تکنولوژی Shielded Virtual Machines datacenter security چیست؟

گردآوری شده توسط جامعه گیک‌های کامپیوتر

همانطور که از Shielded Virtual Machines datacenter security نامش پیداست یکی از تکنولوژی های امنیتی شرکت مایکروسافت برای زیرساخت مجازی خود موسوم به **Hyper-V** است.

ایده پشت این تکنولوژی محافظت از **Workload**ها است. به خصوصی یا عمومی در مقابل **Malicious Administrator** عنوان مثال **Rouge Administrator** یک **VM** را در می تواند یک زیرساخت مجازی شما بر روی یک حافظه کپی کرده و از سازمان شما خارج نماید، سپس توسط استفاده از ابزارهای هک یا **Hacking Tools** قادر به بازیابی اطلاعات از **VM** مورد نظر خواهد بود.

جهت جلوگیری از چنین مشکلاتی و دسترسی ادمین های واقعی از جمله **Backup admin**ها، **Storage admin**ها، **Virtualization admin** ها و.. این راهکار پیشنهاد می شود.

ماشین های مجازی که به این روش محافظت می شوند اصطلاحاً نامیده می شوند و شما می توانید از راهکار مزبور در **Shielded VM** **2019** و همینطور در ویندوز سرور جدید **2016** و **2012** ویندوز سرورهای **Shielded VM**ها را به **Gen-2 VM** استفاده نموده و ها تبدیل نمایید.

Shielded VM

Microsoft Shielded V ها از تکنولوژی **BitLocker Encryption** **VM file**ها به **administrator** جهت قفل کردن دسترسی سایر **vDisk**ها را رمزنگاری می کند).استفاده می کند(

tenantها در **administrator** به این طریق سایر **Shielded Virtual** های دیگر قادر به **VM** دسترسی به های دیگر نیستند. بنابراین راهکار یکی از بهترین راهکارهای امنیتی **Machines datacenter security**

مایکروسافت به **Multi-Tenancy**ها در محیط های **VM**جهت دسترسی به شمار می رود.

> ***در معماری Multi-Tenancy، چندین کاربر می‌توانند از یک نمونه (Single Instance) از اپلیکیشن نرم‌افزاری استفاده کنند. یعنی این نمونه روی سرور اجرا می‌شود و به چندین کاربر سرویس می‌دهد. هر کاربر را یک Tenant می‌نامیم. می‌توان به Tenantها امکان تغییر و شخصی‌سازی بخشی از اپلیکیشن را داد مثلا رنگ رابط کاربری یا قوانین کسب‌وکار، اما آنها نمی‌توانند کدهای اپلیکیشن را شخصی‌سازی کنند.***

نیز می **Windows Azure** از جمله **Microsoft Cloud**در محیط های **Azure**گزینه‌توانید از این راهکار امنیتی استفاده نمایید و در رابط کاربری ها تعبیه شده است.**Shielded VM**ای برای ایجاد

Microsoft مبتنی بر تکنولوژی ای به نام **هاShielded VM**در واقع ایجاد می شوند، که یک مرز ایزوله**Guarded Fabric Technology** شما ایجاد کرده تا جاییکه میزبان نمی تواند به **VM**شده قوی بین میزبان و شما دسترسی داشته باشد.**یVM Data**

> ***[آشنایی با مدل OSI و لایه های آن]***

بطور کلی دارای 4 کامپوننت است:**Guarded Fabric**معماری

1. **Code Integrity Component**
2. **Virtual Security Mode**
3. **Trusted Platform Module V2**
4. **Host Guardian Service**

که بر روی یک **HGS** یا به اختصار **Host Guardian Service**سرویس راه‌**Attestation Service**ها و **Security-key** اجرا شده و **cluster** با سه **cluster**اضافه و از آنها محافظت می کند که معمولاً شامل یک می باشد.**node**

چیست و چرا محافظت از Shielding Data آن ضروری است؟

که اصطلاحاً **Shielding Data File**یک پرونده داده محافظ یا نیز نامیده می شود ،**PDK file** یا به اختصار **Provisioning Data File** است که شامل اطلاعات پیکربندی**VM** یا **Tenant**فایل رمزنگاری شده یک مورد نظر می باشد که شامل موارد زیر است:**VM**مهم

1. **Administrator Password**
2. **RDP Certificates and other identity-related certificates**
3. **Domain join credentials**
4. **....**

نویسنده: ریحانه غفوریان