

**DA YARIX, CYBER DIVISION DI VAR GROUP, 4 LEZIONI CHE POSSIAMO APPRENDERE
DALLA VICENDA UBER****I DATI SONO L'OBIETTIVO PIÙ AMBITO DALLA CRIMINALITÀ CIBERNETICA:
CYBER INTELLIGENCE, SECURITY ASSESSMENT E CONSULENZA GDPR
SONO LE RISORSE FONDAMENTALI PER TUTELARSI**

Empoli 23 novembre 2017 – 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 4% 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.

Var Group Spa

Var Group www.vargroup.it aiuta le imprese a disegnare l'evoluzione del proprio business. Realizziamo con i nostri clienti soluzioni che li rendono più competitivi. Il nostro valore sono le competenze, la capacità di modellarle, questo permette alle aziende di raggiungere i propri obiettivi. Le imprese si trovano di fronte a sfide sempre più complesse: devono poter contare su soluzioni innovative e specializzate. L'offerta Var Group trae la sua forza dall'integrazione di più elementi che si arricchiscono e si integrano reciprocamente, frutto del lavoro di Business Unit focalizzate nello sviluppo di soluzioni tecnologiche, Managed Services, ERP & Vertical e Strategie Digital, il tutto arricchito dal lavoro dell'R&D. Con un fatturato di 240 milioni di € al 30 aprile 2017, 1185 dipendenti e una presenza su tutto il territorio italiano grazie a 33 sedi capillarmente distribuite, Var Group è uno dei principali partner per l'innovazione del settore ICT.

Yarix – Cyber Division Var Group

Yarix, Cyber Division Var Group, esprime una leadership riconosciuta nel comparto della cybersecurity, avendo orientato la propria missione allo sviluppo di soluzioni specifiche per le aziende sanitarie, scuole, università, industrie ed enti governativi. Yarix è parte di **Var Group**, uno dei principali partner per l'innovazione del settore ICT. Fondata a Montebelluna, l'azienda è presente anche nelle città di Roma, Milano e Tel Aviv. Yarix è l'unica azienda privata in Italia ammessa al **FIRST**, la rete di protezione globale che riunisce player come Nasa, Apple e Google con l'obiettivo di contrastare le minacce emergenti. Yarix dispone del Security Operation Center in Italia più evoluto in Italia: un bunker informatico dotato di misure di sicurezza fisica e biometrica di ultima generazione, in grado di monitorare le reti aziendali senza soluzione di continuità. Yarix collabora con i maggiori player mondiali dell'IT e promuove iniziative per la diffusione di una più ampia cultura digitale. Maggiori informazioni sono disponibili su www.yarix.com e su www.vargroup.it.

Informazioni per la stampa

Tommasina Cazzato – tommasina.cazzato@allea.net (345 7357751)
Simona Seminario – simona.seminario@allea.net (335 1821270)

Var Group Spa

Sara Lazzeretti – s.lazzeretti@vargroup.it (3391705791)