AI SENSI DEL NUOVO REGOLAMENTO GDPR:

Racconto di due attacchi di ransomware

Dal 25 maggio 2018, data di entrata in vigore del GDPR, le violazioni dei dati personali sono diventate talmente pericolose per le aziende e i service provider, a livello sia finanziario che procedurale, che sarebbero pronti a fare qualsiasi cosa per evitarle, o almeno questo è l'obiettivo.

Non imparare la lezione sulla tua pelle: scopri quanto un po' di protezione in più può fare la differenza nel proteggere la tua attività dalle pesanti sanzioni pecuniarie per le violazioni al GDPR.

AZIENDA X

RISCHI ELEVATI, FORTI RIMPIANTI

Mentre si adoperano per soddisfare i requisiti di conformità del GDPR, molte aziende sottovalutano una delle violazioni della sicurezza dei dati personali più comuni e più in crescita di oggi: gli attacchi di ransomware.

Il processo attualmente adottato, in caso di attacco:

SI IGNORA LA PROTEZIONE DAL RANSOMWARE

L'ATTACCO DI RANSOMWARE COLPISCE

Molti server, desktop e laptop vengono colpiti.

L'IT RILEVA L'ATTACCO

Le app di produzione critiche vengono paralizzate.

L'IT AGISCE PER CONTENERE L'INFEZIONE. AVVIA IL CONTO ALLA ROVESCIA DELLA NOTIFICA GDPR DI 72 ORE

Lo strumento di crittografia inizia a diagnosticare quali sono i dati personali che sono stati violati. Senza pressioni.

L'AZIENDA PROCEDE NELL'ANALISI DELL'ATTACCO E NEL MITIGARNE I DANNI

Tutti, dall'ufficio legale ai tecnici, operano per bloccare il danno.

L'IT AVVIA IL RIPRISTINO DEI FILE CRITTOGRAFATI DAL BACKUP

L'IT inizia il ripristino dei file danneggiati dal backup più recente.

IL RESPONSABILE DELLA PROTEZIONE DEI DATI AVVISA L'AUTORITÀ DI CONTROLLO GDPR LOCALE

Il responsabile della protezione dei dati informa l'autorità di controllo locale della violazione: il tipo di attacco, quanto sono stati i dati personali interessati e cosa viene fatto per il ripristino.

L'AZIENDA INVIA LA SEGNALAZIONE AI CLIENTI

Se la violazione è grave, tutti i soggetti interessati devono essere messi a conoscenza dell'accaduto, devono sapere chi contattare, cosa aspettarsi e quali passaggi sono in corso ai fini della gestione dei danni.

L'AZIENDA PAGA LA SANZIONE PER MANCATA CONFORMITÀ

È probabilmente ora di pagare la sanzione pecuniaria per la mancata conformità al GDPR pari al 2-4% del fatturato annuo, o a 10-20 mln. di euro, a seconda di quale dei due importi è maggiore.

IL CICLO SI RIPETE

Senza un miglioramento delle difese anti-ransomware, questo ciclo inevitabilmente si ripete con l'attacco di ransomware successivo.

AZIENDA Y

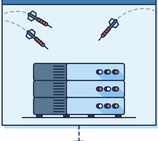
NIENTE VIOLAZIONI, NESSUN PROBLEMA

Le aziende che guardano all'intero contesto in cui si colloca il GDPR riconoscono che il ransomware è una grave minaccia alla conformità e agiscono per indirizzarla altrove prima che la violazione si verifichi.

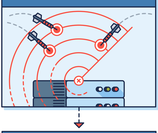
Il processo:

L'AZIENDA INSTALLA ACRONIS BACKUP CON ACTIVE PROTECTION PER PREVENIRE GLI ATTACCHI DI RANSOMWARE

L'ATTACCO DI RANSOMWARE COLPISCE



ACRONIS ACTIVE PROTECTION RILEVA AUTOMATICAMENTE E BLOCCA IL PROCESSO



L'AZIENDA EVITA L'ESIGENZA DELLE NOTIFICHE SULLE VIOLAZIONI DI SICUREZZA GDPR

(Grande sospiro di sollievo)

MANTIENI LA CONFORMITÀ GDPR CON ACTIVE PROTECTION

Muoversi tra le complessità della conformità al GDPR è una sfida, ma ti basta creare una difesa effettiva contro il ransomware per eliminare in partenza una pericolosa minaccia. Installa Acronis Backup e Acronis Backup Cloud con protezione attiva e smetti di preoccuparti della causa della rapida diffusione delle violazioni di sicurezza GDPR.

Avvia la versione di prova

Finanziata da

Acronis