PDPA, A PERFECT BACKDOOR FOR HACKERS

Everyone has heard about **PDPA**, the recent Personal Data Protection Act applicable after May 2022 in which any company that possesses data about any individual residing in Thailand must comply with their request to verify, correct, or even erase the data in their database. This is regardless of the company location, and yes if you are a company in Asia or USA and you process data about individuals living in Thailand, you are under obligation to conform to this law. Conforming means replying to satisfy each individual's request and accept to disclose the information you are holding and accept to validate it or possibly erase it. Penalty for not conforming within one month of the initial request can reach a value of 5 million THB, and potentially a Prosecution by the data owner.

Despite great intentions to protect the privacy of personal information, the implementation seems to have resulted in exactly the opposite.

Let's review how it has already been abused by hackers in Europe under the similar GDPR:

1. REQUESTING INFORMATION THAT DOES NOT BELONG TO YOU:

A white hacker decided to test the system and simply sent requests to 150 companies demanding to be handed over all information they possessed about his girlfriend, using her name and an email address on an account he quickly created with her name on google… A very simple exploit.

Our of 150 requests, 83 companies disclosed that they had information on her and 37 accepted to remit all information they had based on a simple email request with a phone number as a proof of ID! Some others requested additional information but evading the request was quite simple.

The kind of information disclosed included credit card, social security numbers, passwords, and even her mother's maiden name, in reality, a volume of information that could easily be used to purchase items online, possibly even opening an account with a credit line in online shopping and all sorts of exploits based on Identity theft.

WHAT IS WRONG HERE

GDPR has certainly great value for privacy, the intention was good, but the implementation failed massively. First, businesses have very limited time to respond facing huge fine if they don't, second while GDPR concerns data privacy, it is rarely handled by an IT security specialist and more than often left in the hands of an HR division manager. There is no approved mechanism to confirm the identity of the claimer, and it is left to the Data Controller to assess if he is dealing with the right person. This is utterly wrong and will lead to more damage to the final end-user whom the law was trying to protect.

2. REVERSE RANSOMWARE

Ransomware is the action where hackers access your data and encrypt it, demanding a ransom to provide you with a decrypted version. A 10 billion-a-year industry. Huge ransoms have been paid by large institutions as Jackson County in Georgia (US$400,000), Lake City Florida (US$500,000), Riviera Beach Florida (US$600,000) and Nayana, South Korean web provider (US$1,000,000)

Reverse ransomware is the idea that once private information held in a company has been hacked, the ransom is demanded to avoid the public disclosure of the information, subjecting the company to public embarrassment and a huge fine from the EU. Considering 4% of a company turnover as a fine, you can easily see that a much cheaper option seems to be paying the hacker and hiding the hack.

WHAT IS WRONG HERE

Once again, the pressure of the huge fine, the time to react and the consequences of general embarrassment are so important that the blackmail is working. GDPR has given hackers an incredibly strong negotiating position. Now no longer the company risks losing some data, which with a good backup procedure is an annoying but remediable situation, however this time, there is no way out, it is either 20 million Euros or whatever ransom the hacker demands.

3. EXPLOITING A HACK TO GET FULL DISCLOSURE OF ALL INFORMATION

Once an account has been breached from a user in a large company as it did happen to Spotify, having access to a client account allows you to request all information detained in this person's name. You might not be worried if your playlist or favorite music becomes public knowledge, but all your bank transactions, private identity details, and credit card have a real hacking value. They were easily obtained from Spotify after the users' account was cracked, and who has a strong password on his Spotify account?

Imagine if this situation happens with a car rental company, delivery company, medical institution, the sensitivity of information the hacker can obtain takes a totally new dimension. Don't get hacked and kidnapped the same day…

WHAT IS WRONG HERE

GDPR has transformed what was an annoying hack of your basic account, with very little consequences into a potential nightmare handing over the keys of the safe to the bad guys… Once again, a clear well-defined policy became the hacker's best friend through poor implementation.

Implementing a request to solidify their identification procedure with a 2-factor authentication would have protected the user entirely, but this is not a legal requirement and Spotify was here not at fault.

Is there more to come? Sure is, hackers spent their entire time thinking about ways to breach security, companies have other jobs to take care of like marketing, selling, producing, quality control, etc… it is an unfair battle, but when government implement policies that can be clearly hacking weapons you really wonder what they had in mind when they created them.

WHERE WILL WE GO FROM HERE?

The lawmakers must implement bulletproof procedures to solidify the identity of the requester, currently the weakest link in the procedure. The process for users to prove their identity must be clearly defined however this cannot be a knee-jerk reaction. Badly thought out mechanisms could easily turn out to be phishing exploit to collect privacy authentication data this time.

You don't want to see fake companies advertising their compliance to GDPR and inviting people to authenticate to verify their private data while in fact, users would simply feed another level of hackers with their authentication keys…

Author**: Bernard Collin is a long-time resident in Thailand and the CEO of SafeComs, a company focusing on IT Support and Security. For information on the PDPA or its implementation, please write to **dpo@safecoms.com