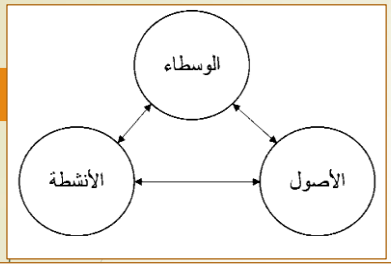
أمن المعلومات

GS224 - 10

التهديدات :



تنشأ التهديدات من أشخاص لهم دوافع (الوسطاء) للقيام بأنشطة محددة لاستغلال الأصول. إن التفاعل بن الوسطاء والأنشطة والأصول ذات العلاقة يمثل نموذج التهديد الذي يواجه المؤسسة، وهذا التفاعل موضح في الشكل التالي.

وفي هذا الفصل سنستخدم جزءاً من نموذج تصنيف الحوادث المعروف (VERIS)، وهو الجزء الذي يتعامل مع التهديدات بوصفها أساساً للمناقشة. وبينما يعتمد بعض الوسطاء والأنشطة في هذا الفصل على نموذج التهديد (VERIS)، والفكرة عامة هي كون التهديدات أنشطة للوسطاء تهدف للتأثير في الأصول.

ويعد نموذج (VERIS) نموذجاً عاماً يسمح لأي تهديد، بما في ذلك التهديدات التي لم تُكتشف بعد، ليكون ضمن هذا النموذج. وينسجم النموذج أيضاً مع الأدبيات الأكاديمية حول هذا الموضوع وكذلك مع نماذج المخاطر القياسية، ومن هنا تأتي أهمية استخدام نموذج التهديد (VERIS) .

التهديدات : نموذج التهديد (STRIDE) من مايكروسوفت

يعتبر نموذج (STRIDE) أحد النماذج المستخدمة في تصنيف التهديدات، وقد سمي باسم الفئات الست المستخدمة في تصنيف تهديد معين.

1. انتحال الهوية (**S**poofing identity): وأحد أمثلة انتحال الهوية هو الوصول غير المشروع للنظام واستخدام معلومات الاعتماد لمستخدم آخر مثل اسم المستخدم وكلمة المرور.
2. العبث بالبيانات (**T**ampering with data) : وينطوي العبث بالبيانات على التعديلات الخبيثة في البيانات. ومن الأمثلة على ذلك التغييرات غير المصرح بها على البيانات الثابتة، مثل تلك الموجودة في قاعدة البيانات، وتغير البيانات التي تنتقل بين أجهزة الحاسب الآلي عبر شبكة مفتوحة مثل الإنترنت.
3. التنصل (**R**epudiation): ترتبط تهديدات التنصل بالمستخدمين الذين ينفون تنفيذهم لنشاط معين دون وجود وسيلة إثبات خلاف ذلك لدى الأطراف الأخرى-على سبيل المثال، مستخدم يقوم بإجراء نشاط غير قانوني على نظام يفتقر لقدرة تتبع العمليات المحظورة. ويشير عدم التنصل (Non-repudiation) إلى قدرة النظام على مواجهة تهديدات التنصل. ً مثلا شراء المستخدم لغرض ما قد يستوجب التوقيع على ُ إيصال الاستلام. ويمكن للمورد استخدام الايصال المَوقع ليكوّن دليلا على أن المستخدم استلم المشتريات.
4. الإفصاح عن المعلومات (**I**nformation disclosure) : وتتضمن تهديدات الإفصاح عن المعلومات انكشاف المعلومات إلى أشخاص يفترض ألا يكون لديهم وصول لتلك المعلومات - على سبيل المثال، قدرة ُ المستخدمين على قراءة ملف ما بحيث لم يمنح لهم حق الوصول لهذا الملف، أو قدرة المتسلل على قراءة ُ البيانات المنتقلة بين جهازي حاسب آلي.
5. رفض الخدمة (**D**enial of service) : وتجرى هجمات رفض الخدمة النظام على رفض تقديم الخدمة . إلى مستخدمين حقيقين - على سبيل المثال، جعل خادم الشبكة غير متوفر أو صالح لاستخدام مؤقتاً ويجب الحماية ضد أنواع معينة من هجمات رفض الخدمة وذلك لتحسين الجاهزية والاعتمادية.
6. رفع الامتيازات (**E**levation of privilege) : وفي هذا النوع من التهديد يحصل المستخدم الذي لا يملك امتيازات الوصول إلى النظام على تلك الامتيازات ومن ثم يكون لديه حق الوصول لاختراق أو تدمير النظام بأكمله. وتتضمن تهديدات رفع الامتيازات تلك الحالات التي يتمكن فيها المهاجم من الاختراق الفعال لجميع دفاعات النظام، ويصبح جزءاً من النظام الموثوق نفسه وهذا وضع خطر حقا .

وسطاء التهديد : (الدخلاء/المتسللين)

وسيط التهديد:

وسيط التهديد هو فرد أو منظمة أو مجموعة تقوم بتأسيس نشاط تهديد معين. ويمكن تصنيف وسطاء التهديد إلى ثلاثة أنواع مختلفة، ولكل منها دوافع مختلفة للمبادرة في تأسيس التهديد:

1) الوسطاء الخارجيون.
2) الوسطاء الداخليون.
3) الشركاء.

وسطاء التهديد : الوسطاء الخارجيون

كما يوحي المسمى فإن الوسطاء الخارجيين هم وسطاء خارج المؤسسة ولا تربطهم أي صلة بالمؤسسة نفسها. ووفقاً لتقرير خرق البيانات (VERIS) لعام 2000 فإن 98% من الهجمات في عام 2000 نشأت من وسطاء خارجين. والتالي يوضح قائمة سريعة للوسطاء الخارجيين :

- **مجموعات الناشطين:**
  أصبحت مجموعة (المجهول) منتشرة في السنوات القليلة الماضية باعتبارها منظمة «اختراق سياسية» (hacktivist) ، وهذه المجموعة تخلط بن النشاط السياسي او الاجتماعي وأنشطة قرصنة المعلومات. وتتكون مجموعة (المجهول) من قراصنة المعلومات وغيرهم من المتحمسين الانترنت، وهم أعضاء مجهولون يصورون أنفسهم على أنهم يعارضون كل أنواع القمع الموجودة، والترويج لقضيتهم والإعلان عنها، كما يعارضون رقابة الجهات الحكومية على الإنترنت في جميع أنحاء العالم. وذلك من خلال هجمات تشويه الموقع ، او هجمات الحرمان من الخدمة، او سرقة البيانات وتوزيعها مما يؤدي إلى دعاية سلبية أو المساومة من اجل أهدافهم.

وسطاء التهديد : الوسطاء الخارجيون

الحكومات الأجنبية (الدخلاء):
ترعى الحكومات مجموعات قراصنة للقيام بأنشطة تجسس أو تخريب. تُعرف أيضًا بالتهديدات المستمرة المتقدمة (APTs) نظرًا لطبيعتها السرية والمثابرة و الاستمرارية على مدى فترات طويلة. وفقًا للتقرير الصادر عن مكتب مكافحة التجسس الوطني الامريكي في عام 2006 فإن «المعلومات الاقتصادية والتقنية الأمريكية الحساسة مستهدفة من قبل أجهزة المخابرات وشركات القطاع الخاص والمؤسسات الأكاديمية والبحثية، ومواطني عشرات الدول».
وتضمنت إحدى الحوادث التي حظيت بتغطية إعلامية الاشتباه بسرقة تصاميم طائرات عسكرية. ووفقا للتقرير فإن الصين تأتي على رأس القائمة وذلك للهجوم المتكرر للقراصنة الصينين على الشركات الأمريكية. وتجري الاستخبارات الروسية أيضاً نشاط تجسس إلكتروني ضد أهداف أمريكية وذلك لجمع المعلومات الاقتصادية والتكنولوجية ، كذلك حلفاء امريكا وشركاؤها يستخدمون إمكانية وصولهم إلى المؤسسات الأمريكية للوصول إلى المعلومات، وذلك باستخدام العديد من أنشطة التهديد. وتقدر خسائر التجسس الاقتصادي لتتراوح بين 2 مليار إلى 100 مليار دولار أو أكثر في العام الواحد.

ولا تقتصر الهجمات ضد امريكا حيث تشارك الحكومة الأمريكية أيضا في الحرب الإلكترونية. وتدعي صحيفة نيويورك تايمز أن امريكا وإسرائيل شاركتا في نشر دودة ستكسنت (Stuxnet)، والتي أدت إلى الإيقاف المؤقت 20% من أجهزة الطرد المركزي العاملة في المنشآت الإيرانية .

وسطاء التهديد : الوسطاء الخارجيون

التجسس الصناعي

في عام 2010 حكم على "ديفيد ين لي" بالسجن مدة 15 شهراً، كما امر بدفع أكثر من 30 ألف دولار تعويضاً لشركة (Valspar) ، وهي شركة لصناعة الدهانات والطلاءات ألصناعية. كان ديفيد ين لي المدير الفني السابق لتطوير المنتجات الجديدة لمجموعة (Valspar) المعمارية، وقدم استقالته من الشركة بعد عودته من رحلة إلى الصين. وعندما قام موظفو الشركة بفحص الحاسب الآلي المحمول وجهاز البلاك بري التابعة للشركة والتي أعادها "لي" بعد استقالته، لاحظ الموظفون آثاراً لأنشطة تشير إلى أن "لي" كان يحاول تغطية تحركات استخدامه لجهاز الحاسب الآلي المحمول. وكشف الفحص الدقيق لتلك الأجهزة إلى أن الأسرار التجارية للشركة قد تم تحميلها على جهاز الحاسب المحمول.

وسطاء التهديد : الوسطاء الخارجيون

المجرمين (الجرائم الإلكترونية):

في التسعينيات عندما كانت الإنترنت التجارية في مهدها، كان قراصنة الحواسيب «كأطفال البرامج النصية» (script-kiddies) ، أشخاص في سن المراهقة وجدوا برنامجاً نصياً في مكان ما وقرروا تشويه صفحة على الإنترنت فقط لإظهار أن قراصنة الحواسيب قادرون على تعديل بيانات شبكة الإنترنت، كذلك الاجتماع في منتديات سرية لتبادل النصائح والبيانات وتنسيق الهجمات. وقد دمرت العديد من هذه البرامج النصية بيانات الأجهزة المصابة بشكل لا مسؤول وذلك لإثبات هذا المفهوم فقط.

وبعد فترة من العمل المتواصل أصبح طفل البرامج النصية ذكياً. لماذا تقوم بتدمير الأجهزة بينما يمكنك كسب المال من مستخدم هذا الجهاز؟ لماذا تقوم باستبدال صفحة الشبكة في حين يمكنك الجلوس في المنزل ومراقبة كل الأنشطة حتى ترى شيئاً يعجبك؟. (بهدف الحصول على كسب مالي)

والآن ندخل إلى ما يسمى بالجرائم الإلكترونية. إن الجرائم الإلكترونية تجارة مربحة بشكل لا يصدق، فيها أرباح عالية مع انخفاض احتمال التعرف على الهوية ومن ثم المحاكمة مقارنة بالجرائم التقليدية مثل عمليات السطو على البنوك. ويعد «الغش الإلكتروني النيجيري» (Nigerian Scam) ، أحد أشهر وسطاء التهديد للجرائم الإلكترونية. فعندما يتم ارسال الآلاف من الرسائل في وقت واحد، حتما فإن المحتالين سيحصلون على بعض الردود، وتستمر جهود الحكومة لمنع الجرائم المالية الإلكترونية، حيث يتم لصق إعلانات على جدران مقاهي الإنترنت، وذلك لتحذير المستخدمين من الاعتقالات الممكنة للمحتالين الذين يرسلون رسائل البريد الإلكتروني الاحتيالية. ولكن بشكل عام تعلم المستخدمون الإنصات للقول المأثور «إذا كان شيء ما غير معقول، فربما يكون كذلك».

لاغوس، نيجيريا.

عناية: الرئيس / المدير التنفيذي

سيدى العزيز،

عرض عمل سري

بعد التشاور مع زملائي، واستناداً إلى المعلومات التي تم جمعها من غرف التجارة والصناعة النيجيرية، أفيدكم بأنه لدي صلاحية طلب مساعدتكم لنقل مبلغ ٤٧،٥٠٠،٠٠٠،٠٠ $ (سبعة وأربعون مليون وخمس مئة ألف دولار أمريكي) إلى الحسابات البنكية الخاصة بك. المبلغ المذكور نتج عن عقد وعن عمولة منفذة دفعت على مدار خمس سنوات من قبل مقاول أجنبي. وكان هذا العمل متعمداً حيث ظل المبلغ من ذلك الحين في حساب بنكي مُعلق في البنك المركزي النجيري (APEX BANK).

نحن الآن على استعداد لتحويل الأموال إلى الخارج وهنا يأتي دورك. ومن المهم أن أحيطكم علماً بأننا ممنوعون من فتح حسابات أجنبية لأننا موظفون مدنيون، ولهذا السبب نحتاج مساعدتك. وسيتم تقاسم المبلغ الإجمالي على النحو التالي: ٧٠٪ لنا، ٢٥٪ لك، و٥٪ لتكاليف حوادث التحويل المحلي والدولي.

وهذا التحويل خالٍ من المخاطر على كلا الجانبين. أنا محاسب لدى مؤسسة النفط الوطنية النيجيرية (Nigerian National Petroleum Corporation). إذا وجدت هذا العرض مقبولاً، نحتاج منك إلى الوثائق التالية:

اسم المصرف، رقم الهاتف، ورقم الحساب، ورقم الفاكس.

أرقام الهاتف والفاكس الخاصة بك - للسرية ولسهولة التواصل.

رسالة منك مختومة وموقعة.

وبدلاً من لذلك سنقوم بتزويدك بنص الرسالة المطلوب تحريرها بالإضافة إلى معلومات تفصيلية بخصوص المطلوب منك. وهذا العمل سيستغرق ثلاثين (٣٠) يوماً لإنجازه.

الرجاء الرد بسرعة.

تحياتي

وسطاء التهديد : الوسطاء الخارجيون

المجموعات المنظمة (العصابات):

تتطلب بعض التهديدات أن يتعاون العديد من الوسطاء بعضهم مع بعض؛ أن تنظيم بعض المجموعات للجرائم الإلكترونية أمر ملفت للنظر. على سبيل المثال، هناك مواقع تُنسق لبيع وشراء المعلومات المقيدة مثل بطاقات الائتمان، وأرقام الضمان الاجتماعي، ومعلومات الحسابات البنكية، واسرار شركات، غير ذلك. وعادة ما تقوم تلك المواقع الإلكترونية بتوظيف عدد كبير من الأفراد بحيث يكون لكل فرد واجباته الوظيفية الخاصة:

- المديرون: تشغيل حسابات الضمان ومراقبة العضوية.
- الوسطاء الدوليون: الإشراف على المحتوى وتحكيم النزاعات.
- المراجعون: تقييم جودة منتجات الموردين.
- الموردون: لديهم صلاحية بيع السلع والخدمات على أعضاء المنتدى.
- الأعضاء (المحتالون) : شراء السلع

ومن أجل أن تصبح مورداً عليك أن تقدم مجموعة من أرقام البطاقات الائتمانية إلى أحد المراجعين. ويقوم المراجع بعمليات شرائية باستخدام تلك الأرقام. وإذا كانت البطاقات الائتمانية سارية المفعول فإنه يتم قبولك بصفة مورد.

وسطاء التهديد : الوسطاء الخارجيون

المنافسون:

يهتم المنافسون دائماً بتحقيق الميزة التنافسية. وهذا صحيح ليس في القطاع الخاص فحسب ولكن أيضاً في السياسة. ففي عام 2003 بامريكا ، تم توزيع مذكرات داخلية لقادة الأقلية الديمقراطية على وسائل الإعلام الصديقة للحزب الجمهوري. " في البداية، رفضت الغالبية الجمهوريَة أي تواطؤ للحزب الجمهوري بعد تسريب المذكرات ونشرها. وفصلت الوثائق كيف يمكن لأعضاء مجلس الشيوخ الديمقراطيين وضع استراتيجية استشارة جماعات المصالح الخارجية المخصصة لمعارضة بعض المرشحين القضائيين المحافظين التابعين للرئيس الأمريكي (بوش). ولكن بعد استجواب الشرطة ، ناقض السيناتور أورين هاتش (Hatch Orrin) نفسه، وهو الجمهوري عن ولاية يوتا والذي يرأس اللجنة القضائية، حينما أعلن أنه صدم عندما عرف أن من قام باختراق الملفات الحاسوبية التابع للأقلية عضواً من موظفيه " .

وسطاء التهديد : الوسطاء الخارجيون

العملاء:

ويمكن للعملاء بسهولة أن يكونوا وسطاء سواء داخلين أو خارجين اعتماداً على رسم المؤسسة لحدود الخدمة. مستخدمي نظام معلومات التسجيل و الدراسة بالجامعة، على سبيل المثال، هم من الطلاب وكذلك الإداريين في الوحدات المختلفة من نظام المعلومات مثل: المالية، والإسكان الداخلي، المسجل العام، وغيرها. ويعرف هؤلاء المستخدمون عادة «المستخدم الوظيفي». وكعملاء يحتاج هؤلاء المستخدمون في أوقات معينة لوظائف وامتيازات تمكنهم من أداء أعمالهم بطريقة أسهل لكن هذا قد يضع الجامعة في خطر. على سبيل المثال، شخص من الإدارة المالية لديه إمكانية الوصول إلى أرقام الضمان الاجتماعي الخاصة بالطالب، لذا قد يميل هذا الشخص إلى بيع قائمة من تلك الأرقام في سوق القراصنة .

وسطاء التهديد : الوسطاء الخارجيون

العوامل الطبيعية وفشل البنية التحتية:
في الولايات المتحدة الأمريكية توجد حرائق برية وزلازل في الغرب، وأعاصير في الغرب الأوسط، وفيضانات وأعاصير على الساحل الشرقي على امتداد ولايات الخليج. وعملياً لا يوجد منطقة في البلاد آمنة 100%. اضاف إلى ذلك التدخل البشري: تسرب الأنابيب، وحرائق المباني المفاجئة، وغيرها. وكل هذه كوارث طبيعية خارجية يمكن أن تؤثر في البنية التحتية لتكنولوجيا الأعمال التجارية. وعندما تفشل البنية التحتية لتقنية المعلومات فإن الضرر المالي قد يكون كبيراً.

وهذا ما حدث مع شركة سيرز (Sears) في عام 2013 "كلف فشل مدة خمس ساعات في وقت الازدحام بعد عطلة الأعياد شركة سيرز 158 مليون دولار من الأرباح وفقاً للدعوى القضائية. وعملت الخوادم على مولدات كهربائية مدة 8 أيام تم خلالها حرق وقود ديزل بتكلفة 189 ألف دولار " .

وسطاء التهديد : الوسطاء الخارجيون

الموظفون السابقون:
يمثل الموظف الساخط نوعاً خطراً من الوسطاء لأنه في كثير من الأحيان يكون لديه فكرة عن الأعمال الداخلية للمؤسسة، كما يكون الموظف الساخط قادراً على استخدام الثغرات المعروفة لديه للوصول إلى النظام والإضرار بالمؤسسة.
في شهر مايو من عام 2013 تم كشف النقاب عن شكوى جنائية في محكمة اتحادية في المنطقة الشرقية لمدينة نيويورك تتضمن اتهام مايكل مينيسيس (Michael Meneses) الذي اعتقل في وقت سابق من ذلك اليوم في مدينة سميثتاون بولاية لونغ آيلاند، بتهمة اختراق شبكة الحاسب الآلي لشركة تقوم بتصنيع إمدادات طاقة الجهد العالي، ما تسبب في خسارة للشركة بأكثر من 90 ألف دولار.

" قام بتوظيف مختلف الأساليب التقنية المتقدمة لاختراق شبكة الشركة الضحية وسرقة بيانات الاعتماد الأمنية لزملائه السابقين، بما في ذلك كتابة برنامج يستولي على بيانات تسجيل الدخول وكلمات السر. كما أنه استخدم بيانات الاعتماد الأمنية لزميل واحد سابق على الأقل وذلك للوصول إلى الشبكة عن بعد عبر شبكة افتراضية خاصة (Virtual Private Network) وقام بذلك من منزله ومن فندق يقع بالقرب من عمله الجديد، مما أدى إلى إفساد الشبكة" .

وسطاء التهديد : الوسطاء الخارجيون

تعتبر هجمات الموظفون السابقون من أكثر الهجمات التي يصعب اكتشافها ومنعها. يتمتع الموظفون بالفعل بإمكانية الوصول والمعرفة حول بنية قواعد بيانات الشركة ومحتواها، لذلك يمتلك الموظفون السابقون قدرة الوصول ومعرفة بالأنظمة، لذلك فهجمات الموظفون السابقون من بين الأكثر صعوبة في الكشف والمنع. ويمكن أن يكون الدافع وراء هجماتهم هو الانتقام لمجرد الشعور بالسخط او الانتقام (عند إنهاء او الطرد من العمل او عند الانتقال للعمل مع منافس).

مثال على السابق هو حالة "كينيث باترسون" ، الذي طرد من منصبه كمدير اتصالات البيانات لشركة (American Eagle Outfitters) عطّل باترسون قدرة الشركة على معالجة مشتريات بطاقات الائتمان خلال 5 أيام من موسم العطلات لعام 2002. أما بالنسبة للشعور بالسخط ، فقد كان هناك دائمًا العديد من الموظفين الذين شعروا بحقهم في الحصول على لوازم مكتبية إضافية للاستخدام المنزلي ، ولكن هذا يمتد الآن إلى بيانات الشركة. مثال على ذلك نائبة رئيس المبيعات لشركة تحليل الأسهم التي استقالت للذهاب إلى منافس. قبل أن تغادر ، قامت بنسخ قاعدة بيانات العملاء لأخذها معها. ذكرت الجانية أنها لا تشعر بأي عداء تجاه موظفها السابق ؛ لقد أرادت البيانات لأنها ستكون مفيدة لها. على الرغم أن أنظمة منع الاختراق يمكن أن تكون مفيدة في مواجهة الهجمات الداخلية ، إلا أن اساليب الأخرى مباشرة لها أولوية أعلى. تتضمن الأمثلة: فرض الامتياز الأقل ، ومراقبة السجلات ، وحماية الموارد الحساسة بمصادقة قوية ، وعند الإنهاء ، احذف وصول الكمبيوتر والشبكة للموظف وعمل صورة معكوسة للقرص الصلب للموظف قبل إعادة إصداره.

وسطاء التهديد : الوسطاء الخارجيون

سلوك المتسللين من الموظفين السابقين:

- إنشاء حسابات شبكة لأنفسهم ولأصدقائهم
- الوصول إلى الحسابات والتطبيقات التي لا يستخدمونها عادةً في وظائفهم اليومية
- البريد الإلكتروني لأصحاب العمل السابقين والمحتملين
- إجراء محادثات مراسلة فورية سرية (سرا)
- يقوم بزيارة مواقع الويب التي تلبي احتياجات الموظفين الساخطين .
- يقوم بإجراء تنزيلات كبيرة ونسخ الملفات
- الوصول إلى الشبكة في غير أوقات الدوام

وسطاء التهديد : الوسطاء الداخليون

الوسطاء الداخليون هم الأشخاص الذين لهم صلة بالمؤسسة وغالباً ما يكونون موظفين. ويشمل الوسطاء المتوقعون ما يلي: مسؤولي النظم، وموظفي مكتب الدعم الفني، ومطوري البرمجيات. لكن غيرهم من الأفراد غير المتوقعين، كموظفي النظافة، يمكن أن يكونوا أيضاً وسطاء تهديد .

مكتب الدعم الفني (Help Desk) :

قد يتم تخصيص بعض الامتيازات لموظفي مكتب الدعم الفني، عن طريق الخطأ أو عن طريق سوء الاستخدام، مما قد يؤثر في عمليات المؤسسة. وليس من غير المألوف السماح لموظفي مكتب الدعم الفني بإمكانية تغير كلمات المرور للمستخدمين، بعد التحقق من هوياتهم. وهذه الميزة قد تفتح الباب لرشوة وابتزاز الموظفين في حال عدم التحقق من تلك الأنشطة .

الموارد البشرية:

تعيين الموظفين وإنهاء خدماتهم في المؤسسة، والذي يتم التعامل معه عادة من قبل إدارة الموارد البشرية، يستلزم بعضاً من الأنشطة التي يحتمل أن يكون من ضمنها تخصيص امتيازات جديدة أو سحبها من أنظمة تقنية المعلومات. ويعرف نشاط إضافة موظف جديد إلى النظام (onboarding) ، في حين أن حذف الموظف من النظام يعرف (offboarding) . وفي حال تنفيذ هذه الأنشطة أوتوماتيكياً فإن العواقب ستكون وخيمة. ففي عام 2005 توجب على أحد البنوك المجتمعية الصغيرة في ولاية فلوريدا استرداد جميع الرسائل الإلكترونية للموظفين من الأشرطة الاحتياطية، وذلك بعد حدوث خطأ في نظام الموارد البشرية أدى إلى فصل جميع الموظفين، كما أدى إلى إلغاء وصولهم إلى حسابات البريد الإلكتروني.

وسطاء التهديد : الوسطاء الداخليون

خدمات النظافة:

تعد غرف الخوادم ومراكز البيانات منطقة محظورة على أي شخص ليس هناك حاجة لوجوده في تلك الغرف. لكن ليس كل الخوادم يكون مكانها في غرف الخوادم. ففي البيئة الجامعية ليس من غير المألوف أن تكون الخوادم في المكاتب المشتركة للموظفين دون وجود حماية مادية ودون وجود بديل لتلك الخوادم.

ففي عام 2003 لاحظ عامل نظافة في جامعة جنوب فلوريدا أن أحد المكاتب كان قذراً قليلًا فقرر أن ينظف الغرفة بالمكنسة الكهربائية. ولإيصال قابس المكنسة الكهربائية قام بفصل القابس الخاص بجهاز مصدر الطاقة غير المنقطعة (UPS-uninterruptible power supply) ، ولكنه لم يقم بتوصيله عندما انتهى من التنظيف. ونفذ جهاز مصدر الطاقة غير المنقطعة من الطاقة ما أدى إلى انقطاع خدمة البريد الإلكتروني عن الجامعة إلى اليوم التالي عندما جاء مسؤول النظام إلى المكتب.

وسطاء التهديد : الوسطاء الداخليون

المدققون الداخليون (المفتشون):

هناك أصناف مختلفة من المفتشين. فبعض منهم مستعد للعمل مع المسؤولين لفهم الأولويات المختلفة، وتخصيص الموارد، وكيف أن عمليات تقنية المعلومات تتلاءم مع الرسالة العامة للمؤسسة. البعض الآخر مهتم بالإشارة إلى الفشل الملحوظ في تقنية المعلومات. والبعض الثالث على استعداد تام لمناقشة مخططات قاعدة البيانات وتوجيهات الشبكة، ً فضلا عن الايراد النقدي والمساعدات المالية. كما أن البعض في الصناعة ينظر إلى المفتشين بأنهم ماهرون وذوو خبرة عامة، ُ ويضرب بهم المثل بأنهم متعددو المواهب والمهارات، لكن ليس بالضرورة أن يكون متخصصين في أي منها.

إن الشغل الشاغل للمفتشين هو الامتثال للوائح والأنظمة. ويجب أن تكون أنظمة تقنية المعلومات متوافقة مع القوانين. كما يجب أن تضمن اتباع جميع السياسات والإجراءات الرسمية المعتمدة من قبل المؤسسة. ومع أخذ ذلك في الاعتبار، من الضروري تأكيد أن الامتثال يختلف عن الأمن. وهذا الفرق الذي قد ُيحول المفتش في بعض الأحيان إلى وسيط تهديد.

على سبيل المثال، افترض أن لدى مؤسستك سياسة تنص على «تشفير جميع أرقام بطاقات الهوية للموظفين عند تخزينها إلكترونياً». وافترض من أجل النقاش في هذا المثال أنه يتم تخزين أرقام بطاقات الهوية على خادم قاعدة البيانات بحيث يتم تشغيل هذا الخادم فقط عند الحاجة للبيانات. ويقع مكان هذا الخادم في منشأة يتم مراقبة الوصول إليها، وأنت الشخص الوحيد الذي يملك الوصول إلى ذلك الخادم. قد يكون من وجهة نظرك أن خطر حدوث تسرب للبيانات أو فقدانها صغير جداً. لكن، الامتثال التنظيمي والامتثال للقوانين والتي ُأنشئت بقصد حماية خصوصية المستخدمين تكون ذات هدف منفرد ولا تنظر إلى أمن النظام بأكمله بل ُتركز على الجزء الذي تحتاج إلى حمايته. ولذلك فإن أي مفتش داخلياً كان أم خارجياً ُيصر على أن البيانات يجب تشفيرها أو يجب تعديل السياسة إذا كانت المؤسسة تحتمل المخاطر، حتى إذا كانت المؤسسة سوف تضطر إلى إنفاق آلاف الدولارات من أجل تشفير البيانات.

وقد يؤثر المفتشون أيضاً في عمليات تقنية المعلومات. ففي ولاية فلوريدا إذا كانت غرفة الخادم لا تتفق مع معايير المباني الخاصة باستخدام التوصيلات الكهربائية فإنه يحق لرجال الإطفاء قطع التيار الكهربائي على الفور حتى لو تعطلت العمليات الهامة للمؤسسة بسبب انقطاع التيار الكهربائي .

وسطاء التهديد : الوسطاء الداخليون

الإدارة العليا:

يمكن اعتبار المديرين وسطاء تهديد من خلال طرق متعددة. ولكن التهديد الأكثر هو عدم دعم الإدارة العليا لتقنية المعلومات بشكل عام وعدم فهم المخاوف الأمنية. إن أنظمة تقنية المعلومات موجودة في كل مكان في المؤسسات في الوقت الحاضر، لكن الناس لا تدرك التبعية التي تنشئها تلك النظم. ففي الجامعة، رواتب أعضاء هيئة التدريس، والتسجيل، وكشوف الدرجات، والادارة المالية، كلها تعتمد على حقيقة أن تتوفر أنظمة تقنية المعلومات وتعمل بشكل صحيح.

ومعظم تقنية المعلومات تعمل في عالم «لا خبر يعد خبراً جيداً». وبينما يكون ذلك حسناً من وجهة نظر تشغيلية إلا أنه يخلق حاجزاً مع المستخدمين. لكن من وجهة نظر المستخدم فإنه من الصعب تبرير النفقات المرتبطة بشراء خادم جديد إذا كانت الخدمات ُ ما زالت تقدم دون أي تأثير في الأداء. وعلى المدى الطويل يمكن أن يتسبب نجاح تقنية المعلومات في فشل تلك التكنولوجيا، إذا لم يتم تذكير الإدارة باستمرار باعتمادية الأعمال على الخدمات التي توفرها تقنية المعلومات

جامعة جديدة: جامعة فلوريدا المتعددة الفنون (Florida Polytechnic)

في عام ٢٠١٢ وافق مسؤولو ولاية فلوريدا على إنشاء جامعة معتمدة من الولاية اسمها جامعة فلوريدا المتعددة الفنون (Florida Polytechnic) أو (FPU). وكانت هذه الجامعة سابقاً جزءاً من نظام جامعة جنوب فلوريدا. وقد سبّب هذا القرار من قبل حكومة الولاية لإنشاء هذا الكيان الجديد في ظهور تحديات تقنية المعلومات، وهذا يُظهر نموذجاً لقرارات الإدارة العليا التي تؤسس لمشكلات تنتقل آثارها السلبية الممكنة إلى الأمن العام للمنظمة.

يجب مراجعة جميع رخص البرمجيات لأن أجهزة الحاسب الآلي والخوادم تعود ملكيتها الآن للجامعة الجديدة وليس لجامعة جنوب فلوريدا. وقد يؤدي عدم القيام بذلك إلى قضايا قانونية خطيرة.

يجب إعادة تخصيص موظفي تقنية المعلومات لتقديم الدعم ونقل المحتوى من خوادم جامعة جنوب فلوريدا إلى الخوادم الأخرى المملوكة لجماعة فلوريدا المتعددة الفنون، مما يؤدي إلى ترك بعض المناطق بدعم محدود.

وبينما يُنقل بعض الموظفين إلى النظام الجديد فإن العديد من الموظفين يفصلون. وهذا يخلق السيناريو المثالي والمحتمل لموظف ساخط ليصبح وسيط تهديد بارتكاب الغش.

وسطاء التهديد : الشركاء

ويشمل أي طرف ثالث يتقاسم علاقة العمل مع المؤسسة. وهذا يشمل الموردين والبائعين ومقدمي الاستضافة، ومقدمي الدعم التقني الخارجين، وغيرهم. وعادة ما تنطوي العلاقة بن شركاء العمل على مستوى معين من الثقة والامتيازات (الشكل)

الخدمات الاستشارية والمقاولون:

وتشمل هذه الفئة أيضاً خدمات التركيب والصيانة. وهذه خدمات مدفوعة من قبل المؤسسة من أجل أداء وظيفة معينة أو لزيادة الموظفين المحلين.

وتبذل المؤسسات الاستشارية قصارى جهدها لامتثال لأي متطلبات خاصة لعملائها. لكنَ العملاء من ذوي الاحتياجات الخاصة قد يصدمون إذا كان تدقيق التفاصيل مهما للغاية بالنسبة لهم. تأمل في قضية التسرب الأمنية التي حدثت مؤخراً في وكالة الأمن القومي (National Security Agency) والتي تورط فيها إدوارد سنودن (Edward Snowden) . كان السيد سنودن موظفاً في شركة بوز ألن هاملتون (Booz-Allen Hamilton)، وهي الشركة التي قدمت الكثير من العمل التقني لوكالة الأمن القومي وغيرها من الوكالات الفيدرالية الحساسة.

ففي يونيو من عام (2013) , كشفت صحيفة الجارديان (Guardian) أوامر سرية للغاية بالسماح لوكالة الأمن القومي بجمع معلومات عن المواطنين الأمريكيين. وفوجئ مشرعو القانون والجمهور بكشف صحيفة الجارديان عن هذا الخبر. وتراوحت ردود الأفعال بين تسمية السيد سنودن بطلا لتسليطه الضوء على تلك الأنشطة، وبين وصفه بخائن لكشفه عن الإجراءات الأمنية التي حافظت على أمن أمريكا، وأدت هذه الحادثة إلى الاهتمام بالعديد من الأمور.

وسطاء التهديد : الشركاء

فنظراً لطبيعة المؤسسة فإنه من المستحيل تأكيد كيف قام السيد سنودن بإخراج البيانات من الشركة حتى يتم الكشف عن ذلك في جلسة المحاكمة، ومن الطرق الرسمية الأخرى. لكن كان هناك تخمين بأن السيد سنودن قد استخدم قرص الناقل التسلسلي العالمي (USB thumb drive) لحفظ بياناته. لكن المؤسسات الحساسة تقوم عادة بتعطيل هذه المنافذ على أجهزة الحاسب الآلي لمنع هذا التسرب. لذا تفاجأ العديد من الخبراء بإمكانية هذه الاحتمال في وكالة الأمن القومي. وجدير بالملاحظة أيضاً كيف أن موظفاً يتبع لشريك (مقاول) قد تمكن من الوصول إلى تلك الوثائق الحساسة .

في بداية عام ٢٠٠٠ كانت شركة (Sun Microsystems) مسؤولة عن تركيب العديد من أنظمة الأداء العالي في جامعة جنوب فلوريدا. ومن أجل تسهيل عملهم قام مهندسو الصيانة من شركة (Sun Microsystems) بتجهيز جميع الصناديق، بما في ذلك تجهيز صناديق المنظمات الأخرى، بنفس بيانات تسجيل الدخول وكلمات المرور. ومما يُضيف إلى الخلل الأمني هذا أن كلمة المرور كانت مستندة إلى قاموس الكلمات.

وسطاء التهديد : الشركاء

خدمات الحوسبة السحابية:

تمثل خدمات الحوسبة السحابية فئة كبيرة جداً من الخدمات. وتحدد إدارة مخاطر تقنية المعلومات خمس خصائص أساسية للحوسبة السحابية: الخدمة الذاتية بناء على الطلب، والوصول إلى الشبكة ذات النطاق الواسع، وتجميع الموارد، والمرونة السريعة أو التوسع، والخدمة المقاسة. كما ذكرت أيضاً ثلاثة من «نماذج الخدمة» (البرمجيات، والمنصة، والبنية التحتية)، وأربعة من «نماذج النشر» (الخاصة، والمجتمعية، والعامة، والهجينة) والتي تقوم جميعها بتصنيف طرق تقديم الخدمات السحابية، وجميع تلك الخدمات كانت في وقت من الأوقات مرتبطة بمصطلح (Outsourcing) والذي يعني (التعاقد الخارجي). ونظراً لارتباط مصطلح (Outsourcing) بفقد بعض الأشخاص لوظائفهم، أعادت الصناعة تصميم نفسها كما أعادت تصنيف الخدمات تحت مسمى «خدمات الحوسبة السحابية» .

فعندما تتجه المؤسسات لنقل بعض خدماتها للسحابة الإلكترونية فسيكون هناك فرضية لتطوير وجود بديل للأجهزة المستخدمة، وكذلك تطوير الموثوقية مع عدة خوادم تستضيف تطبيقات بميزة الانتقال التلقائي في مواقع جغرافية متعددة. وفي حين أن هذا هو الحال في معظم الحالات إلا أنه لا يكون كذلك دائماً، لكن يجب على منظمات الأعمال ألا تفترض تلك الفرضية. فعندما تنتقل بعض الخدمات إلى السحابة الإلكترونية، لابد من التحقق من بعض الأمور:

- هل لدى مراكز البيانات الشهادات الأمنية المطلوبة؟
- ما المواقع الجغرافية للمركز؟
- ما الضوابط التي تم وضعها لحماية البيانات؟

ومن الأهمية بمكان أيضاً أن يكون هناك من البداية استراتيجية للخروج. فلا بد من تأسيس الطرق التي من خلالها يمكن نقل البيانات إلى موقع آخر في حالات الطوارئ، فالفشل في أي من هذه النقاط يمكن أن يحول مزود الخدمة الخارجي من شريك إلى وسيط تهديد.

تعد الاستعانة بمصدر خارجي لتهيئة البنية التحتية لغرفة الخادم أمراً شائعاً حيث يساعد ذلك على التخلص من المخاوف الطبيعية ويسمح للمؤسسة بالتركيز على الجزء المهم من أعمالها. وهذا ينطبق بشكل خاص على مدونات المواقع الإخبارية وبعض وسائل الإعلام.

أمثلة على بعض قضايا مزودي خدمات الحوسبة السحابية

شركة (Dropbox):

في شهر يوليو من عام ٢٠١١ قامت شركة تخزين البيانات السحابية (Dropbox) بتغييرات جذرية على اتفاقيات التراخيص والشروط نتيجة لمشكلة سابقة اشتملت على خلل برمجيات في نظام التوثيق. «من خلال إرسالك الملفات إلى الخدمات فإنك تمنحنا، وتمنح الجهات العاملية التي تعمل معها لتقديم الخدمات، الحق في استخدام وتوزيع ونسخ وأعداد أعمال مشتقة (مثل الترجمة وتغييرات في التصميم) وعرض الملفات علانية بالقدر اللازم للخدمة ويكون ذلك الحق غير حصري ودون رسوم وقابلاً للترخيص لطرف ثالث». لكن شركة (Dropbox) غيرت موقفها بسرعة بعد أن بدأ العملاء برفض الاتفاقية وسحب بياناتهم من الشركة.

شركة (Salesforce.com):

وهذه الشركة معروفة ببرمجيات إدارة علاقات العملاء (Customer Relation Management)، وهي معروفة أيضاً بعروض الخدمات السحابية: مبيعات السحابة (Sales Cloud) لإدارة المبيعات، خدمات السحابة (Service Cloud) وهي خدمة مقدمة لمراكز الاتصال.

لكن شركة (Salesforce) لا يوجد لديها مراكز بيانات خاصة بها حيث تتعامل مع شركة تدعى (Equinox) وذلك للاستفادة من هيكلة تُسمى بهيكلة (DR) من أجل الحفاظ على خدماتها.

وفي شهر يوليو من عام ٢٠١٢، حدث انقطاع وجيز لمدة دقيقة واحدة في التيار الكهربائي في أحد مواقع مراكز البيانات في كاليفورنيا التابع لشركة (Equinox) مما أدى إلى سلسلة من المشكلات أدت في نهاية المطاف إلى التعطل الكامل لشبكة (Salesforce) لما يقارب من ٦ ساعات.

وسطاء التهديد : الشركاء

الموردون والبائعون:

عندما لا يتمكن الباعة أو الموردون من توريد الموارد المطلوبة، أو مراقبة مستوى جودة الأجهزة، أو تقييم علاقاتها التجارية بشكل صحيح فإن التأثير على نطاق العمل قد يكون كبيرا.

في شهر مايو من عام ٢٠١٣ فازت شركة نوكيا (Nokia) بأمر قضائي ضد شركة إتش تي س (HTC) في هولندا وذلك فيما يختص ببيع هاتف أندرويد يُسمى (HTC One). ويظهر أن (HTC) استخدمت ميكروفوناً في هاتف (HTC One) مُطور من شركة (STMicroelectronics)، لكن على ما يبدو أن شركة نوكيا لديها حقوق حصرية لاستخدام هذا الميكروفون في أجهزتها.

مستويات مهارة وسطاء التهديد (المخترقين):

- **المتدرب:** قراصنة لديهم الحد الأدنى من المهارات التقنية الذين يستخدمون في المقام الأول مجموعات أدوات الهجوم الحالية. من المحتمل أنهم يشكلون أكبر عدد من المهاجمين ، بما في ذلك العديد من المهاجمين المجرمين والنشطاء. نظرًا لاستخدامهم للأدوات المعروفة الموجودة ، فإن هؤلاء المهاجمين هم الأسهل للدفاع ضدهم. يُعرفون أيضًا باسم "script-kiddies" نظرًا لاستخدامهم للنصوص الموجودة (الأدوات).
- **المهرة:** قراصنة يتمتعون بمهارات تقنية كافية لتعديل وتوسيع مجموعات أدوات الهجوم لاستخدام نقاط الضعف المكتشفة أو المشترة حديثًا ؛ أو التركيز على مجموعات مستهدفة مختلفة. قد يكونون قادرين أيضًا على تحديد الثغرات الجديدة لاستغلالها والتي تشبه بعض الثغرات المعروفة. من المحتمل العثور على عدد من المتسللين الذين يتمتعون بهذه المهارات في جميع فئات الدخلاء (الوسطاء) المذكورة سابقا ، مع تكييف الأدوات لاستخدامها من قبل الآخرين. تؤدي التغييرات في أدوات الهجوم إلى زيادة صعوبة تحديد مثل هذه الهجمات والدفاع عنها.
- **الخبراء:** قراصنة يتمتعون بمهارات تقنية عالية المستوى قادرين على اكتشاف فئات جديدة من نقاط الضعف ، أو كتابة مجموعات أدوات هجوم قوية جديدة. بعض المتسللين الكلاسيكيين المعروفين هم من هذا المستوى ، كما هو واضح من أولئك الذين يعملون من قبل بعض المنظمات التي ترعاها الدولة ، كما يوحي التصنيف (APT). هذا يجعل الدفاع ضد هذه الهجمات من الصعوبة القصوى.

نشاط وسطاء التهديد:

الوسطاء (المتسللين) هو الجزء الأول من التهديد. لكن لن يكون هناك أي تهديد حتى يقوم الوسيط ببعض الأنشطة لإضرار بأحد الأصول. النشاط هو العمل الذي يقوم به الوسيط للتأثير في خصوصية الأصل أو تكامله أو جاهزيته. إن عملية إنشاء قائمة من الأنشطة غير مجد لأن أنشطة التهديدات الجديدة تكون محدودة فقط بمدى براعة الوسطاء. ومع ذلك يمكن تصنيف أنشطة التهديدات الشائعة في الفئات التالية:

1. البرمجيات الخبيثة (Malware)
2. قراصنة الحاسب الآلي (Hackers)
3. الهندسة الاجتماعية (Social engineering)
4. المادية (Physical)
5. الأخطاء (Error)
6. البيئة (Environment)

الاختراق والكشف الأمني

- الاختراق الأمني: حدث أمني ، أو مجموعة من الأحداث الأمنية المتعددة ، والتي تشكل حادثًا أمنيًا يكتسب فيه المتسلل ، أو يحاول الوصول إلى نظام (أو مورد نظام) دون الحصول على إذن للقيام بذلك.
- كشف التسلل/الاختراق: خدمة أمنية تراقب وتحلل أحداث النظام بغرض البحث عن ، كذلك تقديم تحذير في الوقت الحقيقي أو شبه حقيقي لمحاولات الوصول إلى موارد النظام بطريقة غير مصرح بها.

امثلة على نشاط الوسطاء/المخترقين

- اختراق عن بعد لخادم البريد الإلكتروني
- اعطاب خادم ويب
- تخمين وتكسير كلمات المرور
- نسخ قاعدة بيانات تحتوي على أرقام بطاقات الائتمان
- عرض البيانات الحساسة ، بما في ذلك سجلات الرواتب والمعلومات الطبية بدون إذن
- تنفيذ حزمة تشمم على محطة عمل لالتقاط أسماء المستخدمين وكلمات المرور
- استخدام خادم (FTP) مجهول لتوزيع البرامج المقرصنة وملفات الموسيقى
- الاتصال بمودم غير آمن والحصول على وصول داخلي للشبكة
- التظاهر كمشرف تنفيذي والاتصال بمكتب المساعدة ، وإعادة تعيين كلمة المرور البريد الإلكتروني للمدير التنفيذي، وتعلم كلمة المرور الجديدة
- استخدام محطة عمل غير مراقبة ومفتوحة بدون إذن

منهجية التسلل/الاختراق

تتغير تقنيات وأنماط سلوك المتسللين (المخترق) باستمرار وذلك نتيجة لاستغلالهم للثغرات المكتشفة حديثًا وكذلك للتهرب من الاكتشاف والتدابير المضادة. ومع ذلك ، يستخدم المتسللون عادةً خطوات منهجية هجوم شائعة، وهى مرتبطة بالخطوات التالية:

1. **تحديد الهدف وجمع المعلومات**: حيث يحدد المهاجم الأنظمة المستهدفة ويميزها باستخدام المعلومات العامة المتاحة للجميع سواء كانت معلومات تقنية وغير تقنية على حد سواء، واستخدام أدوات استكشاف الشبكة لتحديد الموارد المستهدفة.
2. **الوصول المبدئي**: التواصل الأولي مع النظام المستهدف ، عادةً عن طريق استغلال ثغرة أمنية في الشبكة ، او من خلال تخمين بيانات مصادقة ضعيفة مستخدمة في خدمة ما ، أو عن طريق تثبيت برامج خبيثة على النظام باستخدام شكل من أشكال الهندسة الاجتماعية.
3. **تطوير الامتيازات**: الإجراءات التي يتم اتخاذها على النظام، عادةً عبر ثغرة وصول محلية، لزيادة الامتيازات المتاحة للمهاجم لتمكينه من تحقيق أهدافه المرجوة على النظام المستهدف.
4. **جمع المعلومات أو استغلال النظام**: الإجراءات التي يقوم بها المهاجم للوصول إلى المعلومات أو الموارد أو تعديلها على النظام، أو البحث عن نظام مستهدف آخر.
5. **المحافظة على الوصول**: إجراءات مثل تثبيت الأبواب الخلفية أو البرامج الخبيثة الأخرى ، أو من خلال إضافة بيانات مصادقة سرية أو تغييرات التكوين الأخرى على النظام تمكن المهاجم من الوصول المستمر للنظام المستهدف بعد الهجوم الأولي.
6. **اخفاء المتابعة**: حيث يقوم المهاجم بتعطيل سجلات التدقيق أو تحريرها لإزالة الدليل على نشاط الهجوم ، واستخدام أدوات على نظام التشغيل وغيرها من الإجراءات لإخفاء الملفات أو التعليمات البرمجية المثبتة سرًا.

مثال على سلوك القراصنة

تتغير تقنيات وأنماط سلوك المتسللين باستمرار لاستغلال نقاط الضعف المكتشفة حديثًا والتهرب من الاكتشاف والتدابير المضادة. ومع ذلك ، فإن المتسللين عادةً ما يتبعون واحدًا من عدد من أنماط السلوك التي يمكن التعرف عليها ، وتختلف هذه الأنماط عادةً عن تلك الخاصة بالمستخدمين العاديين.

- تحديد الهدف باستخدام أدوات بحث (IP) ، واستعراض الشبكة لاستكشاف الخدمات التي يمكن الوصول إليها.
- تحديد الخدمات التي يحتمل أن تكون عرضة للضعف، واستغلال المحيط عبر المنافذ الضعيفة.
- تخمين كلمات مرور (القوة التحليلية)، أو استخدم التشمم لالتقاط كلمات المرور.
- تثبيت أداة اشراف او سيطرة عن بعد، وارتكب القليل من الأخطاء أو لا ترتكب أي أخطاء.
- انتظر حتى يقوم المشرف بتسجيل الدخول والتقاط كلمة المرور.
- استخدم كلمة المرور للوصول إلى باقي الشبكة .
- يتصرفون بسرعة وبدقة لجعل اكتشاف أنشطتهم أكثر صعوبة (لا تبقى حتى لا تلاحظ).
- استخدم أحصنة طروادة (برنامج مخفي) لترك الأبواب الخلفية للدخول مرة أخرى.

مثال: اقتحام لمؤسسة مالية كبيرة. استغل الدخيل حقيقة أن شبكة الشركة كانت تشغل خدمات غير محمية ، وبعضها لم تكن هناك حاجة له. في هذه الحالة ، كان مفتاح الاختراق هو تطبيق حاسوب " pc Anywhere". تعلن الشركة المصنعة (Symantec) عن هذا البرنامج كحل للتحكم عن بعد يتيح الاتصال الآمن بالأجهزة البعيدة. لكن المهاجم كان لديه وقت سهل للوصول إلى جهاز الحاسوب من أي مكان ؛ استخدم المسؤول نفس اسم المستخدم وكلمة المرور المكونين من ثلاثة أحرف للبرنامج. في هذه الحالة ، لم يكن هناك نظام للكشف عن التسلل على شبكة الشركة المكونة من 700 عقدة. تم اكتشاف الدخيل فقط عندما دخلت نائبة الرئيس إلى مكتبها ورأت المؤشر يحرك الملفات على محطة عمل ويندوز الخاصة بها.

أنظمة كشف التسلل (IDS)

أنظمة كشف التسلل (Intrusion detection systems) أو اختصاراً (IDS) هي مكونات مادية أو تطبيقات برمجية تراقب أنظمة تقنية المعلومات لاكتشاف الأنشطة الضارة أو اكتشاف انتهاكات سياسات الاستخدام التي نشئت من قبل مسؤول النظام.

أما **أنظمة منع التسلل** فيتم بناؤها على أنظمة كشف التسلل بهدف إيقاف الاختراقات المحتملة. وقد أصبحت الآن أنظمة كشف التسلل وإلى حد ما أنظمة منع التسلل أيضاً جزءاً لا يتجزأ من البنية التحتية لأمن تقنية المعلومات في معظم المنظمات.

وبشكل عام هناك نوعان من أنظمة كشف التسلل: **أنظمة معتمدة على الشبكة، وأنظمة معتمدة على المضيف**. أنظمة كشف التسلل المعتمدة على الشبكة تراقب حركة مرور الشبكة ونشاط بروتوكولات التطبيقات لتحديد الاتصالات المشبوهة. وتأتي هذه الأنظمةُ عادة مع الموجهات والجُدر النارية. أما أنظمة كشف التسلل المعتمدة على المضيف فهي تطبيقات برمجية مثبتة على المضيف الذي يراقب النشاط الداخلي مثل الوصول للملفات واستدعاء الأنظمة بهدف اكتشاف الأنشطة المشبوهة. ولزيادة احتمالية كشف محاولات التسلل، تقوم معظم المنظمات بالاستفادة من العديد من أنظمة كشف التسلل، ولكل منها مجموعة من القواعد المحددة وذلك مراقبة نشاط النظام من وجهة نظرها الخاصة. وأحد وظائف (أنظمة كشف التسلل) المثيرة لاهتمام هو إطلاق الإنذارات حول الهجمات الوشيكة. ويتم ذلك من خلال مراقبة نشاط الاستطلاع: مسح المنافذ والمضيف لتحديد أهداف الهجمات اللاحقة. وهذا المسح غالباً ما يسبق الهجمات ذات النطاق الواسع، وإذا تم إخطار مسؤول النظام بعمليات مسح المنافذ، فإنه يستطيع اتخاذ الإجراءات اللازمة لاستعداد لأي هجمات قادمة.

أنظمة كشف التسلل (IDS): المكونات

يتكون نظام كشف التسلل (IDS) من ثلاثة مكونات اساسية:

1) **أجهزة الاستشعار**: أجهزة الاستشعار هي المسؤولة عن جمع البيانات. قد تكون مدخلات جهاز الاستشعار أي جزء من نظام يمكن أن يحتوي على دليل على التسلل. تتضمن أنواع المدخلات إلى جهاز الاستشعار حزم الشبكة وملفات سجلات المتابعة ومتتبعات مخاطبات نظام التشغيل. تقوم المستشعرات بجمع هذه المعلومات وإرسالها إلى المحلل.
2) **أجهزة التحليل**: تتلقى أجهزة التحليل المدخلات من جهاز استشعار واحد أو أكثر أو من أجهزة تحليل أخرى. المحلل هو المسؤول عن تحديد ما إذا كان هناك اختراق ام لا، والنتيجة هي إشارة إلى حدوث اختراق من عدمه. قد تشتمل المخرجات على أدلة تدعم الاستنتاج بحدوث الاختراق. قد يوفر المحلل إرشادات حول الإجراءات التي يجب ان تتخذ نتيجة هذا الاختراق. يمكن أيضًا تخزين مدخلات أجهزة الاستشعار لتحليلها ومراجعتها في المستقبل في وحدة تخزين أو قاعدة بيانات.
3) **واجهة المستخدم**: تتيح واجهة المستخدم لنظام كشف التسلل (IDS) للمستخدم إمكانية عرض مخرجات النظام أو التحكم في سلوك النظام. في بعض الأنظمة ، قد توازى واجهة المستخدم واجهة المدير أو المشرف أو متحكم عادى .

أنظمة كشف التسلل (IDS): الاصناف

قد يستخدم نظام كشف التسلل (IDS) مستشعرًا ومحللًا منفردًا ، مثل (HIDS) التقليدي على مضيف أو (NIDS) في جهاز جدار الحماية. يمكن أن تستخدم معرفات (IDS) الأكثر تعقيدًا أجهزة استشعار متعددة ، عبر مجموعة من الأجهزة المضيفة والشبكات ، وإرسال المعلومات إلى محلل مركزي وواجهة مستخدم في بنية موزعة.

غالبًا ما يتم تصنيف نظم كشف التسلل (IDS) بناءً على مصدر ونوع البيانات التي تم تحليلها ، على النحو التالي:

1) **نظام كشف التسلل المستضاف** (HIDS): (يعتمد على المضيف) تراقب خصائص المضيف والأحداث التي تحدث داخل ذلك المضيف ، مثل معرفات العمليات ومخاطبات النظام التي يجريها نظام التشغيل ، وذلك للحصول على دليل على نشاط مشبوه.
2) **نظام كشف التسلل الشبكي** (NIDS): (يعتمد على الشبكة) يراقب حركة مرور الشبكة او قطاعاتها أو أجهزة شبكة معينة بها ويحلل بروتوكولات الشبكة والنقل والتطبيقات لتحديد ما اذا كان هناك نشاط المشبوه.
3) **نظم كشف التسلل الموزعة أو الهجينة**: تجمع المعلومات من عدد من أجهزة الاستشعار ، غالبًا ما تكون المعتمدة على الأنظمة المستضافة والشبكية ، في محلل مركزي قادر على تحديد نشاط التسلل والاستجابة له بشكل أفضل.

أنظمة كشف التسلل (IDS): طرق الكشف

تعتمد أنظمة كشف التسلل المعاصرة على ثلاث طرق لاكتشاف الاختراقات:

- **التوقيعات،**
- **والانحرافات،**
- **وحالات البروتوكول.**

وتستخدم معظم التطبيقات التجارية مزيجاً من الطرق الثلاثة لتحقيق أقصى قدر من الفعالية.

1- أنظمة كشف التسلل المعتمدة على التوقيعات: التوقيع هو سلسلة من القيم الثنائية (البايتات) المعروف عنها أنها جزء من البرمجيات الخبيثة. وتقوم "أنظمة كشف التسلل المعتمدة على التوقيعات" مقارنة الأحداث المرصودة بقاعدة بيانات التوقيعات وذلك لتحديد الحوادث المحتملة. ومن أمثلة التوقيعات، الرسائل الإلكترونية التي عنوانها (ILOVEYOU) وتحتوي على ملف مرفق باسم (LOVE-LETTER-FOR-YOU.txt.vbs) . وهذه الرسائل الإلكترونية تتوافق مع فيروس (ILOVEYOU) المعروف. وتعد "أنظمة كشف التسلل المعتمدة على التوقيعات" فعالة جداً ضد التهديدات البسيطة والمعروفة. وحسابياً فإن هذه الأنظمة فعالة جداً لأنها تستخدم عمليات مقارنة السلاسل البسيطة. لكن هذه الأنظمة غير مفيدة في الكشف عن التهديدات غير المعروفة سابقاً، أو التهديدات المتنكرة، أو التهديدات المعقدة.

أنظمة كشف التسلل (IDS): طرق الكشف

على سبيل المثال، إن فيروس (ILOVEYOU) يكون فعالاً بالقدر نفسه عند تغير عنوان رسالة البريد الإلكتروني إلى (job offer for you) وتغيير اسم الملف المرفق إلى (interview-script.vbs) ، لكن هذا التنكر البسيط يجعل اكتشاف الفيروس أمراً صعباً للغاية بالنسبة لأنظمة كشف التسلل المعتمدة على التوقيعات. والعيب الآخر في أنظمة كشف التسلل المعتمدة على التوقيعات هو أن مطابقة التوقيع يقتصر فقط على الوحدة الحالية من النشاط، مثلا حزمة واردة أو إدخال سجل فردي. وهذه الأنظمة لا تميز عمليات بروتوكولات الشبكة. ونتيجة لذلك لا يمكن لأنظمة كشف التسلل المعتمدة على التوقيعات اكتشاف عمليات مسح المنافذ لأن كل حزمة فردية يتم فحصها تمثل حزمة مشروعة ويتم تشكليها بشكل جيد. ويتطلب كشف التهديد لعمليات مسح المنافذ تجميع المعلومات عن الحزمة الحالية، ومعلومات عن الحزم التي تم استقبالها في الماضي، ولا تستطيع مطابقة التوقيعات للحزمة الحالية لوحدها القيامُ بهذا الأمر. وبشكل عام فإن أنظمة كشف التسلل المعتمدة على التوقيعات لا تستطيع كشف الهجمات التي تتألف من أحداث متعددة، حيث ان أي من الأحداث الفردية لا يتطابق بشكل واضح مع توقيع هجوم معروف.

أنظمة كشف التسلل (IDS): طرق الكشف

2- أنظمة كشف التسلل المعتمدة على الانحرافات: أنظمة كشف التسلل المعتمدة على الانحرافات هي عبارة عن عملية الكشفُ عن الانحرافات بين الأحداث الملاحظة وأنماط النشاط المحدد. ويحدد مسؤول النظام أوضاع السلوك الطبيعي الذي يعتمد على المستخدمين، أو المضيف، أو اتصال الشبكة، أو التطبيقات. على سبيل المثال، قد يحدد وضع السلوك الطبيعي لحاسوب مكتبي أن تصفح الإنترنت يتضمن 20% في المتوسط من استخدام الشبكة خلال ساعات العمل العادية. وبعد ذلك تقوم أنظمة كشف التسلل المعتمدة على الانحرافات مقارنة النشاط الحالي ورفع الإنذار عندما يشتمل نشاط شبكة الإنترنت على نطاق ترددي أكثر مما هو متوقع. وتشمل الصفات الأخرى التي يمكن من خلالها إنشاء أوضاع السلوك الطبيعي على عدد رسائل البريد الإلكتروني المرسلة من قبل المستخدم، ومستوى استخدام المعالج للمضيف في فترة معينة من الزمن. وتعد أنظمة كشف التسلل المعتمدة على الانحرافات أنظمة فعالة جداً في الكشف عن التهديدات التي لم تكن معروفة سابقاً. على سبيل المثال، في حالة إصابة حاسوب بنوع جديد من البرمجيات الخبيثة التيُ ترسل كميات كبيرة من البريد الإلكتروني غير المرغوب فيها، أو تستخدم موارد المعالجة للحاسوب لكسر كلمات المرور، فإن سلوك الحاسوب سيكون مختلفاً بشكل كبير عن أوضاع السلوك الطبيعي التي أنشئت لهذا الجهاز. وعندها ستكون أنظمة كشف التسلل المعتمدة على الانحرافات قادرة على الكشف عن هذه الانحرافات وتنبيه مسؤول النظام. والمشكلة الوحُيدة في بناء أوضاع السلوك الطبيعي لأنظمة كشف التسلل المعتمدة على الانحرافات هي الصعوبة الكبيرة في تطوير أوضاع مرجعية ودقيقة للسلوك الطبيعي .

على سبيل المثال، قد يقوم جهاز الحاسوب بعمليات نسخ احتياطي كاملة والتي تنطوي على كميات كبيرة من نقل البيانات الشبكية في اليوم الأخير من الشهر. وإذا لم يكن ذلك جزءاً من أوضاعُ السلوك الطبيعي، فإن صيانة مرور البيانات العادية سوف تعد انحرافاً كبيراً عن أوضاع ذلك السلوك ما يؤدي إلى إطلاق الإنذارات.

أنظمة كشف التسلل (IDS): طرق الكشف

3- أنظمة كشف التسلل المعتمدة على حالات البروتوكول: تقوم أنظمة كشف التسلل المعتمدة على حالات البروتوكول بمقارنة الأحداث الملاحظةُ بنشاط البروتوكول المحدد وذلك لكل حالة بروتوكول بهدف تحديد الانحرافات. وفي حين تُستخدم أنظمة كشف التسلل المعتمدة على الانحرافات أوضاع سلوك طبيعي محددةُ للشبكة أو للمضيف، فإن تحليل حالات البروتوكول يحدد كيف تستخدم بروتوكولات معينة أو لا تُستخدم. على سبيل المثال، إن أنظمة كشف التسلل المعتمدة على حالات البروتوكول تعلم ما إذا كان المستخدم في حالة (غير مصادق) فإنه يجب أن يحاول عدد محدود من محاولات تسجيل الدخول، أو يجب أن يحاول فقط مجموعة من الأوامر الصغيرة في حالة (غير مصادق). إذاً فإن الانحرافات عن السلوك المتوقع للبروتوكول يمكنُ اكتشافها من خلال أنظمة كشف التسلل المعتمدة على حالات البروتوكول. ومن القدراتُ الأخرى لأنظمة كشف التسلل المعتمدة على حالات البروتوكول هي القدرة على تحديد التسلسل غير المتوقع للأوامر. على سبيل المثال، إصدار الأمر نفسه مراراً وتكراراً يمكن أنُ يشير إلى هجوم القوة الغاشمة. كما تستطيع أنظمة كشف التسلل المعتمدة على حالات البروتوكول تتبع هوية المستخدم المستخدمة في كل جلسة وهو أمر مفيد عند التحقيق في حادث ما. ويمكن أن يشمل تحليل البروتوكول فحص الأوامر الفردية مثل مراقبة أطوال المعاملات. فإذا كان يحتوي الأمر عادة على معامل (اسم المستخدم)، وكان طول هذا المعامل 1000 حرف فإن ذلك مثير للشك. وبالإضافة إلى ذلك، إذا كان اسم المستخدم يحتوي على بيانات غير نصية، فإن طول المعامل السابق يصبح أكثر غرابة ويستحق الإشارة إليه.

والعيب الأساسي في أنظمة كشف التسلل المعتمدة على حالات البروتوكول هو أن تتبع الحالة لجلسات عديدة في وقت واحد يستنزف الموارد الحاسوبية بشكل كبير مما يتطلب استثمارات كبيرة في المكونات المادية للحاسب الآلي.

أنظمة كشف التسلل (IDS): هيكلة أنظمة كشف/منع التسلل

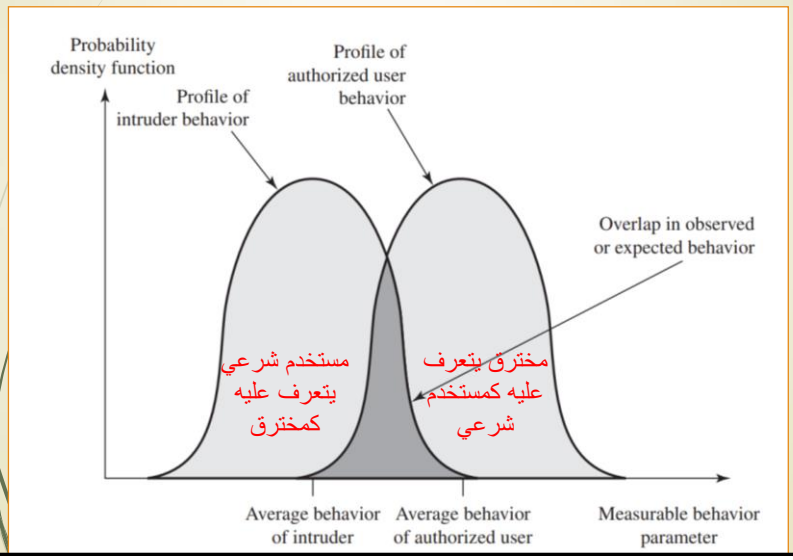
يتبع نشر أنظمة كشف/ منع التسلل في المؤسسة للهيكلة العادية للأنظمة الموزعة. وتحتوي المؤسسة على العديد من عوامل الاستكشاف المنتشرة في جميع انحاء المؤسسة والتيُ تقوم بجمع معلومات من الشبكة ومعلومات من المضيف. وترسل عوامل الاستكشاف تلك بياناتها إلى محطة الإدارة المركزية والتي تقوم بتسجيل جميع البيانات الواردة في قاعدة بيانات، كما تقوم بالتحليلات المختلفة والمعتمدة على التوقيعات والانحرافات وحالات البروتوكول. ويستخدم مسؤولو النظام وحدة تحكم مكتبية أو وحدة تحكم على الشبكة لتهيئة عوامل الاستكشاف، ومراقبة الإنذارات، واتخاذ الإجراءات الدفاعية المناسبة.

أنظمة كشف التسلل (IDS): القيود

تتضمن تقنية كشف/ منع التسلل اثنين من القيود المعروفة: الإيجابيات **الكاذبة** و الإيجابيات **المراوغة**.
مع الحالة الراهنة لهذه التكنولوجيا فإن أنظمة كشف التسلل ليست دقيقة تماماً ً فالعديد من الإنذارات التي تطلقها أنظمة كشف التسلل لا تمثل تهديدات حقيقة، كما أن العديد من التهديدات الحقيقية تمر دون إطلاق إنذارات.
وعملية الإشارة إلى نشاط آمن بأنه نشاط ضار تدعى **إيجابية كاذبة**، أما الفشل في تحديد النشاط الضار فيدعى **سلبية كاذبة**، والحد من إحدى هاتين العمليتين يؤدي عادة إلى زيادة العملية الأخرى. على سبيل المثال، نظام كشف التسلل الحساس جداً سيكشف هجمات أكثر واقعية، لكنه في الوقت ُ نفسه سيشير إلى العديد من المعاملات الآمنة بأنها معاملات ضارة. ونظام كشف التسلل الأقل حساسية لن يثير الكثير من الإنذارات الكاذبة، لكن العديد من الهجمات الحقيقية قد يمر دون اكتشافها. وأن الهجمات الحقيقية مكلفة جداً ُ ، فإن المؤسسات تفضل زيادة احتمالية اكتشاف حركة المرور الضارة حتى لو كان ذلك يؤدي إلى الاستجابة لكثير من الإنذارات الكاذبة. ويأتي ذلك على حساب فريق أمن المعلومات حيث يتوجب عليهم تخصيص المزيد من الموارد للتدقيق في جميع الإنذارات الكاذبة للعثور على الأحداث الضارة بالفعل.
أما المراوغة فهي إجراء نشاط ضار بحيث يبدو آمناً. ويستخدم المهاجمون إجراءات المراوغة للحد من احتمال اكتشافهم من قبل أنظمة كشف التسلل. على سبيل المثال، يمكن أن يتم مسح المنافذ ببطء شديد (خلال عدة أيام) ومن عدة مصادر لتجنب الاكتشاف. كما يمكن إرسال البرمجيات الخبيثة بوصفها أجزاء من مرفقات الملفات وتظهر بأنها آمنة.
ومن ثم فلا يمكن الوثوق بأنظمة كشف/ منع التسلل لكشف جميع الأنشطة الضارة. ولكن يمكن أن تكون تلك الأنظمة فعالة بوصفها جزءاً من النشر العام لأمن المعلومات في ُ المؤسسة كما هو الحال في الجُدران النارية.

أنظمة كشف التسلل (IDS): القيود

التفسير الفضفاض مقارنة بالصارم :
اصطياد المزيد (ايجابيات كاذبة) او اصطياد القليل (سلبيات كاذبة).



متطلبات أنظمة كشف التسلل (IDS)

نظام كشف التسلل يجب:

- يعمل باستمرار بأدنى حد من الإشراف البشري.
- يكون متسهلا مع الأخطاء بمعنى أنه يجب أن يكون قادرًا على التعافي من أعطال النظام وإعادة التهيئة.
- مقاومة للتخريب ، حيث يجب أن يكون نظام كشف التسلل قادرًا على مراقبة نفسه واكتشاف ما إذا كان قد تم تعديله بواسطة مهاجم.
- فرض حد أدنى من الاجهاد على النظام عند تشغيله.
- • أن يكون قادرا على التهيئة وفقًا لسياسات الأمن للنظام الذي تتم مراقبته.
- ان يكون قادرا على التكيف مع التغييرات في النظام وسلوك المستخدم بمرور الوقت.
- ان يكون قادرا على التوسع لمراقبة عدد كبير من المضيفين.
- توفير تدهور سلس للخدمة بمعنى أنه إذا توقفت بعض مكونات نظام كشف التسلل عن العمل لأي سبب من الأسباب ، فيجب أن لا يتأثر الباقي.
- • السماح بإعادة التكوين الديناميكي ، أي القدرة على إعادة تكوين نظام كشف التسلل دون الحاجة إلى إعادة تشغيله.

تقنية مصيدة وعاء العسل (Honeypot)

احدى تقنيات الكشف عن التسلل هي تقنية مصيدة وعاء العسل (**Honeypot**). وعاء العسل (مصيدة جذب) هي أنظمة خادعة مصممة لجذب المخترق المحتمل بعيدًا عن الأنظمة المهمة. تم تصميم الموضع من أجل:

1. تحويل المخترق عن الوصول إلى الأنظمة الهامة.
2. جمع المعلومات حول نشاط المخترق.
3. تشجيع المخترق على البقاء على النظام لفترة كافية حتى يستجيب المسؤولون ويتم اصطياده.

تمتلئ هذه الأنظمة بمعلومات ملفقة مصممة لتبدو ذات قيمة ولكن ليس للمستخدم الشرعي للنظام. وبالتالي ، فإن التواصل مع نظام وعاء العسل يعتبر مشبوه. يتم تجهيز النظام بمراقبات حساسة ومسجلات للأحداث تكتشف عمليات الوصول هذه وتجمع معلومات حول أنشطة المخترق. نظرًا لأن أي هجوم على نظام وعاء العسل يبدو ناجحًا ، فإن المسؤولين لديهم الوقت لاصطياد وتسجيل وتعقب المهاجم دون تعريض الأنظمة المهمة على الإطلاق.

نتيجة ان وعاء العسل هو مورد ليس له قيمة إنتاجية، فلا يوجد سبب مشروع لأي شخص خارج الشبكة للتفاعل معه. وبالتالي ، فإن أي محاولة للاتصال بوعاء العسل هي على الأرجح مسبار أو مسح أو هجوم. على العكس من ذلك ، إذا بدأ وعاء عسل باتصال خارجي فمن المحتمل أن يكون قد تعرض للاختراق.

تقنية مصيدة وعاء العسل (Honeypot)

تصنف مواضع وعاء العسل عادةً على أنها إما منخفضة أو عالية التفاعل:

- مصيدة جذب منخفضة التفاعل: تتكون من حزمة برامج تحاكي خدمات أو أنظمة معينة لتقنية المعلومات بشكل جيد بما يكفي لتوفير تفاعل أولي واقعي ، ولكنها لا تنفذ نسخة كاملة من تلك الخدمات أو الأنظمة.
- مصيدة جذب عالية التفاعل: هو نظام حقيقي ، مع نظام تشغيل كامل ، وخدمات وتطبيقات ، يتم تجهيزها ونشرها حيث يمكن الوصول إليها من قبل المهاجمين.

مصيدة الجذب عالية التفاعل هو نظام أكثر واقعية قد يشغل المهاجم لفترة طويلة. ومع ذلك ، فإنه يتطلب المزيد من الموارد بشكل كبير ، وإذا تم اختراقه يمكن استخدامه لشن هجمات على أنظمة أخرى. قد يؤدي هذا إلى مشاكل قانونية أو تتعلق بالسمعة غير مرغوب فيها للمؤسسة التي تديره. توفر مصيدة الجذب منخفضة التفاعل نظاما أقل واقعية ، قادرًا على تحديد المتسللين باستخدام مراحل منهجية الاختراق. غالبًا ما يكون هذا النظام كافيًا لاستخدامه كعنصر من مكونات (IDS) الموزعة للتحذير من هجوم وشيك.

تضمنت الجهود الأولية لتقنية وعاء العسل حاسوب واحد منفردًا مع عناوين (IP) مصممة لجذب المتسللين. ركزت الأبحاث الحديثة على بناء شبكات مصائد جذب كاملة تحاكي مؤسسة ، ربما باستخدام حركة مرور وبيانات فعلية أو محاكاة. وبمجرد دخول المتسللين إلى الشبكة ، يمكن للمسؤولين مراقبة سلوكهم بالتفصيل و وضع الدفاعات.

نشر مصيدة وعاء العسل (Honeypot)

يمكن نشر مصيدة وعاء العسل في مجموعة متنوعة من المواقع، يوضح الشكل بعضها. يعتمد الموقع على عدد من العوامل ، مثل نوع المعلومات التي تهتم المنظمة بجمعها ومستوى المخاطر التي يمكن للمنظمات تحملها للحصول على أقصى قدر من البيانات. مصيدة وعاء عسل خارج جدار الحماية الخارجي (الموقع 1) مفيد لتتبع محاولات الاتصال بعناوين (IP) غير المستخدمة داخل نطاق الشبكة. موقع المصيدة في هذا الموقع لا يزيد من مخاطر الشبكة الداخلية. ويتم تجنب خطر وجود نظام مخترق خلف جدار الحماية. علاوة على ذلك ، نظرًا لأن موضع المصيدة يجذب العديد من الهجمات المحتملة ، فإنه يقلل من التنبيهات الصادرة عن جدار الحماية وأجهزة استشعار (IDS) الداخلية ، مما يخفف من العبء الإداري. عيب المصيدة الخارجية هو أنه لديها قدرة قليلة أو معدومة على اصطياد المهاجمين الداخليين ، خاصة إذا كان جدار الحماية الخارجي يقوم بتصفية حركة المرور في كلا الاتجاهين. شبكة الخدمات المتاحة خارجيًا ، مثل الويب والبريد ، والتي تسمى غالبًا "المنطقة المنزوعة السلاح " (DMZ)، هي مرشح آخر لتحديد موقع مصيدة وعاء العسل (الموقع 2). يجب أن يتأكد مسؤول الأمن من أن الأنظمة الأخرى في المنطقة المجردة من السلاح (DMZ) آمنة ضد أي نشاط يتم إنشاؤه بواسطة نظام وعاء العسل. من عيوب هذا الموقع أنه لا يمكن الوصول إلى (DMZ) النموذجي بشكل كامل ، ويقوم جدار الحماية عادةً بحظر حركة المرور إلى (DMZ) في محاولات الوصول إلى الخدمات غير الضرورية. وبالتالي ، يجب على جدار الحماية إما أن يفتح حركة المرور بما يتجاوز المسموح به ، وهو أمر محفوف بالمخاطر ، أو يحد من فعالية مصيدة وعاء العسل. يتميز موقع المصيدة الداخلي بالكامل (الموقع 3) بالعديد من المزايا. أهم ميزة له هي أنه يمكن أن يصاب بهجمات داخلية. يمكن أيضًا أن يكتشف موضع المصيدة في هذا الموقع جدار حماية خاطئ يقوم بإعادة توجيه حركة المرور غير المسموح بها من الإنترنت إلى الشبكة الداخلية. هناك عدة عيوب. والأخطر من ذلك هو إذا تم اختراق نظام وعاء العسل بحيث يمكنه مهاجمة الأنظمة الداخلية الأخرى. لا يتم حظر أي حركة مرور أخرى من الإنترنت إلى المهاجم بواسطة جدار الحماية لأنه يعتبر حركة مرور إلى مصيدة وعاء العسل فقط. هناك صعوبة أخرى في موقع نظام وعاء العسل هذا وهي أنه ، كما هو الحال مع (الموقع 2) ، يجب على جدار الحماية ضبط التصفية للسماح بحركة المرور إلى نظام وعاء العسل ، مما يعقد تكوين وتهيئة جدار الحماية ويحتمل أن يعرض الشبكة الداخلية للخطر.

نشر مصيدة وعاء العسل (Honeypot)

1- مصيدة وعاء عسل خارجية ؛ تتبع محاولات الاتصال بعناوين (IP) غير مستخدمة؛ لا يمكن اكتشاف المهاجمين الداخليين.

2- مصيدة وعاء عسل في (DMZ) ، يجب التأكد ان الأنظمة الأخرى في (DMZ) آمنة؛ فربما يحجب الجدار الناري حركة المرور عن نظام وعاء العسل.

3- مصيدة وعاء عسل داخلية؛ يمكنه كشف الهجمات الداخلية.