DZP
more than law

Contatto continuo con il consulente?

LEX ALERT 3.2020
Cybercriminalità – protezione contro i crimini informatici durante la pandemia

Il momento in cui tutti gli occhi sono puntati sulla lotta contro il virus è anche il momento in cui **gli imprenditori sono maggiormente esposti al rischio di criminalità informatica, ossia di reati commessi via Internet.** La diminuzione del numero di dipendenti che svolgono attivamente le loro mansioni, la necessità di introdurre il lavoro a distanza e l'attenzione al mantenimento della continuità dei servizi fanno sì che la protezione dei sistemi informatici e delle banche dati passi in secondo piano. Tuttavia, vale la pena ricordare **che la vigilanza e la cura per la sicurezza digitale non sono mai state così importanti come oggi**.

Cosa possono fare i criminali informatici?

- **frode su Internet**: creazione di un falso gateway per gli agenti di pagamenti (ad es. PayU); acquisizione dell'accesso a una casella di posta elettronica, impersonificazione di un contraente e invio di una fattura contenente il numero di conto del criminale a suo nome;
- **furto di banche dati**: violazione delle misure di sicurezza per accedere a una banca dati (ad es. informazioni sui clienti, cronologia delle transazioni), copia di documenti, vendita di informazioni acquisite illegalmente;
- **spionaggio informatico**: l'uso di software malware per acquisire conoscenza dell'attività;
- ***ransomware**:* blocco dell'accesso al sistema informatico e richiesta di un riscatto per la sua rimozione;
- ***carding**:* furto dei dati della carta di pagamento per l'acquisto di prodotti o servizi a spese del titolare effettivo della carta.

Cosa può o deve fare un imprenditore?

- istruire i dipendenti **per essere particolarmente vigili** quando si scaricano file di origine sconosciuta, si ordinano bonifici *online* o si effettuano transazioni online con carta di pagamento;
- informare del **divieto di trasmettere via e-mail o telefonicamente i dati che potrebbero essere utilizzati per violare la sicurezza dei sistemi informatici** (ad es. login, password, numeri di conto);
- **installare/aggiornare antivirus** e lasciare il firewall attivo;

- *backup* regolari;
- prendersi cura **dell'archiviazione dei log** del server e del sito web;
- **registrare qualsiasi informazione relativa ad eventi perturbanti o insoliti**.

Come comportarsi quando si identifica un crimine informatico?

A causa della varietà della condotta dei criminali informatici, non è possibile creare un modello di comportamento universale. Se si sono verificate violazioni della sicurezza, è importante cambiare le password e indagare sull'integrità dei dati. Se l'autore del reato ha sottratto denaro, è importante informare la banca, che può stabilire un blocco sul conto utilizzato per commettere il reato. In caso di richiesta di riscatto, va ricordato che soddisfare le aspettative dell'autore del reato non garantisce la possibilità di accedere nuovamente al sistema informatico o di perdere i dati.

È importante reagire il più presto possibile. Meno tempo passa dall'evento, più è probabile che si riducano al minimo le perdite e si garantiscano prove che possano poi essere utilizzate in un procedimento penale o civile.

Se è già stato commesso un reato, **è essenziale cooperare con le autorità di polizia, intervenire per la protezione dei dati personali ed eventualmente prendere in considerazione iniziare una causa civile con i fornitori di servizi che forniscono soluzioni tecniche adeguate**.

Siamo a Vostra disposizione

avv. Rafał Karbowniczek

Senior Associate | Dipartimento processuale

E: Rafal.Karbowniczek@dzp.pl

avv. Małgorzata Karasińska

Associate | Dipartimento processuale

E: Malgorzata.Karasinska@dzp.pl