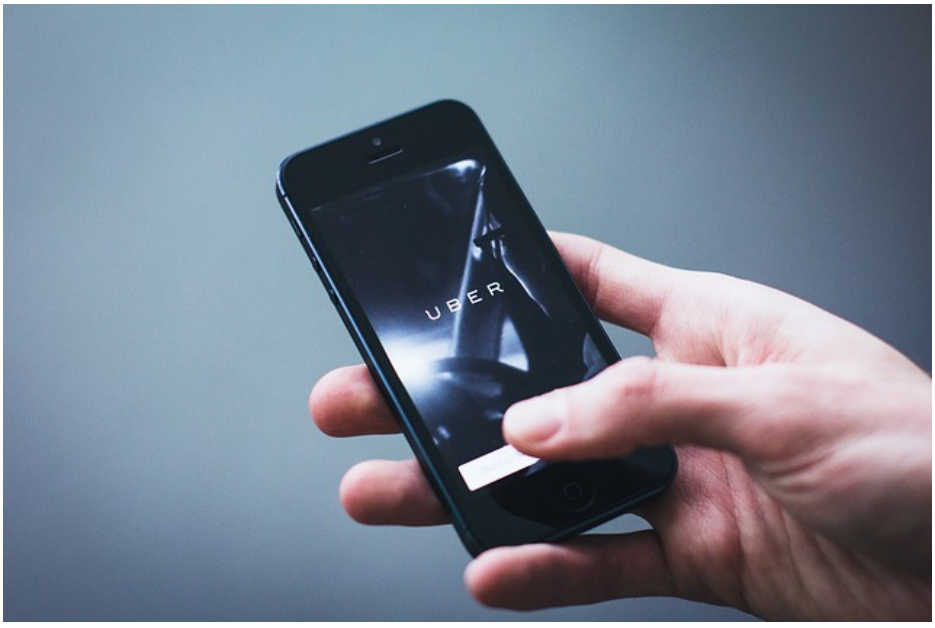
#gonews.it®
Empolese | Valdelsa
venerdì 24 novembre 2017 - 15:55

Hacker contro Uber, le quattro lezioni da apprendere secondo Yarix

23 novembre 2017 18:00 Economia e Lavoro Empoli



Uber è stata vittima di un attacco hacker, conclusosi con il furto dei dati dei 57 milioni di utenti in tutto il mondo. È solo l'ultimo degli episodi che, su scala globale, confermano come i dati siano il patrimonio più prezioso e ambito dai cybercriminali.

Le aziende e istituzioni italiane non sono immuni da questo rischio. Yarix – Cyber Division di Var Group e tra i player più accreditati nel campo della cybersecurity – desidera condividere le 4 lezioni che possiamo apprendere dalla vicenda Uber. Per mettere a fuoco i confini della vulnerabilità del sistema e le contromisure da adottare.

#1 Accordo con i cybercriminali di non divulgazione dei dati?
Meglio non scendere a compromessi con la cybercriminalità e non cedere a ricatti. Altrimenti si contribuisce ad incrementare il business della malavita e incentivare la rete del cybercrime. Nessun accordo stretto con chi commette crimini può essere considerato un accordo lecito, affidabile e proficuo.

#2 Sbagliato cercare di mettere tutto a tacere, per evitare danni di immagine e sanzioni governative
Trasparenza e condivisione tempestiva di informazioni sono la sola via percorribile per ridurre l'impatto dell'incidente e tutelare quanti sono coinvolti. In caso di data breach e data leak (diffusione di dati personali e sensibili), la nuova normativa sulla protezione dei dati personali (GDPR), a partire dal 25 maggio 2018, impone ad aziende e istituzioni colpite l'obbligo di notifica all'Autorità Garante Privacy e, in alcuni casi, anche agli interessati dalla violazione. In caso di mancato rispetto dell'obbligo di notifica, le aziende o le istituzioni potranno subire sanzioni amministrative pecuniarie fino a 10 milioni o, in caso di aziende, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

#3 Crittografia come scelta strategica
Secondo la normativa GDPR, i dati personali e sensibili nonché le informazioni strategiche per il business o per lo svolgimento della funzione istituzionale devono essere protetti con la crittografia. Non solo. La crittografia presenta il vantaggio ulteriore di consentire, in caso di data breach, di porsi al riparo da qualsiasi danno (i dati crittografati non sono utilizzabili).

#4 Proteggersi, proteggersi, proteggersi: i data leak sono e saranno sempre più frequenti
Con sempre maggiore frequenza vengono resi noti data leak che coinvolgono governi e aziende, compromettendo la privacy di utenti di servizi digitali, consumatori, e più in generale interessati che abbiano conferito i loro dati. Tra i trend emergenti e più preoccupanti c'è, in particolare, lo spear phishing, che comporta attacchi sempre più mirati verso aziende e il loro management.
La portata del danno potenziale è in grado di compromettere seriamente – come nel caso di Uber – reputazione e continuità del business aziendale. La scelta di attivare un servizio professionale di Penetration Test, Vulnerability Assessment e Insider Intelligence non rappresenta, dunque, solo una opzione, ma è un imperativo cui non è più possibile sottrarsi.

Fonte: Var Group

Tutte le notizie di Empoli

<< Indietro