulieren und Hintertüren in die Anwendung einzubetten.
Die Gruppe könnte dann zur letzten Phase übergehen: Angriff auf die Anwendung in der Produktionsumgebung
und die gewünschten Daten in Besitz nehmen.

Zielsetzung

DEvelop-Fähigkeiten zur Abwehr gezielter Cyberangriffe auf einem geschäftskritischen System.

Blue Team Actions

Die Teilnehmer müssen:

- enthalten den Angriff so schnell wie möglich
- die Sicherheit gewährleisten der Lieferkette der Anwendung
- Minimieren Sie die Menge von kompromittierten Informationen
- Aufrechterhaltung der Verfügbarkeit

der Zielwebanwendung und der gesamten Lieferkette

Das Blue Team kann alle Methoden und Tools anwenden, um seine Infrastruktur zu schützen. Sie können auch Systemschwachstellen beheben, indem Sie den Servicecode und die Konfiguration verbessern.

Szenario 2. Antwort

Legende

Das Blue Team schützt das Ökosystem einer großen Unternehmensgruppe. Einer der Workstation-Benutzer der Muttergesellschaft meldet verdächtige Dateien in einem Verzeichnis. Die Untersuchung identifiziert den Kompromissvektor, insbesondere das installierte Update auf eine geschäftskritische Anwendung, die von einer Tochtergesellschaft entwickelt wird.

Das Blue Team erhält Zugriff auf die Threat Hunting-Plattform des Mutterunternehmens, auf der EDR- und NTA-Ereignisse zusammengefasst sind. Die Teilnehmer werden beauftragt, mithilfe des Threat Hunting-Ansatzes so viele Artefakte wie möglich zu finden.
Darüber hinaus stellt das Team fest, dass die Infrastruktur durch eine Änderung kompromittiert wurde

Update in einer geschäftskritischen Anwendung installiert. Das Update wurde von einer Tochtergesellschaft bereitgestellt, die für die Softwareentwicklung zuständig ist. Deshalb,
Der Schwerpunkt der Untersuchung wird wechseln an die Infrastruktur der Tochtergesellschaft.

Die untergeordnete Organisation verwendet keine EDR-Lösung. Aus diesem Grund müssen die Teilnehmer auf die klassische Forensik zurückgreifen und so viele Artefakte der Verletzung wie möglich finden.

Zielsetzung

Entwickeln Sie Fähigkeiten in der Untersuchung von Vorfällen auf einen erfolgreichen Phishing-Angriff.

Blue Team Actions

In beiden Fällen muss das Blaue Team eine Reihe von Aufgaben lösen und die bereitgestellten Daten analysieren. Die Analysemethoden unterscheiden sich jedoch.

Muttergesellschaft

Die Teilnehmer werden nachforschen den Vorfall durch Bewerbung der Threat Hunting-Ansatz, bei dem Telemetrie gesammelt wird die Hosts und Netzwerkserver.

Tochtergesellschaft

Das Blaue Team wird nachforschen der Vorfall mit den Methoden und Werkzeugen der klassischen digitalen Forensik.