CyberEco

معًا لدعم السّلامة الرّقميّة

Together to support digital safety

ضَوابِط الأمن السّيبرانيّ للحَوْسَبَة السَّحابيَّة

محتوى تدريبي موجه للمعلمين

شرائح العَرْض

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency

حُقُوق المِلْكِيَّة الفِكْرِيَّة

المـادَّة مَمْلُوكـة للوكالـة الوطنيَّـة للأمـن السِّـيبرانيّ فـي دولـة قطـر، وكافَّـة حقـوق المِلكيَّـة الفكريَّـة التـي تشـمل حـقّ المؤلِّـف وحقـوق التَّأليـف والنَّشـر والطِّباعـة، كُلّهـا مكفولـة للوكالـة الوطنيَّـة للأمـن السِّـيبرانيّ فـي دولـة قطـر. وعليه، فجميع الحقوق محفوظة للوكالة، ولا يجوز إعادة نَشْر أيّ أجزاء من هذه المادَّة، أو الاقتباس منها، أو نَسْخ أيّ جُزْء منها، أو نَقْلها كليًّا أو جزئيًّا في أيّ شكلٍ وبأيّ وسيلة، سواءٌ بطرق إلكترونيَّة أو آليَّة، بما في ذلك التَّصوير الفوتوغرافيّ، أو التَّسجيل، أو استخدام أيّ نظام مِن نُظُم تخزين المعلومات واسترجاعها سواءٌ من الأنظمة الحاليَّة أو المُبْتَكَرَة في المُسْتَقبَل؛ إلَّا بعد الرُّجُوع إلى الوكالة، والحُصُول على إذن خطّيّ منها.

ومَن يُخالف ذلك يُعرِّض نفسه للمُساءَلة القانونيَّة.

ديسمبر 2023م

الدوحة، قطر

هذا المحتوى إنتاج فريق

إدَارة التَّميُّز السّيبرانيّ الوَطنيّ، الوكالة الوطنيَّة للأَمْن السّيبرانيّ.

للاستفسار عن المُبادَرة أو البرنامج؛ يمكن التَّواصُل عن طريق المواقع الإلكترونيَّة أو الأرقام الهاتفيَّة التَّالية:

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

https://www.ncsa.gov.qa/
cyberexcellence@ncsa.gov.qa
00974 404 663 78
00974 404 663 62

التَّوزيع الزَّمنيّ للوَرشَة

المحتوى	الوقت المُخصَّص
تَمْهيد	15 دقيقة
الجانب النَّظريّ من المادَّة	45 دقيقة
عَرْض الفيديوهات التَّدريبيَّة	25 دقيقة
اسْتِراحَة قَصِيرَة	20 دقيقة
حِوَار ونِقَاش مع المُتَدرِّبين	15 دقيقة
المُدَّة الزَّمنيَّة للوَرْشَة	ساعتان

فِهْرِس المحتوى العِلْميّ للحَقيبَة التَّدريبيَّة

مُقدِّمـة 17

الفَصْل الأوَّل

مفهـوم الحَوْسَبَة السَّحابيَّة..... **19**

- أهمِّيَّـة الحَوْسَبَة السَّحابيَّة..... 20
- أنـواع الحَوْسَبَة السَّحابيَّة..... 22
- تحدِّيـات الحَوْسَـبَة السَّـحابيَّة..... 30

الفَصْل الثَّاني

المَخاطِـر الرَّقميَّة التي تواجه الحَوْسَبَة السَّحابيَّة **33**

- فقـدان البيانـات..... 34
- البرمجيَّـات الضَّـارَّة..... 36
- الوصـول غير المصرَّح بـه..... 39

الفَصْل الثَّالث

كيفيَّة حماية الحَوْسَبَة السَّحابيَّة من الهجمات الرَّقميَّة..... **41**

- الأمـن السَّـحابيّ..... 42
- حمايـة البيانـات في الحَوْسَبَة السَّحابيَّة من القَرْصَنَـة 46
- البطاقـات التدريبيـة..... 49

الفَصْل الأوَّل
مَفْهوم الحَوْسَبَة السَّحابيَّة

الحَوْسَبَة السَّحابيَّة

هي تقديم مَجْموعةٍ من الخِدْمَات عَبْر الإنترنت، بما يتضمَّن أدوات وتطبيقات مثل تخزين البيانات والخوادم وقواعد البيانات والشَّبَكات والبرامج؛ فبدلًا من الاحتفاظ بالمِلفَّات على مُحرِّك أقراصٍ ثابتٍ أو خاصّ (تَخْزين محلِّيّ)، يمكن الاعتماد على السَّحابة وتخزين المُسْتَنَدَات في قاعدة بيانات على الشَّبكَة، طالما أنَّ الأجهزة الإلكترونيَّة لديها القُدْرة على الوصول إلى الويب، ومن ثَمَّ التَّمتُّع بإمكانيَّة الوصول إلى البيانات والبرامج اللَّازمة لتشغيله.

لماذا تمَّت تَسْمِية الحَوْسَبَة السَّحابيَّة بهذا الاسم؟

تمَّت تَسْمِية الحَوْسَبَة السَّحابيَّة بهذا الاسم لأنَّ المعلومات التي يتمّ الوصول إليها موجودة عن بُعْد في السَّحابة أو في الفضاء الافتراضيّ، حيث تُتيح الشَّركات التي تُقدِّم الخدمات السَّحابيَّة للمُسْتَخْدِمِين تخزين المِلفَّات والتَّطبيقات على خوادم بعيدة، ومن ثَمَّ الوصول إلى جميع البيانات عَبْر الإنترنت، فهو مصطلح عامّ يستخدمه العاملون في صناعة التِّكنولوجيا لوَصْف هذه الخوادم والبِنَى التَّحتيَّة للشَّبَكات، ولا تحتاج من المُسْتَخْدِم الحضور في مكانٍ مُحَدَّدٍ للوصول إليها.

أهمِّيَّة الحَوْسَبَة السَّحابيَّة

1. توفير التَّكاليف.
2. زيادة الإنتاجيَّة.
3. السُّرعة والكفاءة والأمان.
4. التَّعاون: تُوفِّر شركات الحَوْسَبَة السَّحابيَّة فِرَقًا من المُتَخصِّصين والتِّقنيِّين العاملين على توفير الأمن للبيانات على الخوادم.
5. القابليَّة للتَّطوير: تتميَّز السَّحابة بالمرونة والقابليَّة للتَّطوير بِشَكْلٍ كاملٍ وَفْق احتياجات العمل، فيمكن للمُسْتَخْدِمين توسيع نطاق الحِزْمة الخاصَّة بهم أو تخفيضها وَفْق مُتَطلَّباتهم الشَّخصيَّة والعمليَّة.

أنواع الحَوْسَبَة السَّحابيَّة

أوَّلًا: السَّحابة العامَّة

هي سحابة مفتوحة ومُتاحة للجميع لتخزين المعلومات والوصول إليها عَبْر الإنترنت باستخدام طريقة الدَّفع لكُلّ استخدامٍ.

سُهُولة الوصول.
البِنْية التَّحتيَّة المُشْتَرَكَة.
الدَّفع لكُلّ استخدامٍ.
خصائص الحَوْسَبَة السَّحابيَّة العامَّة
قابليَّة التَّوسُّع.
سُهُولة الصِّيانة والإدارة.

عُيُوب الحَوْسَبَة السَّحابيَّة العامَّة

1. أقلّ أمانًا لأنَّ الموارد تتمّ مُشارَكَتها بِشَكْلٍ عامّ.
2. الاعتماد على مُزوِّد الخدمة السَّحابيَّة.
3. يعتمد الأداء على ارتباط شبكة الإنترنت عالية السُّرعة بمُوفِّر السَّحابة.
4. المَخاوِف بشَأْن خصوصيَّة البيانات وسرِّيَّتها.
5. البيانات ليست تحت سَيْطرة المُسْتَخْدِم.
6. احتماليَّة تكبُّد تكاليف غير مُتَوقَّعَة مع نماذج التَّسعير القائمة على الاستخدام.
7. الافتقار إلى خيارات التَّخصيص والمُرُونة.

ثانيًا: الحَوْسَبَة السَّحابيَّة الخاصَّة

يُطلَق على الحَوْسَبَة السَّحابيَّة الخاصَّة مُسمَّيات مِثْل السَّحابة الدَّاخليَّة أو سَحابة الشَّركات، حيث يتمّ استخدامها من قِبَل المُؤسَّسات لبناء وإدارة مراكز البيانات الخاصَّة بها داخليًّا أو بواسطة جهةٍ خارجيَّةٍ.

أنواع الحَوْسَبَة الخاصَّة

01

الحَوْسَبَة السَّحابيَّة الخاصَّة داخل المُؤسَّسة: حيث توجد السَّحابة الخاصَّة ضِمْن البِنْية التَّحتيَّة الماديَّة للمُؤسَّسة.

02

الحَوْسَبَة السَّحابيَّة الخاصَّة التي يتمّ فيها الاستعانة بمصادر خارجيَّة: يُقصَد بها الاستعانة بمصادر خارجيَّة مثل الشَّراكة مع مُزوِّد خدمةٍ خارجيّ لاستضافة البِنْية التَّحتيَّة السَّحابيَّة وإدارتها نيابةً عن المُؤسَّسة.

خصائص الحَوْسَبَة السَّحابيَّة الخاصَّة

1. تمنح المُؤسَّسات مزيدًا من التَّحكُّم في بياناتها وتطبيقاتها وأَمْنها.
2. تُعتبر مُناسِبَة بِشَكْلٍ خاصّ للمُؤسَّسات التي لديها مُتطلَّبات امتثالٍ صارمة، أو بيانات حسَّاسة.
3. الاستخدام الحَصْريّ، حيث تُخصَّص الحَوْسَبَة السَّحابيَّة الخاصَّة لمُؤسَّسةٍ واحدةٍ.
4. تُوفِّر تحكُّمًا وأمانًا أعلى من خيارات السَّحابة العامَّة.
5. تسمح للمُؤسَّسات بتخصيص البِنْية التَّحتيَّة وَفْقًا لمُتطلَّباتها المُحَدَّدة.
6. تتيح السَّحابة الخاصَّة للمُؤسَّسات توسيع نطاق الموارد وتخصيصها وَفْقًا للطَّلَب.
7. تمنح المُؤسَّسات المزيد من التَّحكُّم في البِنْية التَّحتيَّة لها، ممَّا يُحسِّن الأداء والاعتماديَّة.
8. يمكن دَمْج السَّحابة الخاصَّة مع الخدمات السَّحابيَّة العامَّة، ممَّا يعني الاستفادة من فوائد السَّحابة الخاصَّة والعامَّة معًا.

عُيُوب الحَوْسَبَة السَّحابيَّة الخاصَّة

1. تتطلَّب أشخاصًا ماهرين لإدارة وتشغيل الخدمات السَّحابيَّة.
2. يمكن الوصول إلى السَّحابة الخاصَّة داخل المُؤسَّسة، وبالتَّالي فإنَّ منطقة العمليَّات محدودة.
3. ليست مُناسِبَة للمُؤسَّسات التي ليس لديها بِنْية تحتيَّة مُعدَّة مُسْبَقًا لصيانة السَّحابة وإدارتها.
4. ارتفاع التَّكاليف الأوَّليَّة ونفقات الصِّيانة المُستمرَّة.
5. قد يكون توسيع نطاق الموارد أمرًا صعبًا مُقارَنَةً بخيارات السَّحابة العامَّة أو المُخْتَلطَة.
6. تعتمد على مُوظَّفي تكنولوجيا المعلومات الدَّاخليِّين للإدارة في استكشاف الأخطاء وإصلاحها.
7. وصول محدود إلى أحدث التَّطوُّرات والابتكارات التي يُقدِّمها مُوفِّرو الخدمات السَّحابيَّة العامَّة.
8. الحاجة إلى تحديثاتٍ مُنْتَظِمَةٍ للبِنْية التَّحتيَّة.

ثالثًا: السَّحابة الهجينة

هي مزيجٌ من الحَوْسَبَة السَّحابيَّة العامَّة والحَوْسَبَة السَّحابيَّة الخاصَّة، وفي هذا النَّوْع من السَّحابات يمكن للمُؤسَّسات الاستفادة من فوائد السَّحابة العامَّة والخاصَّة لإنشاء بيئة حَوْسَبَة مَرِنَة وقابلة للتَّطوير.

مُميِّزات السَّحابة الهجينة

1. تعمل على دَمْج خصائص السَّحابة العامَّة والخاصَّة؛ ممَّا يسمح بالاستفادة من مُميِّزات السَّحابة العامَّة والخاصَّة معًا.
2. تُوفِّر مُرونة في تخصيص الموارد وقابليَّة التَّوسُّع.
3. تُوفِّر بيئة آمِنَة ومُخَصَّصة، بينما يمكن استخدام موارد السَّحابة العامَّة للمَهامّ غير الحسَّاسة.
4. تحسين التَّكاليف من خلال استخدام السَّحابة للأعمال غير المُهمَّة، مع الاحتفاظ بالتَّطبيقات والبيانات المُهمَّة على السَّحابة الخاصَّة.
5. إمكانيَّة نَقْل البيانات والتَّطبيقات بين السَّحابات العامَّة والخاصَّة حسب الحاجة.
6. تُسهِّل مُهمَّة التَّعافي من الكوارث واستمراريَّة الأعمال، من خلال نَسْخ البيانات والتَّطبيقات المُهمَّة بين السَّحابة الخاصَّة والعامَّة، ممَّا يُقلِّل من مخاطر فقدان البيانات أو انقطاع الخدمة.

عُيُوب السَّحابة الهجينـة

1. ضَعْف مَيْزة الأمان.
2. تُعدّ إدارة السَّحابة المُخْتَلطَة أمرًا مُعقَّدًا لوجود أكثر من نوعٍ واحدٍ من نماذج النَّشر.
3. تعتمد مَوْثوقيَّة الخدمات على مُقدِّمي الخدمات السَّحابيَّة.
4. تزايد التَّحدِّيات المُحْتَمَلَة في تكامل البيانات وضمان الاتِّصال بين الأنظمة الأساسيَّة السَّحابيَّة المُخْتَلِفَة.
5. ارتفاع التَّكاليف بسبب الحاجة إلى إدارة وتكامل البيئات السَّحابيَّة المُتَعدِّدة.
6. زيادة التَّعقيد في إدارة البيانات عَبْر مُوفِّري الخدمات السَّحابيَّة المُخْتَلِفين.
7. الاعتماد على اتِّصالات الإنترنت المُستقرَّة وذات النِّطاق التَّرَدُّديّ العالي لإجراء عمليَّات سحابيَّة هجينة فعَّالة.
8. تتطلَّب مُوظَّفين ماهرين في مجال تكنولوجيا المعلومات من ذَوِي الخِبْرة.

رابعًا: سحابة المُجْتَمَع

تسمح بالوصول إلى الأنظمة والخدمات من قِبَل مجموعة من عِدَّة مُؤسَّسات لمُشارَكَة المعلومات بين المُؤسَّسة ومُجْتَمَعٍ مُعيَّنٍ، وهي مملوكة ومُدارة من قِبَل واحدة أو أكثر من المُؤسَّسات في المُجْتَمَع، أو طرفٍ مجهولٍ أو مجموعةٍ منهم، مثل: سحابة مُجْتَمَع الرِّعاية الصِّحِّيَّة.

خَصائِص سحابة المُجْتَمَع

1. تُوفِّر بِنْية أساسيَّة مُشْتَركَة يمكن الوصول إليها من قِبَل مُجْتَمَعٍ مُحدَّدٍ من المُؤسَّسات.
2. تُوفِّر الموارد والتَّطبيقات والخدمات التي تتكيَّف مع مُتَطلَّبات المُؤسَّسات المُشارِكَة، مع تعزيز التَّواصل الفعَّال وتبادل المعلومات.
3. تسمح بتنفيذ ضوابط أمنيَّة قويَّة وإدارة الوصول وأُطُر الامتثال التي تُلبِّي المُتَطلَّبات التَّنظيميَّة للمُجْتَمَع ومعايير الصِّناعة.
4. تستفيد المُؤسَّسات المُشارِكَة من تَقاسُم التَّكاليف.
5. تُشجِّع على التَّواصل وتبادل المعلومات بين المُشارِكِين.
6. تُتيح للمُؤسَّسات إمكانيَّة توسيع نِطَاق مواردها أو تقليلها استجابةً للطَّلَب.

عُيُوب سحابة المُجْتَمَع

01 مُميِّزات الأمان ليست جيِّدة كما في السَّحابة الخاصَّة.

02 ليست مُناسِبَة إذا لم يكن هناك تعاون بين المُشارِكِين فيها.

03 خيارات قابليَّة التَّوسُّع محدودة، حيث تُحدِّد الموارد المُشْتَرَكَة سَعَة سحابة المُجْتَمَع.

04 تَضارُب المَصالِح المُحْتَمَل بين أفراد المُجْتَمَع فيما يَتَعلَّق بتخصيص الموارد واستخدامها.

05 إنَّ أُطُر الحَوْكَمَة والاتِّفاقيَّات الشَّفَّافة مطلوبة لمُعالَجَة النِّزاعات المُحْتَمَلَة وضمان التَّوزيع العادل للموارد.

تحدِّيات الحَوْسَبة السَّحابيَّة

01 تحدِّيات الأمان؛ تخزين البيانات في السَّحابة يجعلها أكثر عُرْضة للقَرْصَنة والجرائم الإلكترونيَّة.

02 تحدِّي الأداء، لا بُدّ من التَّأكُّد أنَّ السَّحابة غير مُعَرَّضَة لخطر الانقطاعات.

03 ضرورة وَضْع خُطَّة احتياطيَّة في حالة انقطاع التَّيَّار الكهربائيّ.

04 ضرورة الحَذَر من تراكُم المِنصَّة السَّحابيَّة دون قصدٍ، على سبيل المثال، إذا لم تكن موارد السَّحابة مُنَظَّمَة ومُحَسَّنَة، فمن المُمْكِن أن تتراكم مساحة تخزين المِلفَّات في وقتٍ قصيرٍ.

الفَصْل الثَّاني
المَخاطِر الرَّقميَّة التي تُواجِه الحَوْسَبَة السَّحابيَّة

فقدان البيانات

يُعدّ فقدان البيانات من المَخاطِر الأمنيَّة السَّحابيَّة الأكثر شيوعًا للحَوْسَبَة السَّحابيَّة، ويُطلَق عليه أيضًا اسم "تسرُّب البيانات"، وفقدان البيانات هو العمليَّة التي يتمّ فيها حَذْف البيانات وإتلافها وجعلها غير قابلة للقراءة بواسطة مُسْتَخْدِمٍ أو برنامجٍ أو تطبيقٍ.

العوامل الأكثر شُيُوعًا لفقدان البيانـات في السَّحابـة

الحَذْف العَرَضيّ (خطأ المُسْتَخْدِم)

الحذف غير المقصود هو المصدر الأكثر شُيُوعًا لفقدان البيانات، لكنَّ عمليَّات النَّسْخ الاحتياطيّ التِّلقائيَّة تُعدّ حلًّا لهذه المشكلة.

الكِتابَـة فـوق البيـانـــات

من المُمْكِن استبدال المعلومات عن طريق الخطأ بواسطة المُسْتَخْدِمِين أو التَّطبيقات.

الإجـراءات الضَّــارَّة

ويُقصَد بها الهجمات الإلكترونيَّة التي تستهدف البيانات في السَّحابة.

كيفيَّة حماية البيانات المُخَزَّنة على السَّحابة من الفقدان

01

إجراء نَسْخ احتياطيّ للبيانات الأكثر أهمِّيَّة وَفْقًا لجَدْوَلٍ زمنيّ يتماشى مع أهداف العمل.

02

إيجاد حلّ نَسْخ احتياطيّ يُناسِب احتياجات وأولويّات العمل، واختبار النُّسَخ الاحتياطيَّة.

03

ضَعْ في اعتبارك كيفيَّة حِفْظ النُّسَخ الاحتياطيَّة الخاصَّة بك بنجاحٍ في مراكز بياناتٍ مُخْتَلِفَةٍ.

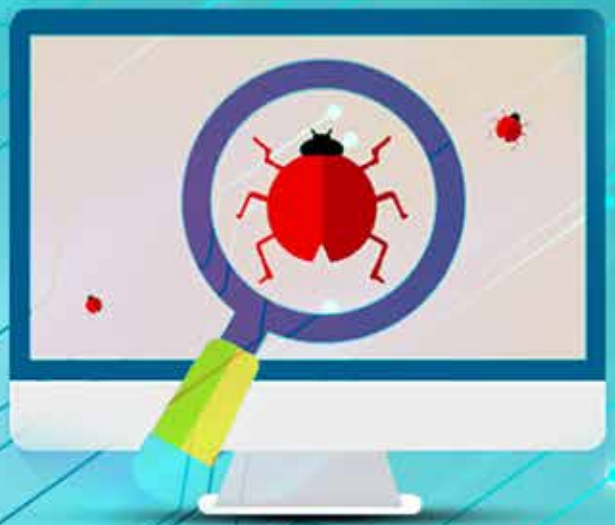
04

فَهْم أهمِّيَّة تخزين البيانات بطريقة لا يمكن التَّلاعب بها أو تشفيرها بواسطة برمجيات الفِدْية.

البرمجيّات الضَّارَّة

البرمجيات الضَّارَّة السَّحابيَّة

هي برمجيات ضارَّة تمَّ إنشاؤها وتوزيعها من خلال بيئات الحَوْسَبَة السَّحابيَّة لسرقة البيانات من المُسْتَخْدِمِين والمُؤسَّسات وتعطيل عمليَّاتها والتَّسبُّب في الكثير من المُشْكِلَات.



أنواع هجمات البرمجيات الضَّارَّة في السَّحابة

هجمات الحَقْن

هو هجومٌ سيبرانيّ يستخدمه مُجْرِمُو الإنترنت لإحداث الفَوْضَى عَبْر نقاط الوصول غير المُصحَّحة لسرقة البيانات والهُوِيَّات، وكذلك نَشْر برمجيات الفِدْية أو حتَّى الاستفادة من المعلومات المسروقة.

عمليَّات التَّصيُّد الاحتياليّ

تتمّ عَبْر إرسال رسائل بريدٍ إلكترونيّ أو رسائل نصِّيَّة تبدو كأنَّها من مصادر معروفة، لكنَّها مُحاوَلَة لسرقة بيانات سرِّيَّة أو تثبيت تعليماتٍ برمجيَّةٍ ضارَّةٍ على الجهاز.

سرقة البيانات

هي شكل شائع من هجمات البرمجيات الضَّارَّة السَّحابيَّة.

أنواع هجمات البرمجيات الضَّارَّة في السَّحابة

أَحْصِنَة طـروادة

هي نَوْعٌ من البرمجيات الضَّارَّة السَّحابيَّة التي تتنكَّر كبرنامجٍ شرعيّ من أجل الوصول إلى النِّظام أو سرقة البيانات.

مُهاجَمَة الوظائف وواجهات برمجة التَّطبيقات

بدون خادمٍ، ويتمّ تنفيذ هذا الهجوم عن طريق استغلال نقاط الضَّعف في برمجة التَّطبيقات؛ ممَّا يسمح للجهات الفاعلة الخبيثة بتنفيذ تعليمات برمجيَّة عشوائيَّة أو مُشوَّهة على النِّظام.

هجمات DOS Hypervisor

برنامج Hypervisor هو نَوْعٌ من البرمجيات التي تسمح بتشغيل أنظمة تشغيل مُتَعدِّدة على نفس الحاسوب في الوقت نفسه، وتحدث الهجمات عندما يحاول المُهاجِمُون تحميل النِّظام بِشَكْلٍ زائدٍ؛ ممَّا يُؤدِّي إلى تعطُّله أو عدم استجابته.

أنواع هجمات البرمجيات الضَّارَّة في السَّحابة

استغلال التَّرحيـل المُباشِـر

عمليَّة يمكن من خلالها نَقْل الأجهزة الافتراضيَّة من مضيفٍ فعليّ إلى آخر، ممَّا يسمح بتحسين استخدام الموارد وتحسين الأداء، لكن يمكن استغلال هذه العمليَّة من قِبَل المُهاجِمِين في حالة وجود أيّ ثغراتٍ أمنيَّةٍ في بروتوكولات الأمان الخاصَّة بالنِّظام.

التَّنصُّت على الواي فاي Wi-Fi

وسيلة لهجوم الوصول عن بُعْد؛ حيث يحاول المُهاجِمُون الوصول إلى الجهاز المُسْتَهْدَف عن طريق اعتراض وفَكّ تَشفير الشَّبَكة.

عمليَّات استغلال الثَّغرَات غير المُكْتَشَفة

نَوْعٌ من الهجمات الإلكترونيَّة التي تَسْتغلّ نقاط الضَّعْف غير المعروفة سابقًا في أنظمة الحاسوب أو التَّطبيقات.

الفَصْل الثَّالث
كيفيَّة حماية الحَوْسَبَة السَّحابيَّة من الهجمات الرَّقميَّة

الأمن السَّحابيّ

هو الإجراءات والتِّقنيَّات التي تعمل على تأمين بيئات الحَوْسَبَة السَّحابيَّة من تهديدات الأمن السّيبرانيّ الخارجيَّة والدَّاخليَّة، فأمان الحَوْسَبَة السَّحابيَّة يقوم بإدارة جميع التَّطبيقات والأجهزة والبيانات الخاصَّة بك مركزيًّا لضمان حماية كُلّ شيءٍ، فهو يُتيح أداء المَهامّ بسهولةٍ أكبر، مثل تنفيذ خُطَط التَّعافي من الكوارث، وتبسيط مُراقَبَة أحداث الشَّبَكة، وتحسين تصفية الويب.

هجمات حجب الخدمة المُوَزَّعَة (DDoS)

من أكبر التَّهديدات التي تُواجِه الحَوْسَبَة السَّحابيَّة لكَوْنها تستهدف حركة مرور كبيرة على الخوادم في وقتٍ واحدٍ لإحداث الضَّرَر، فالأمان السَّحابيّ هنا يحمي الخوادم من هذه الهجمات من خلال مُراقَبَتها وتوزيعها.

هل السَّحابة آمِنَة بما فيه الكفاية؟

يعتمد المُسْتَخْدِمُون بِشَكْلٍ أكبر على التَّخزين السَّحابيّ والمُعالَجَة، لكنَّهم عادةً ما يشعرون بالقلق، إلَّا أنَّ التَّجربة أثبتت أنَّ هذا الخوف لا أساس له من الصِّحَّة. فمُوَفِّرو الخدمة السَّحابيَّة يقومون بتنفيذ الإجراءات والتِّقنيَّات التي تمنع مُوَظَّفيهم من عَرْض بيانات العملاء.

وعمليًّا فإنَّ مُقدِّمي الخدمات السَّحابيَّة مسؤولون عن الحفاظ على تطبيق بيئة التَّشغيل الخاصَّة بالمُسْتَخْدِم، بينما يتحمل المُسْتَخْدِمون مسؤوليَّة ما يحدث داخل تلك البيئة.

باختصارٍ، يمكن أن تكون السَّحابة آمِنَة للمحتوى الخاصّ بك إذا فهمت أدوات الأمان الخاصَّة بالسَّحابة بِشَكْلٍ جيِّدٍ.

جوانب أساسيَّة للأمان السَّحابيّ

- تقييد عمليَّة الوصول: من الضَّروريّ التَّأكُّد من مَنْح الأشخاص المُناسبين فقط حقّ الوصول إلى الأدوات المُناسِبَة في الوقت المُناسِب.
- حماية البيانات: فمُسْتَخْدِمُو خدمات الحَوْسَبَة يحتاجون إلى معرفة مكان وجود بياناتهم ووَضْع ضوابط مُناسِبَة لتأمين البيانات والبِنْية التَّحتيَّة المُسْتَضِيفَة لتلك البيانات.
- اسْتِعادة البيانات: يجب توفير نُسَخ احتياطيَّة جيِّدة للبيانات وخُطَّة استعادة بيانات لتجنُّب التَّعرُّض لأي ضررٍ عند حدوث خَرْقٍ أمنيّ.
- خُطَّة الاسْتِجابة: عند التَّعرُّض للهجمات، يجب أن تكون هناك خُطَّة لتقليل تأثير تلك الهجمات.
- التَّحقُّق المُبكِّر من الثَّغرات الأمنيَّة.
- توجيه تركيز فِرَق الأمان نحو التَّخلُّص من التَّهديدات النَّاشِئَة عَبْر تعزيز تكوينات موارد السَّحابة من خلال البرمجيَّات؛ لتقليل مشكلات الأمان التي تواجه بيئات الإنتاج.

حماية البيانات في الحَوْسَبَة السَّحابيَّة من القَرْصَنَة

- استخدام كلمات مرور قويَّة تتكوَّن من الأَحْرُف والأرقام والرموز الخاصَّة.
- حماية جميع الأجهزة التي تُسْتَخدَم للوصول إلى بياناتك السَّحابيَّة، بما في ذلك الهواتف الذَّكيَّة والأجهزة اللَّوْحيَّة، خاصَّةً إذا كانت بياناتك مُتَزامِنَة عَبْر العديد من الأجهزة.
- إنشاء نُسْخة احتياطيَّة من البيانات، وذلك بوَضْع نُسْخَةٍ على جهاز الحاسوب المَنْزليّ الخاصّ بك.
- استخدام الأُدُونات لمَنْع أيّ فردٍ أو جهازٍ من الوصول إلى جميع بياناتك.
- استخدام أحد برامج مُكافَحَة الفيروسات والبرمجيات الضَّارَّة.
- لا تصل إلى بياناتك عبر شَبَكة Wi-Fi عامَّة.
- تُعدّ المُصادَقَة مُتعدِّدة العوامل (MFA) طريقة ذكيَّة لحماية وصولك، سواءٌ عَبْر بصمات الأصابع، أو كلمة مرور ورمز مُنْفَصِل يتمّ إرساله إلى جهازك المحمول.
- إذا لم تعد تستخدم إحدى الخدمات أو البرامج، فأغلقه بِشَكْلٍ صحيحٍ، وتأكَّد من عدم تَرْك حسابٍ قديمٍ مفتوحًا لأنَّ القَراصِنَة يَستغلُّونه لإيجاد ثغرةٍ إلى نظامك وأجهزتك.

البطاقات التّدريبيّة

الحَوْسَبَة السَّحابيَّة

هي تقديم مَجْموعةٍ من الخِدْمَات عَبْر الإنترنت، بما يتضمّن أدوات وتطبيقات مثل تخزين البيانات والخوادم وقواعد البيانات والشَّبَكات والبرامج؛ فبدلًا من الاحتفاظ بالمِلفَّات على مُحرّك أقراصٍ ثابتٍ أو خاصّ (تَخْزين محلّيّ)، يمكن بالاعتماد على السَّحابة تخزين المُستندَات في قاعدة بيانات على الشَّبكَة.

أهمِّيَّة الحَوْسَبَة السَّحابيَّة

- توفير التَّكاليف.
- زيادة الإنتاجيَّة.
- السُّرعة والكفاءة والأمان.

الحَوْسَبَة السَّحابيَّة العامَّة

مُتاحة للجميع لتخزين المعلومات والوصول إليها عَبْر الإنترنت باستخدام طريقة الدَّفع لكُلّ استخدامٍ، وتتمّ إدارة موارد الحَوْسَبَة وتشغيلها من قِبَل مُزَوِّد الخدمة السَّحابيَّة الذي يعتني بالبِنْية التَّحتيَّة الدَّاعمة، ويضمن أن تكون الموارد مُتاحة وقابلة للتَّطوير للمُسْتَخْدِمين.

الحَوْسَبَة السَّحابيَّة الخاصَّة

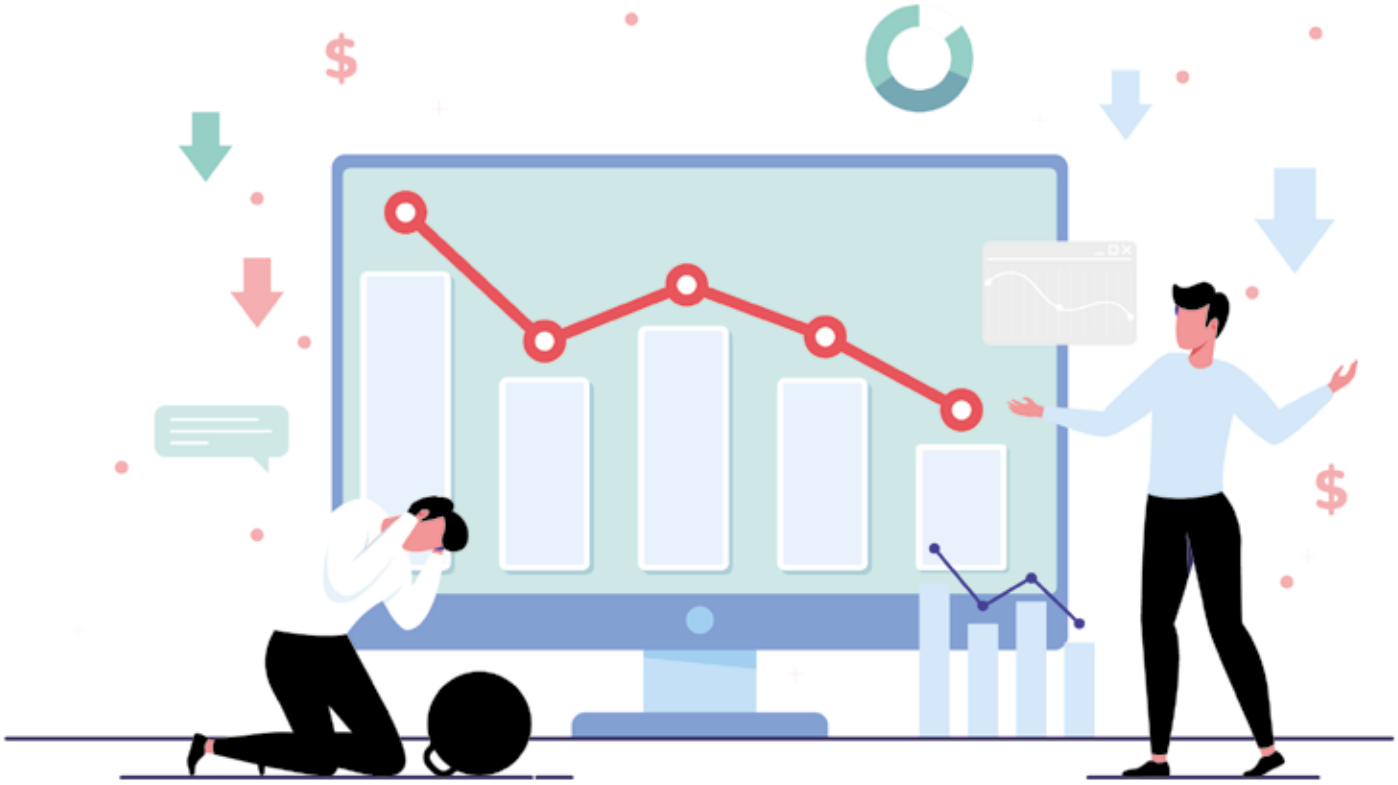
يُطلَق عليها مُسمّيات مثل السّحابة الدّاخليّة أو سحابة الشّركات، حيث يتمّ استخدامها من قِبَل المُؤسّسات لبناء وإدارة مراكز البيانات الخاصّة بها داخليًّا أو بواسطة جهةٍ خارجيّةٍ.

السّحابة الهجينة

هي مزيجٌ من الحَوْسَبَة السّحابيّة العامّة والحَوْسَبَة السّحابيّة الخاصّة، وفي هذا النّوْع من السّحابات يمكن للمُؤسّسات الاستفادة من فوائد السّحابة العامّة والخاصّة لإنشاء بيئة حَوْسَبَة مَرِنَة وقابلة للتّطوير.

سحابة المُجْتَمَع

تسمح بالوصول إلى الأنظمة والخدمات من قِبَل مجموعةٍ من عدّة مُؤسّسات لمُشارَكَة المعلومات بين المُؤسّسة ومُجْتَمَعٍ مُعيّنٍ. وهي مملوكة ومُدارة من قِبَل واحدة أو أكثر من المُؤسّسات في المُجْتَمَع، أو طرفٍ ثالثٍ، أو مجموعةٍ منهم، مثل: سحابة مُجْتَمَع الرّعاية الصّحّيّة.



فقدان البيانات

يُعدّ من المخاطر الأمنيَّة السَّحابيَّة الأكثر شيوعًا للحَوْسَبَة السَّحابيَّة، ويُطلَق عليه أيضًا اسم "تسرُّب البيانات"، وهو العمليَّة التي يتمّ فيها حذف البيانات وإتلافها وجعلها غير قابلة للقراءة بواسطة مُسْتَخْدِمٍ أو برنامجٍ أو تطبيقٍ.

البرمجيّات الضّارّة السّحابيّة

هي برمجيّات ضارّة تمّ إنشاؤها وتوزيعها من خلال بيئات الحَوْسَبَة السّحابيّة لسرقة البيانات من المُسْتَخْدِمين والمُؤسّسات وتعطيل عمليّاتها والتّسبُّب في الكثير من المشكلات.

هجمات DOS Hypervisor

برنامج Hypervisor هو نَوْعٌ من البرمجيَّات التي تسمح بتشغيل أنظمة تشغيل مُتَعدِّدة على نفس الحاسوب في الوقت نفسه، وتحدث الهجمات عندما يحاول المُهاجِمُون تحميل النِّظام بِشَكْلٍ زائدٍ عن طريق إرسال عددٍ كبيرٍ جدًّا من طلبات البيانات أو الموارد، ممَّا يُؤدِّي إلى تَعطُّله أو عدم استجابته.

أحْصِنة طروادة

هو نَوْعٌ من البرمجيّات الضّارّة السّحابيّة التي تتنكّر كبرنامجٍ شرعيّ من أجل الوصول إلى النّظام أو سرقة البيانات.

عمليّات التّصيُّد الاحتياليّ

تتمّ عَبْر إرسال رسائل بريد إلكترونيّ أو رسائل نصّيّة تبدو كأنّها من مصادر معروفة، لكنّها مُحاوَلة لسرقة بيانات سرّيّة أو تثبيت تعليمات برمجيّة ضارّة على الجهاز.

هجمات الحَقْن

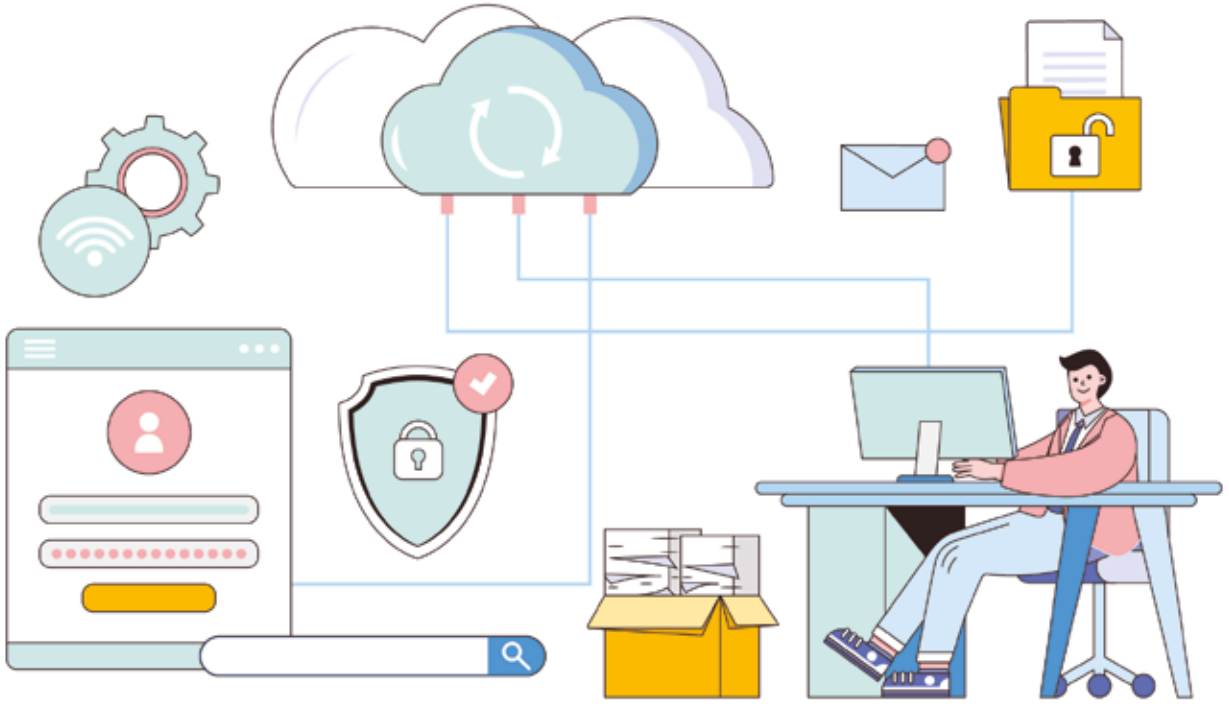
هجومٌ سيبرانيّ يستخدمه مُجْرِمُو الإنترنت لإحداث الفَوْضَى في الخوادم الطَّرفيَّة غير المحميَّة من خلال التَّسلُّل عَبْر نقاط الوصول غير المُصَحّحة، لسرقة البيانات والهُوِيَّات وكذلك نَشْر برمجيَّات الفِدْية أو حتَّى الاستفادة من المعلومات المسروقة.

التَّرحيل المُباشِر

هو عمليَّة يمكن من خلالها نَقْل الأجهزة الافتراضيَّة من مُضيفٍ فعليّ إلى آخر، ممَّا يسمح بتحسين استخدام الموارد وتحسين الأداء. لكن يمكن استغلال هذه العمليَّة من قِبَل المُهاجِمين في حالة وجود أيّ ثغراتٍ أمنيَّةٍ في بروتوكولات الأمان الخاصّة بالنِّظام.

هجوم الثُّغرَات غير المُكْتَشَفة

تُسمّى هجوم يوم الصّفر، وهي نَوْعٌ من الهجمات الإلكترونيّة التي تستغلّ نقاط الضّعف غير المعروفة سابقًا في أنظمة الحاسوب أو التّطبيقات.



الأمن السَّحابيّ

هو الإجراءات والتِّقنيَّات التي تعمل على تأمين بيئات الحَوْسَبَة السَّحابيَّة ضِدّ تهديدات الأمن السّيبرانيّ الخارجيَّة والدَّاخليَّة, فأمان الحَوْسَبَة السَّحابيَّة يقوم بإدارة جميع التَّطبيقات والأجهزة والبيانات الخاصَّة بك مركزيًّا لضمان حماية كُلّ شيءٍ، فهو يُتيح أداء المَهامّ بسهولةٍ أكبر، مثل تنفيذ خُطَط التَّعافي من الكوارث، وتبسيط مُراقَبَة أحداث الشَّبَكة، وتحسين تصفية الويب.

هجمات حجب الخدمة المُوَزَّعة (DDoS)

من أكبر التَّهديدات التي تواجه الحَوْسَبَة السَّحابيَّة لكَوْنها تستهدف حركة مرورٍ كبيرةٍ على الخوادم في وقتٍ واحدٍ لإحداث الضَّرر، فالأمان السَّحابيّ هنا يحمي الخوادم من هذه الهجمات من خلال مُراقَبَتها والتَّعامُل معها فور حدوثها.

الإسكتشات

كيف نمنع فقدان البيانات في السَّحابة؟

1. إجراء نَسْخ احتياطيّ للبيانات الأكثر أهمّيّة.

2. حِفْظ النُّسَخ الاحتياطيَّة الخاصَّة بك في مراكز بياناتٍ مُخْتَلِفَةٍ.

3. فَهْم أهمِّيَّة تخزين البيانات بطريقةٍ لا يمكن التَّلاعب بها أو تشفيرها بواسطة برمجيَّات الفِدْية.

ما أسباب فقدان البيانات في السَّحابة؟

1. الحَـذْف العَرَضيّ (خطأ المُسْتَخْدِم).
2. الكتابة فوق البيانات.
3. البرمجيَّات الضَّارَّة.

لماذا تمَّت تسمية الحَوْسَبَة السَّحابيَّة بهذا الاسم؟

تمَّت تسمية الحَوْسَبَة السَّحابيَّة بهذا الاسم لأنَّ المعلومات التي يتمّ الوصول إليها موجودة عن بُعْد في السَّحابة أو في الفضاء الافتراضيّ، حيث تُتيح الشَّركات التي تُقدِّم الخدمات السَّحابيَّة للمُسْتَخْدِمين تخزين المِلفَّات والتَّطبيقات على خوادم بعيدةٍ، ومن ثَمَّ الوصول إلى جميع البيانات عَبْر الإنترنت.

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency