CyberEco

معًا لدعم السلامة الرقمية

Together to support digital safety

ضَوابِط الأمن السّيبرانيّ للحَوْسَبَة السَّحابيَّة

محتوى تدريبيّ مُوَجَّه للمُعَلِّمين

حقيبة خاصَّة بالمُدرِّب

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency

ضَوابِط الأمن السّيبرانيّ للحَوْسَبَة السَّحابيَّة

محتوى تدريبيّ مُوَجَّه للمُعَلِّمين

المادَّة التَّدريبيَّة

(حَقيبَة خاصَّة بالمُدَرِّب)

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

المحتوى العام للحقيبة

أولاً: مدخل عام للحقيبة

ثانياً: المادة العلمية

أولًا: مَدْخل عامّ إلى الحَقيبَة التَّدْريبيَّة

فيمـا يلـي تبيـان لبعـض التَّفاصيـل ذات الصِّلَـة المُباشِـرَة بأهـداف الحَقيبَـة التَّدْريبيَّـة، مـع توجيهـات عامَّـة للمُـدَرِّب حـول كيفيَّـة التَّعامُـل مـع هـذه الحَقيبَـة، وتزويـده بالمحتـوى العِلْمـيّ الـذي سـيَعْتَمِد عليـه فـي التَّدريـب.

الفكرة العامَّة

تقـوم فِكْـرة هـذه الحَقيبَـة التَّدريبيَّـة علـى تزويـد المُـدَرِّب بـأدوات ووسـائل تدريبيَّـة؛ بحيـث يسـهل عليـه تقديـم المعلومـات للمُتَدَرِّبيـن. وتُعـدّ هـذه الحَقيبَـة مُوجِّهًـا عامًّـا للمُـدَرِّب وداعِمًـا لـه، إضافـةً لتزويـد المُـدَرِّب بـأدواتٍ ووسـائل تدريـب تَدْعَمـه فـي عمليَّـة التَّدريـب.

أهداف الحَقيبَة التَّدْريبيَّة

1. تَزويـد المُـدَرِّب بوسـائل تدريـب تُساعده علـى إيصـال المحتـوى التَّدريبـيّ للمُتَدَرِّبيـن.
2. تَقديم المعلومات والمحتوى التَّدريبيّ بشكلٍ سَهْل ومُبسَّط.
3. تَقْديم المحتوى التَّدريبيّ الخاصّ بالحَوْسَبَة السَّحابيَّة مُرفقًا بأدوات ووسائل تدريب مُتَعَدِّدَة.

محتوى الحَقيبَة التَّدْريبيَّة

تتضمَّن الحَقيبَة التَّدريبيَّة عدَّة أدوات تدريبيَّة، فيما يلي توضيح لها:

1. **ملفّ العَرْض.**
2. **فيديوهات تدريبيَّة.**
3. **بطاقات تدريبيَّة،** وهي على شَكْل معلومات عامَّة مُرفَقة بصُوَر تعبيريَّة، يَعْرضها المُدَرِّب على المُتَدَرِّبين.
4. **إسكتشات،** تتضمَّن معلومات حول المَحاوِر الرَّئيسة في المُحتَوى التَّدريبيّ.

فِهْرِس المحتوى العِلْميّ للحَقيبَة التَّدريبيَّة

مُقدِّمـة 15

الفَصْل الأوَّل

مفهـوم الحَوْسَبَة السَّحابيَّة..... **17**

- أهمِّيَّـة الحَوْسَبَة السَّحابيَّة..... 19
- أنـواع الحَوْسَبَة السَّحابيَّة..... 21
- تحدِّيـات الحَوْسَـبَة السَّـحابيَّة..... 29

الفَصْل الثَّاني

المَخاطِـر الرَّقميَّة التي تواجه الحَوْسَبَة السَّحابيَّة **31**

- فقـدان البيانـات..... 33
- البرمجيَّـات الضَّـارَّة..... 35
- الوصـول غير المصرَّح بـه..... 38

الفَصْل الثَّالث

كيفيَّة حماية الحَوْسَبَة السَّحابيَّة من الهجمات الرَّقميَّة..... **40**

- الأمـن السَّـحابيّ..... 41
- حمايـة البيانـات في الحَوْسَبَة السَّحابيَّة من القَرْصَنَـة 45

البطاقـات التدريبيـة..... **47**

المراجـع

الجَدْوَل الزَّمنيّ للوَرْشَة التَّدريبيَّة

المُحْتَوى	الوقت المُخصَّص
تَمْهيد	15 دقيقة
الجانب النَّظريّ من المادَّة	45 دقيقة
عَرْض الفيديوهات التَّدريبيَّة	25 دقيقة
اسْتِراحَة قَصيرَة	20 دقيقة
حِوَار ونِقَاش مع المُتَدرِّبين	15 دقيقة
المُدَّة الزَّمنيَّة للورشَة	ساعتان

دليل إرشادي للمُدَرِّب

فيما يلي تبيان لبعض الإرشادات العامَّة للمُدَرِّب، والتي تتمحور حول كيفيَّة اسْتِخدام هذه الحَقيبَة.

1. المحتوى العِلْمِيّ قد يتضمَّن مفاهيم خارج اختصاص المُتَدَرِّبين، لذلك لا بُدّ للمُدَرِّب من تقديم المعلومات بِشَكْلٍ مُبَسَّطٍ.
2. يعرض المُدَرِّب شرائح العَرْض عند كُلّ نقطةٍ يتحدَّث عنها، فمثلًا عند الحديث عن مفهوم الحَوْسَبَة السَّحابيَّة يَتمّ عَرْض الشَّريحة التي تَتَناوَل ذات المفهوم.
3. في أثناء عرض المادَّة العِلْمِيَّة لكلّ فَصْلٍ يَتمّ استقطاع فترةٍ من الوقت المُخصَّص له لعَرْض عددٍ من الرَّوابِط ذات الصِّلة بمضمون الفَصْل.
4. يعرض المُدرِّب الجزء الخاص بـ "إسكتشات"، في نهاية المُحاضَرة.
5. يُرجَى فَتْح باب المُناقَشَة مع المُتَدَرِّبين في المواضع التي يراها المُدَرِّب مُناسِبَة.

ثانيًا: المادَّة العِلْمِيَّة

مُقدِّمة

مع التَّطوُّر التِّكنولوجيّ الهائل بدأت تظهر العديد من المصطلحات ذات الصِّلة بهذا التَّطوُّر، ومن بين هذه المصطلحات "الحَوْسَبَة السَّحابيَّة" الذي أخذ في الانتشار بِشَكْلٍ واسعٍ في الفترة الأخيرة، سواءٌ بين المُتَخصِّصين بالمجال التِّقنيّ أو غيرهم من غير المُتَخصِّصين. فالحَوْسَبَة السَّحابيَّة أصبحت من التِّقنيَّات المُهمَّة التي تُستخدَم يوميًّا.

ويُقصَد بالحَوْسَبَة السَّحابيَّة المكان الذي يتمّ فيه تخزين البيانات والوصول إليها ومُعالَجَتها من خلال شبكة الإنترنت، فهي مكان يُسَمَّى بلغة الحاسوب "الخادم" Server، أي أنَّها تقنيَّة تُقدِّم خدمات مُخْتَلِفة بما في ذلك تخزين البيانات وتقديم موارد حاسوبيَّة مثل الخوادم وقواعد البيانات وبرامج حاسوبيَّة مُتَنَوِّعَة، وكذلك مُعالَجَة البيانات وتحليلها.

وهناك العديد من المُؤَسَّسات العَالَميَّة التي تُقدِّم خدمات الحَوْسَبَة السَّحابيَّة مثل "Sky Drive"، وهو من إحدى خدمات الحَوْسَبَة السَّحابيَّة المُقدَّمة من شركة "مايكروسوفت" التي تُقدِّم مجموعة مُتَنَوِّعَة من الحلول السَّحابيَّة من خلال الإنترنت، وهذه الخدمات تختصّ بخدمة التَّخزين السَّحابيّ على خوادم شركة "مايكروسوفت" بعد أن يقوم المُسْتَخْدِم بإنشاء حسابٍ خاصّ على نطاق الشَّركة، واليوم أصبح يُطلَق على تلك الخدمة اسم One Drive.

وليس ببعيدٍ عن خدمات "مايكروسوفت"، تُقدِّم شركة "جوجل" العَالَميَّة أيضًا خدمات الحَوْسَبَة السَّحابيَّة، ومن أشهرها خدمة التَّخزين السَّحابيّ بواسطة Google Drive Storage وبعضها مجَّانيّ وبعضها الآخر مدفوعة حيث تسمح للمُسْتَخْدِمين بتخزين مِلفَّاتهم المُخْتَلِفَة من أيّ جهازٍ وفي أيّ وقتٍ، لكن يجب أن تكون مُتَّصلة بشبكة الإنترنت لسهولة الوصول إلى المِلفَّات واسترجاعها والتَّعامُل معها.

الفَصْل الأَوَّل

مفهوم الحَوْسَبَة السَّحابيَّة

- أهمِّيَّة الحَوْسَبَة السَّحابيَّة.
- أنواع الحَوْسَبَة السَّحابيَّة.
- تحدِّيات الحَوْسَبَة السَّحابيَّة.

0 1

أهمِّيَّة الحَوْسَبَة السَّحابيَّة

يُشير مفهوم الحَوْسَبَة السَّحابيَّة إلى 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 محلّيّ)، يمكن الاعتماد على السَّحابة وتخزين المُستنَدات 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.

وتعود أهمِّيَّة الحَوْسَبَة السَّحابيَّة إلى عِدَّة أسبابٍ، في مُقدِّمتها؛ توفير التَّكاليف وزيادة الإنتاجيَّة، فضلًا عن السُّرعة والكفاءة والأمان. فالحَوْسَبَة السَّحابيَّة تُقدِّم خدمات مُخْتَلِفَة عَبْر الإنترنت، بما في ذلك تخزين البيانات والخوادم وقواعد البيانات والشَّبَكات والبرامج، وأصبح من الشَّائع استخدامها بِشَكْلٍ مُتَزايِدٍ بين الأفراد والشَّركات الذين يبحثون عن مساحة تخزينٍ أكبر لبياناتهم؛ فهي حَلّ فعَّال للنَّسْخ الاحتياطيّ للبيانات خارج المواقع[1].

ويُتيح التَّخزين المُسْتَنَد إلى السَّحابة إمكانيَّة حِفْظ المِلفَّات في قاعدة بياناتٍ بعيدةٍ واسترجاعها عند الطَّلَب، سواءٌ كانت تلك الخدمات عامَّة أو خاصَّة، حيث يتمّ تقديم الخدمات العامَّة عَبْر الإنترنت مُقابِل رسوم، بينما تتمّ استضافة الخدمات الخاصَّة على الشَّبَكة لعملاء مُحَدَّدين.

وفيما يتعلَّق بسبب تسمية الحَوْسَبَة السَّحابيَّة بهذا الاسم، فالسَّبب يعود 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 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 البقاء في مكانٍ مُحدَّدٍ للوصول إليها[2].

1. Frankenfield, Jake. What is Cloud Computing? Pros and Cons of Different Types of Services, investopedia, April 2023. On site: https://www.investopedia.com/terms/c/cloud-computing.asp
2. Weinberger, Matt. Why 'cloud computing' is called 'cloud computing', businessinsider, Mar 2015. On site: https://www.businessinsider.in/why-cloud-computing-is-called-cloud-computing/article-show/46544750.cmsshow/46544750.cms

فالحَوْسَبَة السَّحابيَّة تحمل كُلّ الأعباء الثَّقيلة المرتبطة بمُعالَجَة البيانات بعيدًا عن الجهاز الذي تحمله أو تجلس وتعمل عليه، كما أنَّه ينقل كُلّ هذا العمل إلى مجموعات حاسوب ضخمة بعيدة في الفضاء الإلكترونيّ، وبهذا يصبح الإنترنت بمثابة السَّحابة، أما بياناتك وعملك وتطبيقاتك مُتاحَة من أيّ جهازٍ يمكنك من خلاله الاتِّصال بالإنترنت في أيّ مكانٍ في العَالَم.

وإجمالًا تظهر أهمِّيَّة الحَوْسَبَة السَّحابيَّة من خلال النِّقاط الآتية:

1. توفير المال والتَّكاليف

على المدى الطويل، تُقدِّم خدمات الحَوْسَبَة السَّحابيَّة فرصة لتوفير المال وبالتَّالي إمكانيَّة استثماره في مجالاتٍ أخرى ذات صِلَة بالعمل، فأغلب خدمات الحَوْسَبَة يتمّ الدَّفع فيها مُقابِل الاستخدام، أي لا مجال لإهدار المال في خدمات لن تُسْتَخْدَم.

فمن خلال الحَوْسَبة السَّحابيَّة لن يكون المستخدم مُضطرًّا لشراء وسائط تخزين لتخزين البيانات عليها، ولا لتحمُّل تكاليف صيانتها، فكل ما عليه تخزين بياناته على السَّحابة.

2. بيئة مَوْثوقة وآمِنَة

تُعدّ الحَوْسَبَة السَّحابيَّة أكثر ضمانةً ومَوْثوقيَّةً من الأنظمة المحلِّيَّة، حيث يمتلك مُوَفِّرو الخدمات السَّحابيَّة فِرَقًا من الخبراء الذين يديرون البِنْية التَّحتيَّة ويحافظون على سَيْر الأمور بدقة، ما يجعل المُسْتَخْدِمين لتلك الخدمات يُركِّزون على عملهم، وهذا بالطَّبع يشمل حالات الطَّوارئ مثل انقطاعات التَّيَّار الكهربائيّ والكوارث الطَّبيعيَّة مثل الحرائق، فهذه الخوادم تحفظ البيانات الخاصَّة بالمُسْتَخْدِمين في أمانٍ.

3. التَّعاون

مع ما تُواجِهه بعض الشَّركات من صُعُوبةٍ في الوصول للبيانات على أنظمتها، ومن ثَمَّ خسارة الوقت والمال من جرَّاء ذلك، ظهرت الحاجة لمكان تخزين للبيانات بعيدًا عن الأنظمة الدَّاخليَّة، وهذا ما تُوفِّره شركات الحَوْسَبَة السَّحابيَّة التي تتضمَّن فرقًا من المُتَخصِّصين والتِّقنيِّين العاملين على توفير الأمن للبيانات على الخوادم، وبالتَّالي تَوفُّر التَّعاون بين الفِرَق بِشَكْلٍ سَلِسٍ يُوفِّر الوقت ويزيد من التَّعاون بين العاملين، سواءٌ داخل مبنى الشَّركة أو في أماكن مُخْتَلِفَةٍ من العَالَم.

4. القابليَّة للتَّطوير

تتميَّز السَّحابة بالمرونة والقابليَّة للتَّطوير بِشَكْلٍ كاملٍ وَفْق احتياجات العمل، فيمكن للمُسْتَخْدِمين توسيع نطاق الحِزْمة الخاصَّة بهم أو تخفيضها وَفْق مُتَطَلَّباتهم الشَّخصيَّة والعمليَّة[1].

1. Linao, Portia. Why is it called “The Cloud”? officesolutionsit, February 2023. On site: https://www.officesolutionsit.com.au/blog/why-is-it-called-the-cloud

أنواع الحَوْسَبَة السَّحابيَّة

تستخدم شركات الخدمات السَّحابيَّة تقنيَّات الأمان المُتَقدِّمة والتي تشمل التَّشفير وجُدْران الحماية وقيود الوصول؛ لتأمين البيانات من الوصول غير المُصَرَّح به. فعليها تحفظ المعلومات حتَّى لو كانت أجهزتك القريبة تَضرَّرت أو سُرِقت؛ وبِشَكْلٍ عامّ توجد عِدَّة أنواع من الحَوْسَبَة السَّحابيَّة؛ **فيما يلي تبيان لأهمّها:**

1. السَّحابة العامَّة:

هي مفتوحة ومُتاحة للجميع لتخزين المعلومات والوصول إليها عَبْر الإنترنت باستخدام طريقة الدَّفع لكُلّ استخدام، وتتمّ إدارة موارد الحَوْسَبَة وتشغيلها من قِبَل مُزَوِّد الخدمة السَّحابيَّة الذي يعتني بالبِنْية التَّحتيَّة الدَّاعِمَة، ويضمن أن تكون الموارد مُتاحة وقابِلَة للتَّطوير للمُسْتَخْدِمين؛ ويجوز لأيّ شخصٍ لديه اتِّصال بالإنترنت أن يستخدم السَّحابة العامَّة بغضّ النَّظر عن الموقع أو حجم الشَّركة، وذلك لتخزين بياناته وتشغيل التَّطبيقات، ومن أمثلتها:- IBM SmartCloud En terprise و Microsoft و Google App Engine و Windows Azure Services Platform. و Amazon Elastic Compute Cloud (EC2)

وتتميَّز الحَوْسَبَة السَّحابيَّة العامَّة بعددٍ من الخصائص هي:

1. **سُهُولة الوصول:** فهي مُتاحَة لأيّ شخصٍ لديه اتِّصال بالإنترنت، حيث يمكن للمُسْتَخْدِمين الوصول إلى بياناتهم وبرامجهم في أيّ وقتٍ ومن أيّ مكانٍ.
2. **البِنْية التَّحتيَّة المُشْتَرَكَة:** يشارك العديد من المُسْتَخْدِمين البِنْية التَّحتيَّة في إعدادات السَّحابة العامَّة، ممَّا يساعد في خَفْض التَّكاليف.
3. **قابليَّة التَّوسُّع:** يمكن للمُسْتَخْدِمين بسهولةٍ ضَبْط الموارد التي يحتاجونها بناءً على مُتَطَلَّباتهم، ممَّا يسمح بتوسيع النِّطاق أو تحجيمه كما يرغبون.
4. **الدَّفع لكُلّ استخدام:** يعتمد الدَّفع على الاستخدام فقط في السَّحابة العامَّة، أي مُقابِل الموارد التي يستعملها المُسْتَخْدِم بالفعل، ممَّا يُقلِّل من التَّكاليف.
5. **سُهُولة الصِّيانة والإدارة:** لأنَّ الحَوْسَبَة السَّحابيَّة العامَّة تتمّ إدارتها بواسطة مُقدِّمي الخدمة، فهم مسؤولون عن إدارة وصيانة البِنْية التَّحتيَّة لها ويتعاملون مع صيانة الأجهزة وتحديثات البرامج والمَهامّ الأمنيَّة بِشَكْلٍ أفضل وبعيدًا عن المُسْتَخْدِمين[1].

1. Stephen J. Bigelow. What is public cloud? Everything you need to know, techtarget. On site: https://www.techtarget.com/searchcloudcomputing/definition/public-cloud

عُيُوب الحَوْسَبَة السَّحابيَّة العامَّة:

- تُعدّ السَّحابة العامَّة أقلّ أمانًا من وسائط التَّخزين الأخرى، وذلك لأنَّ البيانات والمعلومات المُخَزَّنة تتمّ مُشارَكَتها بِشَكْلٍ عامّ.
- ترتبط فاعليَّة الحَوْسَبَة السَّحابيَّة العامَّة بجَوْدة خدمة الإنترنت وسُرْعته، فأيّ خَلَلٍ أو ضَعْفٍ في شبكات الإنترنت ينعكس بِشَكْلٍ مُباشِرٍ على أداء الحَوْسَبَة السَّحابيَّة العامَّة وعلى إمكانيَّة الوصول للبيانات المُخَزَّنة عليها.
- يمتلك المُسْتَخْدِم سيطرة محدودة نِسْبيًّا على البيانات المُخَزَّنة في الحَوْسَبَة السَّحابيَّة العامَّة.
- المخاوف بشَأْن خصوصيَّة البيانات وسرِّيَّتها.
- احتمال تكليف المُسْتَخْدِم بتكاليف إضافيَّةٍ غير مُتَوَقَّعةٍ في حال تعديل شروط الاستخدام.
- الافتقار إلى خيارات التَّخصيص والمرونة مُقارَنَةً بالبيئات السَّحابيَّة الخاصَّة أو الهجينة[1].

1. Types of Cloud, javatpoint. On site: https://www.javatpoint.com/types-of-cloud

2. الحَوْسَبَة السَّحابيَّة الخاصَّة

يُطلَق على الحَوْسَبَة السَّحابيَّة الخاصَّة مُسَمَّيات مثل السَّحابة الدَّاخليَّة أو سحابة الشَّركات، حيث يتمّ استخدامها من قِبَل المُؤَسَّسات لبناء وإدارة مراكز البيانات الخاصَّة بها داخليًّا أو بواسطة جهةٍ خارجيَّةٍ، **ومن أمثلتها:**

VMware vSphere, OpenStack, Microsoft Azure Stack, Oracle Cloud at Customer, and IBM Cloud Private

وتنقسم الحَوْسَبَة السَّحابيَّة الخاصَّة إلى نوعَيْن هما:

الحَوْسَبَة السَّحابيَّة الخاصَّة داخل المُؤسَّسة: حيث توجد السَّحابة الخاصَّة ضِمْن البِنْية التَّحتيَّة الماديَّة للمُؤسَّسة، وتشتمل على إنشاء وتشغيل مركز بيانات مُحَدَّد يُقدِّم خدمات سحابيَّة للاستخدام الدَّاخليّ فقط من قِبَل الشَّركة، أي أنَّ البِنْية التَّحتيَّة بالكامل تكون في أيدي المُؤسَّسة، مما يمنح القائمين عليها حُرِّيَّة التَّعديل وإعدادها بأيّ طريقةٍ يرونها مُناسِبَة. فيمكن للمُؤسَّسة هنا إدارة مشكلات الأمان.

لكن الوجه الآخر لهذا النَّوْع من السَّحابة الخاصَّة يكمن في تَطلُّبها نفقات كبيرة على الأجهزة والبرامج ومعرفة بتكنولوجيا المعلومات.

الحَوْسَبَة السَّحابيَّة الخاصَّة التي يتمّ الاستعانة بمصادر خارجيَّة: ويُقصَد بها هنا الاستعانة بمصادر خارجيَّة مثل الشَّراكة مع مُزَوِّد خدمةٍ خارجيّ لاستضافة البِنْية التَّحتيَّة السَّحابيَّة وإدارتها نيابةً عن المُؤسَّسة.

ويجوز لموفِّر الخدمة تشغيل السَّحابة الخاصَّة في مركز البيانات الخاصّ به أو في مُنْشأة مُشْتَرَكة، وبهذا تستفيد المُؤسَّسة من خِبْرات وموارد مُزَوِّد الخدمة، ممَّا يُخفِّف عِبْء إدارة البِنْية التَّحتيَّة، ويمكن لمُوَفِّر الخدمة الخارجيَّة ضَبْط الموارد بناءً على احتياجات المُؤسَّسة.

ويُعدّ هذا النَّموذج مرغوبًا فيه للمُؤسَّسات التي ترغب في الحصول على مزايا نَشْر السَّحابة الخاصَّة دون إنفاق المال على الصِّيانة والبرامج والأجهزة[1].

وللحَوْسَبَة السَّحابيَّة الخاصَّة العديد من المزايا:

1. تمنح المُؤسَّسات مزيدًا من التَّحكُّم في بياناتها وتطبيقاتها وأَمْنها.
2. تُعدّ مُناسِبَة بِشَكْلٍ خاصّ للمُؤسَّسات التي لديها مُتَطَلَّبات امتثالٍ صارمةٍ، أو بيانات حسَّاسة، أو أعباء عملٍ مُتَخصِّصة تَتَطلَّب مستويات عالية من التَّخصيص والأمان.
3. الاستخدام الحَضْريّ، حيث تُخَصَّص الحَوْسَبَة السَّحابيَّة الخاصَّة لمُؤسَّسةٍ واحدةٍ، ممَّا يضمن أنَّ الموارد والخدمات مُصمَّمة خصِّيصًا لتلبية احتياجاتها.
4. تُوفِّر تَحكُّمًا وأمانًا أعلى من خيارات السَّحابة العامَّة للمُؤسَّسات.

1. What is private cloud? Types, process, benefits, examples, knowledgehut. On site: https://2u.pw/vtxJ57Q

5. تتيح السَّحابة الخاصَّة للمُؤسَّسات بتخصيص البِنْية التَّحتيَّة وَفْقًا لمُتَطَلَّباتها المُحَدَّدة.
6. القابليَّة للتَّوسُّع وتخصيص الموارد، حيث تُتيح السَّحابة الخاصَّة للمُؤسَّسات توسيع نطاق الموارد وتخصيصها وَفْقًا للطَّلَب.
7. تمنح السَّحابات الخاصَّة المُؤسَّسات المزيد من التَّحكُّم في البِنْية التَّحتيَّة لها، ممَّا يُحسِّن الأداء والاعتماديَّة.
8. يمكن للمُؤسَّسات أن تفي ببعض معايير الامتثال والتَّنظيم بسهولةٍ أكبر باستخدام السَّحابة الخاصَّة، فهي تُوفِّر الحُرِّيَّة في وَضْع تدابير أمنيَّةٍ قويَّةٍ، واتِّباع قوانين إقامة البيانات، واتِّباع المعايير الخاصَّة بالصِّناعة.
9. يمكن دَمْج السَّحابة الخاصَّة مع الخدمات السَّحابيَّة العامَّة، ممَّا يُشكِّل بِنْية تحتيَّة سحابيَّة هجينة، ما يعني الاستفادة من فوائد السَّحابة الخاصَّة والعامَّة معًا[1].

عُيُوب الحَوْسَبَة السَّحابيَّة الخاصَّة

1. تتطلَّب كفاءات عالية لإدارة وتشغيل الخدمات السَّحابيَّة.
2. يمكن الوصول إلى السَّحابة الخاصَّة داخل المُؤسَّسة، وبالتَّالي فإنَّ مَنْطِقَة العمليَّات محدودة.
3. ليست مُناسِبَة للمُؤسَّسات التي لديها عددٌ كبيرٌ من المُوظَّفين، والذين يحتاجون جميعًا لخدمات السَّحابة، فهي لا تستطيع تقديم خدمات التَّخزين لأعدادٍ كبيرةٍ من المُستخدِمين، كما ليست مُناسِبَة للمُؤسَّسات التي ليس لديها بِنْية تحتيَّة مُعدَّة مُسبقًا وقُوى عاملة كافية لصيانة السَّحابة وإدارتها.
4. ارتفاع التَّكاليف الأَوَّليَّة ونفقات الصِّيانة المُستمرَّة.
5. قد يكون توسيع نطاق الموارد أمرًا صعبًا مُقارَنَةً بخيارات السَّحابة العامَّة أو المُخْتَلِطَة.
6. يعتمد على مُوظَّفي تكنولوجيا المعلومات الدَّاخليِّين للإدارة واستكشاف الأخطاء وإصلاحها.
7. جداول زمنيَّة بطيئة للنَّشر والتَّنفيذ مُقارَنَةً بحلول السَّحابة العامَّة[2].
8. وصول محدود إلى أحدث التَّطوُّرات والابتكارات التي يُقدِّمها مُوَفِّرو الخدمات السَّحابيَّة العامَّة.
9. انخفاض المرونة وبطء المعالجة مُقارَنَةً بخيارات السَّحابة العامَّة.
10. التَّحدِّيات في مُواكَبَة ترقيات الأجهزة والبرامج والتَّوافق.
11. الحاجة إلى تحديثاتٍ مُنْتَظِمَةٍ للبِنْية التَّحتيَّة[3].

1. What is private cloud? ovhcloud. On site: https://www.ovhcloud.com/en-gb/learn/what-is-private-cloud/
2. Public and Private Cloud Advantages and Disadvantages, connectria. On site: https://cutt.us/cMN8I
3. 6 Advantages and Disadvantages of Private Cloud | Limitations & Benefits of Private Cloud, hitechwhizz. On site: https://cutt.us/CpICr

3. السَّحابة الهجينة

هي مزيج من الحَوْسَبَة السَّحابيَّة العامَّة والحَوْسَبَة السَّحابيَّة الخاصَّة، وتُعدّ آمنة نِسْبيًّا لأنَّ الخدمات التي يتمّ تشغيلها على السَّحابة العامَّة يمكن لأيّ شخصٍ الوصول إليها، بينما لا يمكن الوصول إلى الخدمات التي يتمّ تشغيلها على السَّحابة الخاصَّة إلا بواسطة مُسْتَخْدِمي المُؤسَّسة.

في هذا النَّوْع من السَّحابات يمكن للمُؤسَّسات الاستفادة من فوائد السَّحابة العامَّة والخاصَّة لإنشاء بيئة حَوْسَبَة مَرِنَة وقابلة للتَّطوير. ويسمح الجزء السَّحابيّ العامّ باستخدام الخدمات السَّحابيَّة التي يُقدِّمها مُوَفِّرو الطَّرف الثَّالث، والتي يمكن الوصول إليها عَبْر الإنترنت، **من أمثلتها:**

Google Application Suite (Gmail و Google Apps و Google Drive)، و Office 365 (MS Office One Drive، وAmazon Web Services.

مُمَيِّزات السَّحابة الهجينة:

تتميَّز السَّحابة الهجينة بعِدَّة خصائص، **فيما يلي تبيان لأهمّها:**

- تعمل السَّحابة الهجينة على دَمْج السَّحابة العامَّة والخاصَّة؛ ممَّا يسمح بالاستفادة من خصائص السَّحابتَيْن معًا.
- الحَوْسَبَة السَّحابيَّة الهجينة تُوفِّر مرونة في تخصيص الموارد وقابليَّة التَّوسُّع، من خلال استخدام موارد إضافيَّة من السَّحابة العامَّة، مع الحفاظ على التَّحكُّم في أعباء العمل المُهمَّة على السَّحابة الخاصَّة.
- تعمل على تعزيز الأمان والتَّحكُّم، فهي تُوفِّر بيئة آمنة ومُخصَّصة، بينما يمكن استخدام موارد السَّحابة العامَّة للمَهامّ غير الحسَّاسة.
- تحسين التَّكاليف من خلال استخدام السَّحابة العامَّة من حيث التَّكلِفَة للأعمال غير المُهمَّة مع الاحتفاظ بالتَّطبيقات والبيانات ذات المَهامّ الحَرِجَة على السَّحابة الخاصَّة الأكثر فعاليَّة من حيث التَّكلِفَة.
- إمكانيَّة نَقْل البيانات والتَّطبيقات بين السَّحابتَيْن العامَّة والخاصَّة حسب الحاجة.
- تساعد السَّحابة الهجينة على مُعالَجَة مُتَطَلَّبات الامتثال والمُتَطَلَّبات التَّنظيميَّة بِشَكْلٍ أكثر فعاليَّة، بحيث يمكن الاحتفاظ بالبيانات والتَّطبيقات الحسَّاسة داخل السَّحابة الخاصَّة، مع الاستفادة من السَّحابة العامَّة في العمليَّات الأخرى غير الحسَّاسة.
- تُسهِّل السَّحابة المُخْتَلِطَة مَهمَّة التَّعافي من الكوارث واستمراريَّة الأعمال، من خلال نَسْخ البيانات والتَّطبيقات المُهمَّة بين السَّحابة الخاصَّة والعامَّة، ممَّا يضمن التِّكرار ويُقلِّل من مخاطر فقدان البيانات أو انقطاع الخدمة[1].

1. What is hybrid cloud? netapp. On site: https://cutt.us/8N9QZ

عُيُوب السَّحابة الهجينة:

- مَيْزة الأمان ليست بنفس جودة السَّحابة الخاصَّة.
- تُعدّ إدارة السَّحابة المُختلطَة أمرًا مُعقَّدًا لأنَّه من الصَّعب إدارة أكثر من نوعٍ واحدٍ من نماذج النَّشر.
- تعتمد مَوْثوقيَّة الخدمات على مُقدِّمي الخدمات السَّحابيَّة.
- تزايد التَّحدِّيات المُحْتَمَلَة في تكامل البيانات وضمان الاتِّصال بين الأنظمة الأساسيَّة السَّحابيَّة المُخْتَلِفَة.
- ارتفاع التَّكاليف بسبب الحاجة إلى إدارة وتكامل البيئات السَّحابيَّة المُتَعدِّدة.
- زيادة التَّعقيد في إدارة البيانات عَبْر مُوَفِّري الخدمات السَّحابيَّة المُخْتَلِفَيْن.
- الاعتماد على اتِّصالات الإنترنت المُسْتَقِرَّة وذات النِّطاق التَّرَدُّديّ العالي لإجراء عمليَّات سحابيَّة هجينة فعَّالة.
- تَتَطلَّب مُوظَّفين ماهرين في مجال تكنولوجيا المعلومات من ذَوِي الخبرة في إدارة السَّحابة المُخْتَلِطَة.

4. سحابة المُجْتَمَع

تسمح سحابة المُجْتَمَع بالوصول إلى الأنظمة والخدمات من قِبَل مجموعةٍ من عِدَّة مُؤسَّسات لمُشارَكَة المعلومات بين المُؤسَّسة ومُجْتَمَعٍ مُعيَّنٍ. وهي مملوكة ومُدارة من قِبَل واحدة أو أكثر من المُؤسَّسات في المُجْتَمَع، أو طرفٍ ثالثٍ، أو مجموعةٍ منهم[1].

في إعداد السَّحابة المُجْتَمَعيَّة، تتعاون المُؤسَّسات المُشارِكَة، والتي يمكن أن تكون من نفس الصِّناعة أو القطاع الحكوميّ أو أيّ مُجْتَمَعٍ آخر، لإنشاء بِنْية أساسيَّة سحابيَّة مُشْتَرَكَة، بما يُتيح لهم الوصول إلى الخدمات والتَّطبيقات والبيانات المُشْتَرَكَة ذات الصِّلة بمُجْتَمَعهم. مثال: سحابة مُجْتَمَع الرِّعاية الصِّحِّيَّة.

خصائص سحابة المُجْتَمَع

1. تُوفِّر سحابة المُجْتَمَع بِنْية أساسيَّة مُشْتَرَكَة يمكن الوصول إليها من قِبَل مُجْتَمَعٍ مُحدَّدٍ من المُؤسَّسات.
2. تُوفِّر سحابة المُجْتَمَع الموارد والتَّطبيقات والخدمات التي تتكيَّف مع مُتَطَلَّبات المُؤسَّسات المُشارِكَة، ويتمّ إنشاء هذه الخدمات لتلبية المُتَطَلَّبات مع تعزيز التَّواصُل الفعَّال وتبادل المعلومات.
3. تمتلك سحابة المُجْتَمَع وتديرها مُؤسَّسة واحدة أو أكثر من المُجْتَمَع، أو جهة خارجيَّة، أو مزيج من الاثنين معًا، وتَتَمتَّع المُؤسَّسات المُشارِكَة بدَوْر في إجراءات الحَوْكَمَة واتِّخاذ القرار لضمان تلبية البِنْية التَّحتيَّة السَّحابيَّة لأهدافها المُشْتَرَكَة.
4. تتمسَّك سحابة المُجْتَمَع بإجراءات الأمان والامتثال ذات الصِّلة بمُجْتَمِعٍ مُعيَّنٍ، أي تسمح بتنفيذ ضوابط أمنيَّة قويَّة وإدارة الوصول وأُطُر الامتثال التي تُلبِّي المُتَطَلَّبات التَّنظيميَّة للمُجْتَمَع ومعايير الصِّناعة.
5. تستفيد المُؤسَّسات المُشارِكَة في السَّحابة المُجْتَمَعيَّة من تقاسم التَّكاليف.
6. تُشجِّع سحابة المُجْتَمَع التَّواصل وتبادل المعلومات بين المُشارِكين.
7. تُتيح السَّحابة المُجْتَمَعيَّة للمُؤسَّسات إمكانيَّة توسيع نطاق مواردها أو تقليلها استجابةً للطَّلَب[2].

1. Mohanakrishnan, Ramya. What Is Community Cloud? Definition, Architecture, Examples, and Best Practices, spiceworks. On site: https://cutt.us/ORUiy
2. Tucakov, Dejan. What is Community Cloud? Benefits & Examples with Use Cases, JUNE 18, 2020. On site: https://cutt.us/ghrCz

عُيُوب سحابة المُجْتَمَع:

1. ميزات الأمان ليست جيِّدة مثل السَّحابة الخاصَّة.
2. ليست مُناسِبَة إذا لم يكن هناك تعاون بين المُشارِكِين فيها.
3. التَّحدِّيات في ضمان الأداء المُتَّسق والتَّوافر عندما تتشارك عِدَّة مُؤسَّسات في نفس الموارد.
4. خيارات قابليَّة التَّوسُّع محدودة حيث تُحدِّد الموارد المُشْتَرَكَة سَعَة سحابة المُجْتَمَع.
5. تَضارُب المصالح المُحْتَمَل بين أفراد المُجْتَمَع فيما يتعلَّق بتخصيص الموارد واستخدامها.
6. إنَّ أُطُر الحَوْكَمَة والاتِّفاقيَّات الشَّفَّافة مطلوبة لمُعالَجَة النِّزاعات المُحْتَمَلَة وضمان التَّوزيع العادل للموارد.
7. عدم كفاية الدَّعم الفنِّيّ واتِّفاقيَّات مستوى الخدمة مُقارَنَةً بخيارات السَّحابة الخاصَّة أو العامَّة.

تحدِّيات الحَوْسَبَة السَّحابيَّة

على الرَّغم من أهمِّيَّة الحَوْسَبَة السَّحابيَّة في التَّعاون وتخزين البيانات، إلَّا أنَّها تواجه عِدَّة تحدِّيات، **وفيما يلي تبيان لأبرز هذه التَّحدِّيات:**

- الأمان: فمُنْذ ظهور الإنترنت، كان أمن البيانات دائمًا مصدر قَلَقٍ، وأكثر من ذلك بكثير الآن بعد أن انتقلت المزيد من الشَّركات إلى السَّحابة. وسواءٌ كنت تستخدمها لأسبابٍ شخصيَّةٍ أو مِهَنيَّةٍ يجب أن تظل السَّحابة آمِنَة، عَبْر التَّأكُّد من مُزوِّد الخدمة السَّحابيَّة الخاصّ بك وأنَّه يتمتَّع بسُمْعةٍ طيِّبةٍ في تنفيذ إجراءاتٍ صارمةٍ لأمن البيانات مثل المُصادَقَة مُتَعدِّدة العوامل، وتشفير البيانات، والتَّحكُّم في الوصول، وما إلى ذلك.

فتخزين البيانات في السَّحابة، يجعلها أكثر عرضة للقَرْصَنَة والجرائم الإلكترونيَّة، وإذا لم تكن مُسْتَعدًا، فأنت عُرْضَة للمخاطر السّيبرانيَّة مثل التَّصيُّد الاحتياليّ وبرمجيَّات الفِدْية وسَرِقة الهُوِيَّة، والإصابة بالبرمجيَّات الضَّارَّة والتي قد تؤدي إلى تلف البيانات المخزّنة على السَّحابة.

فمثلًا إذا كانت المُؤسَّسة تعتمد عليها في حِفْظ بياناتها، يجب التَّأكُّد من عدم الوصول إليها إلَّا من قِبَل الأفراد المُصَرَّح لهم بذلك، كما يجب القيام بتشفير البيانات والتَّأكُّد من أنَّ مُزوِّد السَّحابة الخاصّ لديه إجراءات أمنيَّة كافية.

- تحدِّي الأداء: كأنْ يكون أداء مِنَصَّة الخدمة السَّحابيَّة لا يرقى إلى مستوى متطلبات المستخدم؛ وهذا قد يعني عدم رضا العملاء عن أداء المُؤسَّسة، وبالتَّالي انخفاض أرباحها، فالتَّأخير البسيط في تطبيق السَّحابة قد يسبب ضررًا للمستخدمين، كما يجب التَّأكُّد أنَّ السَّحابة غير مُعرَّضة لخطر التَّوقف عن العمل، فهذا يُؤدِّي في النِّهاية إلى تعطيل العمليَّات التي تعتمد على ما تمَّ تخزينه عليها.
- ضرورة وَضْع خُطَّة احتياطيَّة في حالة انقطاع التَّيَّار الكهربائيّ أو مُواجَهَة الكوارث الطَّبيعيَّة.
- ضرورة الحَذَر من تراكُم المِنَصَّة السَّحابيَّة دون قصدٍ؛ على سبيل المثال، إذا لم تكن موارد السَّحابة مُنَظَّمَة ومُحَسَّنَة، فمن المُمْكِن أن تتراكم مساحة تخزين المِلفَّات في وقتٍ قصيرٍ، وينتهي الأمر إلى دَفْع ثمن حِزْمةٍ ذات مساحة تخزينٍ أكبر لن يحتاج إليها المستخدم[1].

1. وَاقِع استخدام تطبيقات الحَوْسَبَة السَّحابيَّة في تفعيل التَّعليم المحاسبيّ، دراسة استطلاعيَّة لآراء أساتذة قِسْم العلوم الماليَّة والمَحاسَبَة بجامعة 20 أوت 1955 سكيكدة، الجزائر، مِجلَّة دفاتر بوادكس، المُجلَّد 11، العدد: 02، 2022م.

الفَصْل الثَّاني

المَخاطِر الرَّقميَّة التي تُواجِه الحَوْسَبَة السَّحابيَّة

- فقدان البيانات.
- البرمجيَّات الضَّارَّة.
- الوصول غير المصرَّح به.

02

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 حذف البيانات وإتلافها وجعلها غير قابلة للقراءة بواسطة مُسْتَخْدِم أو برنامج أو تطبيق. وفي بيئة الحَوْسَبَة السَّحابيَّة، يحدث فقدان البيانات عندما تكون البيانات الحسَّاسة والمُهمَّة في أيدي شخصٍ آخر، ولا يمكن لمالك البيانات استخدام عُنْصرٍ واحدٍ أو أكثر من عناصر البيانات، ولا يعمل القرص الصّلب بِشَكْلٍ صحيحٍ، ولا يتمّ تحديث البرنامج[1].

ولمُواجَهَة تحدّي فقدان البيانات، ينبغي استخدام أدوات التَّشفير كُلَّما أمكن ذلك. ويجب أن تكون ضوابط الوصول إلى السَّحابة موجودة للحَدّ من وصول المُسْتَخْدِمين غير المُصَرَّح لهم إلى المعلومات الحسَّاسة داخل البيئة السَّحابيَّة. كما يجب على أصحاب الأعمال أيضًا تدقيق مُقدِّمي الخدمات السَّحابيَّة بانتظام للتَّأكُّد من أنَّهم يتَّبعون أفضل المُمارَسات في مجال الأمان السَّحابيّ. فهذه الخُطُوات تساعد في تقليل المَخاطِر عندما يتعلَّق الأمر بفقدان البيانات من بيئات الحَوْسَبَة السَّحابيَّة.

وبِشَكْلٍ عامّ يعود فقدان البيانات لِعِدَّة أسبابٍ، **فيما يلي تبيان لأهمّها:**

1. الحَذْف العَرَضيّ (خطأ المُسْتَخْدِم)

يُعدّ الحَذْف غير المقصود هو المصدر الأكثر شيوعًا لفقدان البيانات عند استخدام التَّخزين السَّحابيّ، لكنَّ عمليَّات النَّسْخ الاحتياطيّ التِّلقائيّ المُضَمَّنة في حلول الحَوْسَبَة السَّحابيَّة يمكنها استعادة المِلفَّات المحذوفة أو استعادة إصدارٍ قديمٍ من مُسْتَنَد أو قاعدة بيانات.

2. الكتابة فوق البيانات

من المُمْكِن أيضًا أن يتمّ استبدال المعلومات عن طريق الخطأ بواسطة المُسْتَخْدِمين أو التَّطبيقات، وتُعدّ تطبيقات البرامج كخدمة (SaaS) مصدرًا مُحْتَمَلًا لفقدان البيانات بِشَكْلٍ كبيرٍ إذ تحتفظ هذه التَّطبيقات بمجموعاتٍ كبيرةٍ من البيانات وتقوم بتحديثها باستمرارٍ. فالمعلومات الجديدة لديها القُدْرة على الكتابة فوق المعلومات القديمة؛ ممَّا يتسبَّب في فقدان البيانات.

1. What are the Security Risks of Cloud Computing? Auditboard, on site: https://cutt.us/qJsln

3. البرمجيَّات الضَّارَّة

يواصل مُوَفِّرو خدمات التَّخزين السَّحابيّ بَذْل الجهود لتأمين شبكاتهم والبيانات المخزَّنة عليها، لمَنْع جميع الهجمات الإلكترونيَّة. ولحُسْن الحظّ، تتوفَّر أفضل المُمارَسات وأُطُر العمل التي تمَّ اختبارها جيِّدًا لمساعدة أقسام تكنولوجيا المعلومات على إدارة التَّحكُّم في الوصول إلى البيانات المُسْتَضَافة في السَّحابة بِشَكْلٍ أكثر أمانًا.

كيفيَّة حماية البيانات المُخَزَّنة على السَّحابة من الفقدان

1. تخصيص الوقت والموارد اللَّازمة لتطوير إستراتيجيَّة النَّسْخ الاحتياطيّ والتَّعافي من الكوارث، عَبْر إجراء نَسْخ احتياطيّ للبيانات الأكثر أهمِّيَّة وَفْقًا لجَدْوَلٍ زمنيّ يتماشى مع أهداف العمل ويمكن استردادها في الوقت المُناسِب.
2. إيجاد حَلّ نَسْخ احتياطيّ يناسب احتياجات وأولويَّات العمل، حيث لا يتمّ إنشاء جميع الحلول على قدم المساواة.
3. الحصول على نُسَخ مُتَعدِّدة متاحة لاستعادة البيانات.
4. ضَعْ في اعتبارك كيفيَّة حِفْظ النُّسَخ الاحتياطيَّة الخاصَّة بك بنجاحٍ في مراكز بيانات مُخْتَلِفَة، بحيث إذا ظهرت مشكلة في إحدى النُّسَخ الاحتياطيَّة، يكون من المُمْكِن استرداد المعلومات من موقعٍ مُخْتَلِفٍ.
5. فَهْم أهمِّيَّة تخزين البيانات بطريقةٍ لا يمكن التَّلاعب بها أو تشفيرها بواسطة برمجيَّات الفِدْية[1].

1. Brandt, Charles. What Are the Chances of Losing Information in Cloud Storage? Marconet, August, 2023. On site: https://cutt.us/FFJGN

البرمجيَّات الضَّارَّة

هناك عِدَّة أنواع من الهجمات الأكثر شيوعًا للبرمجيَّات الضَّارَّة في السَّحابة، حيث يستغلّ المُهاجِمون الإلكترونيُّون بقاء البيانات المُهمَّة على المِنصَّات السَّحابيَّة ويحاولون اختراقها لسَرِقة تلك البيانات وابتزاز المُسْتَخْدِمين فيما بعد .

البرمجيَّات الضَّارَّة السَّحابيَّة هي برمجيَّات تمَّ إنشاؤها وتوزيعها من خلال بيئات الحَوْسَبَة السَّحابيَّة، لسَرِقة البيانات من المُسْتَخْدِمين والمُؤسَّسات وتعطيل عمليَّاتها والتَّسبُّب في الكثير من المشكلات. ونظرًا للطَّبيعة المُترابِطَة للسَّحابة، فإنَّ تأثير هجوم البرمجيَّات الخبيثة النَّاجح على السَّحابة يمكن أن يكون كارثيًّا.

وفيما يلي الأنواع الأكثر ضررًا من هجمات البرمجيَّات الضَّارَّة في السَّحابة والتي يتأثَّر بها المُسْتَخْدِمون عادةً الذين يعملون في أيّ نوعٍ من البيئات السَّحابيَّة:

1. هجمات الحَقْن

هو هجومٌ سيبرانيّ يستخدمه مُجْرِمُو الإنترنت لإحداث الفَوْضَى في الخوادم الطَّرفيَّة غير المحميَّة من خلال التَّسلُّل عَبْر نقاط الوصول غير المُصحّحة، لسرقة البيانات والهُوِيَّات وكذلك نَشْر برمجيَّات الفِدْية أو حتى الاستفادة من المعلومات المسروقة. ويمكن للمُهاجِم تعطيل ما يصل إلى 100 نظامٍ في وقت واحد بضربةٍ واحدةٍ.

وأفضل دفاع ضِدّ هذا النَّوْع من هجمات البرمجيَّات الضَّارَّة السَّحابيَّة هو توظيف برامج مُخَصَّصة يمكنها استخدام القوَّة الحاليَّة للبِنْية التَّحتيَّة السَّحابيَّة للتَّحكُّم جيِّدًا في الوصول ومُراقَبَة حركة المرور المُستمرَّة باستخدام أدوات أمان السَّحابة سريعة المفعول.

2. عمليَّات التَّصيُّد الاحتياليّ

يتضمَّن هذا النَّوْع من الهجمات إرسال رسائل بريد إلكترونيَّة أو رسائل نصِّيَّة تبدو كأنَّها من مصادر معروفة لكنَّها مُحاوَلَة لسرقة بيانات سرِّيَّة أو تثبيت تعليمات برمجيَّة ضارَّة على الجهاز.

وللحماية من التَّصيُّد الاحتياليّ، يجب التَّأكُّد من صحَّة الرَّوابط قبل النَّقر عليها، وتجنُّب فَتْح مُرْفَقات أو رسائل غير معروفة، واستخدام المُصادَقَة الثُّنائيَّة.

3. سَرِقة البيانات

هي شكل شائع من هجمات البرمجيَّات الضَّارَّة السَّحابيَّة. فعلى سبيل المثال، في عام 2013 تعرَّض 110 ملايين مُسْتَخْدِم من حاملي بطاقات الائتمان الذين أجروا عمليَّات شراء في متاجر Target لسَرِقة معلوماتهم الشَّخصيَّة من قِبَل مُجْرِمي الإنترنت. والسَّبب هو وجود بائعٍ خارجيّ أنظمته ضعيفة؛ ممَّا مكَّن المُهاجِمون من الوصول إلى تلك البطاقات، وهي شركة Fazio Mechanical Services المُتَخصِّصة في خدمات التَّبريد.

4. أَحْصِنة طروادة

هو نوع من البرمجيَّات الضَّارَّة السَّحابيَّة التي تتنكَّر كبرنامجٍ شرعيّ من أجل الوصول إلى النِّظام أو سرقة البيانات. لذا يجب تجنُّب تنزيل أيّ برنامجٍ من مواقع الويب غير المَوْثوق بها، وعدم فَتْح مُرْفَقات البريد الإلكترونيّ المشكوك فيها.

5. مُهاجَمَة الوظائف وواجهات برمجة التَّطبيقات بدون خادم

غالبًا ما يتمّ استهداف الوظائف وواجهات برمجة التَّطبيقات بدون خادمٍ من قِبَل المُهاجِمين المُتَقدِّمين الذين يرغبون في الوصول إلى البيئة السَّحابيَّة للمُؤسَّسة. يتمّ تنفيذ هذا الهجوم عن طريق استغلال نقاط الضَّعف في وظيفةٍ بدون خادم أو واجهة برمجة التَّطبيقات، ممَّا يسمح للجهات الفاعلة الخبيثة بتنفيذ تعليمات برمجيَّة عشوائيَّة أو مُشوَّهة على النِّظام.

لذا على المُؤسَّسات مُراقَبَة وظائفها بدون خادم وواجهات برمجة التَّطبيقات الخاصَّة بها بحثًا عن نقاط الضَّعف المُحْتَمَلَة، واستخدام أدوات الفحص الأمنيّ لاكتشاف أيّ نشاطٍ مشبوهٍ، والتَّأكُّد من أنَّ وظائفها وواجهات برمجة التَّطبيقات بدون خادم مُحَدَّثة دائمًا بأحدث تصحيحات الأمان.

6. 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 تعطُّله أو عدم استجابته. وللحماية من هذا النَّوْع من الهجمات يجب التَّأكُّد من أنَّ بروتوكولات الأمان السَّحابيَّة الخاصَّة بك مُحَدَّثة، ويتمّ مُراقَبَتها بانتظامٍ بحثًا عن أيّ نشاطٍ مشبوهٍ.

7. استغلال التَّرحيل المُباشِر

التَّرحيل المُباشِر هو 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 المُهاجِمين في حالة وجود أيّ ثغراتٍ أمنيَّةٍ في بروتوكولات الأمان الخاصَّة بالنِّظام.

8. التَّنصُّت على شبكة WiFi

يُعدّ التَّنصُّت على شبكة WiFi وسيلة لهجوم الوصول عن بُعْد، حيث يحاول المُهاجِمُون الوصول إلى جهازٍ مُسْتَهْدَفٍ عن طريق اعتراض وفَكّ تشفير الشَّبَكة. لذا يجب تعيين كلمة مرور قويَّة للشَّبَكة، وتشغيل الأجهزة بأحدث تصحيحات الأمان.

9. هجمات الثَّغرات غير المُكْتشَفَة

هو نَوْعٌ من الهجمات الإلكترونيَّة التي تستغلّ نقاط الضَّعف غير المعروفة سابقًا في أنظمة الحاسوب أو التَّطبيقات. ولتفادي هذه الهجمات يجب الاطِّلاع على أحدث التَّصحيحات الأمنيَّة ومُراقَبَة أيّ سُلُوكٍ غير عاديّ للنِّظام[1].

1. The 10 Most Common Attack Types of Malware in the Cloud, What They Do and How to Defend Against Them, Buchanan. On site: https://cutt.us/PknJl

الوُصُول غير المُصرَّح به

يُعدّ الوصول غير المُصَرَّح به أو غير القانونيّ تهديدًا كبيرًا لأَمْن السَّحابة، فقد وُجِد تقرير سلَّط الضَّوْء على أمن السَّحابة أكَّد من خلاله أنَّ 53% من المُؤسَّسات التي شملتها الدِّراسة ترى أنَّ الوصول غير المُصَرَّح به من خلال سوء استخدام بيانات اعتماد المُوَظَّفين وضوابط الوصول غير المُناسِبَة هو أكبر تهديدٍ منفردٍ لأمن السَّحابة. و 96% من المُؤسَّسات التي شملتها الدِّراسة لديها بعض أو كُلّ تطبيقاتها في السَّحابة. ويمكن مُعالَجَة التَّحكُّم في الوصول من خلال حلول الأمان السَّحابيَّة، جنبًا إلى جنبٍ مع سياسات إدارة الهُوِيَّة والوصول[1].

ويُعدّ إدارة الهُوِيَّة والوصول (IAM) هو النِّظام الأمنيّ الذي يُمكِّن الأفراد المُناسِبين من الوصول إلى الموارد المُناسِبَة في الأوقات المُناسِبَة للأسباب الصَّحيحة، كما يسمح برنامج الوصول الآمن للتَّطبيقات بتجزئة الوصول إلى التَّطبيقات السَّحابيَّة بناءً على ثقة المُسْتَخْدِم. فعلى سبيل المثال، يحتاج البائعون إلى الوصول إلى تطبيقٍ مُؤسَّسيّ يعتمد على الوصول السَّحابيّ فقط إلى التَّطبيق الفرديّ المطلوب لإكمال عملهم. لذا يُوفِّر الوصول الآمن للتَّطبيقات تتبُّعًا كاملًا ومُراقَبَة وإعداد تقارير للوصول إلى التَّطبيقات؛ ممَّا يسمح لمُؤسَّسات تكنولوجيا المعلومات بالامتثال للوائح أمان البيانات.

وهناك تحدّيات أمنيَّة سحابيَّة رئيسيَّة مع الوصول غير المُصَرَّح به:

1. خروقات البيانات

ففي عام 2021م تمّ الإبلاغ عن 738 انتهاكًا للبيانات، وكانت القَرْصَنَة هي السَّبب الأكثر شيوعًا. لذا أصبح الحفاظ على أمان المعلومات الخاصَّة أكثر أهمِّيَّة من أيّ وقتٍ مضى، بالإضافة إلى ذلك، هناك خطر فقدان البيانات سواءٌ بسبب كوارث طبيعيَّة مثل الحرائق أو لسرقة البيانات المُهمَّة.

2. نقاط دخول غير آمِنَة

عند استخدام السَّحابة، يمكنك الوصول إلى بياناتك من أيّ مكانٍ ومن أيّ جهازٍ. وعلى الرَّغم من ذلك، تُشكِّل الواجهات غير الآمِنَة، ولا سِيَّما واجهات برمجة التَّطبيقات، تهديدًا يمكن استغلاله في سرقة والتَّلاعب بالبيانات، من خلال العثور على عُيُوبٍ ببرمجة التَّطبيقات واستغلالها أو ما نُطلِق عليه "الثَّغرات"[2].

1. Unauthorized access is the biggest threat to Cloud security, Cdnetworks, December 11, 2018. On site: https://cutt.us/r76hP
2. McCaw, Billy. 5 Key Cloud Security Challenges with unauthorized access, extreme compute, 2021. On site: https://cutt.us/OigBo

الفَصْل الثَّالث

كيفيَّة حماية الحَوْسَبَة السَّحابيَّة من الهجمات الرَّقميَّة

- الأمن السَّحابيّ.
- حماية البيانات في الحَوْسَبَة السَّحابيَّة من القَرْصَنَة.

0 3

الأمن السَّحابيّ

يتضمَّن الأمن السَّحابيّ الإجراءات والتِّقنيَّات التي تعمل على تأمين بيئات الحَوْسَبة السَّحابيَّة ضِدّ تهديدات الأمن السّيبرانيّ الخارجيَّة والدَّاخليَّة. إنَّ أفضل مُمارَسات الأمن السَّحابيّ وإدارة الأمان المُصَمَّمة لمَنْع الوصول غير المُصَرَّح به مطلوبة للحفاظ على البيانات والتَّطبيقات في السَّحابة آمِنَة من تهديدات الأمن السّيبرانيّ الحاليَّة والنَّاشئة؛ ونظرًا لأنَّه يتمّ تخزين البيانات الموجودة في السَّحابة العامَّة بواسطة طرفٍ ثالثٍ ويمكن الوصول إليها عَبْر الإنترنت، تنشأ العديد من التَّحدِّيات في القُدْرة على الحفاظ على سحابةٍ آمِنَةٍ.

في كثيرٍ من الحالات، يمكن الوصول إلى الخدمات السَّحابيَّة خارج شبكة المُؤسَّسة ومن الأجهزة التي لا يديرها قسم تكنولوجيا المعلومات، ففي بيئة مُوفِّري الخدمة السَّحابيَّة التَّابعة لجهةٍ خارجيَّةٍ، تتمتَّع فرق تكنولوجيا المعلومات بإمكانيَّة وصول أقل إلى البيانات ممَّا كانت عليه عندما كانت تتحكَّم في الخوادم والتَّطبيقات في أماكن العمل الخاصَّة بها، حيث يتمّ مَنْح عُمَلاء السَّحابة تحكُّمًا محدودًا بِشَكْلٍ افتراضيّ، ولا يتوفَّر الوصول إلى البِنْية التَّحتيَّة الماديَّة الأساسيَّة.

كما يمكن للمُسْتَخْدِمين الوصول إلى التَّطبيقات والبيانات السَّحابيَّة عَبْر الإنترنت، من أيّ مكانٍ أو جهازٍ، بما في ذلك تقنيَّة إحضار جهازهم الخاصّ ممَّا يزيد من التَّحدِّيات الأمنيَّة، إلى جانب أنَّ الوصول المُمَيَّز من قِبَل مُوظَّفي مُوفِّري الخدمة السَّحابيَّة إلى بيانات المُسْتَخْدِمين يمكن أن يتجاوز عناصر التَّحكُّم الأمنيَّة الخاصَّة بهم[1].

وعمومًا تمنح الحَوْسَبَة السَّحابيَّة المُسْتَخْدِمين موقعًا مركزيًّا للبيانات والتَّطبيقات، مع العديد من نقاط النِّهاية والأجهزة التي تتطلَّب الأمان. فأمان الحَوْسَبَة السَّحابيَّة يقوم بإدارة جميع التَّطبيقات والأجهزة والبيانات الخاصَّة بك مركزيًّا لضمان حماية كُلّ شيء، فهو يُتيح أداء المَهامّ بسهولةٍ أكبر، مثل تنفيذ خُطَط التَّعافي من الكوارث، وتبسيط مُراقَبَة أحداث الشَّبَكة، وتحسين تصفية الويب، فضلًا عن تحسين حماية DDoS، حيث تُعدّ هجمات حجب الخدمة المُوَزَّعة (DDoS) من أكبر التَّهديدات التي تواجه الحَوْسَبَة السَّحابيَّة لكَوْنها تستهدف حركة مرور كبيرة على الخوادم في وقتٍ واحدٍ لإحداث الضَّرر، فالأمان السَّحابيّ هنا يحمي الخوادم من هذه الهجمات من خلال مُراقَبَتها وتوزيعها.

1. What is Cloud Security? sky high security. On site: https://cutt.us/3g7wy

والسُّؤال هنا... هل السَّحابة آمِنَة بما فيه الكفاية للمحتوى الخاصّ بنا؟

يعتمد المُسْتَخْدِمون بِشَكْلٍ أكبر على التَّخزين السَّحابيّ والمُعالَجَة، لكنَّهم عادةً ما يشعرون بالقلق من أنَّ التَّخلّي عن نموذج الأمن الخاصّ بهم قد يعني التَّخلّي عن طريقتهم الوحيدة للتَّحكُّم في الوصول إلى بياناتهم، إلَّا أنَّ التَّجربة أثبتت أنَّ هذا الخوف لا أساس له من الصِّحَّة، فمُوَفِّرو الخدمة السَّحابيَّة يقومون بتنفيذ الإجراءات والتِّقنيَّات التي تمنع مُوَظَّفيهم من عرض بيانات العملاء، وعادةً ما يأخذ هذا المَنْع شكل التَّشفير وسياسة الشَّركة المُصَمَّمة لمَنْع العاملين من الاطِّلاع على البيانات.

وعمليًّا تحدث خروقات البيانات وأغلب الانتهاكات نتيجة سوء فَهْمٍ حول الدَّوْر الذي يلعبه المُسْتَخْدِمون في حماية بياناتهم الخاصَّة أو عن خطأ في استعمال المُسْتَخْدِم لأدوات الأمان المُقَدَّمة كجزءٍ من الخدمة السَّحابيَّة، أي أنَّ مُقَدِّمي الخدمات السَّحابيَّة مسؤولون عن الحفاظ على تطبيق بيئة التَّشغيل الخاصَّة بالمُسْتَخْدِم، بينما يتحمَّل المُسْتَخْدِمون مسؤوليَّة ما يحدث داخل تلك البيئة.

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

وبِشَكْلٍ عامّ، توجد عِدَّة قضايا لا بُدّ من التَّركيز عليها عند اختيار مُزوِّد خدمة الحَوْسَبَة السَّحابيَّة، **وفيما يلي تبيان لأهمّها:**

1. ضوابط مُصَمَّمة لمَنْع تسرُّب البيانات

ابحث عن مُوَفِّري الخدمة الذين لديهم عناصر تحكُّم حوسبة سحابيَّة آمِنَة تساعد في مَنْع حدوث مشكلات مثل الوصول غير المُصَرَّح به، وتسرُّب البيانات العَرَضيّ، وسرقة البيانات، فهذه الخدمة يجب أن تسمح لك بتطبيق ضوابط أمنيَّة أكثر دِقَّة على بياناتك الأكثر أهمِّيَّة، مثل تصنيفات الأمان الأصليَّة. لذا يجب أن يتأكَّد المُسْتَخْدِم من مدى دِقَّة إعدادات الأذونات.

2. المُصادَقَة القويَّة

تأكَّد من أنَّ مُزوِّد الخدمات السَّحابيَّة يُقدِّم إجراءات مُصادَقَة قويَّة لضمان الوصول المُناسِب من خلال عناصر التَّحكُّم القويَّة بكلمات المرور والمُصادَقَة مُتَعدِّدة العوامل.

3. تشفير البيانات

تأكَّد من إمكانيَّة تشفير جميع البيانات أثناء الرَّاحة وأثناء عمليَّات النَّقل والحِفْظ.

4. الرُّؤْية والكشف عن التَّهديدات

لا بُدّ لمُزوِّد خدمة الحَوْسَبَة السَّحابيَّة من استخدام التَّعلُّم الآليّ لتحديد السُّلوك غير المرغوب فيه، وتحديد التَّهديدات، وتنبيه المُسْتَخْدِمين. على سبيل المثال، قد يلاحظ تحليل سُلوك البيانات أنَّ أحد أفراد فريق المبيعات في مُؤسَّسةٍ ما حاول تنزيل تصميمات مُنْتَجات سرِّيَّة بطريقةٍ مُريبةٍ.

5. الالتزام المُستمرّ

ابحث عن إمكانات إدارة دَوْرة حياة المحتوى، مثل الاحتفاظ بالمُسْتَنَدات والتَّخلُّص منها، والاكتشاف الإلكترونيّ.

6. الأمن المُتَكامِل

لا بُدّ من التَّحقُّق من مدى تكامل أدوات المُوَفِّر بسهولةٍ مع حِزْمة الأمان الخاصَّة بك من خلال واجهات برمجة التَّطبيقات. فَمَهمَّة أدوات المُوَفِّر هي تعزيز التَّعاون وسَيْر العمل الدَّاخليّ والخارجيّ بسلاسةٍ، كما يجب أن تتكامل هذه الأدوات أيضًا مع جميع تطبيقاتك بحيث يمكن أن تمتدّ ضوابط الأمان إلى أيّ تطبيقٍ قد يستخدمه المُسْتَخْدِم للوصول إلى المحتوى الخاصّ به، دون التَّأثير على تجربته[1].

ويُلاحَظ أنَّ مُوَفِّري الخدمات السَّحابيَّة وعملاءهم يتشاركون مسؤوليَّة توفير الأمان السَّحابيّ. وتختلف المسؤوليَّة بناءً على نوع الخدمات المُقَدَّمة، **وفيما يلي تبيان للاختلافات بين إدارة الأمن السَّحابيّ تبعًا لنَوْع السَّحابة:**

- **الحَوْسَبَة السَّحابيَّة العامَّة:** تتمّ إدارتها من قِبَل مُوَفِّري الخدمات السَّحابيَّة، وتتمّ مُشارَكَة الخوادم من قِبَل مُسْتَأجِرين مُتَعدِّدين في هذه البيئة.
- **الحَوْسَبَة السَّحابيَّة الخاصَّة:** قد تكون في مركز بيانات يمتلكه العميل أو يديره مُوَفِّر خدمة سحابيَّة عامَّة. وفي الحالتين، تُعدّ خوادم ذات مُسْتَأجِر فرديّ ولا يتعيَّن على المُؤسَّسات مُشارَكَة المساحة مع الشَّركات الأخرى.
- **الحَوْسَبَة السَّحابيَّة الهجينة:** فهي تُعدّ مزيجًا من مراكز البيانات المحلِّيَّة والخدمات السَّحابيَّة الخارجيَّة.
- **سحابة المجتمع:** تتضمَّن خدمتَيْن أو أكثر من الخدمات السَّحابيَّة التي تتمّ إدارتها من قِبَل جميع مُوَفِّري الخدمات السَّحابيَّة[2].

ومهما كان نوع البيئة أو مجموعة البيئات التي يستخدمها المُسْتَخْدِمون، يكون الهدف الرَّئيسيّ للأمان السَّحابيّ هو حماية الشَّبَكات المادِّيَّة، بما في ذلك أجهزة التَّوجيه والأنظمة الكهربائيَّة والبيانات وتخزين البيانات وخوادم البيانات والتَّطبيقات والبرامج وأنظمة التَّشغيل والأجهزة الإلكترونيَّة.

1. What is cloud security? box. On site: https://cutt.us/j9fxl

2. ما المَقْصود بالأمان السَّحابيّ؟، مايكروسوفت. مُتاح على الرَّابط: https://cutt.us/tS1FI

كيف يعمل الأمان السّحابيّ؟

خدمة تأجير البِنْية التَّحتيَّة

في هذا النَّموذج، يُقدِّم مُوَفِّرو الخدمات السَّحابيَّة موارد للحَوْسَبَة والشَّبَكة والتَّخزين عند الطَّلَب. والمُوَفِّر مسؤول عن تأمين خدمات حَوْسَبَة الذَّاكرة الأساسيَّة. أمَّا العملاء فعليهم تأمين كُلّ شيءٍ مُتَعلِّقٍ بنظام التَّشغيل، بما في ذلك التَّطبيقات والبيانات وأوقات التَّشغيل والبرامج الوسيطة ونظام التَّشغيل نفسه.

خدمة النِّظام الأساسيّ

يُقدِّم مُوَفِّرو الخدمات بيئة للتَّطوير والنَّشر كاملةً في السَّحابة، ويتحمَّلون مسؤوليَّة حماية وقت التَّشغيل والبرامج الوسيطة ونظام التَّشغيل، بالإضافة إلى خدمات حَوْسَبَة الذَّاكرة الأساسيَّة. أمَّا العملاء يجب عليهم توفير الحماية لتطبيقاتهم وبياناتهم وعمليَّة وصول المُسْتَخْدِم وأجهزة وشَبَكات المُسْتَخْدِم.

خدمة تأجير البرامج

يمكن للعملاء الوصول إلى البرامج من خلال نموذج الدَّفع حسب وقت استخدام الخدمة، مثل Microsoft Office 365 أو Google Drive [1]

وبغضّ النَّظر عن الجهة المسؤولة عن أمن البيانات المُخَزَّنة على السَّحابة، توجد جوانب أساسيَّة للأمان السَّحابيّ، **فيما يلي تبيان لأهمّها:**

- **تقييد عمليَّة الوصول،** من الضَّروري التَّأكُّد من مَنْح الأشخاص المُناسِبين فقط حقّ الوصول إلى الأدوات المُناسِبَة في الوقت المُناسِب.
- **حماية البيانات،** لأنَّ مُسْتَخْدِمي خدمات الحَوْسَبَة يحتاجون إلى معرفة مكان تواجد بياناتهم ووَضْع ضوابط مُناسِبَة لتأمين البيانات والبِنْية التَّحتيَّة المُسْتَضِيفَة لتلك البيانات.
- **استعادة البيانات،** يجب وجود نَسْخ احتياطيّ جيِّد للبيانات وخُطَّة استعادة بيانات لتجنُّب التَّعرُّض لأيّ ضررٍ عند حدوث خرقٍ أمنيّ.
- **خُطَّة الاستجابة،** عند التَّعرُّض للهجمات، يجب أن تكون هناك خُطَّة لتقليل تأثير هذه الهجمات.
- التَّحقُّق المُبَكِّر من الثَّغرات الأمنيَّة.
- **توجيه تركيز فرق الأمان نحو التَّخلُّص من التَّهديدات النَّاشئة،** عَبْر تعزيز تكوينات موارد السَّحابة من خلال البرمجيَّات لتقليل مشكلات الأمان التي تواجهها بيئات الإنتاج.

1. What is cloud security? box. On site: https://cutt.us/j9fxl

حماية البيانات في الحَوْسَبَة السَّحابيَّة من القَرْصَنَة

تُعدّ القَرْصَنَة من التَّهديدات الرَّئيسة التي تواجه البيانات المُخَزَّنة على السَّحابة، ولحمايتها من هذا التَّهديد، لا بُدّ من الحرص على اعتماد الإجراءات التَّالية:

- لتحقيق أقصى استفادة من الحَوْسَبَة السَّحابيَّة يجب استخدام كلمات مرورٍ قويَّةٍ تمزج بين الأَحْرُف والأرقام والأَحْرُف الخاصَّة.
- احرص على حماية جميع الأجهزة التي تستخدمها للوصول إلى بياناتك السَّحابيَّة، بما في ذلك الهواتف الذَّكيَّة والأجهزة اللَّوْحيَّة، خاصَّةً إذا كانت بياناتك مُتَزامِنَة عَبْر العديد من الأجهزة.
- أنشئ نُسْخة احتياطيَّة من بياناتك بانتظامٍ؛ حتَّى تتمكَّن من استعادة بياناتك بالكامل في حالة انقطاع الخدمة السَّحابيَّة أو فَقْد البيانات الموجودة لدى مُزَوِّد الخدمة السَّحابيَّة، سواءٌ بوضع نُسْخة على جهاز الحاسوب المَنْزليّ الخاصّ بك، أو على مُحَرِّك أقراص صلبة خارجيّ، أو حتى من خدمةٍ سحابيَّةٍ إلى أخرى، طالما أنَّ مُزَوِّدي الخدمات السَّحابيَّة لا يشتركان في البِنْية التَّحتيَّة ذاتها.
- استخدم الأذونات لمَنْع أيّ فردٍ أو جهازٍ من الوصول إلى جميع بياناتك، إذا كانت لديك شَبَكة مَنْزليَّة، فاستخدم شبكات الضَّيْف لأطفالك ولأجهزة إنترنت الأشياء وللتِّلفاز، واحفظ تصريح «الوصول إلى جميع المناطق» لاستخدامك الخاصّ.
- استخدم أحد برامج مُكافَحَة الفيروسات والبرمجيَّات الضَّارَّة.
- لا تصل إلى بياناتك على شبكة Wi-Fi عامَّة، خاصَّةً إذا كنت لا تستخدم مُصادَقَة قويَّة.
- تُعدّ المُصادَقَة مُتَعدِّدة العوامل (MFA) طريقة ذكيَّة لحماية وصولك، سواءٌ عَبْر بصمات الأصابع، أو كلمة مرور ورَمْز مُنفَصِل 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 يستغلُّون مثل هذه الحسابات لإيجاد ثغرةٍ إلى نظامك وأجهزتك[1].

1. ما هو الأمن السَّحابيّ؟ Kaspersky. مُتاح على الرَّابط: https://cutt.us/CO2Zq

البطاقات التّدريبيّة

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 بالاعتماد على السَّحابة تخزين المُستندَات في قاعدة بيانات على الشَّبكَة.

أهمِّيَّة الحَوْسَبَة السَّحابيَّة

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

الحَوْسَبَة السَّحابيَّة العامَّة

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

الحَوْسَبَة السَّحابيَّة الخاصَّة

يُطلَق عليها مُسمَّيات مثل السَّحابة الدَّاخليَّة أو سحابة الشَّركات، حيث يتمّ استخدامها من قِبَل المُؤسَّسات لبناء وإدارة مراكز البيانات الخاصَّة بها داخليًّا أو بواسطة جهةٍ خارجيَّةٍ.

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 عدَّة مُؤسَّسات لمُشارَكَة المعلومات بين المُؤسَّسة ومُجْتَمَعٍ مُعيَّنٍ. وهي مملوكة ومُدارة من قِبَل واحدة أو أكثر من المُؤسَّسات في المُجْتَمَع، أو طرفٍ ثالثٍ، أو مجموعةٍ منهم، مثل: سحابة مُجْتَمَع الرِّعاية الصِّحِّيَّة.

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 إلكترونيّة أو رسائل نصّيّة تبدو كأنّها من مصادر معروفة، لكنّها مُحاوَلة لسرقة بيانات سرّيّة أو تثبيت تعليمات برمجيّة ضارّة على الجهاز.

هجمات الحَقْن

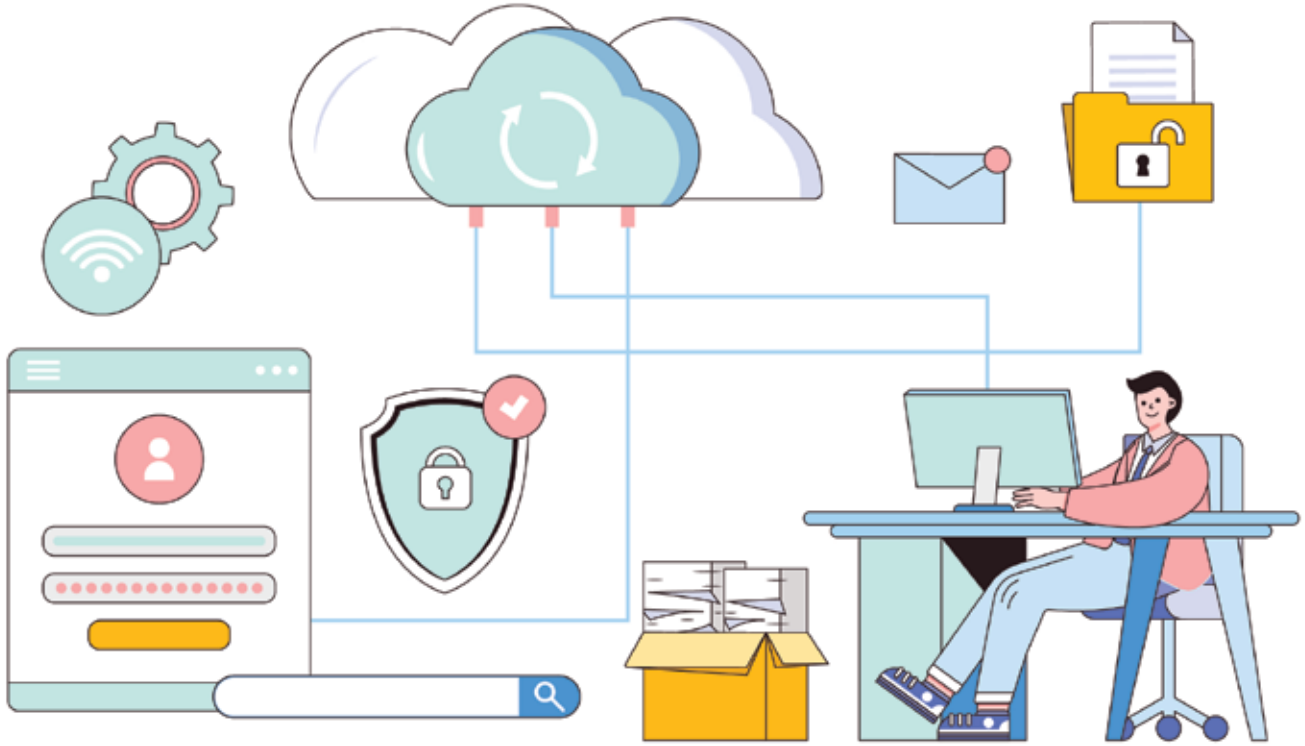
هجومٌ سيبرانيّ يستخدمه مُجْرِمُو الإنترنت لإحداث الفَوْضَى في الخوادم الطَّرفيَّة غير المحميَّة من خلال التَّسلُّل عَبْر نقاط الوصول غير المُصَحَّحة، لسرقة البيانات والهُوِيَّات وكذلك نَشْر برمجيَّات الفِدْية أو حتَّى الاستفادة من المعلومات المسروقة.

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 الخاصَّة بالنِّظام.

هجوم الثَّغرَات غير المُكْتَشَفة

يُسمَّى بهجوم يوم الصِّفر، هو نَوْعٌ من الهجمات الإلكترونيَّة التي تستغلّ نقاط الضَّعْف غير المعروفة سابقًا في أنظمة الحاسوب أو التَّطبيقات.



الأمن السّحابيّ

هو الإجراءات والتّقنيّات التي تعمل على تأمين بيئات الحَوْسَبَة السّحابيّة ضِدّ تهديدات الأمن السّيبرانيّ الخارجيّة والدّاخليّة. فأمان الحَوْسَبَة السّحابيّة يقوم بإدارة جميع التّطبيقات والأجهزة والبيانات الخاصّة بك مركزيًّا لضمان حماية كُلّ شيءٍ، فهو يُتيح أداء المَهامّ بسهولةٍ أكبر، مثل تنفيذ خُطَط التّعافي 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.

الإستكشات

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 أهمّيَّة 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 تمّت تسمية الحَوْسَبَة السَّحابيَّة بهذا الاسم؟

تمّت 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.

مراجـــــع

المحتوى العلمي

في الحـــــقيبة

المراجع العربيَّة:

1. ما المَقْصود بالأمان السَّحابيّ؟، مايكروسوفت. مُتاح على الرَّابِط: https://cutt.us/tS1FI
2. Kaspersky. ما هو الأمن السَّحابيّ؟ مُتاح على الرَّابِط: https://cutt.us/CO2Zq
3. وَاقِع استخدام تطبيقات الحَوْسَبَة السَّحابيَّة في تفعيل التَّعليم المحاسبيّ، دراسة استطلاعيَّة لآراء أساتذة قِسْم العلوم الماليَّة والمُحاسَبَة بجامعة 20 أوت 1955 سكيكدة، الجزائر، مِجلَّة دفاتر بوادكس، المُجلَّد 11، العدد: 02، 2022م.

المراجع الأجنبيَّة:

1. 6 Advantages and Disadvantages of Private Cloud | Limitations & Benefits of Private Cloud, hitechwhizz. On site: https://cutt.us/CplCr

2. Brandt, Charles. What Are the Chances of Losing Information in Cloud Storage? Marconet, August, 2023. On site: https://cutt.us/FFJGN

3. Frankenfield, Jake. What is Cloud Computing? Pros and Cons of Different Types of Services, investopedia, April 2023. On site: https://www.investopedia.com/terms/c/cloud-computing.asp

4. Linao, Portia. Why is it called "The Cloud"? officesolutionsit, February 2023. On site: https://www.officesolutionsit.com.au/blog/why-is-it-called-the-cloud

5. McCaw, Billy. 5 Key Cloud Security Challenges with unauthorized access, extreme compute, 2021. On site: https://cutt.us/OigBo

6. Mohanakrishnan, Ramya. What Is Community Cloud? Definition, Architecture, Examples, and Best Practices, spiceworks. On site: https://cutt.us/ORUiy

7. Public and Private Cloud Advantages and Disadvantages, connectria. On site: https://cutt.us/cMN8I

8. Stephen J. Bigelow. What is public cloud? Everything you need to know, techtarget. On site: https://www.techtarget.com/searchcloudcomputing/definition/public-cloud

9. The 10 Most Common Attack Types of Malware in the Cloud, What They Do and How to Defend Against Them, Buchanan. On site: https://cutt.us/PknJI

10. Tucakov, Dejan. What is Community Cloud? Benefits & Examples with Use Cases, JUNE 18, 2020. On site: https://cutt.us/ghrCz

11. Types of Cloud, javatpoint. On site: https://www.javatpoint.com/types-of-cloud

12. Unauthorized access is the biggest threat to Cloud security, Cdnetworks, December 11, 2018. On site: https://cutt.us/r76hP

13. Weinberger, Matt. Why 'cloud computing' is called 'cloud computing', businessinsider, Mar 2015. On site: https://www.businessinsider.in/why-cloud-computing-is-called-cloud-computing/articleshow/46544750.cms

14. What are the Security Risks of Cloud Computing? Auditboard, on site: https://cutt.us/qJsln

15. What is Cloud Security? sky high security. On site: https://cutt.us/3g7wy

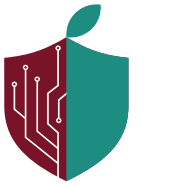
16. What is cloud security? box. On site: https://cutt.us/j9fxl

17. What is cloud security? box. On site: https://cutt.us/j9fxl

18. What is hybrid cloud? netapp. On site: https://cutt.us/8N9QZ

19. What is private cloud? ovhcloud. On site: https://www.ovhcloud.com/en-gb/learn/what-is-private-cloud/

20. What is private cloud? Types, process, benefits, examples, knowledgehut. On site: https://2u.pw/vtxJ57Q



CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency