MelTechnologies

SOSARCHIVI
ASSOCIAZIONE PER LA TUTELA DEL PATRIMONIO ARCHIVISTICO

SALVAGUARDARE IL PATRIMONIO CULTURALE DALL'INNOVAZIONE DIGITALE

PREVENZIONE E PROTEZIONE DEI DATI DIGITALI ATTRAVERSO L'ADOZIONE DI MODELLI E PROCEDURE '' PROCEDURE '' **SECURITY ORIENTED**''

«LA MACCHINA TECNOLOGICAMENTE PIÙ EFFICIENTE CHE L'UOMO ABBIA MAI INVENTATO È IL LIBRO»

NORTHROP FRYE

La digitalizzazione degli archivi è diventato un processo ormai necessario che espone il dato a rischi e vulnerabilità.

SOSARCHIVI

MelTechnologies

Processo di dematerializzazione

Il processo di trasformazione da fisico a digitale può nascondere la perdita/furto del dato se non viene presa in considerazione un' adeguata progettazione dei sistemi

IoT (Internet of Things)

Il sistema viene utilizzato anche in campo archivistico e logistico per taggare e monitorare il posizionamento dei documenti ottimizzando i processi di ricerca e di organizzazione del lavoro.
Ma attenzione alle vulnerabilità

Cosa succede ..... .

Presenza digitale = **Rischio digitale**

- Archiviazione
- Backup
- Furto informazioni
- Disservizi
- Criptazione del dato

SOSARCHIVI

MelTechnologies

PERICOLO DIGITALE

Sicurezza: le aziende italiane hanno un problema: il **90%** ha subito almeno una violazione nell'ultimo anno (al 19 febbraio 2019)

Il quadro che emerge dai dati italiani è in linea di massima quello che un esperto si aspetta, ma cionondimeno preoccupante (sono stati intervistati 250 CIO, CTO e CISO di aziende italiane operanti in vari settori).

Lo studio apre con una domanda classica, ma essenziale: la vostra azienda ha subito almeno una violazione di sicurezza negli ultimi 12 mesi? La risposta è stata sì nel 90% dei casi e questo lascia aperto l'interrogativo su quel 10% rimanente: sono riuscite a rintuzzare tutti gli attacchi o semplicemente la violazione è riuscita così bene da passare inosservata? Un indizio sulla possibile risposta sta nella domanda successiva che chiedeva se gli intervistati avevano notato un aumento del numero di attacchi. Il 93% ha risposto positivamente, ma ci risulta davvero difficile credere che il 7% non abbia notato nulla di strano quando il 48% degli altri riporta aumenti che vanno dal 51 al 300%. Qualche caso di stabilità nel numero di attacchi ci sarà, ma il 7% ci sembra troppo elevato per essere veritiero.

SOSARCHIVI

MelTechnologies

QUANTO COSTA LA SICUREZZA?

Il **94%** degli intervistati denuncia di riscontrare un aumento considerevole nella complessità degli attacchi che deve fronteggiare, a conferma del fatto che i gruppi di cyber criminali stanno migrando i loro interessi dagli attacchi generici a largo spettro verso gli attacchi mirati.

La spesa per le difese sta aumentando

Alla luce di questa situazione e della tutto sommato elevata consapevolezza che caratterizza le aziende di medio/grandi dimensioni, non sorprende più di tanto il fatto che il 96% degli intervistati intenda aumentare il budget destinato alla sicurezza informatica, anche in virtù dei processi di digitalizzazione del business che continuano a prender piede nel nostro Paese. Il 36% delle aziende prevede di aumentare il budget di una cifra compresa tra l'11 e il 30%, il 13% delle aziende tra 31 e il 40% mentre il 31% degli intervistati pensa di spendere tra il 31 e il 50% in più. Solo il 4% crede di aumentare la spesa di una cifra superiore al 50%.

SOSARCHIVI

MelTechnologies

VIOLAZIONI INFORMATICHE

Violazioni informatiche: una su 5 arriva dai dipendenti/operatori

Secondo un recente report rilasciato da Verizon, le **violazioni imputabili a dipendenti** o soggetti interni alle aziende sono in aumento e la loro scoperta è di solito molto tardiva, impiegando diversi mesi almeno nel **65%** dei casi. La prima motivazione che muove chi agisce dall'interno è, prevedibilmente, il profitto personale, con il 47,8% dei casi analizzati in cui un dipendente è stato corrotto o ha venduto di sua volontà i dati.

Il secondo motivo, però, è più preoccupante, in quanto nel **23,4%** dei casi l'interno ha rubato dati o causato violazioni informatiche per il semplice gusto di farlo. Questo significa che è complesso capire fino in fondo le motivazioni che spingono queste persone e per rendere le cose più semplici **Verizon ha raccolto in 5 categorie differenti** il personale di fornitori che tipicamente rappresenta un pericolo per i dati aziendali.

SOSARCHIVI

MelTechnologies

VIOLAZIONI INFORMATICHE

La prima è quella in cui trova posto il **lavoratore distratto**: una persona che ha scarsa considerazione per le politiche di sicurezza dell'azienda e installa programmi non autorizzati, sposta dati su dispositivi non autorizzati o, più in generale, compie azioni non approvate dal dipartimento It e delle quali i responsabili restano all'oscuro, rendendo difficile chiudere le falle che questi lavoratori aprono verso l'esterno.

SOSARCHIVI

MelTechnologies

VIOLAZIONI INFORMATICHE

La seconda è quella del classico **dipendente insoddisfatto**, una persona che danneggia l'azienda per la quale lavora o nella quale si trova temporaneamente per un sentimento di rivalsa. Di solito questa categoria tende a distruggere i dati piuttosto che inviarli all'esterno.

VIOLAZIONI INFORMATICHE

Come terza classificazione troviamo il tipico **fornitore incompetente**, un partner commerciale che non ha implementato politiche di sicurezza adeguate e accede in modo improprio, o tramite equipaggiamenti compromessi, alle risorse aziendali.

SOSARCHIVI

MelTechnologies

VIOLAZIONI INFORMATICHE

Si passa poi alla categoria dei **criminali per scelta** che si divide in due:

- La prima è quella degli **agenti infiltrati**, ovvero dipendenti che sono stati contattati da concorrenti o organizzazioni criminali per compiere del lavoro sporco dall'interno in cambio di denaro. Spesso lavorano su commissione e vengono pagati per compiere operazioni precise come impiantare del malware o rubare dati ben selezionati.
- L'altra categoria **dei criminali per scelta** è quella dei dipendenti che agiscono di propria iniziativa e rubano dati da vendere poi ad acquirenti senza scrupoli.

SOSARCHIVI

MelTechnologies

SOCIAL ENGINEERING

Un elemento che tende sempre ad essere trascurato o minimizzato, è quello della crescita **formativa e informativa delle risorse interne**.

In questo modo però si ignora completamente il fatto che oggi gli attacchi più grandi e invalidanti sono stati, per la maggior parte dei casi, condotti da **attaccanti** che hanno sfruttato le **"vulnerabilità" delle persone** e la loro, a volte, incauta fiducia.

Tecnologie di sicurezza sempre più sofisticate **rendono arduo** e a volte impossibile sfruttare i punti deboli legati alla tecnologia, è per questo che gli attaccanti decidono sempre più spesso di sfruttare **l'anello debole** della catena rappresentato **dal fattore umano .**

Bypassare questo tipo di "protezione" è facile, comporta rischi **minimali** e praticamente non richiede **alcun investimento**.

SOSARCHIVI

MelTechnologies

Cosa dobbiamo / possiamo fare ……

SOSARCHIVI
ASSOCIAZIONE PER LA TUTELA DEL PATRIMONIO ARCHIVISTICO

MelTechnologies

SISTEMA DI GOVERNANCE

Implementare il **sistema di governance**

- Insieme di processi e procedure per garantire Sicurezza e continuità

Individuare le **competenze necessarie**

- Interne
- Esterne

Definire il **perimetro da proteggere**

- Fisico
- Logico

Erogare **Formazione e sessioni di awareness**

SOSARCHIVI

MelTechnologies

SOLUZIONI

1. Utilizzare la struttura delle norme **ISO** (ad esempio: **27001**:2013: Sistemi di gestione della Sicurezza delle Informazioni – **22301**: Business Continuity)

2. Formazione ed Awareness (Sensibilizzazione)

3. Strumenti per minimizzare i costi (Fondi Paritetici Interprofessionali – Credito d'Imposta)

SOSARCHIVI

MelTechnologies

Il problema esiste ed è quello ROSSO posizionato tra la sedia e la tastiera

Problem **E**xists **B**etween **K**eyboard **A**nd **C**hair

SOSARCHIVI

MelTechnologies

PER INFORMAZIONI

MEL TECHNOLOGIES SRL
VIA TOLMINO 12 – ROMA (RM)
VIA BRUNO BUOZZI 26 – MONTEROTONDO (RM)
datisicuri@meltec.it

06-92.93.80.50

SOSARCHIVI
ASSOCIAZIONE PER LA TUTELA DEL PATRIMONIO ARCHIVISTICO

MelTechnologies