CYBER SECURITY IN SOCIETY ASSESSMENT 1

Infrastructure

Introduction

Between the21st August and 5th September 2018, British Airways' network was attacked. "Hackers managed to breach its website and app, stealing data from many thousands of customers in the process." (Anon, 2018).

This attack was directed at the payment page of BA's website as British Airways itself "did not mention breaches of anything else, namely databases or servers—anything indicating the breach affected more than the payment information entered into the website." (Klijnsma 2018). The infiltration was implemented either by an internal threat actor implanting malicious code to the webpage directly or via third party software infected by an outside element.

The type of network used for payment/booking services has integral pieces of hardware all open to exploitation. Shown below are viable attack vectors that may be inside British Airways' network and would be particularly open to exploitation:

Device/ Method	Description	Vulnerabilities	Exploits that can be used
Mobile API	Links mobile devices to internal system (usually displaying html)	Poor Coding and authentication, High Privileges for everyone	API Abuse, Cross-site Scripting
Database Servers	Used for storing most if not all information	Poor Coding	SQL Injection
Web Servers	Used to interact with devices or Mobile API to provide webpages	Software or Firmware not up to date, Poor Coding	DDOS, Cross-site Scripting
Internal Payment Information	A copy of payment information kept by the company	Poor Encryption and storage	Cross-site Scripting, Social Engineering
External Payment Information	Data sent to bank/ payment system outside the company	Insecure Transmission	Cross-site Scripting, Data Interception (e.g. Wiretapping)
Logging/ Marketing Data	Data kept by the company for later use	Accessible by many entities, sent to third parties	Social Engineering
Hardware Firewall	Device that data packets must pass through, identifies and authenticates	Software or Firmware not up to date	DDOS, Trojan Horse
Cabling	The connections between main devices that don't use wireless	Transmission via electrical signals	Wiretapping
Staff	The employees of the company	Human error, Inconsistent Security	Social Engineering

Possible attacks, including software, hardware and physical, are discussed below, together with options to reduce vulnerability.

Distributed Denial of Service (DDoS) –

This is “a coordinated attack, generated by using many compromised hosts” (Hogue et al., 2015); the main goal being to overload a system with requests. BA’s web servers would be the main target for this attack due to it being within the De-militarized zone (DMZ) on the edge of the network and hence accessible from the internet. This attack can also be done from within a private network but a threat actor needs access to do so, if important hardware is kept a large enough physical distance from users there is usually no issue. To reduce the effectiveness of this attack, firewalls, Intrusion detection systems or Intrusion prevention systems can be implemented, these systems are necessary to ensure the acknowledgement and blocking of malicious data.

SQL Injection –

Running several databases is a must for large companies, this leaves them open to SQL Injection as “SQL is the standard language for accessing Microsoft SQL Server, Oracle, MySQL, Sybase and Informix (as well as other) database servers.”(Clarke 2012). If not coded correctly to limit user input the credentials of users can be pulled from the database. Fully testing the error handling using penetration testing and having code reviewed before wide scale use can ensure that this attack is mitigated.

Cross-site Scripting (XSS) –

> “These Attacks make use of vulnerabilities in the code of web-applications, resulting in the serious consequences, such as theft of cookies, passwords and other personal credentials.” (Shalini and Usha, 2011).

This is believed to be how BA was breached recently. Third-party advertisements on the payment page were not properly vetted and so were able to collect user bank credentials. A more secure vetting procedure for third parties and consistent review of their code is necessary to reduce this risk.

API Abuse –

> “An Application Programming Interface (API) provides an abstraction for a problem and specifies how clients should interact with software components that implement a solution to that problem” (Reddy, 2011).

The mobile API would be designed to make accessing HTML webpage resources easier and more efficient, these code solutions are often developed quickly and this can mean they are “often done without full consideration of security implications.” (Mendoza 2018). This opens them to attacks such as Cross-site Scripting mentioned earlier or social engineering. Coding best practises and peer reviews should be implemented to curb this issue.

Social engineering –

A user of the system, be that an end user or a company employee, can be deceived into giving away information such as usernames, passwords or even full account access to a threat actor using social engineering. A threat actor will attempt to interact with a user as the victim they want to steal data from or as a member of staff with authoritative power. Training can be given to improve awareness but only teaches very specific scenarios and ultimately a charismatic attacker can work around these. Data taken in other attacks or during reconnaissance can also be used to improve the lie created by the attacker; if marketing lists, payment forms and other user data are not secured properly or are given to third party businesses who have lax encryption they can be intercepted and used maliciously.

Trojan Horses –

Malicious code can be disguised as harmless so that a user or computer system will activate it. A user may be sent an email that appears legitimate but when they follow a built in link or open a document attached to it their computer will become infected. An attacker may use another attack such as DDOS or ARP Poisoning to shut a system down or put devices in a weakened state before hiding the Trojan within, to be executed at a later date.

Confidentiality, Integrity and Availability (CIA) Model –

To ensure the best use of data, the CIA model can be followed. In relation to the breach of BA, they provided Availability but fell short on Integrity which "requires us to feel safe that data transmitted, processed and stored has not been changed from its original" (Nweke 2017). Because data was taken from their payment page they did not have full Integrity and as a result confidentiality was also lost.

Authentication, Authorisation and Accounting (AAA) Model –

To better enact the CIA model, the AAA model can be followed. British Airways' payment page was most likely able to find the cause of the breach by using accounting to keep logs of webpage changes. The third party who was used as a source for delivering the malicious code failed authentication and authorisation by allowing the attacker to input said code.

Strategy document

To reduce vulnerability of a company system several policies can be put in place, several are discussed below:

User Policies –

Users including those that work at BA can be manipulated for an attacker's gain, including being a victim of Social Engineering and Trojans as discussed in the report above.

Password Policies are one way to reduce this, they involve creating long passwords with a variety of numbers, letters and special characters along with other safety techniques. Using this policy can be effective in decreasing hacking attempts based on guessing user passwords using brute force or dictionary attacks. Downsides to this sort of policy such as changing the user's password every six weeks increases the chance that the user's will be unable to "cope with the number and complexity of passwords, and resort to insecure workarounds as a consequence" (Inglesant and Sasse 2010). This can come in the form of users "writing passwords down" *(ibid),* allowing an attacker who sees it to acquire system entry. To improve this it may be important to keep the number of passwords and how quickly they are rotated low but have them be longer, ways to do this include using a passphrase instead, several random words put together that would defeat most password cracking software and be remembered easier by users.

Implementing an Acceptable use policy (AUP) may also lower the chance of offences occurring within the business by detailing what a user can or can't do when working within the company. The computer misuse act should be one of the laws used to create this policy as it aims to secure computing devices against unauthorised use (*Computer Misuse Act* 2015). The focus should be on making users fully aware of their rights and ability when interacting with the company.

Network security policies –

To curb the issues with network security, standards can be followed to ensure secure transmission:

Using Access Control lists and firewalls can be a good solution to make sure connections coming through are correct by verifying their source, destination and content. Subnetting and using VLANs can help contain any infection that does managed to breach the network. The goal should be to create an architecture that uses these to reduce privilege to only the bare minimum needed for each user.

Cabling can be secured from wiretapping by implementing fibre optic cables on all connections to outside services. Fibre optic cable should be used for higher speed connections and because "information sent via fiber-optic cabling is much more difficult to intercept because light can't be read in the same way signals sent via copper cabling can be." (Bishop, 2013). Copper cable should only be allowed inside the network and should be tested to ensure they have not been tampered with but also this test should only be done every few months ensuring the employees doing the checking can be thorough.

Data collection Policies –

A company like BA that interacts with user data needs to be protected in accordance with the law.

The GDPR, a new privacy law that states “Personal data shall be: … adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed” (GDPR 2018). This is to ensure only necessary is stored and will help the company minimise the data an attacker can use. There are several other principles that minimise how data can be kept and used, not following this document can lead to a company receiving a hefty fine.

References

Anon. (2018) *British Airways breach: How did hackers get in?*. London: BBC. Available from https://www.bbc.co.uk/news/technology-45446529?intlink_from_url=https://www.bbc.co.uk/news/topics/c0ele42740rt/data-breaches&link_location=live-reporting-story [accessed 29 November 2018].

Bai, H., Atiquzzaman, M. and Lilja, D. (2004) Wireless sensor network for aircraft health monitoring. In: *1st International Conference on Broadband Networks*, San Jose, CA, USA, 24-29 October. New York, USA: IEEE, 748-750.

Bishop, E. (2013) *Ethernet vs. Fiber – Everything You Need to Know.* Available from https://www.business.org/services/internet/ethernet-vs-fiber-basics/ [accessed 01 December 2018]

Cheng, S., Chen, P., Lin, C. and Hsiao, H. (2017) Traffic-Aware Patching for Cyber Security in Mobile IoT. *IEEE Communications Magazine*. 55(7).

Clarke, J. (2012) *SQL Injection Attacks and Defense*. Waltham, Mass: Syngress.

Computer Misuse Act 2015 (c.18). UK: TSO. Available from https://www.legislation.gov.uk/ukpga/1990/18/contents [accessed 04 December 2018]

Edwards, B., Hofmeyr, S. and Forrest, S. (2016) Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity. 2(1)* 3–14.

General Data Protection Regulation (GDPR). (2018). General Data Protection Regulation (GDPR) – Final text neatly arranged. Available at: https://gdpr-info.eu/ [Accessed 01 December 2018].

Hoque, N., Bhattacharyya, D.K. and Kalita, J.K. (2015) Botnet in DDoS Attacks: Trends and Challenges. *IEEE Communications Surveys & Tutorials*, 17(4) 2242-2270.

Hydara, I., Sultan A.B.Md, Zulzalil, H. and Admodisatro, N. (2014) Current State of research on cross-site scripting (XSS) – A systematic literature review. *Information and Software Technology*, (58).

Inglesant, P. and Sasse, M. A. (2010) The True Cost of Unusable Password Policies: Password Use in the Wild. In: *28th international conference on Human factors in computing systems (CHI 2010)*, Atlanta, GA, USA, 12-15 April. New York, USA: ACM, 383-392

Klijnsma, Y. (2018) *Inside the Magecart Breach of British Airways: How 22 Lines of Code Claimed 380,000 Victims* [blog]. 11 September. Available from: https://www.riskiq.com/blog/labs/magecart-british-airways-breach/ [accessed 30 November 2018]

Kumar, S. and Tapaswi, S. (2012) A centralized detection and prevention technique against ARP poisoning. In: *2012 International Conference on Cyber Security, Cyber Warfare & Digital Forensic (CyberSec)*, Kuala Lumpur, Malaysia, 26-28 June. New York, USA: IEEE, 259-264.

Kumar, S.A.P. and Xu, B. (2017) Vulnerability Assessment for Security in Aviation Cyber-Physical Systems. In: *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing*, New York, NY, USA, 26-28 June. New York, USA: IEEE, 145-150.

Liu, Y. Sarabi, A. Zhang, J. Naghizadeh, P. Karir, M. Bailey, M. and Liu, M. (2015) Cloudy with a Chance of Breach: Forecasting Cyber Security Incidents. In: *24th USENIX Security Symposium*, Washington, D.C., USA, 12-14 August.

Mendoza, A. and Gu, G. (2018) Mobile Application Web API Reconnaissance: Web-to-Mobile Inconsistencies & Vulnerabilities. In: *2018 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 20-24 May. New York, USA: IEEE, 756-769.

Nweke, L.O. (2017) Using the CIA and AAA Models to Explain Cybersecurity Activities. PM World Journal, 6(12).

Reddy, M. (2011) *API Design for C++*. Boston: Morgan Kaufmann.

Rensing, C., Karsten, M. and Stiller, B. (2001) A Survey on AAA Mechanisms, Protocols, and Architectures and a Policy-based Approach beyond: Ax. Zurich. Available from https://www.researchgate.net/publication/244390366_A_Survey_on_AAA_Mechanisms_Protocols_and_Architectures_and_a_Policy-based_Approach_beyond_Ax

Sampigethaya, K. Poodvendran, R. and Bushnell, L (2008) Security of Future eEnabled Aircraft Ad hoc Networks. In: *The 26th Congress of ICAS and 8th AIAA ATIO*, Anchorage, Alaska, 14-19 September.

Shalini, S. and Usha, S. (2011) Prevention Of Cross-Site Scripting Attacks (XSS) On Web Applications In The Client Side. *International Journal of Computer Science*, 8(4) 650-654.

Xiao, Y., Chen, H., Yang, S., Lin, Y. and Du, D. (2009). Wireless Network Security. *EURASIP Journal on Wireless Communications and Networking*, 2009 1-3.