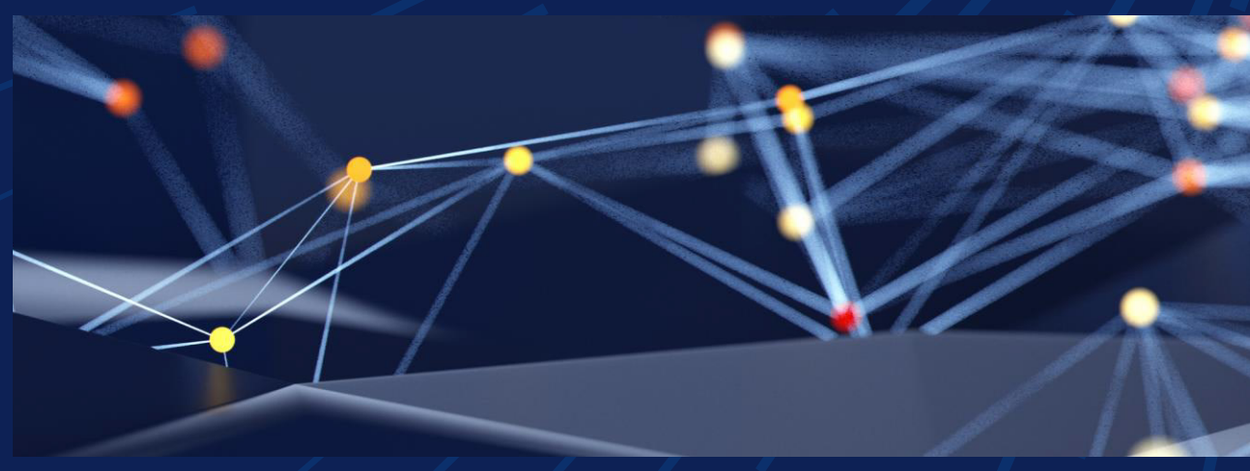
DELL Technologies

Il futuro della sicurezza informatica:

Adattarsi alla nuova era digitale



Mentre molti esperti di sicurezza informatica si concentrano completamente sulla prevenzione degli attacchi e sulla creazione dei piani di ripristino, occorre ricordare che l'intero ambiente di sicurezza è in continua evoluzione. Di conseguenza, è importante ragionare in prospettiva.

Guardando al futuro, emergono tre tematiche principali: la crittografia post-quantistica, la continua evoluzione del panorama giuridico e le minacce emergenti. Occorre pertanto attivarsi fin da ora, pianificando e implementando le soluzioni a mano a mano che sono disponibili.

L'alba della crittografia post-quantistica

L'elaborazione quantistica promette di rivoluzionare tutti i settori, offrendo una potenza di elaborazione straordinaria per risolvere problemi che vanno ben oltre la portata dei computer tradizionali. Tuttavia, questa potenza potrebbe anche rendere obsoleti i metodi crittografici attuali. Un computer quantistico sufficientemente avanzato potrebbe violate in pochi secondi algoritmi come RSA ed ECC, che oggi sono alla base di gran parte delle comunicazioni sicure. Questa minaccia incombente ha aumentato l'urgenza di ricorrere alla crittografia post-quantistica.

La crittografia post-quantistica (PQC) è incentrata sullo sviluppo di algoritmi crittografici che continueranno a garantire sicurezza anche nell'era dell'elaborazione quantistica. Il National Institute of Standards and Technology (NIST) ha riconosciuto questo rischio imminente e sta promuovendo la standardizzazione degli algoritmi resistenti agli attacchi dei computer quantistici.

La preparazione delle aziende a questa transizione non è negoziabile. L'adozione preventiva delle soluzioni PQC garantirà la sicurezza dei dati quando i malintenzionati avranno accesso alle funzionalità di elaborazione quantistica.

Come sottolinea Bobbie Stempfley, VP of Cybersecurity and Business Unit Security Officer di Dell, per avviare questo processo occorre concentrandosi su due aree chiave:

Identificazione e inventario di tutti i modelli di crittografia attualmente in uso.
Oltre a proteggere i dati archiviati, è necessario tenere conto anche dei data in-flight, come quelli utilizzati per la gestione delle chiavi, la firma del codice, l'identificazione dei dispositivi, l'accesso sicuro e la telemetria. Occorre creare un inventario completo e quindi stabilire una roadmap.

Analisi del profilo dei fornitori.
Oggi le aziende si rivolgono a migliaia di fornitori, pertanto devono prestare attenzione ai potenziali rischi provenienti da questi canali, assicurandosi che anche tali aziende si stiano preparando per il cambiamento.

Ma questo è solo il punto di partenza, che deve essere seguito da assessment dei rischi per l'identificazione dei sistemi vulnerabili, valutazione della possibilità di implementare modelli crittografici ibridi per garantire l'operatività durante la transizione e collaborazione con i vendor che stanno già studiando potenziali soluzioni per proteggersi dagli attacchi quantistici, ricordando che non ci sarà mai un singolo fornitore o una singola tecnologia capace di offrire una soluzione chiavi in mano.

Cambiamenti normativi in un mondo globalizzato

Il futuro della sicurezza informatica dipende anche in modo cruciale dall'evoluzione dell'ambiente giuridico. Le norme di oggi vanno ben oltre la conformità, e si stanno trasformando in un framework essenziale per instillare un senso di responsabilità, promuovere l'upgrade delle tecnologie e proteggere i cittadini in un mondo sempre più interconnesso e basato sui dati. Tuttavia, queste leggi si evolvono rapidamente e presentano differenze significative a seconda dell'area geografica, pertanto garantire la conformità diventa sempre più difficile.

Ciò premesso, queste normative non si limitano a prevedere sanzioni in caso di violazione, ma costituiscono un catalizzatore per il miglioramento delle pratiche di sicurezza informatica. Le aziende che allineano attivamente le policy ai requisiti di legge possono raggiungere nuovi livelli di affidabilità ed efficienza operativa. A tale scopo, è necessario istituire framework di governance flessibili, per adattarsi ai cambiamenti normativi quando necessario, condurre audit di conformità regolari e investire nella formazione dei dipendenti, in modo da gestire le informazioni sensibili conformemente agli standard più recenti.

Mentre i responsabili della sicurezza si preparano per la conformità, è importante assicurarsi che si esprimano in termini comprensibili e che le loro proposte vengano effettivamente capite. Troppo spesso gli esperti utilizzano un gergo tecnico che non viene compreso dai clienti, dalle autorità e dagli altri stakholder. Tuttavia, sono i professionisti che devono cercare di farsi comprendere e non gli ascoltatori che devono sforzarsi di capire quello che dicono.

DELL Technologies

> La transizione alla crittografia post-quantistica può essere paragonata allo spostamento di un'abitazione completamente arredata. Sarà certamente un problema complesso, e la vera sfida consisterà nel riuscire a non rompere nulla nel corso dell'operazione."
>
> ***Bobbie Stempfley***
> *VP of Cybersecurity and Business Unit Security Officer, Dell Technologies*

Evoluzione del panorama delle minacce (e delle difese)

L'intelligenza artificiale (AI) rivoluziona il business, aumenta la produttività e offre agli esseri umani nuove opportunità per esprimere il loro potenziale. Nel caso della sicurezza informatica, l'AI viene sfruttata sia dai malintenzionati che dalle persone responsabili di difenderci dai loro attacchi:

Malintenzionati: sfruttano l'AI per escogitare attacchi sempre più sofisticati, come messaggi di spear phishing e deepfake estremamente convincenti.

Difensori: usano l'AI per:
- Elaborare velocemente enormi quantità di dati di sicurezza.
- Assegnare le giuste priorità alle minacce.
- Aumentare le capacità di rilevamento e risposta.

Tuttavia, gli strumenti di sicurezza continueranno a migliorare solo grazie all'elaborazione del linguaggio naturale, che viene utilizzato dagli esperti di sicurezza per interfacciarsi in modo più diretto con i sistemi e offre a tali sistemi la possibilità di adottare misure di correzione proattiva della sicurezza informatica.

Oltre a sfruttare le funzionalità dell'AI, le aziende devono anche provvedere a tenere corsi di aggiornamento e adottare meccanismi difensivi al passo con i tempi. La formazione costituisce l'arma più efficace per proteggere i dipendenti dagli attacchi più sofisticati.

Eliminazione delle password

Le password non possono più essere considerate un metodo sicuro per gestire identità e accessi.

I tradizionali sistemi basati su password presentano vulnerabilità notevoli, che li rendono sempre più incapaci di rispondere alle esigenze di sicurezza informatica attuali. Vulnerabili al credential stuffing, al phishing e agli attacchi di forza bruta, molto spesso le password espongono le aziende a rischi evitabili. Queste vulnerabilità sono ulteriormente aggravate dai comportamenti inadeguati degli utenti, che tendono a riutilizzare le password o a creare password troppo deboli.

I metodi di autenticazione senza password, come il riconoscimento biometrico, i certificati e i token hardware, offrono un'alternativa più affidabile e sicura, eliminando intere categorie di minacce correlate alle password. Il passaggio ai sistemi senza password rappresenta una fase cruciale nell'evoluzione della gestione di identità e accessi, poiché consente di adottare misure di sicurezza capaci di rispondere a minacce informatiche sempre più sofisticate.

L'adozione di tecnologie senza password offre alche molti altri vantaggi, come la riduzione della superficie di attacco, il miglioramento dell'esperienza utente, tramite un accesso più rapido e trasparente, e la riduzione dei costi IT derivante dalla riduzione degli incidenti correlati alle password. L'utilizzo di metodi avanzati garantisce un profilo di sicurezza più efficace e aiuta le aziende a rispettare gli standard di legge. Il passaggio ai sistemi senza password non è solo una tendenza, ma una scelta necessaria per dare vita a un ecosistema digitale più sicuro ed efficiente, sia per le persone che per le aziende.

Conclusioni

Per la sicurezza informatica si prospetta un'era caratterizzata da trasformazioni rivoluzionarie, alimentata da fenomeni come l'elaborazione quantistica, normative in continua evoluzione e minacce sempre più sofisticate. Per tenere il passo, occorre adottare innovazioni come la crittografia post-quantistica, le difese basate sull'AI e l'autenticazione senza password. Concentrandosi su preparazione, collaborazione e investimenti strategici, è possibile creare un ambiente digitale più sicuro e resiliente. È il momento di agire.

Prodotti e soluzioni Dell utili allo scopo

Soluzione Dell consigliata	Descrizione
Servizi di consulenza per la sicurezza informatica	Indicazioni specialistiche utili per prepararsi all'evoluzione del panorama di minaccia, incluse le minacce attuali e quelle emergenti.
vCISO	Un CISO (Chief Information Security Officer) ed esperto di sicurezza informatica virtuale, che può aiutare le aziende a identificare e gestire il rischio, oltre che a prendere decisioni strategiche efficaci.

Scopri come affrontare alcune delle principali sfide della sicurezza informatica di oggi su **dell.com/cybersecuritymonth**