IT•NEWS

N. 20 LUG./AGO. 2024

L'indispensabile road-book

per rendere sempre più digitale e competitiva la tua impresa

IN QUESTO NUMERO

L'EDITORIALE

A cura di **Gianluigi Peana**

La comunicazione SOSTENIBILE

Brand Identity Sostenibile

L'Agenda 2030 per lo Sviluppo Sostenibile rappresenta una pietra miliare negli sforzi globali per affrontare le sfide economiche, sociali e ambientali del nostro tempo. Tuttavia, il raggiungimento dei suoi ambiziosi obiettivi non può prescindere da una comunicazione efficace e sostenibile. In questo contesto, ogni paese, attraverso le sue organizzazioni pubbliche e private, è chiamato a sviluppare una strategia personalizzata, il cui progresso deve essere comunicato in modo trasparente e coordinato sotto l'egida delle Nazioni Unite.

La Comunicazione come chiave dello Sviluppo Sostenibile

La comunicazione è un elemento chiave in questo processo. Deve essere chiara, accessibile e coinvolgente, capace di tradurre gli obiettivi dell'Agenda 2030 in messaggi comprensibili e motivanti per il propri stakeholder. I referenti di comunicazione delle aziende, e le agenzie di comunicazione con le quali collaborano, hanno un ruolo centrale in questo contesto, fornendo le competenze e gli strumenti necessari per creare esperienze uniche e di alto impatto che possano sensibilizzare e le persone dentro e fuori le organizzazioni.

I·TEAM

La comunicazione delle Organizzazioni è fondamentale

Un fattore determinante e distintivo sul mercato, è la capacità di combinare creatività e strategia nel raccontare la propria responsabilità ambientale e sociale. Con questo obiettivo, devono essere sviluppate soluzioni innovative, ad esempio, per migliorare la user experience e il web design, con un approccio centrato sull'utente e sulla sostenibilità. L'ottimizzazione delle prestazioni dei siti web per ridurre il consumo di risorse è solo un esempio di come la tecnologia possa essere utilizzata responsabilmente, così come l'adozione di server certificati Green.

Sostenibilità anche nei dettagli

Il design grafico assume un ruolo cruciale nella comunicazione visiva di un'azienda o di un'iniziativa. L'uso di tecniche di stampa eco-friendly o di materiali riciclati o l'energia proveniente da fonti sostenibili dimostra un impegno concreto verso la sostenibilità ambientale. Ogni scelta, dai colori ai font, dalle immagini ai materiali, può essere fatta per comunicare in modo efficace i valori dell'azienda e per promuovere una cultura della sostenibilità.

L'importanza di avere un partner con competenze specifiche

Fondamentale, in genere, è anche l'avvalersi di partner che siano essi stessi attenti alla sostenibilità e competenti su questi temi. Avere un partner qualificato che supporta le aziende nel valorizzare il proprio percorso di integrazione della sostenibilità nel business è molto importante per comunicare, attraverso un sapiente e ponderato storytelling, gli sforzi e i risultati raggiunti.

Perché parliamo di comunicazione sostenibile?

La creazione di una Brand Identity Sostenibile è un processo complesso e fondamentale che deve riflettere i valori, la visione e la missione dell'azienda. Una brand identity ben costruita non solo rappresenta l'azienda nel panorama competitivo, ma ne evidenzia l'impegno verso un futuro sostenibile. Questo impegno deve essere evidente in ogni aspetto della comunicazione, dal logo ai toni di comunicazione, creando una sinergia visiva e verbale che renda l'azienda riconoscibile e memorabile.

A cura di
Marco Cecchi

NOVITÀ sulla conservazione dei Metadati e responsabilità dei datori di lavoro

Il Garante per la protezione dei dati personali, il 6 giugno 2024 ha emesso il provvedimento n.364 riguardante la conservazione dei metadati e le responsabilità dei datori di lavoro, sia nel settore pubblico che privato.

Cosa sono i metadati

I metadati sono informazioni registrate automaticamente dai sistemi di gestione della posta elettronica, sia dai server di smistamento (MTA) sia dalle postazioni client (MUA).

I metadati includono gli indirizzi email del mittente e del destinatario, gli indirizzi IP dei server o dei client coinvolti, gli orari di invio, ritrasmissione o ricezione, la dimensione del messaggio, la presenza e dimensione degli allegati e, in alcuni casi, l'oggetto del messaggio. Questi dati sono registrati automaticamente e non dipendono dalla volontà dell'utente.

Le responsabilità dei datori di lavoro

Ecco i principi e le iniziative dove devono avere maggiore attenzione.

Illiceità del trattamento e necessità di garanzie:

> L'utilizzo di programmi/servizi di gestione della posta elettronica senza le necessarie garanzie (accordo sindacale) può configurare un trattamento illecito dei metadati.

> La raccolta preventiva e sistematica dei metadati relativi all'utilizzo della posta elettronica da parte dei dipendenti richiede un accordo sindacale e la loro conservazione per un periodo limitato, solitamente entro 7 giorni più 48 ore.

Violazione del principio di correttezza e trasparenza:

> È fondamentale che i lavoratori siano adeguatamente informati sul trattamento dei dati personali relativi alle comunicazioni elettroniche che li riguardano.

> I datori di lavoro devono verificare che la raccolta e la conservazione dei dati avvengano nel rispetto dei principi di correttezza e trasparenza.

Principio della data retention:

> I tempi di conservazione dei metadati devono considerare le finalità connesse alla sicurezza informativa e informatica, con l'obiettivo di individuare e mitigare eventuali incidenti di sicurezza.

Principi di privacy by design e by default:

> I datori di lavoro devono assicurarsi che i programmi e servizi informatici utilizzati consentano all'utente di modificare le impostazioni di default per limitare o impedire la raccolta dei metadati.

> I produttori dei servizi e delle applicazioni devono tenere conto del diritto alla protezione dei dati durante lo sviluppo e la progettazione dei loro prodotti.

Iniziative di compliance per i datori di lavoro:

> I datori di lavoro pubblici e privati devono adottare tutte le misure necessarie per conformarsi alle indicazioni del Garante.

> È responsabilità del datore di lavoro verificare che i programmi e servizi informatici utilizzati dai dipendenti soddisfino i requisiti di conservazione dei metadati e permettano la modifica delle impostazioni di default.

> Le indicazioni del Garante si applicano a tutti i datori di lavoro, inclusi quelli del settore pubblico che utilizzano convenzioni o piattaforme per l'acquisto di beni e servizi, come il cloud.

Il provvedimento del Garante per la protezione dei dati personali fornisce linee guida per la corretta conservazione dei metadati da parte dei datori di lavoro e sottolinea l'importanza dei principi di correttezza, trasparenza e privacy by design e by default. È fondamentale che i datori di lavoro adottino misure di conformità e garantiscano l'informazione adeguata ai lavoratori riguardo al trattamento dei dati personali.

A cura di
Paolo Vannini

Sicurezza del Server
e Buone Pratiche per proteggere i Dati Sensibili

Proteggere i dati sensibili e prevenire danni economici e d'immagine derivati da accessi non autorizzati? Tutto passa dalla Sicurezza dei Server.

Per Sicurezza del Server si intendono tutte gli hardware e i software volti a proteggere le informazioni memorizzate nei sistemi e a garantire la sicurezza delle attività aziendali. L'obiettivo è ridurre la superficie di attacco sensibile alle violazioni, implementando strategie complesse che corrispondano all'importanza dei dati presenti e veicolati; comprende anche la difesa della rete di computer e dei dispositivi che si collegano.

Le tipologie di attacco

Gli attacchi ai server possono assumere forme diverse, secondo la loro natura e i loro obiettivi. Fra le principali categorie, segnaliamo:

1. **Denial of Service (DoS) e Distributed Denial of Service (DDoS):** mirano a rendere il server non disponibile sovraccaricandolo con un'elevata quantità di richieste di accesso
2. **SQL Injection:** sfrutta vulnerabilità nelle applicazioni web per eseguire codice SQL non autorizzato.
3. **Tunnelling:** manipola il protocollo DNS per bypassare i sistemi firewall e veicolare dati alterati
4. **Side Movement Attack:** sfrutta la supply chain per installare malware con lo scopo di carpire informazioni riservate o ottenere accesso ai sistemi.

Le modalità di difesa

Ecco alcune delle migliori pratiche da attuare per difendere il Server:

1. **Stabilire una connessione sicura:** utilizzare il protocollo SSH per una connessione crittografata e modificare la porta predefinita per ridurre la superficie di attacco. È preferibile autenticare il server SSH tramite una coppia di chiavi di sicurezza anziché una password normale.
2. **Utilizzare certificati Secure Sockets Layer (SSL):** l'uso di certificati SSL protegge le informazioni scambiate tra i sistemi e consente l'identificazione e l'autenticazione degli utenti in ingresso.
3. **Gestire gli utenti del server:** disabilitare l'accesso SSH per l'utente root e creare account utente specifici con autorità limitata ma in grado di eseguire attività di alto livello.
4. **Monitorare gli accessi:** implementare un sistema di monitoraggio che identifichi e autentichi gli utenti, supervisioni i registri e rilevi eventuali tentativi di accesso sospetti.
5. **Creare una politica di sicurezza per le password:** stabilire criteri rigorosi per la creazione e il mantenimento delle credenziali degli utenti del server, come l'uso di password complesse, timeout di sessione per inattività e autenticazione a due fattori.
6. **Utilizzare ambienti virtuali isolati o multiserver:** la virtualizzazione dei sistemi con l'isolamento delle macchine server offre un'alta protezione dei dati e consente la creazione di politiche di sicurezza separate per ogni applicativo internet.
7. **Configurare un firewall:** utilizzare un firewall NGFW per proteggere il server ed evitare di esporre i servizi interni all'accesso esterno.
8. **Aggiornamenti regolari:** mantenere aggiornato il software di gestione del server e del sistema stesso per garantire che siano presenti le ultime patch di sicurezza, per mitigare le vulnerabilità note e per proteggere il server da attacchi noti.
9. **Backup dei dati:** effettuare regolarmente backup dei dati critici del server e conservali in una posizione sicura. In caso di violazione o perdita di dati, sarà possibile ripristinare le informazioni importanti e minimizzare l'impatto sugli affari dell'azienda.
10. **Formazione e consapevolezza:** educare il personale sull'importanza della sicurezza informatica e fornire formazione sulle migliori pratiche, come l'identificazione di mail di phishing o l'uso di password sicure.
11. **Penetration test:** eseguire test di penetrazione regolari per identificare eventuali vulnerabilità nel server e nelle applicazioni.
12. **Monitoraggio continuo:** implementare un sistema di monitoraggio continuo per rilevare attività sospette o anomale sul server. Questo ti permette di rispondere prontamente a eventuali minacce.
13. **Crittografare i dati sensibili:** utilizzare la crittografia per proteggere i dati sensibili durante la trasmissione e l'archiviazione. Se i dati sono intercettati, non saranno accessibili senza la chiave di decrittografia corretta.
14. **Gestire gli aggiornamenti dei software di terze parti:** assicurarsi che tutti i software di terze parti utilizzati sul server siano regolarmente aggiornati con le ultime patch di sicurezza.
15. **Monitoraggio delle registrazioni di sistema:** tenere traccia delle registrazioni di sistema per identificare eventuali attività sospette o anomalie.
16. **Segui le linee guida di sicurezza:** consultare le linee guida di sicurezza fornite dai produttori dei sistemi operativi, dei software e dei dispositivi utilizzati sul server. Queste linee guida spesso contengono raccomandazioni specifiche per migliorare la sicurezza dei tuoi sistemi.

Se applicate correttamente, queste procedure possono mantenere attiva la Sicurezza non solo con i Server ma con tutto il vostro ecosistema digitale. Per ogni informazione anche sulle nuove soluzioni di sicurezza disponibili, chiedete di I-TEAM.

A cura di
Marco Melucci

Cosa fare in caso di attacco hacker durante le ferie?

Restare calmi e reagire prontamente, per mitigare i danni e ripristinare la sicurezza. Se siete con I-Team, non siete soli! Andiamo per ordine

- **Informare il responsabile della sicurezza informatica o il team IT:** comunicare immediatamente l'incidente al responsabile della sicurezza informatica o al team IT dell'azienda; fornire tutti i dettagli rilevanti sull'attacco, inclusi i sintomi, gli errori o le anomalie riscontrate.

Se non ne avete uno, **coinvolgete un esperto di cybersecurity esterna.**

Se l'attacco è grave o non si hanno le competenze necessarie per affrontarlo, considera di coinvolgere un team di esperti di sicurezza informatica o una società specializzata. Possono fornire assistenza nell'analisi dell'incidente, nell'identificazione delle vulnerabilità e nell'adozione di misure correttive.

- **Isolare il sistema compromesso:** l'esperto provvederà immediatamente a disconnettere il dispositivo o il sistema colpito dalla rete aziendale per prevenire la diffusione dell'attacco ad altri dispositivi. Questo può aiutare a contenere l'incidente e limitare i danni.
- **Documentare l'incidente:** l'esperto registrerà tutti i dettagli relativi all'attacco, inclusi l'orario di scoperta, i sintomi o i messaggi di errore visualizzati, le azioni intraprese e qualsiasi altro elemento utile per l'analisi successiva. Questa documentazione sarà preziosa per l'indagine e le azioni correttive.
- **Ripristinare i backup:** se l'impresa ha un backup dei dati, utilizzarlo per ripristinare i sistemi compromessi. L'esperto si assicurerà di verificare che i backup siano stati creati prima dell'attacco e che siano privi di malware. Questo aiuterà a ripristinare i dati e i sistemi alla loro condizione precedente all'attacco.
- **Modificare le password e rivedere i permessi di accesso:** una volta risolto l'attacco, cambiare tutte le password compromesse e rivedere i permessi di accesso per garantire che solo il personale autorizzato abbia accesso ai dati e ai sistemi aziendali.
- **Informare le parti interessate:** se l'attacco potrebbe aver compromesso dati sensibili o coinvolto clienti o partner commerciali, è obbligatorio informarli tempestivamente. La trasparenza è fondamentale per la gestione delle relazioni e per dimostrare l'attenzione verso la sicurezza dei dati e verso i propri clienti.
- **Valutare e rafforzare la sicurezza:** dopo l'incidente, valutare le vulnerabilità che hanno consentito l'attacco e prendere misure per rafforzare la sicurezza informatica dell'azienda. Ciò potrebbe includere l'implementazione di misure aggiuntive di protezione, la formazione del personale sulla sicurezza informatica o l'aggiornamento delle politiche di sicurezza.
- **Notificare le autorità competenti:** gli attacchi informatici gravi necessitano di una notifica alle autorità competenti, come la Polizia Postale e l'Autorità Garante per la Protezione dei Dati Personali.

Ricordatevi che la prevenzione è sempre la migliore difesa e che gli hacker non vanno in vacanza, anzi. In particolare, assicuratevi di aver implementato misure di sicurezza solide prima delle ferie aziendali e di mantenere un monitoraggio costante anche durante i periodi di chiusura.

I·TEAM

Cinque società che si sono unite per dare forma a un grande progetto:
aiutare le imprese a crescere nella digitalizzazione
e nella rivoluzione digitale, per avere performance
sempre più efficaci ed efficienti, all'altezza dei grandi cambiamenti
dell'economia e della società contemporanea.

Allyou.srl

ego communication

GlobalNet
Servizi di Telecomunicazioni per la tua Azienda

OMEGA SISTEMI
Soluzioni Informatiche Professionali

NETWORK PRIVACY

PANTAREI INFORMATICA
La tecnologia resa semplice

WWW.I-TEAM.TECH

Via Benedetto Dei 64 • 50127 FIRENZE • Numero Verde 800-199760 • info@i-team.tech