Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Cyber-Attack in Bulgaria: 70% Could Be Affected

July 19. 2019

Introduction

On July 15 2019, an unprecedented cyber-attack in Bulgaria was announced. Hackers have stolen data from the National Revenue Agency (NRA) relating to around 70% of Bulgaria's population, including foreign nationals and businesses, and comprising names of individuals and companies, personal and corporate identification numbers, email addresses, healthcare and pension contributions information and income details. According to news reports, the Bulgarian government had thus far considered the NRA system to be one of the most advanced systems, into which substantial and continuous investment has been made. By contrast, the hackers claimed the opposite. The Chairman of Bulgaria's Commission for Personal Data Protection announced that he would commence an investigation against NRA. In the wake of such a large-scale cyber-attack, we consider certain steps which organisations and individuals might take in the context of cybersecurity and data breach.

An Unprecedented Cyber-Attack: What is Currently Known

On July 15, 2019, a group of hackers sent an email to a number of Bulgarian news agencies, informing them that they had carried out a cyberattack against the National Revenue Agency (NRA), an agency of the Bulgarian Ministry of Finance, responsible primarily for administering taxes and national insurance contributions, for both citizens and businesses. The cyberattack was confirmed by Bulgaria's prime minister, who convened an emergency meeting of the government's Security Council on July 16, 2019. The hackers reportedly announced that the stolen data relate to personal data of over 5 million Bulgarian nationals, as well as foreign nationals and companies. If correct, this would represent around 70% of the 7 million population of Bulgaria.

It has since been confirmed that the information leaked is authentic and has not been falsified.

Parts of the stolen data were sent by the hackers to news agencies and reportedly include names of individuals and companies, personal and corporate identification numbers, email addresses, health care information and income details. The hackers

Contact Information:

If you have any questions regarding this alert, please contact:

Mark Dawkins
Partner
mark.dawkins@akingump.com
London
+44 20.7661.5330

Jenny Arlington
Counsel
jarlington@akingump.com
London
+44 20.7012.9631

have reportedly stated that the initial leak covers 57 out of a total of 110 compromised sets of data, with a total volume of around 21 gigabytes.

The full scale and details of the cyberattack are still under investigation. At this stage, it has been reported that the attack took place on June 29, 2019, when the hackers penetrated one of the servers of the Ministry of Finance. The NRA has stated that it operates around 60 databases, and personal data are stored on various servers. The attack apparently only infiltrated one of those databases, but as the data are interlinked, the hackers gained access to wider data sets.

Immediate Aftermath

This is the first publicly reported successful cyberattack in Bulgaria on such a large scale.

Several Bulgarian national agencies have commenced investigations and are cooperating in the aftermath of the attack, including the State Agency for National Security, the Ministry of the Interior's Lead Agency for the Fight against Organised Crime and the State e-Government Agency. On July 16, 2019, the minister of finance and the minister of the interior spoke before members of the Bulgarian Parliament and answered questions in relation to the attack. One of the hackers, reportedly a 20-year old employee of a cybersecurity company, was arrested on July 17, 2019.

Bulgaria's Commission for Personal Data Protection has reportedly been informed of the cyberattack, as well as the European Union's cybersecurity agency, the European Union Agency for Network and Information Security (ENISA).

According to the Bulgarian minister of the interior, the NRA systems are being checked to prevent similar attacks in the future. In that context, a thorough investigation is being carried out into: attempts to access the NRA's servers and databases; any successful access and any unauthorized access that might have taken place during the months preceding the attack; and the relevant cybersecurity and IT systems in place.

What Can Be Done Now and What Can Businesses Take Away?

According to news reports, the Bulgarian government had thus far considered the NRA system to be one of the most advanced systems, into which substantial and continuous investment has been made. By contrast, the hackers claimed the opposite.

One of the takeaway points at this stage is that businesses, government agencies, and data controllers and processors generally, would be wise to investigate carefully whether their systems comply with cybersecurity regulation, including the GDPR. As recently as July 8, 2019, the Information Commissioner's Office (the U.K. data protection authority) announced its intention to fine British Airways £183 million (approximately $230 million), 1.5 percent of the company's annual turnover, for a data breach under the GDPR, as a result of a similar cyberattack, where stolen data affected around 500,000 customers. CPDP, the Bulgarian data protection authority has announced that an investigation would be undertaken against the NRA (see above) and the outcome remains to be seen. The maximum fine for a data breach under the GDPR is €20 million (approximately $22.5 million), or 4 percent of an organization's annual turnover, whichever is higher.

Further, consideration should be given not only as to whether more could be done to enhance an organization's cybersecurity, but also whether appropriate protocols are in

place and would be followed if and when a cyberattack takes place. As mentioned in our recent alert "A Year of GDPR: Five Recommendations to Help Limit Regulatory Scrutiny," implementing training and education programs, as well as ensuring that internal controls are at satisfactory levels, will help minimize the risk of a breach.

In addition, in light of the large scale of data affected and the attention that the cyberattack has received publicly, individuals and companies affected might wish to consider whether any steps will now be required in order to protect their legal rights.

We will be monitoring the situation for further developments.

akingump.com