DATA PROTECTION

Daniel Markuson *examines why governmental institutions around the world continue to fail to protect their citizens' data*

More and more governments around the world see data encryption as an obstacle that prevents them from fighting criminal activities. For example, the US, UK, Canada, Australia and New Zealand have been asking big technology companies to build back doors into their encrypted products and services for quite some time. The companies, however, are not so quick to comply with such requests – adding the back doors would mean breaking their promise to keep their customers' data private. Moreover, restricting encryption on US-based messaging platforms such as WhatsApp and iMessage would affect millions of users worldwide.

The discussions pose something of a paradox. Data breaches, hacks and cyber attacks, which we hear about every day, affect not just private companies. In recent months, governmental institutions around the globe have been suffering from hacker attacks and data leaks. Due to various software system flaws or simple human error committed by gullible employees, millions of unsuspecting citizens get affected every year. The fact raises some serious questions: Why are our authorities asking for the easy access to our private information while they fail to protect what they already have? Shouldn't the security of databases containing personal data be their top priority?

NO SUCH THING AS TOO SMALL

Some governments have inveterate beliefs that they are too small and insignificant for hackers to attack them. However, recent events in Baltimore, Florida and Texas defy these views, as attacks on local government bodies are multiplying in the US. In May, Baltimore struggled with a cyber attack that froze thousands of computers and disrupted real-estate sales, water bills, health alerts and many other services. A few Florida municipalities had to pay hackers a ransom of $1.1-million after municipal employees were locked out of their email accounts and important files. Just recently, in August, a ransomware attack hit local governments in Texas, affecting up to 23 entities. And it looks like the list will continue growing.

Below are just a few good examples of this year's governmental data breaches. They were sudden and unexpected, so we all might learn something from them. The scope and the number of citizens affected ensure that these cases will go down in the history of infamous hacks on people's data. In May, Ivan Begtin, a co-founder of a Russian NGO called Informational Culture, discovered and documented several leaks from Russian Government sites. The personal information, tax identification numbers and passport details of 2.25-million citizens, including high-profile politicians and Government officials, were exposed online and even available for download. Mr. Begtin investigated online certification centres, Government portals and an e-bidding platform used by Government agencies to find out that most of them were leaking the personal data of Russian citizens.

In June, five million of Bulgaria's seven-million citizens had personal data compromised in an attack on the national revenue agency. Both private and social security information on every adult was exposed – a perfect scenario for identity theft or attacking lucrative targets. The leaked database was shared with journalists and posted on several public forums. The exact date/dates of the attack cannot be specified. Apparently, the agency was not aware of it until the hacker sent an email to various news outlets, mocking the agency's poor state of cyber security.

> HUMAN ERROR CAUSED BY UNTRAINED EMPLOYEES IS THE SECOND BIGGEST SOURCE OF DATA BREACH

In the late spring of this year, an unknown hacker attacked a US Customs and Border Protection sub-contractor and put much of its internal data on the open web for download. The exposed database included photos of travellers' faces and license plates, surveillance equipment schematics and sensitive contracting documents. Now, the border surveillance company – a long-time contractor named Perceptics – is suspended from carrying out business with the federal Government. However, over 400GB of data was stolen, with 100,000 people reportedly affected.

The internal IT ecosystem of Governmental institutions is home to some of the most valuable and sensitive data in the world. Although both the authorities and hackers know that, the former sometimes struggle to employ even the most basic cyber security practices. That leaves Governmental institutions particularly exposed to ransomware.

Even Government institutions that handle sensitive data are vulnerable to attack

Out-of-date software used by some governments and a variety of their contractors makes them easy targets. That's the most common reason why these institutions get hacked. Updating a digital security system and making it immune to cyber attacks requires millions of dollars and high-level skills. Slow internal processes, complicated procurement procedures, and under funding add up to the reasons why some organisations are still using unsafe security software.

However, all governmental institutions must make cyber security one of their top priorities and inevitably find a budget for it. Strong IT department with flawless cyber security software and a powerful firewall is what every government agency must have to protect citizens' private data. What heads of governments sometimes do not realise is that data breaches result in great expenses, and the security of people's sensitive information should be considered priceless.

To restrict unauthorised access to data, it needs to be encrypted. Depending on the software, encryption makes it very difficult or even impossible for third parties to hack. A reliable VPN can encrypt the online traffic of all employees. It also ensures that all digital resources are safe when members of staff need to access them. Moreover, a VPN is the one solution to stay secure when working remotely from home or travelling abroad.

Human error, which is usually caused by untrained employees, is the second biggest source of data breaches. According to the 2019 Data Breach Investigations Report, carried out by Verizon, 34 percent of breaches were caused by insiders. Using weak and non-unique passwords as well as falling for phishing scams can hurt an organisation immensely. It is quite easy to leak email and password information when an employee clicks on a virus link, reveals user credentials or downloads malware attachments. Just one click can compromise the entire database.

Therefore, it is of crucial importance for employees to have cyber security training to stay up to date with recent threats and new software bugs. They should get regular reminders about the latest phishing attacks and social engineering tactics used by scammers. Not every government official has cyber security knowledge, but their secure mindset can be developed through digital literacy.

We can't control what information authorities have about us and how they handle it. However, you should take some measures once you hear a company or an institution relevant to you has been hacked.

First of all, you need some kind of confirmation that your data was really exposed. Due to privacy regulations in some jurisdictions, organisations might be required to inform affected people immediately after a data breach occurs. However, sometimes officials might want to suppress the news, and it goes public only when hackers expose it on their forums. On the other hand, it is very important to know how real the information about your leaked data is. Sometimes scammers send fake warnings just to scare their potential victims and make them share their passwords. If you learn that a breach has affected a government agency that has your personal data, find out what information has been leaked and act accordingly.

IN JUNE, FIVE MILLION OF BULGARIA'S SEVEN-MILLION CITIZENS HAD PERSONAL DATA STOLEN

If the leaked information includes your log-in details, you should change them immediately. Don't forget to renew your passwords from time to time and start using password managers that will help you create strong and unique log ins. They also safely store all your complex passwords for you. Where possible, set up 2-factor authentication, which requires a second password or PIN, usually sent to your smartphone for extra security.

If your payment details were stolen, you should contact your bank as soon as possible and freeze your card. Check your recent statements for any suspicious activity. Set up a fraud alert with the credit bureau that will notify you if someone tries to open new accounts or take out loans using your card.

If your ID, passport or social security number are leaked, inform the relevant authorities right away. Prove your identity before anyone else does, issue a fraud alert and review your social security statement and credit reports for any illegal activities or suspicious charges. All these numbers associated with a person's identification are the most valuable piece of information hackers are looking for. They can use your stolen personal details for various crimes, and recovery from identity theft is not easy.

PLAY IT SAFE

If cyber criminals who have hacked an institution and stolen your personal information send you a threatening email asking for money, never pay them. If you transfer them your money, it's likely that the requests will never stop. Before you send any funds to scammers, contact the relevant authorities, preferably the police. You should also contact the breached institution as they usually provide free assistance in the aftermath to reduce the likelihood of fraud. Their help may include identity theft protection, account blocking or credit file monitoring.

Remember: everyone can become a breach victim. Even governmental institutions that handle our most sensitive information are vulnerable. Just stay alert and notify authorities whenever there is a need to minimise the damage. Hopefully, government agencies will learn from the mistakes others endured and start investing more in cyber security ●

Daniel Markuson is an internet security enthusiast and the digital privacy expert at NordVPN, the virtual private network provider. Daniel loves putting his 10-year expertise into service to help people stay private and secure online.

Governments are increasingly exploring back doors into encrypted products and services