Reactie Ctouvert op hack bij Secureholiday

In response to your demand, we provide you here details about the elements we know.
There are a lot of cyberattacks this spring on tourism industry, on platforms (like ours) and on large and well-known brands.
I suppose you have the information.
We are extremely concerned by the one we have identified on our solution on the 28th of February (we can talk only about this one and cannot give you more info about other leaks)
All phishing activity, especially in May and June are not coming from our solution, far from that.
You probably heard about our solution because we have been informing our clients (campsites) and they have been informing their clients with transparency.
IA provides hackers new tools to use technical weakness that human was not capable to work with.
We have been working with priority on cyber security since the beginning of the year (after a first attack on a French platform in January) to be prepared for those new strategies, we have a massive plan that should end this October.
We are a quit small company (less than 100 people) close to our clients (the campsites), themselves close to their consumers.
We need to provide the right level of security, it is not really an option, and our clients (the campsites) are concerned too. We provide them (fédérations) with a clear report.

Some details:

- we detected an attack on the 28th of February and immediately stopped it by blocking the IP address and on the same day the breach was identified.
- We then determined the nature of the attack and fixed the security vulnerability on our side.
- Two days later, we were able to identify the reservations that had been exposed and confirm that a genuine data breach had occurred.
- We explore immediately if the system has another and similar weakness.
- We filed a criminal complaint with the French public prosecutor.
- We informed all affected campsites, providing them individually with the list of compromised reservations so that they could “notify their customers”.

This is the procedure required under the GDPR framework. We act as a data processor, while the campsites are the data controllers.

We subsequently investigated whether the breach was broader in scope or had occurred over a longer period but found no evidence of this.
Nevertheless, we implemented a series of additional security measures and commissioned a comprehensive security audit.
We expect to receive the audit summary within the next few days, and its recommendations will, of course, be implemented in full.
As a campsite industry technical partner, we share some more (and confidential security details) with campsites federations and large organization partner all new measures.

In response to your questions:

- The hacker compromised a third-party system that had access to a single establishment.
- The breach affected approximately 500 campsites and involved a portion of the reservations made between October and the end of February. The proportion of affected reservations varied by campsite, ranging from 5% to 30% of bookings during that period.
- The affected campsites are located across several European countries, primarily France, Spain and Italy. More than 50% of the affected customers are French, the leak concerns precisely **41 577 Dutch reservations**. All clients have been informed by their respective campsites.
- The data that was stolen consisted of booking information, including guests' names, destination, email address, booking dates and the amount paid for the stay. No payment card or banking information was compromised. Our system doesn't hold the payment part; it is transferred to dedicated PSP solutions. We are PCI DSS Label on this aspect.
- The campsites, as the data controllers, informed the affected customers.
- Are we safe ? The tourism sector has been particularly targeted by cyberattacks this spring. Several major operators have lost all or part of their data.

Although the breach affecting our platform was significant but limited, due to some internal complexity reducing data access (We don’t want to give more details about it)
Nevertheless, we have strengthened our security measures considerably. We are under the largest audit on all aspects of our platform at the moment, we should get the final report in a few days … and we will correct obviously.
So, I can tell you that we have the resources and the investment requested to be safe.

Apart from your questions concerning our solution
There have been some more attacks in June, via email, via Whats app.
These are not concerning the leaks we are recognizing.
(I know I am repeating myself but I don’t want to turn as an easy target because we are transparent and ethics / I hope you understand)

One more element
The consumers are contacting their campsite when they have been abused by the phishing and paid some amount, then the campsite informs us
So far, we know 14 cases of payment, **6 concern Dutch customers**.
They are all in contact with their banks and the campsites.

Last element, it is important to note that the platform has been operating for more than 20 years and this is the first confirmed data breach. Ensuring the security of our systems and our customers' data is now, and will remain, our highest priority.
I hope I have been enough clear and detailed.
Please feel free for more questions

Best regards

Manuel MIRABEL
CEO
ctoutvert
Secureholiday Platform