معهد العراب العالي للتدريب

امن حوسبة سحابية

سمر سعيد الهوارى

نبذة عن المقرر

تقديم المبادئ الأساسية للحوسبة السحابية والافتراضية بالإضافة الى تعلم كيفية حماية البيانات من السرقة والحذف ومعرفة التهديدات العظمى لأمن السحابة وعمل اختبار اختراق للسحابة

معهد العراب العالي للتدريب

الأهداف العامة والتفصيلية من المقرر

اكتساب المعلومات الأساسية لأمن الحوسبة السحابية والافتراضية وانواع السحابة

- فهم الحوسبة السحابية
- الحماية من تهديدات الحوسبة السحابية
- صد الهجمات
- استخدام أدوات امن السحابة
- اختبار اختراق الحوسبة السحابية
- استخدام قوانين الحوسبة السحابية .

مقدمة الحوسبة السحابية

ما الحوسبة السحابية؟

إن الحوسبة السحابية تعني توفير موارد تقنية المعلومات حسب الطلب عبر الإنترنت مع تسعير التكلفة حسب الاستخدام. فبدلاً من شراء مراكز البيانات والخوادم المادية وامتلاكها والاحتفاظ بها، يمكنك الوصول والاستفادة من الخدمات التكنولوجية، مثل إمكانات الحوسبة، والتخزين، وقواعد البيانات، بأسلوب يعتمد على احتياجاتك، وذلك من خلال جهة موفرة للخدمات السحابية مثل Amazon Web Services (AWS).

نماذج خدمه الحوسبة السحابية

1. SaaS(Software as a service)
2. IaaS (Infrastructure as a Service)
3. PaaS(Platform as a service)

1. SaaS(Software as a service)

البرمجيات كخدمة (SaaS)ويعتبر هذا النوع من الخدمات هو الأكثر استخدامًا في الحوسبة السحابية، حيث أنها توفر وصول مستأجرين متعددين من السحابة إلى تطبيق معين. تتيح عروض SaaSالاستفادة من السحابة لبنية البرامج وبالتالي تقليل النفقات العامة للدعم والصيانة والعمليات حيث تعمل التطبيقات على أنظمة تابعة للبائع.
يتفاعل المستخدمون غالباً بشكل مباشر مع تطبيقات SaaS .
SaaSهو عرض قائم على الاشتراك حيث يشترك المستخدمون في البرنامج بشكل شهري بدلاً من شرائه، لذلك لا توجد تكاليف مسبقة متضمنة.

أمثلة على خدمات الحوسبة السحابية SaaS

Netflixأو Gmailأو JIRAأو Dropboxأو Salesforce .
Office 365هو شكل من أشكال SaaSوفيه يمكن لأي شخص فتح اشتراك شهري لاستخدام مجموعة منتجات Microsoft Office .

ميزات وفوائد خدمة الحوسبة السحابية SaaS

- لا توجد تكلفة إعداد أولية
- عملية الدفع تعتبر مرنة حيث يدفع المستخدمون مقابل الخدمات التي يحصلون عليها.
- أي تحديثات تصدر للبرنامج تتم بشكل تلقائي ومجاني.
- لا تحتاج الشركات إلى الاستعانة بخبير في تقنية المعلومات لتنزيل البرنامج

2. IaaS (Infrastructure as a Service)

تشمل البنية التحتية كخدمة ((IaaSالبنية الأساسية للسحابة وتوفر الوصول إلى وظائف الشبكة والأجهزة الافتراضية والأجهزة المخصصة ومساحة التخزين.
تساعد IaaSالمستخدمين على استخدام قوة الحوسبة والمعالجة أو الأجهزة الافتراضية دون الحاجة لاستثمارات في الأجهزة باهظة الثمن أو إدارة الخادم. ماديًا، يتم سحب موارد الأجهزة من مجموعة متنوعة من الشبكات والخوادم الموزعة عبر مراكز بيانات مختلفة، والتي تتم إدارتها وصيانتها جميعًا بواسطة مزود الخدمة السحابية.

أمثلة على خدمات الحوسبة السحابية IaaS:

Amazon EC2و Windows Azureو Rackspaceو Google Compute

ميزات وفوائد خدمة الحوسبة السحابية IaaS

- توفر البنية التحتية النموذجية خدمة توفير الوقت والمال، حيث يتم توفير الأجهزة الأساسية والدعم من قبل مزود الخدمة.
- تتوفر الموارد عند الطلب، أي عند الحاجة لها وبالتالي لا يوجد هدر لأي موارد غير مستخدمة ولا تأخير في إضافة أي موارد.
- نموذج التسعير القائم على المنفعة، أي ادفع فقط مقابل الموارد التي تستخدمها بالفعل.

3. PaaS(Platform as a service)

المنصة كخدمة يشمل الأجهزة وأنظمة التشغيل اللازمة لنشر وإدارة التطبيقات السحابية. تساعد PaaS على زيادة كفاءة الأعمال دون متاعب إدارة الحلول المستندة إلى السحابة والتخطيط لها وشرائها وصيانتها. يسير كل من PaaS و IaaS جنبًا إلى جنب لأنك بحاجة إلى نظام أساسي لإدارة البنية التحتية لتقنية المعلومات.

أمثلة على خدمات الحوسبة السحابية PaaS:

Google App Engine و Rackspace Cloud Sites و OpenShift و Apache Stratos

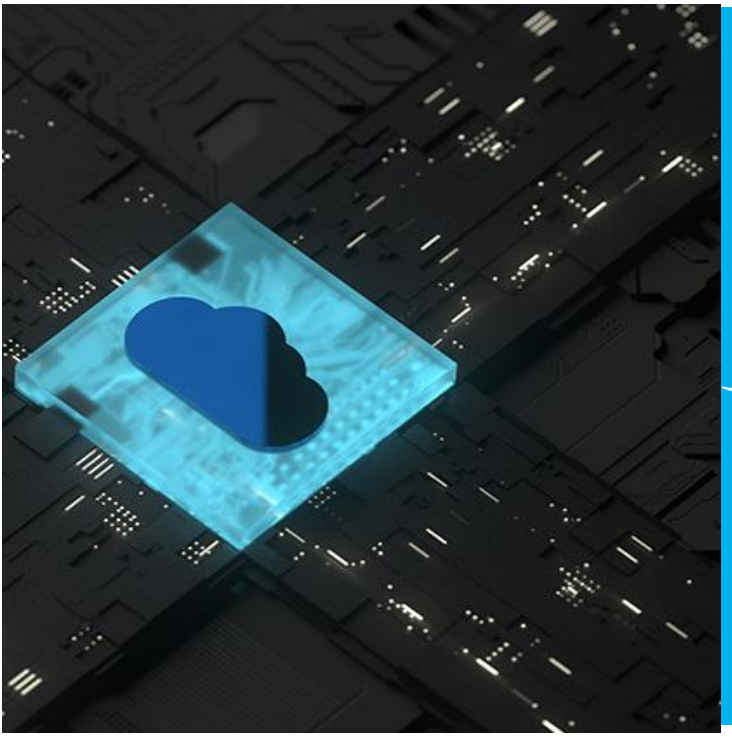
ميزات وفوائد خدمة الحوسبة السحابية PaaS

- تجعل PaaS تطوير البرامج أمرًا سهلاً حتى لغير الخبراء حيث يمكن لأي شخص تطوير تطبيق من خلال متصفح الويب.
- لن يحتاج مستخدمو هذه الخدمة ترقية البنية التحتية أو تحديثها لأن موفر خدمة PaaS يتعامل مع جميع تصحيحات التحديث والترقيات وصيانة البرامج المنتظمة.
- توفر PaaS استقلالية الموقع حيث يمكن للمطورين في مواقع مختلفة العمل معًا على نفس بنية التطبيق.
- ليست هناك حاجة للاستثمار في البنية التحتية المادية.

نماذج تعيين السحابة

1. منصة الحوسبة السحابية العامة public cloud
2. منصة الحوسبة السحابية الخاصة private cloud
3. منصة الحوسبة السحابية المشتركة hybrid cloud

مزايا الحوسبة السحابية

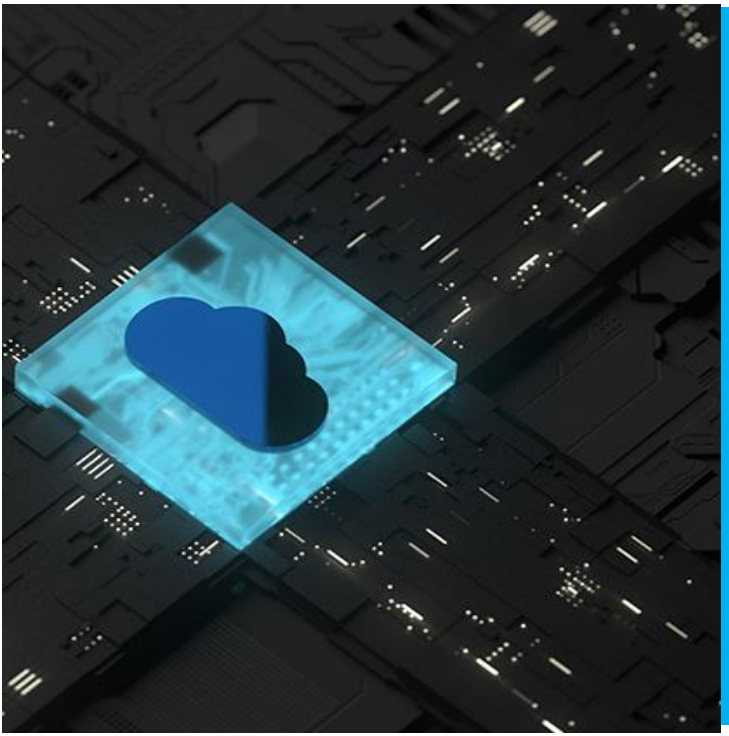


تقليل الإنفاق:

من أهم مزايا هذا النوع من التكنولوجيا أنها توفر الكثير من التكاليف والوقت التي يمكن أن تنفقها إذا قمت بتخزين بيانات شركتك بالطرق التقليدية، فأنت لا تحتاج شراء الخوادم الضخمة وتكبد عناء صيانتها وتأمينها، حيث توفر شركات المتخصصة في هذا المجال كل ذلك كما تقدم خطط أسعار مناسبة لميزانيتك ومتطلباتك مثل الدفع مقابل الاستخدام أو بصور شهرية أو سنوية.

سهولة الوصول:

تمكنك نظم الحوسبة السحابية من الوصول إلى بيانات الخاصة بمؤسستك من أي مكان وفي أي وقت،سواء عن طريق أجهزة الكمبيوتر بمختلف أنواعها أو هواتف المحمول والهواتف.



ضمان استمرارية الخدمة:

وذلك من أهم الخصائص التي يبحث عنها أصحاب الشركات عند الاختيارما بين أنظمة الحوسبة السحابية، فالشركات المثوقة المقدمة لهذه الخدمة تعمل على تقديم نسخ احتياطية بشكل دوري لبيانات عملائها وملفاتهم المهمة، كما تقوم بتحديثات لبرامج التشغيل لضمان عدم تعرض بياناتك للفقدان بسبب انقطاع التيار الكهربائي أو حدوث أية أعطال في برامج التشغيلة.

التأمين والحماية:

تصبح مهمة الشركة المقدمة لخدمة الحوسبة السحابية توفير أعلى مستويات التأمين لكل بيانات وحمايتها من التعرض للسرقة أو القرصنة أو أية مخاطر يمكن أن تهدد أمن بيانات شركتك.

سؤال و إجابة

1- توفير موارد تقنية المعلومات حسب الطلب عبر الإنترنت مع تسعير التكلفة حسب الاستخدام.

A. التشفير
B. الحوسبة السحابية
C. الافتراضية

2- من مزايا الحوسبة السحابية.

A. تقليل الإنفاق
B. زيادة فرص العمل
C. محدودية الخدمة

تهديدات السحابة

- **مخاطر البنية الأساسية المستندة إلى السحابة** بما في ذلك أطُر عمل تكنولوجيا المعلومات القديمة غير المتوافقة، وانقطاعات خدمة تخزين البيانات التابعة لجهات خارجية.
- **التهديدات الداخلية الناتجة عن الأخطاء البشرية** مثل سوء تكوين عناصر التحكم في وصول المستخدمين.
- **التهديدات الخارجية** تصدر بشكل شبه حصري عن جهات خبيثة الغرض، مثل البرامج الضارة وعمليات التصيد وهجمات الحرمان من الخدمة.

تهديدات السحابة

أنواع المهددات

يتم تصنيف المخاطر الأمنية لخدمات الحوسبة السحابية بالطرق التالية:

- **الثغرات الأمنية في النظام:** هي الجانب التقني للتهديدات التي يجب التعامل معها بشكل استباقي من قِبل موظفي تكنولوجيا المعلومات المؤهَّلين.
- **خطأ أو إهمال مستخدمي الأجهزة الطرفية:** هو الجانب البشري الذي يتطلب التدريب والتعليم المستمر لمنعه.
- **الهجمات السيبرانية الضارة** في نهاية المطاف لا تكون إلا بقوة نقاط الضعف البشرية والتقنية في نظام السحابة الذي سمح لهم بذلك. ورغم ذلك، فإن الخبرة في التلاعب بالعناصر التقنية والبشرية تمنح المهاجمين ميزة.

تهديدات التطبيقات

اختراق البيانات
انتهاك البيانات من خلال الوصول إلى الهوية
واجهات التطبيقات غير آمنة
سرقة الحسابات

اختراق البيانات

قد يكون خرق البيانات هو الهدف الرئيسي للهجوم المستهدف أو قد يكون ببساطة نتيجة خطأ بشري أو ثغرات أمنية في التطبيق أو ممارسات أمنية سيئة من قبل المستخدمين ، ويشمل ذلك الهجوم الحصول على معلومات غير مخصصة للتداول العلني ،

مثـل معلومـات الصـحة الشخصـية أو المعلومـات الماليـة أو معلومـات التعريف الشخصية PII)) أو الأسرار التجارية أو الملكية الفكرية .
تكون البيانـات التـي يحصـل عليهـا المختـرق ذات قيمـة لأطـراف أخـرى فمـثلا قـد تكـون المعلومـات الماليـة أو الصـحية أو الشخصـية كافيـة للقيـام بأنشطة احتيالية ؛ كما قد يسعى المنافسون للحصول على تلك المعلومات والأسرار ؛ كما قد يرغب النشطاء في كشف هذه المعلومات التي يمكن أن تسبب أضرارًا أو إحراجًا لأصحابها ،

انتهاك البيانات من خلال الوصول إلى الهوية

غالبًا ما تحدث الهجمات الإلكترونية وانتهاكات البيانات بسبب نقص تأمين وتطوير أنظمة إدارة الوصول إلى الهوية ، والفشل في استخدام المصادقة ، وضعف استخدام كلمة المرور ، والافتقار إلى التدوير الآلي المستمر لمفاتيح التشفير وكلمات المرور ، حيث يمكن للمخترقين التنكر كمستخدمين أو مشغلين أو مطورين والتطفل على البيانات أو إصدار البرامج الضارة التي يبدو أنها تنشأ من مصدر موثوق، ونتيجة لذلك فإن عدم كفاية إثبات الهوية أو إدارة أمان نظام الاعتماد والوصول يمكن أن يتيح الدخول غير المصرح به إلى البيانات مما قد يتسبب في أضرار جسيمة محتملة للمنظمات أو المستخدمين

واجهات التطبيقات غير آمنة

يجب تصميم واجهات مستخدم البرنامج (UIs) وواجهات برمجة التطبيقات (APIs)بنظام حماية قوي للوقوف ضد كل المحاولات الخبيثة للتحايل للوصول إلى داخل الأنظمة ، حيث تعد واجهات برمجة التطبيقات وواجهة المستخدم عمومًا الجزء الأكثر ظهورا، وربما يكون المكان الوحيد الذي يتوفر به عنوان الـ IP المتاح خارج الحدود التنظيمية الموثوق بها ولذا قد يكون هدفًا لهجمات شديدة ، لذا فوضع الضوابط الكافية التي تحمي هذه الواجهات هي الخط الأول للدفاع والكشف .

سرقة الحسابات

ففي حين أن سرقة الحسابات أو الخدمات ليست جديدة ، إلا ان الحلول السحابية تضيف تهديدًا جديدًا إلى هذه النوعية القائمة ، فإذا تمكن المهاجم من الوصول إلى بيانات الاعتماد الخاصة بالمستخدم ، فسيمكنه التنصت على أنشطته ومعاملاته ، ومن ثم يقم بمعالجة البيانات واستخدام هذه المعلومات في سرقة عملائه أو تحويلهم إلى مواقع غير شرعية ، أو قد يجعل الحساب قاعدة للمهاجمين ، أو يمكنه الاستفادة من قوة سمعة العميل في شن هجمات لاحقة

نشاط دراسة حالة اختراق للسحابة

مالعمل في هذه الحالة ؟
كيف نحمي حساباتنا على السحابة الالكترونية ؟

تهديدات البنية التحتية

المجتمعات الحديثة مهددة بشكل كبير من قبل الهجمات الإلكترونية. من خلال الاستثمارات في الأمن السيبراني، تحاول الحكومات والشركات حماية نفسها من الهجمات القاتلة التي يمكن أن تشل أنظمتها بأكملها.

أهم 5 نقاط ضعف فى البنية التحتية الحرجة

- **البرامج القديمة**

البرامج التقليدية التي تفتقر إلى مصادقة المستخدم والنظام الجيدة أو التحقق من صحة البيانات أو ميزات مسح سلامة البيانات التي تخول وصول المهاجمين غير المنضبط إلى الأنظمة.

- **التكوين الافتراضي**

تمكن الأنظمة الجاهزة ذات كلمات المرور الافتراضية أو السهلة والتكوينات الأساسية cyberpunksمن إدراج أنظمة OTواختراقها.

- **عدم وجود تشفير**

تفتقر وحدات تحكم SCADAالتقليدية والبروتوكولات الصناعية إلى القدرة على تشفير الاتصال. يستخدم المهاجمون الإلكترونيون برنامج الشم للعثور على اسم المستخدم وكلمات المرور.

- **السياسات والإجراءات**

تتشكل الثغرات الأمنية عندما تختلف أقسام تكنولوجيا المعلومات و OTفي عملية تأمين الضوابط الصناعية. يجب أن تعمل الإدارات المختلفة معا لبناء سياسة أمنية موحدة تدافع عن كل من تكنولوجيا المعلومات وتكنولوجيا OT.

- **سياسات الوصول عن بعد**

توفر أنظمة SCADAالمرتبطة بخطوط الطلب الهاتفي غير المدققة أو خوادم الوصول عن بعد ل cyberpunksسهولة الدخول إلى الباب الخلفي إلى شبكة OTوالشبكة المحلية للشركات.

أهم 5 تهديدات للبنية التحتية الحرجة

- **عدم وجود تقسيم للشبكة**

توفر ميزات الشبكة وجدار الحماية OTالمسطحة والمهيأة بشكل خاطئ والتي تفشل في ملاحظة أو اعتراض النشاط العدائي لمستخدمي الإنترنت مسارا سهلا للدخول إلى أنظمة OT.

- **هجمات DDOS**

تمكن المصادر المبطلة وضوابط الوصول المحدودة مستخدمي الإنترنت من تخريب أنظمة OTلتنفيذ هجمات DoSعلى الأنظمة الضعيفة غير المصححة.

- **هجمات تطبيقات الويب**

ترتبط أنظمة OTالقديمة ، بما في ذلك واجهات الإدارة البشرية (HMI)وأجهزة الكمبيوتر المنطقية القابلة للبرمجة (PLC) ، بشكل متزايد بالشبكة ويمكن الوصول إليها في أي مكان عبر واجهة الويب. أنظمة OTغير الآمنة عرضة للبرمجة النصية عبر المواقع وهجمات حقن SQL.

- **حقن الأوامر**

- المعلومات المبطلة التي لم يتم التحقق منها كحركة مرور شرعية للنظام تمكن المهاجمين من تشغيل أوامر النظام التعسفية على أنظمة OT.

- **البرامج الضارة**

تتعرض أنظمة OTللهجوم ويجب أن تشمل **أمان مكافحة البرامج الضارة ، وعناصر التحكم في جدار الحماية المستند إلى المضيف ، وإرشادات إدارة التصحيح** للحد من الهجمات الإلكترونية.

تهديدات نقل البيانات

أنواع التهديدات التي تستهدف البيانات

تشير التهديدات المستهدفة للبيانات إلى الإجراءات التي قد تؤثر على تكامل أو سرية أو توافر بيانات مؤسستك، في حين تؤدي هجمات تسريب البيانات إلى عرض بياناتك الحساسة في بيئات غير موثوقة.

الهجوم عبر الإنترنت

يشير الهجوم عبر الإنترنت إلى تدبير محاولة خبيثة لاكتساب وصول غير مصرح به لأنظمة كمبيوتر (الأعمال التجارية والشخصية) وسرقة البيانات أو تعديلها أو تدميرها. ومن أمثلة الهجمات عبر الإنترنتالهجمات الموزعة لحجب الخدمة (DDoS)، وبرامج التجسس وبرامج الفدية الضارة. فأدوات أمان السحابة وأنظمة إدارة الهوية والوصول وإدارة المخاطر ما هي إلا وسائل بسيطة لحماية شبكتك.

البرامج الضارة

غالبًا ما تتخفى البرامج الضارة بما في ذلك الفيروسات المتنقلة والفيروسات وبرامج التجسس في صورة برنامج أو بريد إلكتروني موثوق به (على سبيل المثال، مجلد ملفات أو مستند مشفر). وبمجرد فتحه، فإنه يسمح للمستخدمين غير المصرح لهم بالدخول إلى بيئتك حيث يمكنهم بعد ذلك تعطيل شبكة تكنولوجيا المعلومات بالكامل.

المخاطر الداخلية

قد تتجسد المخاطر الداخلية في صورة أشخاص لديهم معلومات حول البيانات وأنظمة الكمبيوتر وممارسات الأمان مثل الموظفين أو الموردين أو المقاولين أو الشركاء. من أمثلة المخاطر الداخلية: إساءة استخدام الوصول المخول للتأثير سلبياً على مؤسستك.

التعرض غير المقصود

يحدث التعرض غير المقصود عندما يسمح الموظفون عن غير قصد بالوصول إلى مستخدمين غير مصرح لهم أو فيروسات. تساعد أدوات إدارة الهوية والوصول المؤسسات على التحكم في الأشياء التي يمكن للمستخدمين الوصول إليها وما لا يمكنهم الوصول إليها، وتساعد في تأمين الموارد الهامة لمؤسستك، مثل: التطبيقات والملفات والبيانات.

التصيد الاحتيالي

يشير التصيد الاحتيالي إلى عملية إرسال رسائل بريد إلكتروني احتيالية باسم شركات حسنة السمعة أو مصادر موثوقة أخرى. تهدف هجمات التصيد الاحتيالي إلى سرقة أو إتلاف البيانات الحساسة عن طريق خداع الأشخاص للكشف عن البيانات الشخصية مثل كلمات المرور وأرقام بطاقات الائتمان. كما يمكنهم استهداف شخص واحد أو فريق أو قسم أو شركة بأكملها.

برامج الفدية الضارة

برامج الفدية الضارة هي نوع من البرامج الضارة التي تشمل مخاطرها تدمير أو منع الوصول إلى البيانات أو الأنظمة الهامة حتى يتم دفع فدية. أصبح من الصعب منع برامج الفدية الضارة بشرية الإدارة المستهدفة للمؤسسات أو عكسها نظراً لاستغلال المهاجمين لإمكانات ذكائهم الجماعية لاكتساب إمكانية وصول إلى شبكة المؤسسة.

تفادي فقدان البيانات

تصنيف ومراقبة البيانات الحساسة

تؤدي معرفة نوعية بياناتك وكيفية استخدامها عبر أصولك الرقمية إلى مساعدة مؤسستك على تحديد الوصول غير المخول إلى البيانات والمساعدة في حمايتها من الاستخدام السيئ. تشير عملية التصنيف إلى تطبيق قواعد لتحديد البيانات الحساسة والحفاظ على توافق استراتيجية أمان البيانات.

اكتشاف وحظر النشاط المريب

يمكنك تخصيص حل تفادي فقدان البيانات لفحص جميع البيانات المتدفقة عبر شبكتك ومنع النقل من الشبكة عن طريق البريد الإلكتروني، أو عن طريق نسخها على محركات أقراص USB، أو بأي وسيلة أخرى.

أتمتة عملية تصنيف البيانات

يعمل التصنيف التلقائي على جمع معلومات مثل وقت إنشاء مستند ومكان تخزينه وكيفية مشاركته لتحسين جودة عملية تصنيف البيانات في مؤسستك. يستخدم حل تفادي فقدان البيانات هذه المعلومات لفرض نهج تفادي فقدان البيانات الخاص بك والذي يساعدك على منع مشاركة البيانات الحساسة مع المستخدمين غير المعتمدين.

الحفاظ على التوافق التنظيمي

يجب أن تلتزم كل مؤسسة بلوائح وقوانين ومعايير حماية البيانات مثل قانون نقل التأمين الطبي ومسؤوليته (HIPAA) وقانون ساربانيس - أوكسلي (SOX) وقانون إدارة أمن المعلومات الفيدرالي (FISMA). يمنحك حل تفادي فقدان البيانات إمكانات إعداد التقارير التي تحتاجها لإتمام عمليات تدقيق التوافق، والتي قد تتضمن أيضاً توفير خطة استبقاء بيانات وبرنامج تدريبي لموظفيك.

مراقبة عمليات الوصول إلى البيانات وكيفية استخدامها

لمنع التهديدات من التغلغل في بيئتك، ستحتاج إلى مراقبة وصول الأشخاص إلى البيانات، وتحديد هويتهم، وماهية تلك البيانات، والغرض من هذا الوصول. يمكنك منع عمليات الاحتيال وتسريبات البيانات الداخلية عن طريق إدارة الهويات الرقمية للموظفين والموردين والمتعاقدين والشركاء عبر الشبكة والتطبيقات والأجهزة. يعد التحكم في الوصول استناداً إلى الدور أحد صور تقييد الوصول ومنحه فقط للأشخاص الذين يحتاجون إليه لإنجاز مهامهم.

تحسين الرؤية والتحكم

يمنحك حل تفادي فقدان البيانات نطاق رؤية وافر للبيانات الحساسة داخل مؤسستك ويساعدك على رؤية الأشخاص الذين قد يرسلونها إلى أشخاص غير مصرح لهم بذلك. فور أن تحدد نطاق المشكلات المحتملة والفعلية، سيكون بمقدورك إجراء المزيد من التخصيصات لتحليل البيانات والمحتوى وتعزيز الجهود المبذولة لتفادي فقدان البيانات والارتقاء بتدابير الأمان عبر الإنترنت.

تهديدات مزود الخدمة

اختراق البيانات
انتهاك البيانات من خلال الوصول إلى الهوية
واجهات التطبيقات غير آمنة
سرقة الحسابات

اختيار مزود الخدمات السحابية

مكان تخزين البيانات

إنّ معرفة كيف يتعامل مزوّد السحابة مع البيانات وإدارتها شيءٌ أساسيّ، ويُعدُّ صميم أنظمة الإدارة السحابية الجيدة. من المهم التحقق من أن بياناتك محفوظة في مركز بيانات حديث ومُجهّز بأفضل الأنظمة والتقنيات المتطوّرة. من المهم أيضًا معرفة ما إن كان مزود الخدمات السحابية لديه مراكز بيانات احتياطية.

عمليات النسخ الاحتياطي

يُعدُّ النسخ الاحتياطي السحابي أحد العناصر الحاسمة لنظام إدارة سحابي فعال ووظيفة الحوسبة السحابية ككل. كعمل تجاري، إذا حُذفت بياناتك أو أُتلِفَت أو إذا غَدَت ضحيةً لبرامج الفدية أو أي نوع من الاختراقات، فإن أفضل حل هو استعادة نسخة احتياطية حديثة منها.

اختيار مزود الخدمات السحابية

مستوى المرونة

غالبًا ما يُشار إلى أنّ إحدى المزايا الرئيسية للحوسبة السحابية هي القدرة على إضافة سعة وخدمات حسب الحاجة؛ لأنّ الحوسبة السحابية تعتمد على مبدأ الدفع مقابل الاستخدام بشكلٍ أساسي.

اتفاقيات مستوى الخدمة (SLAs)

اتفاقية مستوى الخدمة SLAهي وعد واتفاقية تُلزم مُقدّم الخدمة السحابية بتقديم مستوى معين من الخدمة، يمكن أن يتعلق بأي شيء من وقت التشغيل والنسخ الاحتياطي والاستعادة وأي شيء آخر.

مستويات الأمان

من أهم القضايا الرئيسية في الحوسبة السحابية هي أمن المعلومات، وحقيقة أنّ مقدار التحكّم يصبح أقل في البيانات المخزنة في السحابة؛ يجعل خدمات الحوسبة السحابية محفوفةً بالمخاطر على الأغلب.

الحصول على شهادات دولية وعالمية

معيار ISO 27017، وCSA STAR، وISO 27032، وISO/IEC27001، وضوابط الأمن السيبراني للحوسبة السحابية (CCC-1-2020)التي طوّرتها الهيئة الوطنية للأمن السيبراني في المملكة.

مهددات السحابة في القانون

https://uncitral.un.org/ar/content/%E2%80%8F%D9%85%D9%84%D8%AD%D9%88%D8%B8%D8%A7%D8%AA-%D8%A8%D8%B4%D8%A3%D9%86-%D8%A7%D9%84%D9%85%D8%B3%D8%A7%D8%A6%D9%84-%D8%A7%D9%84%D8%B1%D8%A6%D9%8A%D8%B3%D9%8A%D8%A9-%D8%A7%D9%84%D9%85%D8%AA%D8%B5%D9%84%D8%A9-%D8%A8%D8%B9%D9%82%D9%88%D8%AF-%D8%A7%D9%84%D8%AD%D9%88%D8%B3%D8%A8%D8%A9-%D8%A7%D9%84%D8%B3%D8%AD%D8%A7%D8%A8%D9%8A%D8%A9-%E2%80%8F

الافتراضية في الحوسبة
Visualization

الحوسبة الافتراضية هي تشغيل نسخة نظام حاسوب افتراضية في طبقة مستخرجة من العتاد hardwareالفعلي، ويشير المصطلح غالبًا إلى تشغيل عدة أنظمة تشغيل على الحاسوب في وقت واحد، حيث يبدو للتطبيقات التي تعمل على الجهاز الافتراضي virtualized machineأنها على جهاز مخصص لها،

مزايا الافتراضية

ستخدم الحوسبة الافتراضية لأسباب عدة، أكثرها شيوعًا بالنسبة لمستخدمي سطح المكتب هو تشغيل التطبيقات المخصصة لنظام تشغيل آخر غير النظام المثبت على حواسيبهم، دون الحاجة إلى تبديل أجهزة الحاسوب أو إعادة تشغيل نظام مختلف، أما بالنسبة لمسؤولي الخوادم، فهي توفر لهم القدرة على تشغيل أنظمة تشغيل مختلفة أيضًا، بالإضافة إلى طريقة لتقسيم نظام كبير إلى أجزاء أصغر، مما يسمح باستخدام أكثر كفاءةً للخادم من قبل عدد من المستخدمين المختلفين أو تطبيقات ذات متطلبات مختلفة، كما تسمح بالعزل، وحماية البرامج التي تعمل داخل الجهاز الافتراضي من العمليات التي تحدث في جهاز افتراضي آخر على نفس المضيف.

الجهاز الافتراضي

virtual machine

الجهاز الافتراضي هو المحاكي المكافئ لنظام الحاسوب الذي يعمل على نظام آخر، ويمكنه الوصول إلى أي عدد من الموارد، مثل القدرة على المعالجة computing power، وكذلك الوصول المحدود إلى وحدة المعالجة المركزية والذاكرة في الجهاز المضيف، كما يمكنه استخدام واحد أو أكثر من أجهزة أقراص التخزين المادية أو الافتراضية، والوصول إلى واجهة شبكة افتراضية أو حقيقية، بالإضافة إلى أي أجهزة، مثل بطاقات الفيديو أو أجهزة USB، أو أي عتاد آخر مشترك مع الجهاز الافتراضي، ويشار إلى تخزين الجهاز الافتراضي على قرص افتراضي باسم صورة قرص disk image، وقد تحتوي على ملفات تشغيل الجهاز الافتراضي، أو على أي متطلبات محددة للتخزين.

ما الفرق بين الحوسبة السحابية والمحاكاة الافتراضية؟

ليست الحوسبة السحابية والمحاكاة الافتراضية شيء واحد. على الرغم من الخلط بين المفاهيم في بعض الأحيان بينهما، إلا أن الحوسبة السحابية والمحاكاة الافتراضية منهجيان متميزان للحوسبة، وكلهما مرتبطان ببعضهما بعضًا. توظف المؤسسات كلًا منهما لتوفير المرونة وقابلية التطوير عبر أقسام تقنية المعلومات لديها—الحوسبة السحابية لزيادة إمكانية الوصول إلى كل من التطبيقات وقواعد البيانات الداخلية والخارجية والمحاكاة الافتراضية لتقليل الأجهزة المادية.

يمكن أن تكون المحاكاة الافتراضية جزءًا من إعداد الحوسبة السحابية، لكن الحوسبة السحابية لا تتضمن بالضرورة المحاكاة الافتراضية.

كيف تعمل الهندسة الاجتماعية؟

في هجوم الهندسة الاجتماعية التقليدي، سيتواصل المجرم الإلكتروني مع الضحية المنشودة بزعم أنه من مؤسسة موثوقة. وفي بعض الحالات، سينتحل حتى شخصية أحد الأفراد الذين تعرفهم الضحية جيدًا.

وإذا انطلت الحيلة (صدّقت الضحية أن المعتدي نفس الشخصية التي يزعمها)، فسيشجع المعتدي الضحية على اتخاذ إجراء إضافي. قد يتمثل هذا الإجراء في إفشاء معلومات حساسة مثل كلمات مرور، أو تاريخ الميلاد، أو تفاصيل الحساب البنكي. أو قد يشجع المعتدي الضحية على زيارة موقع إلكتروني يحتوي على برمجيات ضارة مثبتة تستطيع في خلل لحاسوب الضحية. وفي أسوأ السيناريوهات، قد يستحوذ الموقع الإلكتروني على معلومات حسّاسة من الجهاز أو يتحكم في الجهاز بشكل كامل.

لماذا تعتبر الهندسة الاجتماعي خطرة للغاية؟

يتمثل أحد أكبر مخاطر الهندسة الاجتماعية في أنه ليس ضروري أن تنجح الهجمات ضد الجميع: فبإمكان ضحية واحدة مخدوعة أن توفر معلومات كافية لشن هجوم من الممكن أن يؤثر على مؤسسة بأسرها.

كيف أحمي نفسي ومؤسستي ضد الهندسة الاجتماعية؟

في الوقت الذي تختبر فيه الهجمات النفسية قوة أفضل أنظمة الأمان، يمكن للشركات الحد من مخاطر الهندسة الاجتماعية من خلال التدريب على التوعية.

- إدارة كلمات المرور
- المصادقة متعددة العوامل
- تأمين البريد الإلكتروني بدفاعات مكافحة التصيد الاحتيالي

أنواع هجمات الهندسة الاجتماعية

التصيد الاحتيالي

تُعد عمليات التصيد الاحتيالي أكثر أنواع هجمات الهندسة الاجتماعية شيوعًا. فهي عادة تأخذ شكل بريد إلكتروني يبدو كما لو كان من مصدر شرعي. وسيحاول المهاجمون أحيانًا إجبار الضحية على إعطائهم معلومات البطاقات الائتمانية أو غيرها من البيانات الشخصية.

مثال: تتخذ حملات التصيد الاحتيالي هذه شكل بريد إلكتروني مزيف يدّعي أنه من شركة Microsoft. يحتوي هذا البريد الإلكتروني على طلب لتسجيل دخول المستخدم وإعادة تعيين كلمة المرور الخاصة به لأنه لم يسجل الدخول إلى حسابه مؤخرًا، أو يدّعي أن هناك مشكلة في الحساب بحاجة إلى عنايته. ويكون عنوان URL مضمنًا في البريد الإلكتروني، ما يشجّع المستخدم على النقر فوقه ومعالجة المشكلة.

هجمات ثقب الريّ (Watering hole)

هجمات ثقب الريّ عبارة عن نوع شديد الاستهداف من الهندسة الاجتماعية. سينصب المهاجم فخًا باختراق موقع إلكتروني اعتادت مجموعة معيّنة من الأشخاص على زيارته، بدلًا من استهداف تلك المجموعة مباشرة. ومثالًا على ذلك المواقع الإلكترونية المتخصصة التي يزورها مرارًا موظفون في قطاع بعينه مثل قطاع الطاقة، أو قطاع الخدمة العامة. الجناة الذين يقفون وراء هجوم ثُقب الري باختراق الموقع الإلكتروني بهدف القبض على فرد من تلك المجموعة المستهدفة. ومن المحتمل أن ينفذوا هجمات أخرى بمجرد أن يخترقوا جهاز هذا الفرد أو يحصلون على بياناته.

هجمات اختراق البريد الإلكتروني للعمل

تُعد هجمات اختراق البريد الإلكتروني للعمل (BEC) شكلًا من أشكال الاحتيال عبر البريد الإلكتروني، حيث يدّعي المهاجم أنه أحد كبار المديرين التنفيذين ويحاول خداع المستلم لينفذ مهام عمله، لغرض غير قانوني، مثل إرسال حوالات مالية إليه.

الهندسة الاجتماعية المادية

عند الحديث عن الأمن السيبراني، نحن بحاجة إلى الحديث أيضًا عن الجوانب المادية لحماية البيانات والأصول. يتعرّض بعض الأشخاص في مؤسستك - مثل موظفي مكتب المساعدة، وموظفي الاستقبال، والموظفين دائمي السفر - لخطر هجمات الهندسة الاجتماعية المادية أكثر من غيرهم، والتي تحدث لهم بصفة شخصية.

وينبغي على مؤسستك أن يكون لديها ضوابط أمنية مادية فعّالة مثل سجلات الزوار، ومتطلبات المرافقة، وعمليات التحقق من الخلفية الحياتية للشخص. وقد يستفيد الموظفون الذين يشغلن مناصب أكثر عرضة لخطر هجمات الهندسة الاجتماعية من التدريب المتخصص للحماية من الهجمات المادية للهندسة الاجتماعية.

الاصطياد عبر USB

يبدو الاصطياد عبر USBغير واقعي بعض الشيء، ولكنه يحدث أكثر مما قد تظن. فما يحدث في الأساس هو أن المجرمين الإلكترونيين ينصّبون برمجيات ضارة على أقراص USBويتركونها في مواقع استراتيجية، آملين أن يعثر عليها أحد ما ويصلها بالنظام الإلكتروني لشركة ما، وبالتالي يطلق العنان لأكواد ضارة في مؤسسته دون قصد.

معهد العراب العالي للتدريب

مراجعة سريعة

تهديدات السحابة الافتراضية الهندسة الاجتماعية

2023

النهاية

سؤال و إجابة

1- من تهديدات البنية التحتية

A. DDOS

B. البرامج الضارة

C. الاثنان

2- تشغيل نسخة نظام حاسوب افتراضية في طبقة مستخرجة من العتاد

A. الحوسبة الافتراضية

B. البرمجيات الخبيثة

C. الاثنان

Policies and Compliance
السياسات والامتثال

تجدر الإشارة إليه هو أن أمان الحوسبة السحابية لا يقتصر فقط على تأمين البيئة التقنية ضد التهديدات الداخلية أو الخارجية (أي المتسللين) ولكنه يؤمن أيضًا الشركة ضد مخاطر التراجع أو التكاليف أو انتهاكات الامتثال بسبب سوء التخطيط أو الافتقار إلى سياسات التحكم، أو الموقع المناسب.

أحد عيوب سياسة الحوسبة السحابية هو حقيقة أن العديد من الخدمات السحابية تتم محاسبتها لكل وحدة مع مرور الوقت.

على سبيل المثال؛ تعد وحدة المعالجة المركزية (CPU) قيد التشغيل/الدقيقة أو سعة التخزين جيجابايت/اليوم من عوامل الفوترة الشائعة.

business continuity policies

أحد أكبر التحديات التي تواجه الشركات الحديثة هو كيفية الحفاظ على استمرارية الأعمال في مواجهة لحظات الأزمات. يرتبط هذا ارتباطًا وثيقًا بالتعافي الفني من الكوارث، ولكنه يمكن أن يتضمن أيضًا سياسات تتعلق بفقدان البيانات بسبب خطأ بشري

تنقسم الى :

RTO: مقدار الوقت من إعلان الكارثة إلى وقت عودة النظام إلى الإنترنت

RPO: مقدار فقدان البيانات بعد الفشل

Backups vs. Disaster Recovery

تصميم النسخ الاحتياطية لحماية البيانات في وقت واحد، ولاستعادة الأجزاء الفردية من البيانات في حالة الحذف أو الفساد.

تصميم التعافي من الكوارث لحماية التطبيقات بأكملها من انقطاع الخدمة على نطاق واسع. وعلى الرغم من التشابه الكبير بينهما، إلا أن أهدافهما مختلفة والسياسات المحيطة بهما مختلفة جدًا أيضًا.

السجلات Logging

يعد إجراء مراجعة السجل أحد أهم جوانب تأمين أي نظام، بما في ذلك الأنظمة الموجودة في السحابة العامة. يمكن أن تشير السجلات إلى مشكلات تتعلق بالتطبيقات، أو مشكلات التكوين، أو فشل الأجهزة أو البرامج، أو الخروقات الأمنية.

هناك عدد من التطبيقات المتاحة التي تسمح بهذا النوع من مراجعة السجل. يتوفر الكثير منها كجزء من مجموعة تطبيقات موفر الخدمة السحابية. أحد الأمثلة على ذلك هو Cloudwatch من أمازون

أنواع ال log

system logs, **billing logs**, access logs, and configuration logs, Firewall and network access logs

Billing and Access Reports

تعد مراقبة تقارير الفوترة السحابية الخاصة بك أمرًا مهمًا، ليس فقط من الناحية المالية ولكن أيضًا من الناحية الأمنية. يمكن أن يؤدي الوصول غير المصرح به إلى تقارير فواتير عميل السحابة إلى تزويد خصم محتمل بمعلومات

توفر AWS Amazon web Services أداة تسجيل شاملة لذلك باستخدام CloudTrail.

http://docs.aws.amazon.com/awscloudtrail/latest/userguide/awscloudtrail-ug.pdf

Network Firewall Logs

من المحتمل أن تكون سجلات جدار الحماية هي أكثر سجلات الأمان المتاحة شهرةً كما أنها مفيدة للغاية في اكتشاف عمليات التطفل. عندما تنظر إلى هذه السجلات، لا يمكنك فقط معرفة الجهاز الذي يتصل، ولكن أيضًا إذا تم تمكين تعيين المستخدم والمستخدمين المسؤولين عن حركة المرور. قد يشير سجل جدار الحماية القياسي إلى الجهاز المصدر، والمستخدم المصدر، وعنوان الوجهة، بالإضافة إلى نوع حركة المرور، إذا كانت مسموحة أم لا، ومقدار حركة المرور التي تم تمريرها.

http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html

Cloudwatch

هو نظام مراقبة وتسجيل مضمن للبيئات المستندة إلى AWS. إنه قادر على مشاهدة كل شيء بدءًا من الأجهزة الافتراضية 2EC، إلى قواعد البيانات من نظام DBaaS الخاص بهم، إلى السجلات والتنبيهات الداخلية التي تم إنشاؤها بواسطة تطبيقات وخدمات العملاء.

يعد Cloudwatch مثالًا جيدًا لتطبيق التسجيل المستند إلى الموفر للبيئات السحابية العامة. لدى Microsoft منتج مكافئ يسمى "Azure Monitor" والذي يعمل بشكل مشابه جدًا في نظامها الأساسي.

دى Cloudwatch العديد من الطرق المختلفة للوصول إلى البيانات التي تخزنها وتعالجها. يمكن إعداده لتنبيه المستخدم تلقائيًا عند تشغيل أحداث معينة، ويمكن الوصول إليه من خلال بوابة وحدة التحكم على موقعه على الويب، أو يمكن حتى تضمينه في البرامج النصية والتطبيقات المخصصة من خلال واجهة برمجة التطبيقات المتوفرة.

Amazon security services

خدمات امازون الامنية

Amazon WAF (web application firewall)

1- VPC(virtual private cloud)

تعادل شبكة vlan في الشبكات التقليدية

إدارة حركه المرور وفقا لقواعد العميل

2- penetration test

EC2 RDS AURORA Lambda

3- Amazon inspector

4- Amazon shield

AWS Key Management Service

Amazon WAF (web application firewall)

جدار حماية تطبيقات الويب (WAF) هو نوع خاص من جدار الحماية مصمم لحماية مواقع الويب والتحكم فيها، خاصة تلك الموجودة على الإنترنت. في حين أنه يمكن تكوين جدار الحماية للأغراض العامة للقيام بمعظم (أو كل) نفس الأشياء التي يقوم بها WAF مخصص، إلا أن WAF سيكون دائمًا أسهل في التكوين والإدارة والتحكم. بالإضافة إلى ذلك، غالبًا ما يتم تحديث WAFs بقواعد جديدة ضد التهديدات الجديدة الخاصة بمواقع الويب. يعد نشر WAF أمرًا بسيطًا مثل تنشيط الجهاز واختيار القواعد التي سيتم تنفيذها. ما عليك سوى تحديد نوع حركة المرور المسموح بها وأيها يجب حظره.

Amazon inspector

ذا كان من المرغوب فيه إجراء فحص أمني بواسطة أمازون، فإن أمازون لديها خدمة تسمى Inspector. هذه الخدمة عبارة عن فحص تلقائي للثغرات الأمنية والأمان يكتشف الانحرافات عن أفضل الممارسات، ويمكن اكتشاف ثغرات أمنية في التطبيقات

عبارة عن خدمة لإدارة الثغرات الأمنية تلقائيًا تفحص باستمرار أعباء أعمال AWSلضمان عدم وجود أي ثغرات أمنية في البرامج

Amazon shield

تعد هجمات DDOSشائعة جدًا في الشبكات الحديثة. لأسباب تتراوح بين التخريب المحض وتخريب الشركات، إلى الاعتداءات ذات الدوافع السياسية، ستواجه العديد من الشركات حادث رفض الخدمة في مرحلة ما. يساعد AWS Shieldعلى حماية عملاء Amazonمن تأثير هجمات DDOS. لها شكلان، قياسي ومتقدم.

يتم تضمين AWS Shield Standardبدون رسوم إضافية ويحمي من هجمات DDOSالمعروفة من الطبقة 3 و4. يعد AWS Shieldجزءًا من "الحزمة" القياسية التي يتلقاها كل مشترك وتكون دائمًا قيد التشغيل لمراقبة موارد Amazon.

بالإضافة إلى الرسوم السنوية، تُفرض على AWS Shield Advancedرسوم إضافية ورسوم نقل البيانات. وهو متوفر باشتراك لمدة عام واحد، ويحمي من عدد كبير من الهجمات ويتضمن عددًا من مزايا الخدمة، بما في ذلك تحليل ما بعد الهجوم، وتخفيف الهجمات المخصصة، والقدرة على الإبلاغ عن إحصائيات DDOSإلى نظام التسجيل. ويشمل أيضًا استخدامات WAF، دون رسوم إضافية

AWS Key Management Service ادارة مفاتيح خدمات امازون السحابية

خدمة إدارة المفاتيح عبارة عن مستودع كامل المواصفات لمفاتيح التشفير. فهو يسمح للمستخدمين بإيداع مفاتيح التشفير الخاصة بهم في منطقة مركزية وآمنة ثم الوصول إليها من خلال واجهة برمجة تطبيقات معينة. يؤدي هذا إلى زيادة الأمان الإجمالي من خلال منع فقدان مفتاح التشفير، وكذلك من خلال السماح بالاستخدام السهل لمفاتيح متعددة لبيانات مختلفة، بدلاً من نفس المفتاح لتطبيقات متعددة

تعد هجمات .....شائعة جدًا في الشبكات الحديثة:

- **fishing**
- **DDOS**

هذه الخدمة عبارة عن فحص تلقائي للثغرات الأمنية:

- **Amazon inspector**
- **DDOs**

يعد الامتثال مدخلاً جديدًا نسبيًا في مجال أمن المعلومات. مع ظهور المزيد والمزيد من خروقات البيانات للعامة، أصبحت الشركات مهتمة جدًا باستخدام المنصات التي تساعدها على تقديم خدمات متوافقة مع الأمان.

يعد HIPPA (لمعلومات الرعاية الصحية) مثالًا شائعًا جدًا للإطار القانوني للامتثال لأمن المعلومات.

لدى AWS العديد من المنتجات والخدمات المبنية على موضوعات الامتثال، وأحدها AWS Artifact. مع Artifact، تتوفر جميع تقارير الامتثال الخاصة بأمازون لمستخدميها، مما يسمح بالوصول السريع والسهل إليها عند الحاجة.

يمكن بعد ذلك استخدام هذه التقارير عند تدقيق العميل للتأكد من حماية جميع البيانات الحساسة وأن البيئة متوافقة مع القوانين واللوائح المناسبة.

AWS Cloud Directory

أحد منتجات إدارة الهوية الخاصة بـ AWS هو Cloud Directory. يعد Cloud Directory منتجًا محسّنًا جديدًا نسبيًا ومتعدد التسلسلات الهرمية لإدارة الدليل لكل شيء بدءًا من المستخدمين والمجموعات وحتى الأجهزة والسياسات.

تم تصميم Cloud Directory للمطورين الذين يحتاجون إلى دليل مرن وواسع النطاق للتطبيقات التي تتطلب عددًا كبيرًا (بالملايين) من الكائنات.

مثال : IOT (internet of things) انترنت الأشياء

لديها العديد من الميزات الأساسية الرئيسية:

- Directories الدلائل
- Schemas المخططات
- Facets الأوجه
- Objects أشياء
- Attributes صفات
- Hierarchies التسلسلات الهرمية
- Policies سياسات

- **What is a Directory?**

يحدد الدليل نطاق مخزن البيانات (مثل جدول في Amazon DynamoDB)، ويعزله تمامًا عن جميع الدلائل الأخرى في الخدمة. كما أنه يحدد نطاق المعاملة ونطاق الاستعلام وما شابه.

What is a Schema?

يحدد المخطط الجوانب والسمات والقيود المسموح بها داخل الدليل. وهذا يشمل تحديد:

- واحد أو أكثر من أنواع الأوجه التي يمكن تضمينها في الدليل (مثل الشخص أو Organization_Person).
- السمات المطلوبة أو المسموح بها على أنواع مختلفة من الأوجه.
- القيود (مثل أنواع البيانات البدائية المطلوبة أو الفريدة مثل الأعداد الصحيحة والسلسلة وغيرها).

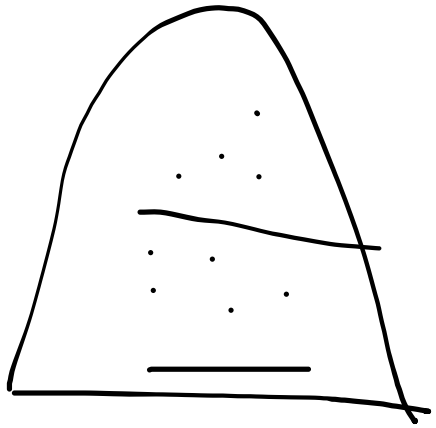
What is an Object?

يمثل الكائن كيان بيانات منظم في الدليل. الغرض من الكائن الموجود في الدليل هو التقاط بيانات تعريف حول كيان مادي أو منطقي، عادةً لغرض اكتشاف المعلومات وإنفاذ السياسات. على سبيل المثال، يعد المستخدمون والأجهزة والتطبيقات جميعها أنواعًا من الكائنات. يتم التعبير عن معلومات بنية الكائن ونوعه باستخدام مجموعة من الجوانب.

What is an Attribute?

السمة هي وحدة محددة من قبل المستخدم من البيانات التعريفية المرتبطة بكائن ما. على سبيل المثال، يمكن أن يحتوي كائن المستخدم على سمة تسمى عنوان البريد الإلكتروني. ترتبط السمات دائمًا بالكائن.

What is a Hierarchy?



التسلسل الهرمي هو طريقة عرض يتم فيها تنظيم المجموعات والكائنات في علاقات بين الأصل والفرع مشابهة لنظام الملفات حيث تحتوي المجلدات على ملفات ومجلدات فرعية أسفلها. يدعم **Amazon Cloud Directory** تنظيم الكائنات في تسلسلات هرمية متعددة.

What is a Policy?

السياسة هي نوع كائن متخصص له سمات تحدد نوع السياسة ووثيقة السياسة. يمكن ربط السياسة بالكائنات أو بجذر التسلسل الهرمي. افتراضيًا، ترث الكائنات السياسات من أصولها.

لا يزال تطوير التطبيقات التي تستخدم Cloud Directory مستمرًا والعديد من التطبيقات إما تستخدمه بالفعل أو ستستخدمه قريبًا. تستخدمه أمازون داخليًا لـ Cognito، حيث يقوم المستخدمون بالتسجيل/تسجيل الدخول إلى مواقع العملاء والمنظمات (تطبيقات إدارة المستخدم القائمة على السياسة). تستخدمه التطبيقات الخارجية الأخرى لأي تطبيق يتطلب تسلسلات هرمية كبيرة للبيانات. تقدم أمازون أمثلة على تطبيقات الموارد البشرية وتطبيقات إدارة التعلم

API Levels

EVENTUAL

توفر الوصول الأسرع إلى البيانات. يأتي هذا الوصول ذو زمن الاستجابة المنخفض مع إمكانية وجود بيانات غير متناسقة. لا يمثل هذا مصدر قلق خطير، ولكن بالنسبة للآخرين، قد يكون مدمرًا.

SERIALIZABLE

توفر واجهات برمجة التطبيقات هذه مستويات أداء أقل بكثير، ولكنها تضمن قراءة جميع البيانات وكتابتها بالترتيب الذي تم به إجراء استدعاءات واجهة برمجة التطبيقات.

يتم تسعير AWS Cloud Directory بناءً على عاملين، حجم الدليل وعدد استدعاءات واجهة برمجة التطبيقات (API) إليه. الحجم واضح ومباشر، وهو عبارة عن رسوم شهرية تعتمد على عدد الجيجابايت التي يستخدمها الدليل، مع تقريبها إلى الأعلى.

يتم تجميع استدعاءات واجهة برمجة التطبيقات (API) في مجموعتين:
الأول يتم دفعه بسعر أقل بكثير من الاثنين الآخرين، بعامل أقل من 10 مرات. تبلغ التكلفة حاليًا 0.0049 دولارًا أمريكيًا/10000 استدعاءات واجهة برمجة التطبيقات (API) لقراءات EVENTUALو0.0053 دولارًا أمريكيًا/1000 استدعاءات واجهة برمجة التطبيقات (APIلاستدعاءات SERIALIZABLE APIوالكتابة عنها.

Number of users	10
Multiply by number of calls per minute per user	5
Total Calls per minute	**50**
Multiply by number of minutes in an hour	60
Total Calls per hour	**3,000**
Multiply by number of hours per day	12
Total Calls per day	**36,000**
Multiply by number of work days	5
Total Calls per week	**180,000**
Multiply by number of weeks per month	4
Total number of Calls per month (720,000 to 780,000 depending on number of working days within month; we will use average of 750,000)	**750,000**
Divide by 10,000	10000
Total Calls per week	**75**
Multiply by rate per 10,000	$ 0.0049
Total cost per month	**$ 0.37**

Number of users		100
Multiply by number of calls per minute per user		5
Total Calls per minute		**500**
Multiply by number of minutes in an hour		60
Total Calls per hour		**30,000**
Multiply by number of hours per day		12
Total Calls per day		**360,000**
Multiply by number of work days		5
Total Calls per week		**1,800,000**
Multiply by number of weeks per month		4
Total number of Calls per month (7,200,000 to 7,800,000 depending on number of working days within month; we will use average of 7,500,000)		**7,500,000**
Divide by 1000		1000
SERIALIZABLE billing quantity		**7,500**
Multiply by rate per 10000 for SERIALIZABLE	$	0.0053
Total cost per month	**$**	**39.75**

Number of users		5
Multiply by number of calls per second per user		100
Total Calls per second		**500**
Multiply by number of seconds in an hour		3,600
Total Calls per hour		**1,800,000**
Multiply by number of hours per day		24
Total Calls per day		**43,200,000**
Multiply by number of work days		7
Total Calls per week		**302,400,000**
Divide by 1000		1000
SERIALIZABLE billing quantity		**302,400**
Multiply by rate per 1000 for SERIALIZABLE	$	0.0053
Total cost per month	**$**	**1,602.72**

AWS Inspector

يسمح Amazon Inspector بالفحص الأمني التلقائي لتطبيقات AWS المستضاف. من خلال مقارنة تكوين التطبيق وإصداراته وإعداداته مع أفضل الممارسات الموثقة ونقاط الضعف المعروفة، يمكن للمفتش بعد ذلك تقديم تقرير يسلط الضوء على أي اختلافات، بترتيب الأولوية. يُستخدم Inspector بشكل شائع مع أنظمة التشغيل.

يتم بعد ذلك إجراء عمليات التفتيش وفقًا لجدول زمني محدد، كل بضع دقائق في كثير من الأحيان. بشكل عام، سيقتصر المسح على مرة واحدة يوميًا على الأكثر، ما لم تكن هناك حاجة إلى إجراءات أمنية مشددة. بمجرد الانتهاء من التفتيش، سيتم إنشاء النتيجة .

إذا قمت بإجراء 10 تقييمات مقابل 10 أجهزة أو تقييمًا واحدًا مقابل 100 جهاز، فستكون التكلفة الإجمالية هي نفسها. يبدأ معدل الفوترة هذا حاليًا عند 0.30 دولارًا أمريكيًا لكل تقييم، ولكنه ينخفض مع إجراء المزيد من التقييمات كل شهر.

Other AWS Compliance Applications

AWS Macie

نظام قائم على التعلم الآلي ("الذكاء الاصطناعي") يحدد ويلاحظ المعلومات التي قد تخضع لمتطلبات الامتثال. وقد يشمل ذلك معلومات التعريف الشخصية، أو أرقام بطاقات الائتمان، أو أنواع أخرى من المعلومات الحساسة.

تقوم Macieبالإبلاغ عن الوصول المشبوه أو البيانات المخترقة أو حتى عمليات نقل البيانات الكبيرة. ويمكن بعد ذلك التصرف بناءً على كل هذه العوامل لمنع حدوث تسوية، أو تصنيف وتحديد خروقات البيانات.

AWS Artifact

Artifact هو المستودع المركزي لجميع تقارير الامتثال واتفاقيات الخدمة المُدارة الخاصة بأمازون. يتيح ذلك للعملاء الحصول على "مركز شامل" لجميع الوثائق اللازمة لاعتماد بيئات AWS الخاصة بهم للبنية التحتية للامتثال الخاصة بهم.

https://aws.amazon.com/artifact/faq/

اتفاقية مستوى الخدمة (SLA)

هي عقد للاستعانة بمصادر خارجية يُبرم مع مُورّد تكنولوجيا ويحدد مستوى الخدمة الذي يَعِد المُزود بتقديمه للعميل. وتحدد الاتفاقية مقاييس مثل وقت التشغيل، ووقت التسليم، ووقت الاستجابة، ووقت الحل. وتوضح اتفاقية مستوى الخدمة أيضًا بالتفصيل مسار العمل المتبع في حالة عدم تلبية المتطلبات، مثل تقديم الدعم الإضافي أو خصومات على التسعير. وعادةً ما يُبرم الاتفاق على اتفاقية مستوى الخدمة بين العميل ومُزود الخدمة، إلا أن وحدات الأعمال داخل الشركة نفسها يمكنها أيضًا إبرام اتفاقيات مستوى خدمة بعضها مع بعض.

https://aws.amazon.com/ar/what-is/service-level-agreement/

معهد العراب العالي للتدريب

2023

مراجعة سريعة

الحوسبة السحابية ونماذج خدماتها واستخدامها ومزاياها

النهاية

سؤال و إجابة

1- توفير موارد تقنية المعلومات حسب الطلب عبر الإنترنت مع تسعير التكلفة حسب الاستخدام.

A. التشفير
B. الحوسبة السحابية
C. الافتراضية

2- من مزايا الحوسبة السحابية.

A. تقليل الإنفاق
B. زيادة فرص العمل
C. محدودية الخدمة

معهد العراب العالي للتدريب

شكرا