ARTICOLO DI ELEARNINGNEWS

Year 8 - number 275 Wednesday 07 february 2024

I costi della mancata sicurezza informatica per le aziende

Scopriamo quali sono gli impatti e i costi della mancata cyber security aziendale e le modalità per mitigare i rischi informatici nelle aziende.

Lo scorso dicembre, un **grave attacco informatico ha colpito la Pubblica Amministrazione italiana**, paralizzando numerosi servizi digitali e causando problemi alla fatturazione elettronica.

L'attacco è stato avviato colpendo Westpole, un'azienda che fornisce servizi cloud a PA Digitale, società che a sua volta offre software e programmi per Comuni e altri enti pubblici. Una volta bucata la sua sicurezza, gli hacker hanno messo fuori uso il software Urbi, utilizzato per gestire anagrafe e servizi ai cittadini, bloccando completamente i sistemi di circa 300 enti pubblici a livello locale e nazionale.

Questo ennesimo e psante attacco all'infrastruttura informatica della Pubblica Amministrazione evidenzia l'importanza di garantire la massima **sicurezza nel trattamento dei dati** in tutte le aziende.

In questo articolo, analizzeremo l'impatto degli attacchi informatici sulle aziende, soffermandoci in particolare sui costi della mancata cyber security e sulle modalità per mitigare i rischi informatici.

L'impatto di un attacco informatico per le aziende

A seconda della tipologia e della quantità di dati trattati, l'impatto di un attacco informatico può variare sensibilmente. In linea di massima, la perdita o il furto di dati espongono l'azienda a danni legali, economici e reputazionali.

In primo luogo, i danni generati da un attacco informatico richiedono l'**intervento di personale qualificato** nel settore della cyber security. Il blocco dei sistemi potrebbe inoltre comportare l'**interruzione momentanea della produzione** aziendale o dell'erogazione di un servizio, con conseguenti **perdite di profitto**.

Per ultimo, la notizia di una compromissione dei propri sistemi informatici intacca inoltre la **reputazione dell'azienda**, generando un impatto negativo su clienti e partner.

Con riferimento ai costi diretti, invece, la mancata ottemperanza delle misure di sicurezza richieste dal GDPR comporta **pesanti sanzioni**, nonché risarcimenti per i titolari dei dati sensibili. E, in alcuni casi (ad esempio in caso di attacchi ransomware) potrebbe essere necessario il **pagamento di un riscatto** per riprendere possesso dei dati e delle funzionalità dei propri sistemi.

Infine, i cyberattacchi possono avere **conseguenze per la salute e il benessere dei lavoratori**, che potrebbero sentirsi colpevoli per l'accaduto, confusi e frustrati. Per ulteriori approfondimenti su questo tema, leggi anche " **Attacchi informatici: quali impatti sulla salute e sicurezza dei lavoratori?**".

Quanto costa alle aziende una violazione dei dati?

Secondo il **Cost of a Data Breach Report 2023** di IBM, il costo medio globale di una violazione dei dati ha raggiunto **4,45 milioni di dollari nel 2023**, con un aumento del 15% negli ultimi 3 anni.

Sempre a livello globale, il report ha rilevato che il 95% delle aziende intervistate ha subito più di una violazione ed è propenso ad **imputare ai clienti i costi degli attacchi subiti** (57%) piuttosto che **aumentare gli investimenti in sicurezza** (51%).

Per quanto riguarda invece il **panorama italiano**, il costo medio complessivo delle violazioni di dati è pari a 3,55 milioni di euro. In media, i **giorni necessari per identificare e contenere una minaccia informatica** sono 235, di cui 174 per identificare

una violazione e 61 per contenerla.

I principali vettori di attacco sono social engineering, phishing e credenziali rubate o compromesse. Quelli più costosi sono invece: insider malintenzionati e compromissione delle e-mail aziendali.

Come mitigare i rischi informatici in azienda?

- Effettuare un attento **risk assessment** che metta in evidenza eventuali punti deboli.
- Implementare politiche e procedure di sicurezza informatica.
- Utilizzare tecnologie di sicurezza come firewall, crittografia dei dati, controlli di accesso, antivirus, ecc.
- Adottare sistemi di backup e ripristino per garantire la disponibilità e l'integrità dei dati, nonché il loro recupero.
- Sensibilizzare il personale sull'importanza della cyber security e fornire adeguata formazione in materia di sicurezza informatica.
- Implementare sistemi di monitoraggio e rilevamento delle minacce informatiche in tempo reale.
- Gestire gli incidenti di sicurezza informatica in modo tempestivo.

L'importanza del fattore umano nella mitigazione dei rischi informatici

Quando si parla di sicurezza informatica, è molto importante essere consapevoli che le tecnologie da sole non bastano. Affinché esse siano efficaci, occorre sviluppare strategie di sicurezza digitale che prendano in considerazione primariamente il fattore umano, con la necessità di una specifica preparazione e tutela del personale materialmente coinvolto nell'uso dei sistemi informatici e nel trattamento dei dati.

L'errore umano (apertura di e-mail di phishing o cattiva gestione delle password) è infatti considerato la causa principale del 90% delle violazioni della sicurezza informatica e può esporre le organizzazioni a gravi conseguenze, come l'installazione di software dannoso nella rete aziendale.

Leggi anche: **Come e perché formare i dipendenti sulla cyber security?**

Quando si parla di formazione continua dei lavoratori, una delle soluzioni al tempo stesso più efficaci ed economiche è quella di svolgere una formazione online specifica. Eccoti quindi alcuni corsi eLearning in materia di cyber security e protezione dei dati promossi da Mega Italia Media:

- **Corso online "Cyber Security: tutela dei dati e delle informazioni aziendali"**: per offrire ai tuoi dipendenti una formazione specifica sui rischi e le responsabilità nel trattamento di dati e informazioni tramite l'utilizzo di dispositivi informatici
- **Corso online "Privacy GDPR: Tutela dei dati personali"**: per illustrare ai tuoi dipendenti come applicare le disposizioni della normativa sulla tutela dei dati personali, garantendo un trattamento dei dati efficiente e garantendone al tempo stesso la tutela
- **Corso online "Phishing ? Guida pratica all'autodifesa"**: per aiutare i tuoi dipendenti a riconoscere e difendersi degli attacchi, tra uso consapevole della tecnologia e umana prudenza.
- **Corso online "Ransomware ? Non cadere in trappola"**: per fornire ai tuoi dipendenti le misure efficaci per conoscere e riconoscere la tecnica del ransomware e proteggersi dalle cyber frodi.

Per ulteriori approfondimenti sulla cyber security in azienda, leggi anche:

- **Cyber Risk: la difensiva delle imprese**
- **Cybersecurity aziendale: i dati sugli attacchi**