Bulgaria: A Whole Nation Hacked

CASE STUDY

In July 2019, an anonymous hacker emailed Bulgarian media outlets to proclaim that they had gained access to the database of the Bulgarian tax service. As is often the case with hacks, many of the details were unclear, but one thing stood out: this was an attack of a staggering scope. Bulgaria has a population of around 7 million people, and the Bulgarian news media reported that the hacker had gained access to the data of 5.1 million. Analysts quickly concluded that almost everyone who paid taxes in the country had been hacked. The precise data that were accessed was not entirely clear, but it was certain that vital information like names, addresses, data regarding income, and social security numbers had been compromised.

The incident prompted a flurry of questions in the press and online: Who did it? How did it take place—what vulnerabilities in the tax service's systems did the hacker use to gain access? Could it have been prevented? Were the Bulgarian authorities sloppy, or were their cybersecurity efforts the best that could be expected and the hack unavoidable? Most importantly, what was the impact of this hack, both for the 5 million Bulgarians whose data had been accessed and the Bulgarian authorities?

The first question is yet to be adequately answered. The Bulgarian police, undoubtedly under severe pressure to produce a suspect, briefly detained Kristiyan Boykov, a young "computer wizard" employed by a firm focusing on cybersecurity. It was believed that he had perpetrated the attack to make the point that Bulgaria needed to do more to protect its data. In 2017, he had exposed vulnerabilities in the website of the Bulgarian Ministry of Education, and he subsequently gave an interview on Bulgarian television explaining that he had exposed these flaws as a matter of "civic duty."

The then 20-year-old suspect denied all involvement and was released, though prosecutors continued to insist that he is the main culprit, conceding only that others may have been involved as well. They pointed to an email linked to the hack that was sent from one of the computers in Boykov's possession. When the hack took place, it was assumed to be an attack from outside the country, for the email in which the hack was announced had been sent from a Russian IP address. However, as the investigation progressed, it became clear that this IP address was simply a smokescreen and the email had in fact originated within Bulgaria.

What vulnerabilities did the hacker exploit? Cybersecurity experts in Bulgaria quickly concluded that the attack was perpetrated through a system created to file VAT returns from outside Bulgaria. They identified it as an SQL injection attack, which takes place when corrupted input is fed into a system; instead of performing the tasks that it is supposed to, the system performs the orders it received through the corrupted input. SQL injection attacks are often explained using the metaphor of a fully automated bus: it obeys the commands it gets and will halt at the right stops if it is told to, but if the commands are corrupted, the bus may, for instance, halt every three minutes whether there is a stop or not.

Could the hack have been prevented? Looking at the statistics, it becomes clear that the Bulgarian hack is not the only one to have been perpetrated by using an SQL injection; between 2017 and 2019, almost two-thirds of all attacks on software applications were carried out by the same method. However, there are ways to protect computer systems against such an attack, and they are not complicated. One of these, is, of course, to use the right software and make sure that the patches for it are applied as soon as they become available. A powerful protection against SQL injection in particular is the use of so-called prepared statements. By using such statements, only certain input is accepted: to use the metaphor of the bus again, you cannot simply, for instance, tell the bus to stop all the time; you can only enter the name of specific streets.

As always, suspicion is a powerful protective tool in cybersecurity. When dealing with sensitive data, it is important to monitor access to the system that hosts it and, importantly, log and study unsuccessful efforts to send input (which sometimes prove to be an attempt to hack the system). It is also useful to try hacking your own system; if the Bulgarian tax service had enlisted its own "hacking squad," it would surely have found the vulnerability early on and prevented the attack.

None of these strategies were in place in Bulgaria, according to the country's cybersecurity experts. The hacker boasted of having obtained access to the system several years before the date of the actual attack, and the email announcement to the press contemptuously referred to cybersecurity in Bulgaria as a "parody" of a real one. That may be a harsh judgment, but it is true that many experts had issued the same warnings as the hacker for a long time. Indeed, several months before the

tax database hack, the Commercial Registry of Bulgaria was attacked as well. After the tax hack took place, it became clear that the Commercial Registry had yet another vulnerability: anyone could gain access to thousands of social security numbers stored on the website of the Commercial Registry merely by performing a search on Google.

The scale and depth of the tax hack, however, alerts us to the fact that official databases and systems around the world have been frequently attacked. One of the most spectacular hacks of a government agency took place in 2016, causing the Central Bank of Bangladesh to lose over $80 million. The loss of money would have been much higher—the hackers targeted a total of around a billion dollars—but for mistakes in the wiring instructions that caused several orders to transfer money from the bank to be blocked in the United States. Investigations into the causes and perpetrators of this hack are still ongoing.

In 2019, Germany was shocked by one of the biggest data hacks in recent history when very personal details of major politicians (including Chancellor Angela Merkel) were published on Twitter. The German authorities immediately stressed that no really sensitive information had been accessed, but the hack was a huge embarrassment nonetheless, compounded by the fact that the data had been online for several months before their discovery. To add insult to injury, the hack had been perpetrated by a 20-year-old student using commonplace techniques.

The Bulgarian case, however, stands apart, as the hack targeted data from almost everyone in the country who paid taxes. But what made cybersecurity in Bulgaria particularly vulnerable—allegedly the real motivation behind the 2019 hack? To begin with, Bulgarian authorities make a distinction between critical infrastructure and non-critical databases. Critical infrastructure is mostly linked to defense facilities and systems. Bulgaria is a member of NATO, so non-members could try to gain access to Bulgarian defense systems to spy on the alliance, hence their categorization as critical. The tax databases were not considered critical and thus received less attention from the state's cybersecurity experts.

These experts are now urging the Bulgarian authorities to step up their efforts to protect their data systems because the impact of such hacks is potentially devastating. Hackers often sell data to criminal gangs, and the data of tax-paying Bulgarians are especially interesting to them as they do not change quickly: people do not change houses or addresses every year and, generally speaking, their income does not fluctuate dramatically either. After the 2019 tax hack, *The New York Times* cited one cybersecurity expert as saying that the data obtained could easily be sold for about $200 million. The Bulgarian news media have already reported fraudulent schemes mostly targeting the elderly in the country, though it is not clear if there is a clear link with the tax hack.

Sadly, the risks will remain in place for many years to come, with two in particular standing out: credit card fraud and identity theft. According to some reports in the Bulgarian news media, the hacked income data goes as far back as 2007. It would be easy for criminals to use this data to make lists of people in Bulgaria who are more affluent and use credit cards. Fortunately, credit card use is not widespread in Bulgaria, but if criminals do succeed in perpetrating this kind of fraud, the costs for both the individual and the bank in question may be huge. There is a huge political price for the Bulgarian authorities to pay as well. Tax-paying citizens need to be sure that their data are being kept safe. Few people like paying taxes to begin with, but they should never feel that they put their financial security at risk the next time they file a tax report. Bulgaria is a member of the European Union and must abide by the General Data Protection Regulation, a strict set of rules that obliges governments and companies to protect the privacy of citizens and clients. The tax authority was fined €3 million for the breach of data by the country's privacy watchdog. While many of the Bulgarians whose data were illegally accessed may feel that this fine is justified, experts say that this does not solve the problem: Bulgaria needs to take steps to hire more cybersecurity experts and review the security of all data systems.

However, being a member of the European Union has added another wrinkle to Bulgaria's cybersecurity problems. Cybersecurity experts are in short supply thanks to freedom of movement, as talented IT workers can easily migrate from Bulgaria to other member states of the European Union where the salaries are more competitive than what the Bulgarian government offers. This point was forcefully made by Boyko Borissov, the Prime Minister of Bulgaria, after the attack on the tax database took place. According to him, the Bulgarian state pays cybersecurity experts a monthly salary of around 1,500 Bulgarian leva (approximately €770), but in the private sector the starting salary is at least six times that amount.

Prime Minister Borissov also said that he had considered the idea of outsourcing Bulgarian cybersecurity to experts in other countries, but the costs had proven prohibitive. Aside from the troubling legal implications of giving foreigners access to the sensitive data of Bulgarian citizens, the government would have to trust that the systems of the company it had hired were safe

themselves—sadly, that is not always the case. The Bulgarian government is now working on a project to create a special cybersecurity unit consisting of experts who are paid well above the average Bulgarian salary.

Sources: Information Security Office, University of California Berkeley, "How to Protect Against SQL Injection Attacks," security.berkeley.edu, accessed January 4, 2021; Appknox, "Biggest Threat to Appliccation Security: SQL Injection Attacks," appknox.com, March 17, 2020; Nural Amin and Shafayat Hossain, "Not Much Progress in Recovering Bangladesh Bank's Stolen Money," *The Business Standard*, tbsnews.net, February 4, 2020; Jeremy Kirk, "Breach Saga: Bulgarian Tax Agency Fined; Pen Testers Charged," bankinfosecurity.com, August 30, 2019; Bill Bostock, "A Hacker Broke into Bulgaria's Tax System and Stole the Details of Every Working Adult in the Country," *Business Insider*, July 22, 2019; Alexander Kolev, "Cybersecurity Is Tragic Despite Millions Spent," www.segabg.com, July 19, 2019; Marc Santora, "5 Million Bulgarians Have Their Personal Data Stolen in Hack," *The New York Times*, July 17, 2019; Tsvetelia Tsolova and Angel Krasimov, "'Wizard' Cybersecurity Expert Charged with Record Hack of Bulgarian Tax Agency," Reuters, July 16, 2019; Kate Connolly, "German Cyber Attack: Man Admits Massive Data Breach, Say Police," *The Guardian*, January 8, 2019; "Hacked: The Bangladesh Bank Heist," Al-Jazeera, May 24, 2018.

CASE STUDY QUESTIONS

8-13 Identify and describe the security and control issues related to the hacking technique discussed in this case.

8-14 What managerial issues are faced by Bulgarian civil servants in charge of cybersecurity?

8-15 Discuss the potential impact of the Bulgarian tax hack.

8-16 How can data breaches like this be prevented?

Case contributed by Bernard Bouwman

Chapter 8 References

2-Spyware. "Messenger Virus. A New Threat for Facebook Users." (January 2020).

Accenture. "Ninth Annual Cost of Cybercrime Study." (March 6, 2019).

Akamai Technologies. "What Is Malware?" www.akamai.com, accessed March 27, 2020.

Anderson, Chad, Richard L. Baskerville, and Mala Kaul. "Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information." *Journal of Management Information Systems* 34, No. 4 (2017).

Bose, Idranil, and Alvin Chung Man Leung. "Adoption of Identity Theft Countermeasures and Its Short- and Long-Term Impact on Firm Value." *MIS Quarterly* 43, No. 1 (March 2019).

Cram, W. Alec, John D'Arcy, and Jeffrey G. Proudfoot. "Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance." *MIS Quarterly* 43, No. 2 (June 2019).

Federal Bureau of Investigation. "2019 Internet Crime Report." (2020).

Fernandez, Manny, David E. Sanger, and Marina Trahan Martinez. "Ransomware Testing Resolve of Cities Across America." *New York Times* (August 22, 2019).

Fruhlinger, Josh. "Recent Ransomware Attacks Define Malware's New Age," *CSO* (February 20, 2020).

Goode, Sigi, Hartmut Hoehle, Viswanath Venkatesh, and Susan A. Brown. "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach." *MIS Quarterly* 41, No. 3 (September 2017).

Gwebu, Kholekile L., Jing Wang, and Li Wang. "The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management." *Journal of Management Information Systems* 35, No. 2 (2018).

Hinks, Gavin. "FRC Chief Indicates Support for a UK Version of Sarbanes-Oxley." Boardagenda.com (March 10, 2020).

Hui, Kai-Lung, Seung Hyun Kim, and Qiu-Hong Wang. "Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks." *MIS Quarterly* 41, No. 2 (June 2017).

Javelin Strategy Research. "2020 Identity Fraud Study." (April 7, 2020).

Kaplan, James, Wolf Richter, and David Ware. "Cybersecurity: Linchpin of the Digital Enterprise." McKinsey & Company (July 2019).

Kaspersky Lab. "Kaspersky Finds Mobile Malware Attacks Doubling from 2018." *TechBarrista* (March 12, 2019).

Kerner, Sean Michael. "Microsoft Patches Out-of-Band Zero-Day Security Flaw for IE." *eWeek* (December 20, 2018).

Liang, Huigang, Yajiong Xue, Alain Pinsonneault, and Yu "Andy" Wu. "What Users Do Besides Problem-Focused Coping When Facing IT Security Threats: An Emotion-Focused Coping Perspective." *MIS Quarterly* 43, No. 2 (June 2019).

Madnick, Stuart. "Blockchain Isn't as Unbreakable as You Think." *MIT Sloan Management Review* 61 No. 2 (Winter 2020).

McMillan, Robert. "Microsoft Announces a Monster Computer Bug in a Week of Them." *Wall Street Journal* (May 15, 2019).

Moody, Gregory D., Mikko Siponen, and Seppo Pahnila. "Toward a Unified Model of Information Security Policy Compliance." *MIS Quarterly* 42, No. 1 (March 2018).

NHS. "Records Management Code of Practice 2020." (October 2020).

Oracle and KPMG. "Oracle and KPMG Cloud Threat Report." (2019).

Panko, Raymond R., and Julie L. Panko. *Business Data Networks and Security*, 11th ed. (Upper Saddle River, NJ: Pearson, 2019).

Parenty, Thomas J., and Jack J. Domet. "Sizing Up Your Cyberrisks." *Harvard Business Review* (November–December 2019).

Ponemon Institute. "2019 Cost of a Data Breach Report." IBM Security (2019).

PriceWaterhouseCoopers. "Business Continuity Management." www.pwc.co.uk, accessed January 2, 2021.