SCC306 Internet Applications Engineering

Consolidated Report

Nicholas Race & Adrian Friday

Name:	**Ben Goldsworthy**
Student Number:	33576556

Executive Summary

£250,000. £400,000. £980,000.

These are the fines levied against Sony, TalkTalk and Nationwide, respectively, for data breaches. Investigating TalkTalk, the ICO concluded that their “failure to implement the most basic cyber security measures allowed hackers to penetrate [their] systems with ease.”[1] For Nationwide, it only took an unencrypted laptop to go missing to leave their systems vulnerable. “During its investigation, the FSA found that the building society did not have adequate information security procedures and controls in place, potentially exposing its customers to an increased risk of financial crime.”[2]

Your company does not need to needlessly put itself at risk by neglecting to implement strong data security practices. This report will outline the primary risks of failing to do so, a series of suggestions of how to go about it and an enumeration of benefits to be reaped once such a system is in place.

Key Risks

1. Social Engineering
Perhaps the most insidious of the possible attacks you will be faced with, social engineering involves an attacker taking a step back from the computer screen and trying to break into your systems via people, using a suite of techniques that involve various social psychology-based tricks. These range from the complex (for example, the attacker ringing up customers at random and pretending to be responding to a tech support query until they hit upon a person that is actually waiting for a tech support response, and then using the access they would likely be willing to give a tech support worker to gain access to the user's account[3]) to the laughably simple (a 2003 study found 90% of workers willing to share their passwords in exchange for a free pen[4]) - though the simplicity of such attacks can be a source of humour in the tech community,[5] the damage they can cause must not be.

1.1. Phishing
In a phishing attack, the attacker tricks a customer into following a link that purports to be for your genuine website, but which in fact leads to a website the attacker controls. When the user enters their details, the attacker gains them and can use them to access the legitimate website. 91% of attacks in 2012 were phishing attacks.[6]

1.2. Whaling
Whaling is a variant of phishing that specifically targets high-level employees of a company, such as yourself. This is a riskier prospect for the attacker, but can obviously prove more lucrative – just think what you could do with CEO-level access to a company's systems! For the sake of your customers, you must also be on your guard.

2. Automated Attacks
These attacks usually involve web spiders that crawl every website they can find on the internet, testing for various vulnerabilities and exploiting them or alerting the attacker to them when they are found. For this reason, you can fall victim to these sort of attacks even without an attacker having to decide to attack your business.

2.1. Distributed Denial of Service (DDoS)
In a DDoS attack, the attacker floods your site with so much fake traffic that legitimate user requests cannot get through as the server is busy dealing with fake requests. This can cause your site to respond slowly to users, or go down entirely – both providing an unsatisfactory user experience.

2.2. Web page vulnerabilities
These include things like SQL injections, XSS, client-side security and other issues. You don't need to know the ins and outs of how they work, only that they are easy to patch up with a little bit of thought when

developing the system, but can be devastating if ignored – an SQL injection can be used to wipe your entire database with a single line of code.

3. Human Error
Human error is considered the leading cause of data breaches and loss, with estimates ranging from it being responsible for anywhere from 24[7] to 95%[8] of cases. This human error can occur at all levels of the organisation, too, from the factory floor or the customer all the way up to your very own office – for example, the Petraeus scandal in the US which starred a four-star General and (now former) Director of the CIA.[9]

3.1. Poor passwords
This happens more often than you may think – for 20 years of the Cold War, the US nuke code was set to '000000'.[10] 91% of user passwords appear in a list of the 1,000 most common.[11] These are trivial to implement in a so-called 'dictionary-attack', where each is tried until one succeeds, which can be added to an automated web crawler's arsenal, as discussed in §2.

4. Man-in-the-Middle
In this attack, the attacker intercepts traffic between the customer and your site. This can allow them to monitor behaviour, or even provide them with the user's credentials.

Recommendations

Firstly, security must be considered as a development concern, rather than as a post-development one. To use an analogy, this means building a house out of fire-redardant materials, with fire doors between rooms and multiple escape routes, rather than making a one-exit, doorless house out of wood and placing a fire extinguisher by the door.

To reduce the potential for human error, you must design the system to only require human input when absolutely unavoidable – a system is only as strong as its weakest link, so you must minimise the presence of those weakest links. Where they are unavoidable, forcing your users to use passphrases is a more secure alternative to passwords[12] (Diceware represents the pinnacle of the form[13]). In the coming years, these may be phased out entirely in favour of biometrics such as fingerprint scanners,[14] but bear in mind these are so far not impervious to attack.[15] They will also likely require distributing specialist equipment to all of your customers.

When it comes to securing yourself against automated attacks, it would be wise to get your website audited by a security professional. For an added layer of certainty, considering hiring penetration testers – these are professional hackers who will attempt to break into your site, and then tell you how they did so. A very important basic principle is to not trust the client, and so not to perform any security or verification functionality on the client's side of the website, rather than the server side.

Finally, you can help alleviate the risks of phishing attacks for customers by ensuring your website uses HTTPS and has an up-to-date certificate – this will tell customers when they are on your legitimate site and not an imposter's. HTTPS also encrypts the requests between user and site, which means a man-in-the-middle attacker will not be able to read anything useful from their intercepted data.

Business Benefits

The benefits to your business are manyfold. Beyond avoiding the large fines imposed on companies that suffer data breaches mentioned in the beginning, customers will appreciate your company for taking their security and privacy seriously – “75 percent of adults in the UK would stop doing business with, or would cancel membership to, an organisation if it was hacked.”[16] If your business deals with sensitive data, in particular (e.g. banking, medical, etc.), strong security is an absolute must. The costs of implementing it now massively outweigh the potential losses down the line as a result of not doing so.

References

[1] https://ico.org.uk/about-the-ico/news-and-events/talktalk-cyber-attack-how-the-ico-investigation-unfolded/
[2] http://www.fsa.gov.uk/library/communication/pr/2007/021.shtml
[3] http://www.social-engineer.org/framework/general-discussion/common-attacks/tech-support/
[4] http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/
[5] http://www.smbc-comics.com/?id=2526
[6] https://www.firmex.com/thedealroom/spear-phishing-whos-getting-caught/
[7] http://datahealthcheck.databarracks.com/2015/#3
[8] https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf
[9] http://www.nytimes.com/2015/03/04/us/petraeus-plea-deal-over-giving-classified-data-to-lover.html
[10] http://arstechnica.com/tech-policy/2013/12/launch-code-for-us-nukes-was-00000000-for-20-years/
[11] http://www.passwordrandom.com/most-popular-passwords
[12] https://xkcd.com/936/
[13] https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/
[14] http://www.networkworld.com/article/3074664/security/google-s-trust-api-bye-bye-passwords-hello-biometrics.html
[15] https://blog.lookout.com/blog/2013/09/23/why-i-hacked-apples-touchid-and-still-think-it-is-awesome/
[16] https://www.helpnetsecurity.com/2016/06/08/companies-take-customers-security-seriously/