

Avon Data Breach Exposes 19 Million Records - Report

July 30, 2020 - Cosmetics giant Avon has apparently experienced a large data breach. Last month, ZDNet reported that the company was "recovering from a mysterious cybersecurity incident." ZDNet's information came from a filing that Avon made with the Securities and Exchange Commission. Now, Infosecurity is reporting that researchers have found a cloud-server that exposed personally identifiable information (PII) contained in 19 million records stored on that server.

Tweet

```
(function() {  
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];  
s.type = 'text/javascript';  
s.src = 'http://widgets.digg.com/buttons.js';  
s1.parentNode.insertBefore(s, s1);  
})();
```

```
(function() {  
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;  
po.src = 'https://apis.google.com/js/plusone.js';  
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);  
})();
```

The incident in June resulted in the shutdown of a large portion of Avon's network. Three days after the company's initial SEC filing, it made another filing stating that it was preparing to restart network operations.

While it isn't clear that the June incident is related to the latest report, the likelihood of it seems strong. According to Infosecurity, the data on the exposed cloud server would have enabled hackers to take control of the company's network including giving them the ability to install and manage ransomware.

Avon is stating that they don't believe that any credit card data was compromised through the exposed server because they don't store that data. But they do store names of employees and customers, birth dates, home addresses and email addresses.

As a global brand it is unclear how many, if any, of the records leaked were of Americans. With that said, anyone who is an employee, independent distributor or customer of Avon's would be well advised to monitor their credit report. Because the data leaked may have included password information, ACCESS is advising anyone with a relationship to the company to change their passwords immediately.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#). Registration is easy and free.

Follow ACCESS

