Data Breach in the News

Tips to help your organisation stay secure

The recent spate of data breaches in the news have served as a timely reminder on why we need to maintain good security hygiene. All organisations hold some form of sensitive data. These can be in the form of customer personal information, health data, credit card or transactional data, login credentials, and Intellectual Property (IP). There is no magic pill that will make you immune, but there are a set of measures that can be put in place to lower your risk of data breach.

In the News

Unfortunately, data breaches happen on a fairly regular basis, and plenty of them have been big enough to make the news. They should serve as a reminder to us about the repercussions of poor security posture.

Most recently, the Equifax data breach exposed the personal data of 143 million Americans, and the Swedish Transport Agency breach cost two ministers their jobs after the negligent handling of sensitive infrastructure and personal information that exposed the data of the majority of Swedish residents. Nearer to our shores, the breach of the Australian Red Cross Blood Service last year exposed the personal details of half a million blood donors.

What this means for you?

You are not immune to data breaches. To help protect you against them, there are a range of security measures that can be implemented within your network to provide enhanced security, and allow for the simple detection and investigation of common attacks. We recommend working with your IT provider (where practical) to uplift network security, enforce controls that reduce entry points for an attacker, and provide a practical solution for investigating incidents.

Actions you can take

- **Maintain an accurate and complete Asset Inventory** – Know what is in your environment so you can quickly identify if you are exposed to a vulnerability.
    - This should include your devices; and their operating systems, patch levels, anti-virus signature definitions, firmware, applications, and databases.
- **Regularly apply critical patches and updates –** Without patching, your network is left vulnerable for an attacker to exploit with ease using already-defined scripts. Updated Antivirus software can prevent known malware from spreading if it is injected into a vulnerable system.
    - Update systems and applications in your environment.
    - Check anti-virus and operating system patches have been successfully installed.
    - Deploy critical security patches on all systems, as soon as they are released.
- **Undertake regular vulnerability assessments** – Even after regular security upgrades, patching, and testing; new and existing vulnerabilities may still appear over time. It is important to validate the controls that are in place, and to regularly check for vulnerabilities such as access points an attacker may use.
    - Perform a regular vulnerability scan of your network to identify if any vulnerabilities exist. Make sure the scanner is using the latest vulnerability databases.
- **Lock down access rights** – Provide access to individuals based only on what they need to complete their job.
    - Support this 'lockdown' with processes and tools that can be put in place to manage privileged access and monitor its use.
- **Incident Response Management** – If an incident were to happen, the last thing you would want to see is fuel added to the fire.
    - Minimise the impact of an incident by being prepared. Have a plan on the key roles, key questions that need to be answered and how important decisions will be made for when an incident occurs. Preparation starts well before an incident has occurred. Build and exercise your organisation's "muscle memory" to respond and recover by exercising your plan through cyber simulations.
- **Data Loss Prevention** – Detect and block any potential leakage of data. Use encryption for data in storage and in motion.

Cyber security cannot be executed effectively using a "point-in-time" or solely tactical approach. It is important for you to consider other areas where you may have cyber exposures, and to create an environment where security is considered and improved upon on an ongoing basis.

We would advise you to:

- **Assess wider security across the business** – to validate the tactical actions above, and identify any other cyber exposures that may exist.
- **Obtain specific security expertise and/or validation** – which your current IT provider may be unable to provide. Partner with people with the real-world expertise in an ongoing relationship, to confirm your business is safe from the changing vulnerability and attack landscape.

Further Readings

[1] World's Biggest Data Breaches. *Information is Beautiful, Sept 2017.*
Link: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

[2] Sweden exposed sensitive data on citizens, military personnel. *ITNews, Australia, July 2017.*
Link: https://www.itnews.com.au/news/sweden-exposed-sensitive-data-on-citizens-military-personnel-469046

[3] Sweden accidentally leaks personal details of nearly all citizens. *The Hacker News, July 2017.*
Link: http://thehackernews.com/2017/07/sweden-data-breach.html

[4] Swedish Government Scrambles to Contain Damage From Data Breach. *NYTimes, July 2017.*
Link: https://www.nytimes.com/2017/07/25/world/europe/ibm-sweden-data-outsourcing.html

[5] Red Cross Blood Service admits to personal data breach affecting half a million donors. *ABC Australia, October 2016.*
Link: http://www.abc.net.au/news/2016-10-28/red-cross-blood-service-admits-to-data-breach/7974036

[6] Australian red Cross Blood Service data breach. *Office of the Australian Information Commissioner, August 2017.*
Link: https://www.oaic.gov.au/media-and-speeches/statements/australian-red-cross-blood-service-data-breach

[7] Failure to patch two-month-old bug led to massive Equifax breach. *Ars Technica, September 2017.*
Link: https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/

[8] Apache Struts vulnerability blamed for Equifax data breach. *TechTarget, September 2017.*
Link: http://searchsecurity.techtarget.com/news/450426409/Apache-Struts-vulnerability-blamed-for-Equifax-data-breach

[9] Millions more Americans hit by government personnel data hack. *Reuters, July 2015.*
Link: http://www.reuters.com/article/us-cybersecurity-usa/millions-more-americans-hit-by-government-personnel-data-hack-idUSKCN0PJ2M420150709

Disclaimer: Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte New Zealand brings together more than 1200 specialist professionals providing audit, tax, technology and systems, strategy and performance improvement, risk management, corporate finance, business recovery, forensic and accounting services. Our people are based in Auckland, Hamilton, Rotorua, Wellington, Christchurch and Dunedin, serving clients that range from New Zealand's largest companies and public sector organisations to smaller businesses with ambition to grow. For more information about Deloitte in New Zealand, look to our website www.deloitte.co.nz.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.