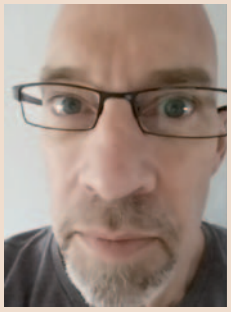
Webwaves



Dave Annetts
ASEG Webmaster
david.annetts@csiro.au

Data breaches

Recently Thomas et al. (2017) presented the results of a year-long longitudinal study of the effects on users of different types of credential theft *viz*: data breaches, phishing and keyloggers. Keyloggers are legal tools designed to covertly capture keystrokes and, while they are sometimes integral components of an operating system, are often installed without users' knowledge in order to steal password or credit card information. Phishing was briefly discussed in PV189, and is the attempt to obtain sensitive information by using a disguise. Data breaches were the third type of credential theft studied, and this type is the main topic of this month's Webwaves.

Data breaches are the intentional or unintentional release of secure or private or confidential information to an untrusted environment. One source (breachlevelindex.com) suggests that, worldwide, some 1 901 866 611 data records were compromised during 918 incidents in the first six months of 2017. This works out to slightly over 10.5 million records per day from organisations such as a motor vehicle registry in Kerala, India, an email marketing organisation in the USA, a data analytics firm working for a USA political party, a restaurant app and the UK's NHS. Only 18% of those breaches were accidental. Most data breaches were malicious, and most (74%) were from outside the organisation. As to the remainder of incidents, only 8% were the result of a malicious insider, and there was one state-sponsored incident.

So what was the nature of these breaches? What data were released without authorisation? Only 13% were directly related to finances. Some 6% were related to account and to data access. Most (74%) data released were directly related to identity theft. Identity theft affected over 770 000 Australians in 2015 (http://www.abc.net.au/am/content/2015/s4215824.htm) and can have far-reaching impacts on its victims.

As any geophysicist is aware, not all data are equal. Of all compromised records it is estimated that some 4.6% were useless because they were encrypted. For this reason, experts currently consider that, whilst some emphasis should remain on network security, it would be better to shift the focus of data protection towards rendering data useless if (when ...) it is released.

With this in mind, the EU has introduced the General Data Protection Regulation (GDPR) to be implemented on 25 May 2018. One requirement of the GDPR is that companies storing data must lodge notification of breaches within 72 hours. Others include the right to be forgotten, the right of individuals to transfer data from one processing system to another, and the necessity for a lawful basis for data processing. Data are required to be protected by default, and therefore data are pseudonymised so that stored data cannot be attributed to individuals without additional information. Decryption keys must be stored separately to pseudonymised data. In this way, if (when ...) data breaches occur, their impact on individuals is minimised.

So why is this matter being discussed in the ASEG's Webwaves column? The ASEG is affected by this Regulation because of our European membership. Therefore, early in 2018, the database that stores Members' details will be moved to two-factor authentication. Member's data will be more secure because two sources of information will be required to access their data – not just one source, which is the current requirement.

So what were the results of the longitudinal study into types of credential theft? Thomas et al. (2017) showed that blocking unusual location-based login attempts that were typically the result of keylogging or successful phishing trips (...) could mitigate the risk of data breaches. Because attempts at identity theft are increasing, recommendations for care when following URLs are likely to remain for the foreseeable future.

In more prosaic web-related news, readers are altered to updates of the manuals section of the website (aseg.org.au/equipment-manuals-brochures). Recently, Peter McMullen (GeoResults Pty Ltd) was able to supply updated manuals for some magnetometers and susceptibility meters. A video recording of the WA Branch's October Technical night featuring Bill Peters (Southern Geoscience Consultants) talking about 'Geophysics for magmatic Ni-CU (PGE) Exploration' has also been added (aseg.org.au/wa-branch-technight-night-bill-peters). The efforts of Kim Frankcombe and Chris Bishop in resolving technical issues before this talk could be advertised on the website are much appreciated.

Reference

Thomas, K., F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comansecu, V. Eranti, A. Moscicki, D. Margolis, V. Paxson, E. Bursztein, 2017, Data breaches, phishing or malware? Understanding the risks of stolen credentials, *24th ACM Conference on Computer and Communications Security*, Dallas, Texas.