

عما في الموبايل موجود في الشركة محو

ما هي الحوسبة السحابية؟

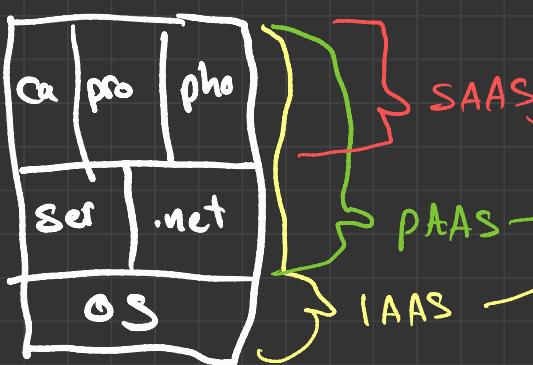
تعريف الحوسبة السحابية؟

هي تكنولوجيا تطبيق تتمد على نقل المعلومات ومساحة التخزين الخاصة بالحاسوب إلى ما يسمى السحابة (Cloud) وهي جهاز خارج يتم الوصول إليه عن طريق الانترنت. تتلورن برامج تكنولوجيا المعلومات من منتهيات إلى خدمات.

هو هو خرج كل معنى يكون المستبعد.

أنواع الحوسبة السحابية

	Private Cloud	Infrastructure as a Service	Platform as a Service	Software as a Service
Customer	Applications Data OS Virtualization Servers Storage Networking	Applications Data OS Virtualization Servers Storage Networking	Applications Data OS Virtualization Servers Storage Networking	Applications Data OS Virtualization Servers Storage Networking
Provider				



Cloud.digitalocean.com

مع اد openstack جيل تعلم Cloud معاصر حديث

ار اس ار opencloud

Private Cloud

ماهي ؟ Private Cloud

هي سحابة تعمل ببنية تحتية خاصة لمنظمة واحدة فقط وكل ما هو ضمن هذه المنظمة.

المميزات:

- التحكم الكامل، المرونة، التحكم بقوانين الاتصال بالسحابة، التحكم بخصوصيات المستخدمين
- مثل: السحابة الداخلية لتجهيز العمل



Public Cloud

ماهي ؟ Public Cloud

السحابة العامة هي نوع من الحوسبة التي يوفر فيها مزود الخدمة الخدمات للمستخدمين عبر الانترنت.

المميزات:

- تدعم جميع المستخدمين، تدعم الاتصال بالانترنت، المرونة
- مثل: Amazon و SaaS, Paas, IaaS (Google و Microsoft)

Community Cloud

ماهي ؟ Community Cloud

يعد هذا النوع من السحابة بشكل تعاوني يتم فيه مشاركة البنية التحتية بين العديد من المؤسسات من المجتمع معين له اهتمامات مشتركة (الأمان ، القوانين...) سواء تمت إدارتها داخلياً أو بواسطة طرف ثالث واستئامتها داخلياً أو خارجياً.

المميزات: بناء مجتمع، مشاركة الملفات والبيانات، التخصيص

مثل: salesforce

Hybrid Cloud

ماهي ؟ Hybrid Cloud

يمكن للمنطقة استخدام السحابة بالتقسيم بين البنية التحتية السحابية العامة والخاصة، تبقى البيانات الحساسة داخل السحابة الخاصة حيث يمكن الحفاظ على معايير الأمان العالمية، يتم تنفيذ العمليات التي لا تستخدم البيانات الحساسة في السحابة العامة.

المميزات: السداد حسب الاستخدام، خدمات الحماية عالية، تسمح بتطوير واختبار التطبيقات داخل السحابة الخاصة، المرونة والتخصيص

مثل: Amazon Web Services (AWS) or Microsoft Azure



الامان اكبر المشكل التي تواجه مستخدمي السحابة.

عدم امكانية الوصول الى معلوماتك عند وجود خطأ في السحابة.

ضعف بنود الاتفاقية بين الموقع والمستخدم بما يخص حماية الحقوق.

التطبيقات لا تعمل جيئها على السحابة.

لا تعمل بشكل جيد مع الاتصالات ذات السرعة المنخفضة.

يمكن فقد وضياع البيانات المخزنة.



Log in!

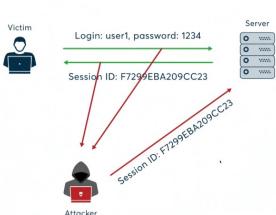
Username: _____
Password: _____

الهندسة الاجتماعية هي طريقة غير قانونية وتziel على التعامل مع مشاعر الإنسان، وغالباً يدخل المخufff كسر خطوات العملية المعاينة.

يمكن للمهتم أن يستهدف خدمات مقدم خدمة السحابة بواسطة استعادة كلمة العبور أو التواصل مع موظفين المعرفة لإاستعادة كلمة المرور.

طرق أخرى لإستعادة كلمة المرور وهي (تخزين كلمات العبور، البرمجيات البينية لسرقة المدخلات في لوحة المفاتيح، إرسال رسالة وهمية للخدعana Phishing Emails

هجوم الهندسة الاجتماعية نتيجة لغافر المستخدمين بعض المعلومات الهامة مثل البيانات الشخصية، خطأ العمل، بيانات الموظفين، سرقة الهوية



اشتمام الغرم في الشبكة يتطلب لمراقبة إدخال البيانات داخل الشبكة والجزء الذي ترسل وتستقبل بين جهاز من أجهزة الحوسبة السحابية

المهاجم يستخدم اشتمام حزم البيانات لانتقاض البيانات الحساسة مثل كلمات المرور، كوكفيز، الخلايا، الخادم الأخرى الخاصة بآدوات الحماية

يهاجم المخترق خوام SQL المشغلة لقواعد بيانات التطبيقات المصاوبة بالثباتات

يتم الاختراق بنجاح عندما يستخدم التطبيق مدخلات ثابتة في قواعد بيانات SQL

يكتب المخترق كود خبيث تم إنشاءه بآخر مخصصة إلى قائدة بيانات SQL ليتمكن من الدخول الغير مصرح به للأدلة البيانات

يمكن المهاجم التعديل على محتوى قواعد البيانات، استبدال بيانات حساسة عن بعد بغير الأدلة الأخرى في النظام، بالإضافة إلى التحكم الكامل في خوام الويب

Man-in-the-Cloud Attack هو نسخة متطرفة من Man-in-the-Middle Attack

Man-in-the-Middle Attack عبارة عن هجوم يستخدم لاستغلال عدد من الأدلة بين طرفين

بينما هجوم Man-in-the-Cloud هو استخدام ملفات الخدمات مثل Google Drive, Dropbox، وخدمات المعرفة والوصول على التحكم عن بعد.

الخدع المستخدمة من المهاجم تثبت كود خبيث بواسطة الضغينة دون علمه

المهاجم يقوم بسرقة الدخول على ملفات المخزن.



- تسريب وفقدان البيانات
- عدم الأمان في الوجهات وخدمات APIs
- المشكل التقني
- المخاطر غير معروفة لملف الشخص
- التصريح والبنية التحتية غير كافية
- فقدان معلم الاتصال للتلقيح والحماية
- العمليات غير الموثوقة لموفدين الدليل
- الخلل الغير مصرح به للسحابة



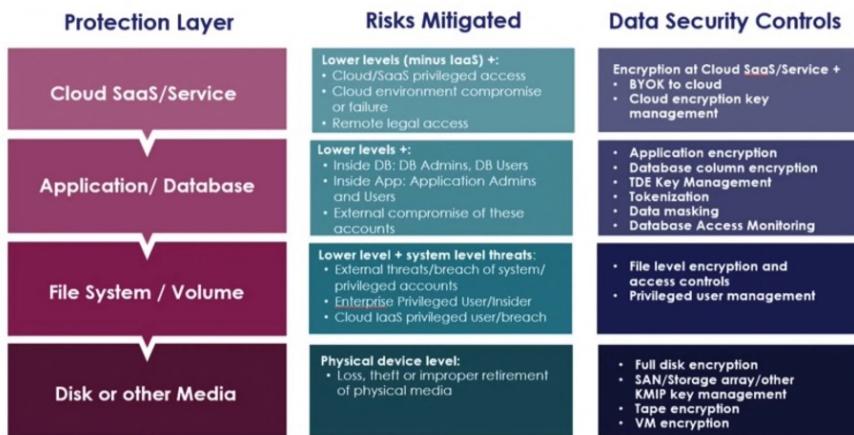
- اختراق العائد
- اختراق التسويق والنشر
- اختفاء الأجزاء بين الأنظمة
- التعذر على إزاحة الشبكة
- اختفاء إدارة الشبكة
- هجوم التفوق
- هجوم الأداة التحليلية
- الكوارث الطبيعية



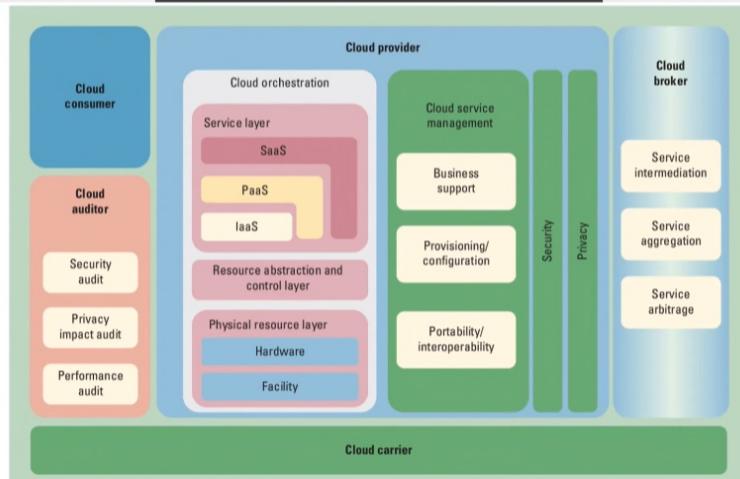
- مخاطر الحقوق والرخص
- فقدان ملائق التشفير
- المخاطر من تغيير القوانين
- سرقة الأجهزة
- مخاطر إيقاف خدمات السحابة المقاضية
- فقدان النسخ الاحتياطية

- يعمل هجوم DoS في مقدم خدمة السحابة، وقد تمنع المستخدمين من الدخول إلى خدماتهم
- (بطيءات كبيرة وFlooding the server) • مهددة للأنظمة المتأثرة
- Passing malicious input الأدلة الخبيثة في الخوام لتقطيع النظيف • (Entering wrong passwords) المخترق يمكنه العبور ما يؤدي لإيقاف الحاسب عن استخدام المستخدمين





NIST cloud computing recommendation





- كلمات المرور
 - الجدار الناري - الاستئضافة
 - التحقق قبل الدخول - Authentication
 - حماية السورس كود (الملفات المصدرية)
 - سلامة الملفات

ادارة الصلاحيات



- استخدام تحقق ثانوي أو أكثر
 - الوصول المشفر إلى النظام
 - التأكد من صلاحيات كل مستخدم
 - rule of least privilege
 - المتابعة الدورية للمستخدمين

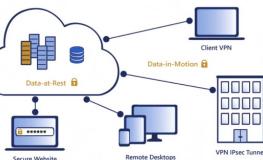


تشفیر البيانات



- استخدام تشفير Standard
استخدام أكثر من طبقة تشفيرية
التأكد من حذف المفاتيح التشفير بشكل سليم
الدخول الصحيح والأمن للمحاكاة
الفصل الأول بين السحبات

الاتصال الآمن



- استخدام نظام مثمر للدخول إلى السحابة - **VPN**
 - استخدام نظام MDM للدخول بالتطبيقات

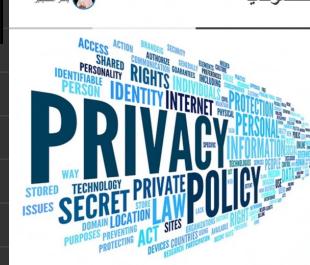
سحلات النشاطات داخلاً، السحابة



- # Security Operations Centre (SOC)

Security Information and Event Management (SIEM)

سياسة الخصوصية



- قوانين الــmicrosoft المتواجدة فيها الحوسبيّة
 - قوانين المشرعة
 - من المسؤول عن الحماية؟
 - هل يمكن تكملة البيانات من متزود الى متزود؟
 - من مسؤول عن صلاحيات الدخول والادارة
 - في حالة وجود اختراق من المسؤول
 - في حالة انتهاء الدقائق او الاستهداوه
 - الرخص و الاشتراكات تلك ملک من؟

