منشآت
monsha'at
الهيئة العامة للمنشآت الصغيرة والمتوسطة
Small & Medium Enterprises General Authority
مركز الابتكار

كتيّب

استخدام نموذج Cyber Kill Chain في كشف الهجمات السيبرانية ومنعها

تأليف
رامي بن عبد الرحمن الغانمي

Thakaa_center Thakaacenter

سياسة الاستخدام

إن المعلومات الواردة في هذا التقرير جُمِعَت ونُسِّقت بجهود موظفي مركز ذكاء التابع للهيئة العامة للمنشآت الصغيرة والمتوسطة "منشآت"، ولا ينبغي لقارئها أن يعمل بها دون مشورة مناسبة من المتخصصين.

للمزيد من المعلومات، نرجو التواصل معنا على البريد الإلكتروني: **support@thakaa.sa**

فهرس الكتيب:

- مدخل
- مراحل Cyber Kill Chain
- ضوابط أمنية لمنع الهجمات من خلال Cyber Kill Chain
- مخاوف حول استخدام Cyber Kill Chain
- ملخص
- مراجع

مدخل:

تتطور الهجمات السيبرانية بشكل لحظي وتستهدف جميع الأفراد والكيانات، غير أن استهداف المؤسسات يتم التخطيط له بشكل مجدول وبطرق احترافية لوجود أنظمة كشف وحماية، بل أن الخطير في اختراق المنظمات محاولة المخترقين في أن يضلوا داخل شبكات ضحاياهم لفترات طويلة دون أن يتم اكتشافهم لتحقيق أكبر مكاسب ممكنة، كما ذكرت هذه الدراسات دقة الهجمات الإلكترونية المتقدمة وأنها تتم من خلال عدة مراحل فهمها يساعد على منعها وهذا بالضبط ما سوف نقوم به من خلال استخدامنا لهذا النموذج.

طورت شركة لوكهيد مارتن هذا الإطار، والذي اشتقته من نموذج عسكري يستخدم لتحييد الأهداف بشكل فعال من خلال توقع الهجمات وإيقافها وكيفته على مجال الأمن السيبراني.
وتدور فكرته في تمثيل دور المخترقين ومحاكات مراحل هجومهم وكيفية عمل كل خطوة من خطواتهم والتي يصلون بها إلى ضحاياهم باستهداف نقاط ضعفهم لاستغلالها تحقيقاً لمكاسب خاصة لهم وضارة بالتأكيد على ضحاياهم، ويعتبر هذا النموذج من أهم المعارف والسبل التي يجب على كل متخصص بمجال الأمن السيبراني الحرص على تعلمها والاستفادة منها، كما يمّكن هذا الإطار الجهات من اكتشاف الهجمات المتقدمة وتحييد ضررها ويساعد في اتخاذ الاحتياطات الوقائية اللازمة لمنع حدوثها.

مراحل Cyber Kill Chain:

أولاً: الاستطلاع Reconnaissance

تحديد الضحية واختيار أفضل وسيلة لاختراقه، من خلال إجراء بحث وتجميع أكبر قدر من المعلومات المفيدة عن الهدف، لاكتشاف نقاط ضعفه والثغرات الممكن استخدامها كنقطة انطلاق للهجوم السيبراني على الضحية، والتي قد تكون على سبيل المثال: عناوين IP و MAC ونوع نظام التشغيل والمنافذ المفتوحة والخدمات الموجودة وتفاصيل البنية التحتية خصوصاً الأمنية من نقاط الضعف، والسياسات والآليات المطبقة وأي تفاصيل تخص المستخدمين للشبكة من أسماء وعناوين وحسابات داخلية أو في مواقع وسائل التواصل، وأرقام الهواتف الخاصة بهم، ويعد هذا كله لتسهيل اختيار طرق الهجوم وأنواع التسليح كما سيأتي معنا في المراحل الأخرى.

ثانياً: التسليح Weaponization

بعد أن ينتهي المخترق من جمع المعلومات اللازمة حول أهدافه المحتملة وتحديده أفضل وسائل الاختراق – نقاط ضعف وثغرات – يبدأ في تخصيص وسيلة - برنامج أو ملف مصاب أو رابط خبيث ...إلخ - لإرساله لضحيته كما سيأتي في المراحل القادمة، ويختلف هذا النوع من التسليح بناءً على نية المهاجم والوضع الأمني للهدف، حتى يحقق الغاية التي يرغب بها هذا المخترق.

ثالثاً: التوصيل Delivery

ببساطة هي عملية نقل وسيلة المخترق في مرحلة Weaponization إلى الضحية حسب الطريقة المخطط لها سواء بالهندسة الاجتماعية باختلاف أنواعها – التصيد الاحتيالي أشهرها – أو توظيف شخص بداخل الجهة أو اختراق ضعف أمني.

رابعاً: الاستغلال Exploitation

هنا يبدأ الهجوم الفعلي بواسطة الطريقة التي تم تصميمها في مرحلة Weaponization بتنشيط الأداة الضارة واستغلال الثغرة الأمنية لدى الهدف، ووصول المخترق لهذه المرحلة يعني أنه نجح في هجمته السيبرانية.

يبدأ المهاجم في تحقيق أهدافه من خلال التنقل في شبكة الضحية والاستفادة مما يجمعه من بيانات حساسة وخاصة عن المستفيدين والأنظمة المستخدمة ويشمل ذلك ما قد تحتويه من معلومات مهمة مثل أسماء المستخدمين والحسابات البنكية والمستندات السرية وكلمات المرور وغيرها من البيانات المهمة.

بالطبع هذه البيانات لا تتواجد كلها في مستوى صلاحية واحدة، بل يحتاج المخترقون بعد نجاح وصولهم لشبكة الضحية إلى تصعيد صلاحياتهم وهنا تبدأ مرحلة أخطر على أنظمة الضحايا لأنها تحقق أهداف كبرى لدى المهاجمين وهي الحصول على أسرار التجارة والبيانات الحساسة التي أثبتت التجارب السابقة لأشهر الاختراقات التي حصلت أنها كلفت الجهات المخترقة ملايين الريالات وأثرت على سمعتها، بل بعضهم أخرجتهم من المشهد.

في هذا المستوى من الهجمة قد يختار المخترقون الاكتفاء بما تم الحصول عليه والبقاء متخفين لمزيد من المكاسب والاستمرار في الهجمة أو الخروج مع ترك باب خلفي في حال الرغبة بالعودة كما هو حال بعض المهاجمين.

خامساً: التثبيت Installation

يحاول المخترق توسيع نقاط وصوله بحيث لا يتم قطع اتصاله وإفشال هجمته بسهوله فيكون لديه عدة طرق للبقاء في نظام الضحية ولهذا هدفه الرئيسي في هذه المرحلة هي إبقاء اتصاله فعالاً ليستمر هجومه وتثبيت برنامجهم الضار Malware واستخدام أدواتهم مثل Trojan Horses وBackdoors على شبكة الضحية ليضمنوا بقائهم متخفين أطول فترة ممكنة.

سادساً: القيادة والسيطرة Command & Control (C2)

عادة مايقوم المخترق المحترف في هذه المرحلة بإنشاء قناة اتصال بين خادم معد للقيادة والسيطرة يسمى عادة Server C2 وجهاز الضحية دون إذن الضحية أو علمه. تتيح قنوات الاتصال التي ينشؤها المخترق مع الأجهزة المخترقة (وتسمى Zombies) التحكم عن بعد من خلال شبكة تسمى Botnet. يقوم المخترق بالتحكم بشبكة Botnet مكونة من عدد كبير من أجهزة ضحاياه لعمل مجموعة من الوظائف التي تخدم المخترق كالإطاحة بالخدمات الالكترونية DDoS Attacks، واستغلال شبكة Botnet كأصول حوسبية لتحقيق عوائد مالية من خلال مايعرف ببيع الاختراق كخدمة Attack-as-a-Service، أوتعدين العملات الرقمية.

سابعاً: الإجراءات على الأهداف Actions on objectives

هي المرحلة النهائية للهجوم السيبراني وفيها يتم تحقيق المستهدفات من هذا الاختراق
بعد أن تم إنشاء بنية تحتية متكاملة لتنفيذه من خلال الوصول لشبكة ونظام الضحية والمحافظة على الاتصال بها وفتح مداخل خلفية لتسهيل دخول الأوامر وخروج البيانات أن لزم وتم التحكم بالنظام والسيطرة عليها هنا يتم استخدامها في تحقيق الأهداف المرسومة مسبقاً لهذا الهجوم السيبراني مثل تعطيل الخدمة عبر مهاجمة خوادم الويب بما يعرف DOS Attack أو سرقة بيانات أسرار.

ضوابط أمنية لمراحل Cyber Kill Chain:

تعتبر الضوابط الأمنية ضرورية لمنع الهجمات السيبرانية والتخفيف من آثارها، بدءاً من مرحلة الاستطلاع وحتى الهدف النهائي، ومن خلال تطبيق الضوابط الأمنية المناسبة في كل مرحلة، يمكن للمؤسسات تعطيل أو إيقاف أي هجوم

1- الاستطلاع: هذه هي المرحلة الأولية التي يجمع فيها المهاجمون معلومات حول أهدافهم، تشمل الضوابط الأمنية لمواجهة الاستطلاع ما يلي:

- جدار الحماية ونظام كشف/منع التسلل (IDS/IPS):

تراقب هذه الأدوات حركة مرور الشبكة ويمكنها اكتشاف الأنشطة المشبوهة أو محاولات الوصول إلى الموارد بشكل غير مصرح له

- تصفية الويب Web filtering: من خلال حظر الوصول إلى مواقع الويب الضارة المعروفة أو تحييد المحتوى المشبوه، الهدف هو منع المهاجمين من جمع المعلومات

2- التسليح: كما ذكرنا سابقاً، يقوم المهاجمون في هذا المستوى بإنشاء برنامج ضار أو تعديل أداة ضارة موجودة مسبقاً لاستغلالها في توصيلها.

تشمل الضوابط الأمنية لمواجهة التسليح ما يلي:

- نشر برامج مكافحة الفيروسات/برامج مكافحة البرامج الضارة Antivirus/Antimalware software's:

تقوم هذه الأدوات بفحص الملفات والبرامج بحثاً عن التعليمات البرمجية أو الأنماط الضارة المعروفة وتمنع تنفيذها أو نشرها.

- تصفية البريد الإلكتروني Email filtering:

باستخدام عوامل تصفية البريد العشوائي وتحليل المحتوى، يمكن للمؤسسات تحديد مرفقات أو روابط البريد الإلكتروني الضارة وحظرها.

3- اكتشاف الهجمات وتعطيلها بعد وصولها لبيئة المنشأة، وعادة ما يتم ذلك من خلال موائمة البيانات السجلات الداخلية للمنشأة مع البيانات الاستخباراتية الأقرب لبيئة المنشأة.

وهناك الكثير من الأمثلة من تطبيقات تستهدف كل واحدة من الفئات المذكورة.

4- التسليم: يقوم المهاجمون بتسليم الحمولة المسلحة إلى الهدف. تشمل الضوابط الأمنية لمواجهة التسليم ما يلي:

- بوابات البريد الإلكتروني: يمكن لهذه البوابات فحص رسائل البريد الإلكتروني الواردة والصادرة بحثاً عن المرفقات أو الروابط الضارة، مما يمنع تسليمها.

- جدران الحماية لتطبيقات الويب (WAF):

تستطيع جدران حماية تطبيقات الويب اكتشاف حركة مرور الويب الضارة وحظرها، مما يمنع المهاجمين من تسليم الحمولات عبر مواقع الويب المخترقة.

5- الاستغلال: يستغل المهاجمون نقاط الضعف والثغرات في الأنظمة والتطبيقات، لهذا تشمل الضوابط الأمنية لمواجهة الاستغلال ما يلي:

- إدارة التصحيح: يساعد تطبيق التصحيحات والتحديثات الأمنية بشكل منتظم في القضاء على الثغرات الأمنية المعروفة التي قد يستغلها المهاجمون.

- أنظمة منع التطفل (IPS): يمكن لأدوات IPS اكتشاف ومنع محاولات استغلال الثغرات الأمنية في الوقت الفعلي.

6- التثبيت: يقوم المهاجمون بتثبيت البرامج الضارة أو إنشاء موطئ قدم لهم داخل البيئة المستهدفة، تشمل الضوابط الأمنية لمواجهة التثبيت ما يلي:

- حماية أجهزة المستفيدين End-Points:

يمكن لبرامج مكافحة الفيروسات وأنظمة كشف التسلل المستندة إلى المضيف HIDS)) وأدوات اكتشاف النقاط النهائية للمستفيدين والاستجابة لها (EDR) واكتشاف البرامج الضارة ومنع تثبيتها على أجهزة المستخدمين.

- القائمة البيضاء للتطبيقات: من خلال السماح بتشغيل التطبيقات المعتمدة فقط، ومنع عمليات تثبيت البرامج غير المصرح بها.

7- القيادة والتحكم: يقوم المهاجمون بإنشاء قنوات اتصال مع الأنظمة المخترقة. تتضمن الضوابط الأمنية لمواجهة C2 ما يلي:

- مراقبة الشبكة:

يمكن للأدوات التي تراقب حركة مرور الشبكة اكتشاف الاتصالات المشبوهة أو أنماط الاتصال المرتبطة بأنشطة القيادة والتحكم.

- إدارة المعلومات الأمنية والأحداث (SIEM): يمكن لحلول SIEM تجميع وتحليل السجلات من مصادر مختلفة، مما يساعد في تحديد أنشطة C2 المحتملة.

8- الإجراءات المتعلقة بالأهداف: يحقق المهاجمون أهدافهم النهائية بهذه المرحلة من سرقة البيانات والأسرار التجارية أو تعطيل الخدمة وغيرها من الأهداف المضرة بضحاياها، لذا تشمل الضوابط الأمنية لمواجهة الإجراءات المتعلقة بالمرحلة الأخيرة من هذه السلسلة ما يلي:

- منع فقدان البيانات (DLP): يمكن لحلول DLP مراقبة ومنع عمليات نقل البيانات غير المصرح بها أو محاولات التصفية.

- ضوابط وصول المستخدمين: يمكن أن يؤدي تنفيذ آليات مصادقة قوية، وضوابط الوصول المستندة إلى الأدوار (RBAC)، ومبادئ الامتيازات الأقل إلى الحد من تأثير حسابات المستخدمين المخترقة.

من المهم ملاحظة أنه يجب تنفيذ هذه الضوابط على طبقات، بحيث تجمع بين الإجراءات الوقائية والكشفية والتصحيحية، بالإضافة إلى ذلك تعد التقييمات الأمنية المنتظمة وتدريب الموظفين وتوعيتهم المستمرة بأحدث تقنيات الهجوم والاستغلال والهندسة الاجتماعية بأنواعها وتنفيذ سيناريوهات وخطط الاستجابة للحوادث والتدرب عليها بشكل متكرر ولو على فترات طويلة – سنوية مثلا - مكونات حاسمة لإستراتيجية الأمن السيبراني الشاملة.

مخاوف حول استخدام Cyber Kill Chain :

على الرغم من أن هذا الإطار مشهور ومفيد للمؤسسات في فهم التهديدات وكيفية تنفيذ الهجمات عليهم وسبل صدها، إلا أن هناك بعض العيوب والمخاوف المحتملة التي يجب دراستها وأخذها بالاعتبار ومنها:

1. محدوديتها:

يركز هذا الإطار على الجانب التقني للهجمات، ويهمل العوامل الأخرى مثل الهندسة الاجتماعية والتهديدات الأخرى الداخلية.

2. التهديدات المتقدمة:

قد يتجاوز بعض المهاجمين المتقدمين من ذوي المهارات العالية والموارد الضخمة هذا النموذج بحيث ينفذون هجمات الثغرات الصفرية Zero Day Attack وبالتالي لا يوفر هذا النموذج الحماية الكافية فنتنبه.

3. التكلفة العالية:

تنفيذ هذا الإطار يتطلب موارد لا يتحملها الجميع من موظفين مهرة وتقنيات متقدمة ومراقبة مستمرة ولهذا قد لا تستفيد منه الجهات ذات الميزانيات المحدودة.

4. تحديات الامتثال:

قد تعترض خطة تنفيذ هذا النموذج تشريعات لبعض القطاعات الحساسة لا تمكنها من استخدامها والاستفادة منها ولذا يجب التأكد من المعايير التنظيمية قبل الشروع في تطبيق الإطار.

5 . عدم فعالية الحلول:

ربما ينتج من استخدام هذا النموذج إلى إنشاء كمية كبيرة من التنبيهات الزائفة، مما يجعل من الصعب تحديد الهجمات الحقيقية ويشغل فرق الأمن عن التهديدات والمخاطر التي ممكن أن تتحقق ولذا يجب على المؤسسات اختيار الحلول التي توفر دقة عالية في التحليل والكشف عن الهجمات بالإضافة لهذا الإطار.

6. التأخر في الكشف:

قد يؤدي الاستخدام المتكرر لهذا الإطار إلى تأخر كشف الهجمات السيبرانية ولذلك من الأفضل أن يتم التنويع استخدام الأدوات والتقنيات الأخرى للكشف عن الهجمات السيبرانية لرفع فرص الكشف والحماية الناجحة.

ملخص:

ناقشنا في هذا الكتيب ماهية وأهمية هذا الإطار وأن فكرته تتلخص بأن نفكر كمدافعين عن شبكاتنا وأنظمتنا بعقلية المهاجمين وذكرنا المراحل السبع التي يستخدمها المخترقين في تنفيذ هجماتهم السيبرانية، ثم انتقلنا لمسار وضع ضوابط أمنية تساعد من التخفيف من هذه المراحل السبع وإخمادها قبل حدوثها ثم ذكرنا المخاوف من استخدام هذا النموذج والسلبيات التي قد نتعرض لها من خلال تنفيذه بشكل عملي.

شكراً