Mega Breaches

Behind the Headlines

ilex
International

A hack is described as gaining unauthorised access to an individual or organisation’s computer system. More often than not, this is for the purpose of gaining private, sensitive data - such as health records, credit card details or personal information.

In the age of ‘big data’, cyber criminals can compromise almost any type of personal information. As technology evolves, the number of routes for cyber criminals to gain access to this information is growing rapidly. Cyber attacks are also increasing due to more businesses using the cloud, adopting Bring Your Own Device (BYOD) and other connected objects.

REASONS BEHIND ATTACKS

Hacks are usually conducted with criminal intent. Many hackers are looking for some kind of personal gain – often financial, although sometimes this can just be to expose or damage the reputation of the parties involved.

The cyber crime landscape is always changing and this is one of the reasons IT security professionals find it difficult to respond/stay one step ahead. Today there are many different forms hacks and cyber attacks take and reasons behind them. These include:

- **STATE-SPONSORED ATTACKS:** Often considered the new form of inter-state spying, state-sponsored cyber attacks, or cyber espionage, are often aligned with either the political, commercial or military interests of the country of those carrying out the attacks. This is usually to uncover state secrets or areas of interest that may be useful to the country in question.

  State-sponsored attacks can often be difficult to uncover, as they do not typically cause too much disruption. Usually the perpetrator will deploy malicious malware on the victim's systems that often remain dormant, staying invisible for long periods of time.

- **INSIDER THREATS:** The risk of insider threats is growing, with 64 percent of security professionals saying insider threats occurred more frequently in 2015[i]. Insider threats are attacks carried out – both accidentally and maliciously – by those within an organisation; employees, contractors and third parties and disgruntled ex-employees.

  Insider threats can be difficult to detect. Despite the increasing risk associated with them, many organisations do not put as much focus or necessary controls in place as they do with external attacks.

- **EXTERNAL ATTACKS:** On a basic level, these are attacks by anyone outside of an organisation. However, beyond that the reasons behind external attacks can differ greatly – state-sponsored attacks are an example. More usually, external hackers are simply cyber criminals out for personal financial gain.
  - **HACKTIVISTS:** A form of external attacker, who has a perceived ideological or moral purpose for carrying out the attack. For example, Anonymous.

[i] Insider Threat Report 2015, Computer Weekly: http://www.computerweekly.com/ehandbook/Insider-Threat-Report-2015

MEGA-BREACH FACT FILE

Weaknesses in controlling access to sensitive data or applications means businesses are effectively leaving the door open to cybercriminals. Eight percent of respondents that had suffered a security breach blamed poor access control. The biggest proportion were from large companies (26 percent), followed by medium companies (15 percent), with only five percent of small companies highlighting access control as the reason for a breach. By putting an increased focus on access control, businesses can also minimise the security risks associated by BYOD and access to data residing in cloud applications.

COMPANY:
Sony

DATE:
November 2014

WHAT WAS STOLEN?
Personal information about Sony employees including private emails and salaries, copies of un-released Sony films.

REASON FOR HACK:
A hacktivist group named ‘Guardians of the Peace’ originally released the data, having made a demand for money which was ignored by Sony.

At first, it was suggested that the hack was a state-sponsored attack carried out by North Korea, who were protesting against the Sony film ‘The Interview’. However, since then many IT security experts have asserted the attack looks like that of the hacking group, with help from insiders. A media interview with a member of Guardians of Peace hinted that a sympathetic insider or insiders aided them in their operation and that they were seeking “equality.”[ii]

COMPANY:
Morgan Stanley

DATE:
January 2014

WHAT WAS STOLEN?
730,000 customer records

REASON FOR HACK:
Former financial advisor with the firm, Galen Marsh, downloaded the confidential information and transferred it to his home computer. He then uploaded the data of around 900 clients, confirming that he would sell additional data. It was reported that the adviser used a reporting tool that gave him access to massive amounts of data on clients.

[ii] Sony Hack, What We Know and Don’t So Far: https://www.wired.com/2014/12/sony-hack-what-we-know/

COMPANY:
Ashley Madison

DATE:
July 2015

WHAT WAS STOLEN?
Unknown amount of company data, including private information of 37 million users.

REASON FOR HACK:
A group named 'The Impact Team' stole the data, threatening to release it if the site did not get shut down immediately. When this failed to happen, the group released the private data of the site's 37 million users. Ashley Madison's chief executive Noel Biderman told security reporter Brian Krebs that it might have been an inside job.

"We're on the doorstep of [confirming] who we believe is the culprit, and unfortunately that may have triggered this mass publication," Biderman, said. "I've got their profile right in front of me, all their work credentials. It was definitely a person here that was not an employee but certainly had touched our technical services."

COMPANY:
TalkTalk

DATE:
October 2015

WHAT WAS STOLEN?
150,000 customer records

REASON FOR HACK:
Four men – including a boy aged 15 – were arrested for committing the attack. It's believed in the days before the attack, the organisation received a ransom demand but ignored it, believing the demand to be a hoax. This wasn't the first time TalkTalk had been targeted, but this attack resulted in the resignation of the organisation's Chief Executive, Dido Harding.
There is limited evidence that this attack was supported by insiders however in January 2016 it was reported that three call centre workers were arrested in suspicion of using customer data to commit fraud.

IMPACT ON BUSINESSES

Cyber-attacks can have serious, damaging effects on organisations. The initial damage that has to be dealt with is the damage to reputation. After an attack, customer and partner trust in an organisation can deteriorate rapidly, leading to a loss in business opportunities. This in turn can have a severe impact on an organisation's finances, with customers looking elsewhere and money being spent on retroactive action and even – in some cases – fines.

However, after time reputation can be fixed to a certain extent. Fixing the problem presents a far greater, on-going problem. After a breach, organisations will face constant scrutiny from board members and auditors to ensure that the same does not happen again. This alone puts IT departments under exacerbated stress to make sure everything is completely secure.

It's almost inevitable that consumer confidence will erode with each high profile breach. Research by Ilex International shows organisations in the UK are still overconfident when it comes to security breaches, despite the sheer amount of them in recent years. Until there are stringent regulations in place which force organisations to disclose a breach, no one will know how many attacks are truly taking place.

WHAT CAN BUSINESSES DO TO MITIGATE RISK?

All organisations, regardless of size, are at risk of a cyber attack. The biggest mistake an organisation can make is to believe a breach won't happen to them – zero risk does not exist in today's world. However, in order to minimise risk of attack, there are simple steps organisations can take.

SECURITY POLICY AND EMPLOYEE EDUCATION

Organisations need to ensure they have a comprehensive security policy and employee education programmes in place. The policy should outline the responsibilities of everyone on the team and the process for reporting suspicious activity. Security software needs to be in place and up to date so that the risks are constantly being monitored.

DATA PROTECTION

Providing the same level of security to all of your data can be difficult and can often lead to holes in your data protection that can be exploited by hackers. To lessen this risk, it's crucial for organisations to focus on their most important and sensitive data. The tightest security controls should be placed around this data to ensure it is properly secure.

ACCESS CONTROL

Knowing who has access to your data – especially the most sensitive data – is a key factor in keeping it safe. Access must be tightly controlled and only granted to those that need it. In addition, the IT department needs to keep a close eye on the access taking place, so they will be able to spot when anomalies occur and take appropriate action. Similarly, when employees or third parties leave an organisation, it is crucial that their accounts and associated access are shut down immediately. Dormant accounts are one of the easiest ways for cyber-criminals to gain access into an organisation's IT systems.

IDENTITY AND ACCESS MANAGEMENT

Key to implementing these security practices is a comprehensive identity and access management system – which is essential for both large and small organisations. It represents the foundation of a secure system. Organisations can spend time and money securing parts of their applications or networks, but it is having unparalleled knowledge of who their users are and being able to control their levels of access that will provide the necessary security.

With insider threats seemingly a main source of security breaches today, identity and access management is the cornerstone to preventing unauthorised access to sensitive company data. Without a comprehensive security policy and identity and access management system, organisations are leaving themselves open to security breaches.

ABOUT ILEX INTERNATIONAL

Ilex International is a European Identity and Access Management (I&AM) software vendor. Founded in 1989 Ilex offers a comprehensive range of solutions including identity management (identity, rights and role management) and access management (authentication, access control, SSO, identity federation and card management.) The organisation invests heavily in R&D, providing state of the art technology and services to a large international customer base across finance, defence, healthcare, government and retail sectors.

ILEX INTERNATIONAL

info@ilex-international.com
www.ilex-international.com/en/