20191CSE0392
5CSE7
Nishanth

CYBER SECURITY- Case Study

Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber-attacks. It aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks and technologies.

The legal requirement for cyber security

The GDPR and DPA (Data Protection Act) 2018 require organizations to implement appropriate security measures to protect personal data. Otherwise, there's a risk of substantial fines. Cyber security is a critical business issue for every organization.

Why is cyber security important?

1. **The costs of cyber security breaches are rising**

   Privacy laws such as the GDPR and DPA 2018 can mean significant fines for organizations that suffer cyber security breaches. There are also non-financial costs to be considered, like reputational damage.

2. **Cyber-attacks are increasingly sophisticated**

   Cyber-attacks continue to grow in sophistication, with attackers using an ever-expanding variety of tactics. These include social engineering, malware and ransomware).

3. **Cyber security is a critical, board-level issue**

   New regulations and reporting requirements make cyber security risk oversight a challenge. The board will need to continue to seek assurances from management that its cyber risk strategies will reduce the risk of attacks and limit financial and operational impacts.

4. **Cyber-crime is a big business**

   In 2018, the cyber-crime economy was estimated to be worth $1.5 trillion, according to a study commissioned by Bromium. Political, ethical and social incentives can also drive attackers.

The scale of cyber crime

Cyber-crime is pervasive, and many organizations are struggling to adapt to the modern threat landscape.

For instance:

- According to the UK government's Cyber Security Breaches Survey 2019: General findings visualization (Business and Charities), almost half (48%) of businesses identified at least one cyber-attack per month.
- The National Crime Agency's Annual Plan 2019/20 estimates that 84% of fraud reported in the UK is cyber-enabled (from almost anywhere in the world).
- The Federation of Small Businesses puts the annual cost of cyber-attacks at £4.5 billion for small businesses.
- The UK government's 'Understanding the UK cyber security skills labor market' research report found that 54% of UK businesses have a basic cyber security skills gap, and 35% were not confident about dealing with a cyber security breach or attack.

Types of cyber criminals

Cyber-attacks are carried out by both individuals and organized groups. Threat actors include:

State-sponsored groups – those that carry out cyber warfare campaigns targeting critical national infrastructure.

Hacktivists – politically motivated attackers who target organizations to promote their ideology. Their activities often relate to human rights, free speech or freedom of information issues.

Insiders – those with privileged access to target systems, including negligent and malicious insiders, as well as external actors who gain access via user credentials.

Script kiddies – unskilled attackers who use off-the-shelf scripts and exploit kits.

20191CSE0392
5CSE7
Nishanth

Fighting cyber crime

1. Cyber Essentials

The Indian government’s Cyber Essentials scheme sets out five security controls that provide organizations with that basic cyber hygiene. Its assurance scheme gives organizations the opportunity to demonstrate that they have implemented these measures via independent certification.

2. Staff awareness training

People are widely acknowledged to be the weakest part of any security system. Even if you implement the best technological measures and put processes in place to ensure they are properly deployed and kept up to date, their effectiveness can be compromised by poorly trained users, putting your organization at risk.

3. Penetration testing

Assess your systems and networks for any potential weaknesses caused by poor or improper system configuration, known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures

Biggest Cyber Attacks Case Study

Biggest Cyber Attacks 2017: How They Happened

Credit reporting agency Equifax aggregates financial data on more than 800 million consumers and 88 million businesses worldwide.

On July 29, 2017, the company detected and blocked suspicious network activity associated with a web portal used by U.S. consumers to file disputes. Later analysis revealed the portal’s application framework, Apache Struts, was outdated and had a severe security vulnerability.

Equifax hired cybersecurity firm Mandiant to conduct a forensic analysis, which revealed a massive data breach affecting 143 million U.S. consumers.

Further investigation later increased the number to 145.5 million – or about 45% of the U.S. population.

Severe Vulnerability Overlooked

Equifax was first alerted to the Apache Struts vulnerability (CVE-2017-5638) on March 8, 2017, more than two months before the breach started, according to testimony to a U.S. House subcommittee by former Equifax CEO Richard Smith. Equifax failed to act on the alert and apply the available_patch. Seven days later, the company also performed vulnerability scans that failed to identify the flaw, said Smith. Hackers launched the attack exploiting the vulnerability about two months later, on May 13, 2017.

By the time the breach was discovered in late July, hackers had accessed dozens of databases and created more than 30 backdoors into Equifax's systems.

Security Takeaways

- **Know your systems –** Equifax failed to realize an alert for a critical vulnerability applied to one of its web portals. A flaw that should have been patched within 48 hours went unpatched for months.

- **Scans Aren't Enough** – Equifax's vulnerability scans, performed seven days after the Apache Struts flaw was public knowledge, did not identify the weakness in its web portal. This is why it's important to perform multiple scans with different tools, and never rely on a tool to "handle" your security.

Uber Data Breach – 57 million Records

Uber's CEO revealed on Nov. 21, 2017, that the ride-hailing service failed to disclose a massive data breach last year.

In Oct. 2016, hackers accessed a server containing personal information for more than 57 million Uber drivers and riders. They demanded a $100,000 ransom to delete their copy of the data, which Uber paid.

The attackers allegedly first accessed a private GitHub repository used by Uber's developers. The repository contained code with login credentials for other Uber systems, which ultimately provided access to the stolen data.

Uber later identified the hackers and pushed them to sign nondisclosure agreements. It also disguised the ransom payment as part of a bug bounty program, according to the New York Times. Lawsuits are now raining down on Uber from attorneys general across the U.S.

Security Takeaways

The Uber data breach may prove to be an example of when the cover-up is worse than the crime. The breach undoubtedly harmed the company’s brand, but the damage caused by hiding the attack has only begun.

And the lawsuits haven’t even started.

The lesson is to know the data breach notification laws and rules that apply at your local, state, and federal level, and those that apply to your industry.

Also, when in doubt, err on the side of transparency. Thousands of companies have been breached. Most customers will forgive you (but some won’t).