CYBER
ANGELS

Cybersecurity

8 temi di sicurezza informatica che ti aiuteranno a capire come proteggere meglio il tuo business

Contenuti

CYBER ANGELS

Cos'è un ransomware?

Il software antivirus era lo strumento di fatto per proteggere i sistemi informatici. Ora è chiamato anti-malware per riflettere la natura mutevole degli attacchi dannosi; gli hacker hanno cambiato le loro motivazioni, passando semplicemente dal causare danni al fare soldi lanciando attacchi.

Cosa significa veramente ransomware? In che modo è diverso da un virus?

I virus spesso cercavano di eliminare i dati per creare disagi agli utenti. Il ransomware invece blocca i tuoi file (crittografandoli), quindi richiede un pagamento per ottenere le chiavi necessarie per sbloccarli, di solito in una forma di criptovaluta come Bitcoin. Il ransomware è stato un grande ostacolo per le aziende di tutte le dimensioni, ma le piccole imprese rappresentano un obiettivo particolarmente interessante per gli hacker.

Le piccole imprese si ritrovano nel mirino di attacchi ransomware a causa del minor numero di risorse dedicate alla gestione IT. Le organizzazioni più grandi hanno maggiori probabilità di disporre di difese o strategie di ripristino per combattere gli attacchi ransomware, mentre le organizzazioni più piccole hanno maggiori probabilità di dover pagare il riscatto.

Come posso proteggere la mia azienda dai ransomware?

Allora cosa deve fare una piccola impresa? Hai a disposizione diverse semplici opzioni sia per prevenire un attacco ransomware che per ripristinare i tuoi sistemi se la tua azienda venisse attaccata.

Software anti-malware

Un software anti-malware come TrendMicro o Windows Defender può aiutare a prevenire il verificarsi di attacchi ransomware. Il ransomware viene spesso attivato quando un dipendente esplora un sito Web sospetto o apre un allegato di posta elettronica. Lo strumento anti-malware può bloccare il ransomware prima che possa crittografare i tuoi file. Assicurati che il software scelto includa la protezione da ransomware e venga aggiornato regolarmente.

Archiviazione centralizzata

Lo storage centralizzato può ridurre l'impatto di una singola macchina compromessa. L'utilizzo di strumenti come Dropbox o Google Drive, invece di archiviare file sui dischi rigidi dell'utente, può aiutare a limitare la diffusione del ransomware. Questi servizi spesso includono protezioni ransomware integrate, quindi anche se il laptop di un utente viene reso inutilizzabile, i file sono al sicuro.

Backup

I backup, se eseguiti regolarmente, possono aiutarti a recuperare i file rubati senza dover pagare il riscatto. Strumenti integrati come Time Machine di Apple o servizi online come Carbonite e Backblaze possono fornire una copia di backup sicura di tutti i tuoi file. Se sei vittima del ransomware, puoi semplicemente eseguire il ripristino dal backup, riducendo al minimo la quantità di dati persi.

Cryptojacking: cos'è e come prevenirlo

Il cryptomining trasforma le risorse di un computer in criptovalute, ossia denaro elettronico che si basa sui principi della crittografia matematica complessa. Inizialmente, chiunque fosse in possesso di un computer aveva la possibilità di generare criptovalute, ma la questione è rapidamente diventata più complessa. Oggi, la maggior parte dei miner utilizza potenti computer appositamente costruiti che generano criptovalute continuamente. Presto le persone hanno iniziato a cercare nuovi modi per generare criptovalute ed è così che è nato il cryptojacking. Anziché pagare per un costoso computer di mining, gli hacker infettano computer normali e li utilizzano come rete per condurre i propri affari.

Cos'è il cryptojacking?

Il cryptojacking (anche chiamato cryptomining dannoso) è una minaccia online emergente, che si nasconde su un computer o dispositivo mobile e utilizza le risorse della macchina per "generare" tipi di denaro virtuale noti come criptovalute. Si tratta di una minaccia in via di espansione, in grado di infiltrarsi nei browser web e di compromettere ogni tipo di dispositivo, dai PC desktop ai laptop fino agli smartphone e perfino i server di rete.

La complessità dei calcoli necessari alla produzione di criptovaluta richiede molta potenza di elaborazione ed elettricità. A tal punto che anche i PC di alta gamma con un processore molto potente hanno problemi a soddisfare la richiesta.

Perché preoccuparsi del cryptojacking?

Il cryptojacking è una tecnica che sfrutta i dispositivi altrui (computer, smartphone, tablet o perfino server) senza che l'utente ne sia consapevole o dia il proprio consenso, per generare criptovalute in segreto a spese della vittima. Anziché costruire un computer per il cryptomining, gli hacker utilizzano il cryptojacking per rubare le risorse di elaborazione dai dispositivi delle loro vittime. Combinando tutte queste risorse, gli hacker sono in grado di competere con sofisticate operazioni di cryptomining senza gli elevati costi associati. Diversamente da altri tipi di malware, il cryptojacking non mira a bloccare la vittima - in realtà, è nell'interesse dell'aggressore mantenere attivi il più a lungo possibile i dispositivi infettati.
A cosa devo stare attento?

ESAURIMENTO DELLE RISORSE:
Se i tuoi dipendenti sono stati infettati da un software di cryptojacking noteranno problemi di prestazioni come app lente e durata della batteria decisamente e minore.

COSTI:
Tieni sotto controllo le bollette!È improbabile che le postazioni di lavoro dei dipendenti rappresentino un grande assorbimento di energia, ma il costo aggiuntivo per un carico di lavoro più elevato non dovrebbe essere ignorato.

Come posso difendermi dal cryptojacking?

La maggior parte dei pacchetti software antivirus includono la protezione contro il cryptojacking, quindi installare e mantenere aggiornati tali software è fondamentale. Per gli ambienti cloud, dovresti assicurarti di avere correttamente configurato i tuoi dispositivi per prevenire che gli hacker vi accedano (è un'azione molto tecnica, quindi assicurati di avere un team di ingegneri consapevole dei rischi e con le giuste capacità per gestirli). E infine, assicurati che il tuo help desk e supporto IT possano riconoscere i sintomi del cryptojacking e prendano le giuste contromisure per rimuovere questi software indesiderati dalla tua azienda.

Autenticazione multifattore

Qualsiasi informazione che il tuo business non condivide pubblicamente ha bisogno di controlli di accesso - l'esempio più noto è username e password. Ma è facile rubare o indovinare una password, cosa possiamo fare allora per assicurarci che solo i nostri fidati impiegati riescano ad accedere correttamente? L'autenticazione a 2 fattori (2FA) e l'autenticazione multifattore sono la soluzione al tuo problema.

Chi sei tu? Sei davvero chi dici di essere?

L'autenticazione è un modo sofisticato di sicurezza che permette a un utente di provare la propria identità. Nel mondo reale, usiamo un documento d'identità con foto come una patente di guida o un passaporto; nel mondo digitale vengono spesso utilizzate password e PIN. Le password, però, possono essere facilmente rubate o scoperte. Quindi, per una maggiore sicurezza, è importante utilizzare più fattori di autenticazione.
Esistono te diversi modi per confermare la propria identità:

1

Una cosa SAI

Password, codici pin, frasi d'accesso, e risposte alle domande di sicurezza.

2

Una cosa HAI

Token o badge di sicurezza, uno smartphone con un app di autenticazione (come Google Authenticator o Duo), messaggi di conferma, e oggetti fisici di sicurezza come una chiavetta usb.

3

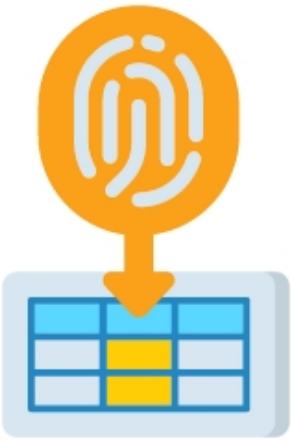
Una cosa SEI

Impronte digitali, riconoscimento vocale e misure biometriche come geometria della mano o del viso.

ATTENZIONE!

Due forme di autenticazione della stessa categoria (es. password e pin) non contano come autenticazione multifattore - devi sceglierne due da diverse categorie affinché funzioni.

Perché l'autenticazione a più fattori è importante?



l furto delle password è diventato incredibilmente facile (e redditizio) per gli hacker. Gli strumenti e le tecnologie per l'individuazione delle password sono diventati più sofisticati e automatizzati, tanto che spesso non richiedono neanche il "password-guessing" manuale. L'uso di più fattori rende più di difficile per un hacker accedere ai nostri dati, perché deve rubare più informazioni. Supponiamo che un utente finisca in una trappola di phishing e riveli il proprio nome utente e password. Con queste informazioni, l'aggressore ha ora tutto ciò di cui ha bisogno per accedere al sistema dell'utente. Ma se si dispone dell'autenticazione a più fattori, questo attacco fallirà. L'aggressore ha la password dell'utente, ma a meno che non abbia anche rubato fisicamente il suo smartphone (che visualizza un codice di accesso tramite un'app), non può accedere ai suoi sistemi.

Come posso implementare l'autenticazione a più fattori nella mia azienda?

Sembra un argomento molto tecnico, ma abilitare l'autenticazione a più fattori è generalmente piuttosto semplice. Strumenti di collaborazione popolari come GSuite e Office365 includono nelle impostazioni l'autenticazione a due fattori, che può essere utilizzata per accedere ad altri siti (ad esempio, puoi accedere a Slack utilizzando il tuo account GSuite protetto con 2FA). Molte app per smartphone popolari possono essere configurate per richiedere dati biometrici come l'impronta digitale o il riconoscimento facciale, aggiungendo un secondo fattore di autenticazione oltre a un PIN. Per ambienti più complessi, esistono strumenti come Duo per fornire soluzioni 2FA o MFA per sistemi che non supportano in modo nativo tali funzionalità.

Cos'è la crittografia?

La crittografia è un sistema pensato per rendere illeggibile un messaggio a chi non possiede la soluzione per decodificarlo. La crittografia in informatica, può essere definita un sistema che tramite l'utilizzo di un algoritmo matematico agisce su una sequenza di caratteri, trasformandola. Tale trasformazione si basa sul valore di una chiave segreta, ovvero il parametro dell'algoritmo di cifratura/decifratura. Proprio la segretezza di questa chiave rappresenta il sigillo di sicurezza di ogni siastema crittografico.

Diversi tipi di crittografia

In base al genere di chiave utilizzato, è possibile suddividere in due tipologie questo sistema di crittografia informatica: cifratura simmetrica e asimmetrica; quando è presente una chiave singola si parla di crittografia a chiave simmetrica o a chiave segreta (la chiave del mittente e quella del destinatario sono la stessa), quando invece vi sono due chiavi di cifratura distinte si parla di crittografia a chiave asimmetrica o a chiave pubblica (la chiave di cifratura è pubblica, mentre la chiave di decifratura è privata).

Esempi di crittografia

AES (-128;-256)

AES sta per Advanced Encryption Standard, l'attuale funzione crittografica approvata dal governo federale degli Stati Uniti e uno standard largamente adottato. Fornisce una crittografia altamente sicura ed è stato ampiamente esaminato e testato. I numeri 128 e 256 si riferiscono alla lunghezza della chiave, che è composta da 0 e 1 (noti anche come bit). Più bit vengono utilizzati, più sicuri saranno i tuoi dati: una chiave a 256 bit è esponenzialmente più sicura di una chiave a 128 bit.

SSL/TLS

Si tratta di implementazioni della tecnologia di crittografia specifica per i dati inviati su una rete. SSL vuol dire "Secure Sockets Layer" (Livello di socket sicuri), una tecnologia standard che garantisce la sicurezza di una connessione a Internet e protegge i dati sensibili scambiati fra due sistemi impedendo ai criminali informatici di leggere e modificare le informazioni trasferite, che potrebbero comprendere anche dati personali.TLS (Transport Layer Security, sicurezza del livello di trasporto) è una versione aggiornata e più sicura di SSL.

HASH

L'hashing è una tecnica di crittografia che permette di proteggere i dati sostituendole con delle stringhe di testo casuali, usando un l'algoritmo di Hash per processare i dati e produce un valore univoco (per esempio se esegui una copia di un messaggio di posta elettronica tramite una funzione hash viene visualizzato "123456"). Dovrebbe essere impossibile per un aggressore ottenere il tuo valore hash e lavorare a ritroso per scoprire il valore originale, per questo viene chiamato univoco.

Gli hashes sono un buon modo fare confronti e assicurarsi che un messaggio non sia stato alterato: copia un email, la esegui con hash, e mandi sia il messaggio che l'hash al tuo destinatario. Il destinatario può eseguire il messaggio tramite una funzione hash e confrontare il valore che ha calcolato con il messaggio che hai inviato; se i due non corrispondono, significa che il messaggio che ha ricevuto non è autentico. Gli hash sono fondamentali per garantire che ciò che hai ricevuto sia uguale a ciò che qualcuno ti ha inviato. Gli hash sono spesso utilizzati per impedire l'esposizione di informazioni di identificazione personale (PII) quando si lavora con i dati dei clienti.

SALT

I salt vengono usati insieme agli hash per aggiungere complessità alla decrittazione delle delle password. Il "salt" non è altro che una stringa che viene apposta in testa o in coda alla password prima che ne venga calcolato l'hash.

La procedura quindi aumenta la difficoltà nell'individuazione della password a partire dal hash.

Il principale errore nell'implementazione della tecnica di "salting" è l'aggiunta di una stringa di "salt" unica per tutte le password. Le funzioni hash producono sempre lo stesso output con lo stesso input - questo significa che due utenti che hanno utilizzato "password" avranno la stessa password hash (questi utenti ovviamente hanno bisogno di una formazione sulla scelta di password migliori). Ciò rende più difficile per un utente malintenzionato indovinare una password e ottenere l'accesso ai dati rubati.

Cos'è il pentesting?

Sai come appare la tua attività a un potenziale aggressore? Se parcheggi la tua auto in una grande città, è probabile che tu dia un'occhiata in giro per assicurarti di non aver lasciato nulla di prezioso in bella vista.

Un penetration test (pen test) fa la stessa cosa, ma con le applicazioni web e le risorse IT della tua azienda

I pen test sono un'ottima pratica informatica

Un pen test viene condotto da un hacker etico, qualcuno che cerca di entrare nei sistemi informatici, ma con l'obiettivo di trovare e segnalare eventuali punti deboli riscontrati, piuttosto che sfruttarli. I pen test ti aiutano a individuare i punti deboli prima che lo faccia un utente malintenzionato e possono essere uno strumento fondamentale per proteggere i tuoi sistemi e dati.

Il pen test fornisce vantaggi di sicurezza sia proattivi che reattivi. Se hai progettato un'applicazione hai implementato corretti sistemi di sicurezza (ad esempio firewall, autenticazione a più fattori e sistemi di monitoraggio), il pen test può controllare che i controlli siano effettivamente attivi ed efficaci, o identificare punti deboli e configurazioni errate.

I pen test possono anche essere un meccanismo investigativo o reattivo. L'infrastruttura IT è in continua evoluzione e ciò che ieri era sicuro, oggi potrebbe presentare nuove vulnerabilità. Un pen test ti aiuta a identificare problemi come software obsoleti o impostazioni non sicure; con un po 'di fortuna, il tuo hacker etico lo troverà prima che uno non etico lo sfrutti!

Con che frequenza dovresti effettuare un pen test?

Lo sforzo costante di stare al passo con i malintenzionati può far sembrare che la sicurezza debba essere uno sforzo costante 365 giorni l'anno, ma devi capire che non puoi fare tutto in una volta. Trovare il momento giusto per eseguire un pen test è facile valutare i vantaggi di eseguirne uno rispetto al costo.

Per molte aziende un pen test è un evento annuale (soprattutto con requisiti normativi come PCI-DSS). Le aziende con una maggiore attenzione alla sicurezza possono utilizzare una società di pen testing esterna per il test annuale e utilizzare competenze interne per eseguire pen test più piccoli durante tutto l'anno per una maggiore sicurezza.

I test basati sul tempo hanno dei meriti, ma c'è un altro fattore che può guidare i pen test: il programma di rilascio. Questo approccio ha senso per le aziende il cui prodotto principale è il software (ad esempio, una piattaforma SaaS) e allinea i pen test con le principali modifiche al software. Ciò ha senso, poiché funzionalità nuove o modificate possono introdurre nuove vulnerabilità, quindi il programma

Vulnerabilità delle applicazioni: attacchi SQL Injection e XSS

Se la tua azienda fa affidamento su sistemi informativi (e quale azienda non lo fa attualmente?), dovresti considerare l'impatto delle vulnerabilità delle applicazioni. Non è necessario diventare un programmatore per capirle, ma sapere quali tipi di vulnerabilità esistono può aiutarti a mantenere la tua attività al sicuro.

Una serie di fattori contribuiscono alla vulnerabilità delle applicazioni, incluso il linguaggio di programmazione in cui è scritta la tua applicazione (persino Apple è entrata in acqua bollente quando un programmatore ha incollato accidentalmente una riga di codice due volte!). Poiché la tua azienda si basa su applicazioni che elaborano e archiviano dati, eventuali vulnerabilità in esse contenute possono essere sfruttate dagli hacker per rubare i tuoi dati. Questi tipi di attacchi includono:

Attacchi Injection

Attacchi injection, come SQL (pronunciato sequel) e Script Injections: in questo tipo di attacchi, gli hacker inviano un codice informatico inaspettato a un'app, con l'obiettivo di costringere l'app a eseguire quel codice e rubare informazioni.

Attacchi cross-site

Attacchi cross-site, come Cross Site Scripting (XSS) e Cross Site Request Forgery (XSRF): questi attacchi si basano sull'aggiunta di codice dannoso alle pagine web, con l'obiettivo di indurre il computer di una vittima a eseguire un'azione. Poiché la maggior parte delle app oggigiorno è basata sul Web, questa è una preoccupazione significativa.

Buffer Overflow

Questi attacchi sfruttano il modo in cui le applicazioni archiviano i dati in memoria. Abusando di questo, un hacker può accedere a dati che normalmente non dovrebbe essere esposti.

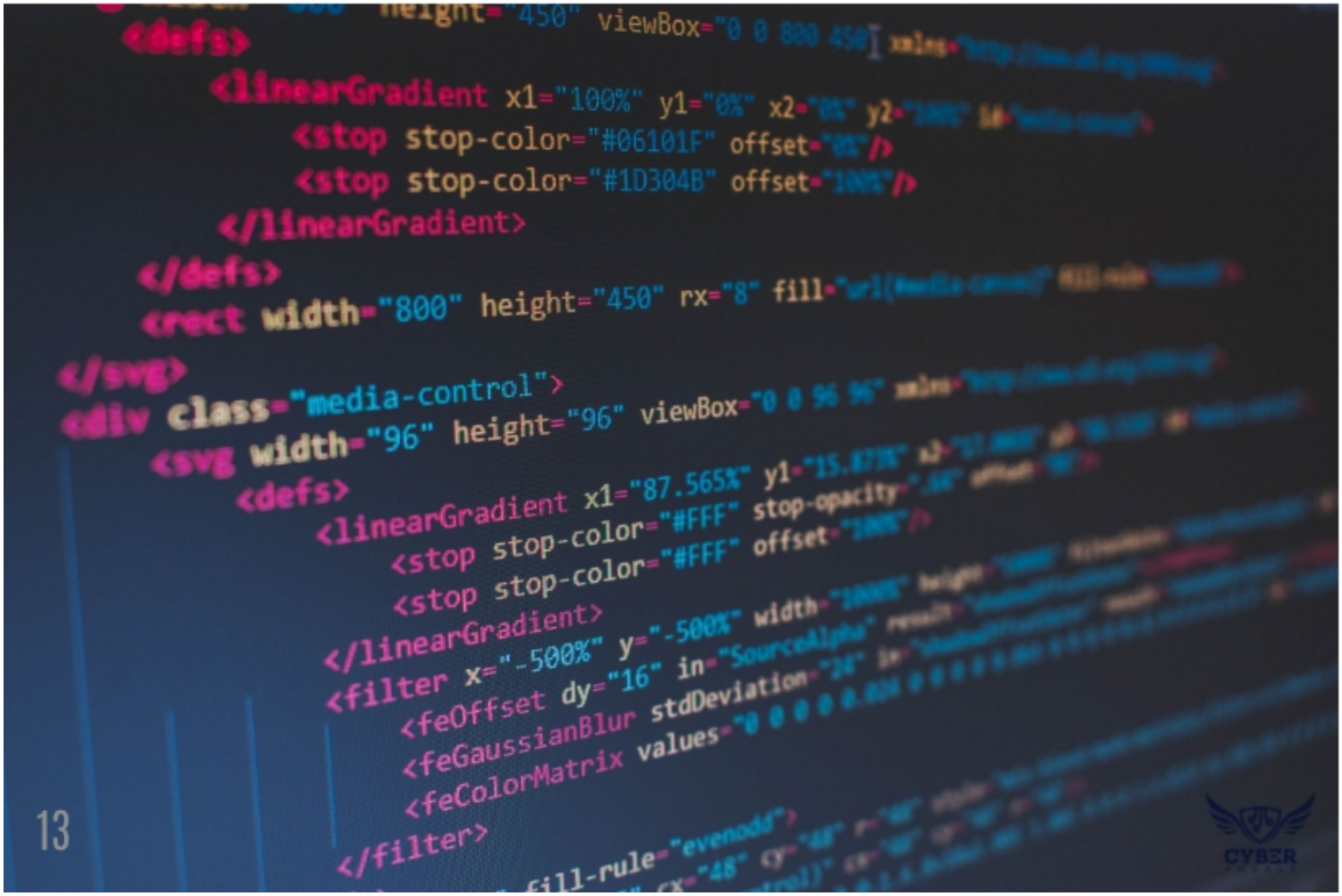
Come posso evitare questi attacchi?

Le applicazioni software sono scritte da persone che, come tutti purtroppo, possono commettere errori. È impossibile evitare completamente questi tipi di vulnerabilità, ma ci sono misure che puoi adottare per assicurarti che la tua azienda non si assuma rischi inutili quando utilizza varie applicazioni.

Per le applicazioni che crei tu stesso, una formazione adeguata del programmatore è fondamentale per prevenire le vulnerabilità delle applicazioni. I programmatori formati sulle pratiche di codifica del rischio possono evitarli, portando ad app con meno vulnerabilità. Pratiche come le revisioni CodePeer e gli strumenti di test che analizzano il codice alla ricerca di vulnerabilità possono anche aiutare a impedire gli errori in fase di produzione.

E se non se tu a progettare le tue app? L'acquisto di software di app commerciali (COTS) riduce lo sforzo necessario per far funzionare un sistema, ma non è privo di inconvenienti. Poiché non controlli il team che ha scritto il codice, non puoi garantire che siano state condotte una formazione adeguata o revisioni del codice. Se hai bisogno della garanzia che il tuo fornitore abbia intrapreso i passi corretti, cercane uno con una certificazione riconosciuta come ISO 9001 o 27001, che il fornitore può utilizzare per dimostrare di aver implementato pratiche di sviluppo sicure.

Sia per le app sviluppate internamente che per le app COTS, è importante implementare dei pen test e dei controlli delle vulnerabilità per identificare errori prima che vengano scoperti da altri; puoi affidare questa pratica esternamente o eseguire i test internamente.



Quanto è sicuro il cloud?

Il cloud computing ha aperto nuove possibilità per i proprietari di piccole imprese: puoi disporre delle stesse risorse di un'azienda della classifica Fortune 500, ma senza la necessità di un reparto IT. Solo perché hai questa capacità, tuttavia, non significa che puoi usarla senza prendere alcune precauzioni. In questo articolo, esploreremo alcune trappole di sicurezza comuni del cloud e i modi per evitarle.

Il vantaggio della specializzazione

I servizi cloud offrono numerosi vantaggi e sbloccano nuove opportunità di business, perché danno anche ai singoli imprenditori la possibilità di gestire un'infrastruttura di livello mondiale. Per le aziende più grandi, il cloud offre vantaggi finanziari chiave. Le economie di scala raggiunte dai fornitori si traducono in costi ridotti, pagamenti misurati pareggiano spese e ricavi, e i servizi cloud spostano i costi IT dal capitale alle spese operative, che offre vantaggi contabili favorevoli.

Cosa potrebbe andare storto?

Sei a rischio quasi dal momento in cui attivi un servizio cloud, più o meno allo stesso modo in cui sei a rischio dal momento in cui ti alzi dal letto ogni mattina. Ma non preoccuparti: proprio come alcune semplici precauzioni ti tengono al sicuro ogni giorno (ad esempio, accendere una luce in modo da non inciampare e cadere dalle scale), alcune precauzioni di base possono proteggere le tue connessioni cloud:

Archiviazione di dati e file:

Un'altra settimana, un'altra violazione dei dati a causa di un errore di configurazione [scegline una: bucket Amazon S3, Dropbox Folder, MongoDB]. Questi servizi forniscono funzionalità di condivisione e archiviazione di dati / file in linea, ma devono essere configurati correttamente.

ATTENZIONE! L'impostazione predefinita di tutto lo spazio di archiviazione deve essere "privato". La condivisione dovrebbe essere eseguita solo quando necessario anziché per impostazione predefinita, preferibilmente con un gruppo limitato piuttosto che pubblicamente. Se è necessario un ampio accesso pubblico, è necessario implementare la supervisione per garantire che i dati archiviati non siano sensibili (come le informazioni di una carta di credito).

Accesso remoto:

Il servizi cloud sono accessibili da qualsiasi luogo, il che è allo stesso tempo un punto di forza e di debolezza. La buona notizia è che puoi ricevere avvisi quando vedi posizioni di accesso sospette. Il tizio che accede alla tua posta dalla Russia è un hacker o uno dei tuoi dipendenti in vacanza?

ATTENZIONE! Abilita i controlli di accesso appropriati, come l'autenticazione a più fattori, per ridurre il rischio di attività dannose. Rivedi l'accesso dei dipendenti almeno una volta all'anno per assicurarti che i dipendenti abbiano ancora accesso solo alle risorse di cui hanno bisogno.

Backup e ripristino:

I servizi cloud sono stati progettati pensando all'alta disponibilità, ma la forza della rete di data center globale di AWS non si traduce automaticamente in un'app a prova di errore per la tua azienda.

ATTENZIONE! La tua architettura cloud deve usare correttamente le funzionalità di alta disponibilità. Tutti i fornitori di servizi cloud offrono un insieme complesso di opzioni per l'uptime come data center regionali e zone di disponibilità definite. Se non sei sicuro, assumi un consulente che ti aiuti a identificare le tue esigenze e a progettare una soluzione appropriata: ad esempio, devi utilizzare più regioni (più costose e più complesse) o più zone si adattano alle tue esigenze (meno complesse, ma più inclini a un'interruzione)?

La crittografia e i tuoi dati

Se non l'hai già fatto, puoi rispolverare la terminologia di crittografia di base nel nostro post Che cos'è la crittografia?. Dopo aver acquisito una solida conoscenza del vocabolario, è importante capire dove e come utilizzare al meglio la crittografia per mantenere la tua piccola impresa al sicuro.

L'importanza dell'autenticazione multifattore

Dove implementi la crittografia dipenderà dal tipo di attività che svolgi e dai sistemi che utilizzi. Le app molto esigenti (come un negozio online che elabora migliaia di transazioni al secondo) potrebbero non implementare la crittografia nel software applicativo, poiché ciò potrebbe rallentare notevolmente l'elaborazione. Invece, questa situazione potrebbe richiedere la crittografia tra i computer del cliente e i tuoi server.

Per lo meno, dovresti esaminare le app utilizzate dalla tua azienda e assicurarti che i dati siano protetti in due punti: in primo luogo, quando vengono archiviati, ad esempio i dati che risiedono sui laptop dei dipendenti o in un'applicazione cloud. Varie tecnologie di crittografia possono essere utilizzate per questi dati a riposo; molte recenti violazioni dei dati sono state causate da un accesso controllato in modo improprio allo storage cloud come Amazon S3 in cui erano archiviati i dati non crittografati. In secondo luogo, dovresti assicurarti che i dati siano adeguatamente protetti quando vengono spostati da un luogo a un altro, di solito su Internet. Tecnologie come TLS o una rete privata virtuale (VPN) possono aiutare a garantire che nessuno spii i tuoi dati mentre sono in movimento.

Come posso implementare l'autenticazione a più fattori nella mia azienda? Ci sono degli svantaggi?

Alcuni tipi di dati presentano problemi di crittografia specifici a causa dei requisiti normativi. Ad esempio: se la tua azienda accetta carte di credito, il Payment Card Industry (PCI) impone che i numeri di carta di credito vengano crittografati quando vengono memorizzati (quando i dati sono a riposo) e che qualsiasi transazione online venga crittografata con una versione specifica di TLS (quando i dati sono in movimento). Altri esempi di normative che potrebbero richiedere l'implementazione della crittografia includono HIPAA, una legge statunitense incentrata sui dati sanitari personali e il GDPR dell'UE, una legge incentrata sui diritti alla privacy dei singoli cittadini dell'UE per controllare l'uso dei propri dati personali. Entrambi richiedono adeguate garanzie quando si tratta rispettivamente di informazioni mediche e privacy; a seconda del tipo di attività che svolgi e del luogo in cui si trova, potresti dover implementare la crittografia per restare conforme alle norme vigenti.

La crittografia dei dati può rendere la vita leggermente più difficile, sebbene esistano molte soluzioni tecnologiche per ridurre al minimo le possibilità che qualcosa vada storto. La prima domanda da porsi prima di implementare la crittografia è se i dati da crittografare sono preziosi e quindi valgono il costo della crittografia. I tuoi materiali di marketing probabilmente non hanno bisogno di essere crittografati: persino Apple, l'azienda più segreta al mondo, è sopravvissuta alle violazioni dei dati di marketing. Ma se disponi di numeri di previdenza sociale o dati di carte di credito, la tua azienda deve adottare misure adeguate per proteggerli.

Il secondo potenziale svantaggio della crittografia è la perdita della chiave di accesso. Se crittografa i dati e poi perdi la chiave, hai perso l'accesso a quei dati! Le informazioni che devono essere conservate per un lungo periodo di tempo richiedono un sistema per archiviare in modo sicuro le chiavi. Se i tuoi dipendenti o clienti gestiscono le chiavi utilizzate nella tua crittografia, probabilmente vorrai fornire loro un modo per recuperarle in modo sicuro; non importa quanto le persone siano diligenti, dimenticheranno le cose di tanto in tanto!