NEWS Euroconference

Edizione di venerdì 22 Novembre 2024

DIGITALIZZAZIONE

La cybersecurity negli Studi professionali: sfide e strategie per la sicurezza dei dati sensibili

di **TeamSystem**

Nel panorama odierno, la *cybersecurity* rappresenta una priorità crescente per tutti, inclusi gli Studi professionali, che sempre più si trovano a gestire informazioni digitali sensibili di clienti e partner. Secondo i recenti dati di Clusit (Associazione Italiana per la Sicurezza Informatica), il primo semestre del 2024 ha visto un picco di attacchi informatici, con oltre 1.600 incidenti registrati globalmente e un aumento del 23% rispetto ai sei mesi precedenti. Questo incremento evidenzia una realtà: **la *cybersecurity* deve essere una priorità per tutte le aziende**.

Gli Studi professionali, spesso con risorse di sicurezza informatica limitate, devono fronteggiare minacce sempre più sofisticate. Come procedere, per proteggersi al meglio?

Avvocati, Commercialisti e Consulenti del lavoro gestiscono ogni giorno dati sensibili come dichiarazioni fiscali, pratiche legali e altre informazioni critiche che, in caso di violazione, potrebbero causare ingenti **danni finanziari e reputazionali**. Inoltre, l'inosservanza di normative sulla protezione dei dati, come il GDPR e le nuovissime NIS2 e DORA, potrebbero comportare **conseguenze legali, oltre che sanzioni finanziarie**. Proteggere questi dati è quindi non solo un dovere professionale, ma anche una forma di tutela per la fiducia e la riservatezza di chi affida i propri dati.

Quali sono le principali minacce informatiche?

Gli Studi professionali sono spesso bersaglio di specifici tipi di attacchi informatici, come *ransomware* e *phishing*, mirati a sottrarre o bloccare l'accesso ai dati. Nel 2024, si registra che il 34% degli attacchi globali sia attribuibile al *malware*, con una predominanza del *ransomware*, mentre il *phishing* resta stabile all'8% degli incidenti totali. Questi attacchi, prevalentemente motivati da fini economici, puntano a ottenere dati sensibili tramite tecniche di social engineering o tramite la compromissione di vulnerabilità del *software*. Gli Studi professionali sono obiettivi attraenti per i cybercriminali, poiché spesso gestiscono dati riservati ma

dispongono di infrastrutture di sicurezza meno complesse rispetto alle grandi aziende.

Quantificare il rischio economico per una *Cybersecurity* consapevole

L'**aspetto economico della *cybersecurity*** non va sottovalutato, soprattutto per realtà professionali più piccole. La quantificazione del rischio consente di comprendere l'impatto finanziario di un possibile attacco e di giustificare gli investimenti necessari per la protezione. Ad esempio, un attacco *ransomware* che interrompe le attività di uno Studio può generare perdite da decine a centinaia di migliaia di euro, tra costi di ripristino, eventuali riscatti e danni reputazionali. Con la quantificazione del rischio, è possibile dimostrare che ogni euro investito in *cybersecurity* si traduce in una riduzione del rischio finanziario.

Strategie di sicurezza: dal *Vulnerability Assessment* alla gestione delle *password*

Per affrontare queste sfide, esistono diverse strategie utili anche per Studi con risorse limitate. La prima è l'implementazione di un *Vulnerability Assessment*, che permette di identificare le principali debolezze del sistema e della catena di fornitura. La piattaforma **Teamsystem *Cybersecurity***, ad esempio, offre una valutazione automatizzata del perimetro d'attacco, adattandosi alle esigenze di studi professionali che desiderano proteggere i dati senza un'architettura complessa.

Tra le misure di base per proteggere le informazioni c'è anche l'adozione di *password* robuste e uniche, generabili e gestibili in modo sicuro tramite *password manager*. Inoltre, è fondamentale educare il personale a riconoscere i segnali di *phishing* e a mantenere aggiornati i dispositivi: una pratica essenziale, dato che molte violazioni avvengono sfruttando *software* obsoleti.

Buone pratiche di *Cyber* Igiene e protezione delle credenziali

Infine, la *cyber* igiene quotidiana è fondamentale. Tenere aggiornati dispositivi e server, ridurre l'accesso a dati personali non necessari e utilizzare l'autenticazione a due fattori (2FA) sono pratiche semplici che possono fare una grande differenza. L'uso consapevole di strumenti digitali e la limitazione dei permessi per le app garantiscono maggiore sicurezza e riducono l'esposizione ai rischi.

Questi temi verranno approfonditi nel prossimo **webinar gratuito per gli Studi professionali**, previsto per il 6 dicembre, organizzato da Euroconference e TeamSystem. L'evento rappresenterà un'occasione unica per scoprire e imparare le migliori pratiche e le ultime soluzioni per proteggere dati e sistemi da minacce sempre più evolute, rafforzando le difese

contro i *cyber* attacchi.