Breach Disclosure

Admitting Failure and Damage Control

Computer Security

Quinn Collins
quinn.collins@tufts.edu

12-13-2017

Abstract

Modern software development has come to value speed and quantity produced, even over quality. Often, organizations would rather have a feature-rich product delivered on time, than a product that has been built defensively and carefully checked for bugs and vulnerabilities, but late or less feature-rich as a result. This has led to a standard of reactive security: expect things to break, and fix mistakes and vulnerabilities as they are found. However, this raises serious security concerns, since little is done to eliminate unnoticed vulnerabilities before public release. To make matters worse, these organizations often lack extensive plans for fixing systems and notifying users when proprietary company data or sensitive user data is exposed. Many, instead of performing immediate damage control and notifying users, dissemble and delay in order to prevent a loss of reputation. Moreover, breach disclosure isn't always in control of the breached organization: the individual who discovers the vulnerability might decide to immediately release it to the public, disclose it only to the company, or disclose it only to the company conditionally. This paper will discuss common paradigms of disclosure and what both organizations and users should do in the event of a breach to minimize damage to personal data.

Introduction

Data breaches originate in vulnerabilities that allow an attacker to access user or organization data. It is therefore critical to understand where these vulnerabilities come from, and under what conditions resulting data breaches are disclosed.

I. Vulnerability Disclosure

One significant problem with vulnerability disclosure is that many organizations that discover vulnerabilities in their own applications have little motivation to disclose them, since it would often make them seem more insecure to the general public. Unfortunately, the resulting lack of an externally enforced deadline means that internally-discovered vulnerabilities often go unfixed for long periods of time. The burden of disclosure therefore falls on third parties, in many cases. There are a number of ways in which individuals who discover vulnerabilities typically handle them, varying on the severity of the vulnerability, who it affects, and what danger the disclosure presents.

No Public Disclosure:

In this case, the finder only discloses the vulnerability to the vulnerable organization. This is the safest case for the organization, since no information is directly given to the public, users and potential hackers alike. On one hand, the organization will have more time to fix the vulnerability. On the other hand, they might not fix it quickly, since there's no imminent risk beyond other third parties discovering the vulnerability on their own.

Responsible Disclosure:

Under responsible disclosure, the finder of the vulnerability informs the organization of their vulnerability and gives or negotiates a date when they will disclose the vulnerability to the public if the organization has not fixed it. This option is a sort of middle ground: the organization is given time to fix the vulnerability, and the public will informed eventually whether the organization takes action or not.

Full Disclosure:

The individual who discovered the vulnerability releases it to the public. The organization, users, and potential hackers are all informed at the same time. The vulnerable organization has little control in this situation, although it provides them with a compelling reason to fix the vulnerability. The individual disclosing the vulnerability should be careful in this case, since the vulnerable organization likely has good reason to pursue legal action against them.

A third party disclosing a vulnerability should also consider how much to disclose, and when. If the vulnerability is in a pacemaker, for example, releasing technical details might be dangerous (ICS-CERT). If the vulnerability might lead to exposure of user data, waiting too long for public disclosure might be dangerous.

II. Vulnerability Analysis

There are, however, deeper problems than methods of disclosure. Too often, applications are not even tested for vulnerabilities. In the past year, 36% of organizations didn't check their applications with any static analysis security testing, and 46% didn't use any dynamic security analysis testing (Veracode, 10). Even the tested applications, however, aren't being fixed: in the past year, Veracode found only a 19% fix rate (flaws fixed per megabyte of code) in tested applications (Veracode, 6). Thus, too few applications are being tested for vulnerabilities, and even in tested applications, vulnerabilities are not being fixed.

To the Community

I. Why Should I Care?

As the world becomes more connected, data breaches are becoming a more serious issue. Data breaches are becoming bigger, as more people are coming to rely on internet services, and worse, as internet services become more interconnected. In 2016, thousands of data breaches were reported, in which tens of millions of records were exposed. There's also been a fairly consistent upward trend in the number of breaches (compare to 157 reported breaches in 2005), and the number of records exposed has stayed fairly consistent (Statista). Veracode also reports that information leakage has affected more applications than any other type of vulnerability since at least 2011, and affected approximately 65% of applications in this past year (Veracode, 11). The impact of these breaches has also become more serious: the rate of breached individuals exposed to fraud rose from one in nine in 2010 to one in three in 2013 (Javelin, 5), and the estimated cost of data breaches this past year was 3.6 million (Ponemon, 6). Thus, data breaches are a serious issue that isn't getting better.

II. What are We Doing to Fix This?

There are a number of preventative measures in place to help mitigate data breach damage. Static and dynamic analysis scans, as mentioned above, aid in identifying particular vulnerabilities. Legislation, on the other hand, serves to enforce methods of preventing data breaches. California, for example, has implemented legislation that requires breached companies, especially in healthcare, to notify the public in the event of a breach, and to disclose not only a description and timeframe of the breach, but also descriptions of what information was involved, what the organization is doing to mitigate the breach, and what actions users should take (Privacy Rights Clearinghouse). Other legislation, like HIPAA, sets standards of cybersecurity and access to help prevent data breaches (US Department of Health and Human Services). While

healthcare is still a large target for data breaches, industry-wide standards of cybersecurity certainly aid in preventing them. The United States federal government has also released the Vulnerabilities Equities Process, which it uses to determine how it treats zero-day vulnerabilities it discovers (Schwartz et al). While formal details are not disclosed, some public record of the process is certainly useful.

Action Items

I. Organizations

There are a number of measures organizations can take to reduce the risk of data breaches. One of the easiest is to perform static and dynamic analysis of applications to find vulnerabilities, and then fix them before release. In the past year, 83% of organizations released code before testing for and fixing vulnerabilities (Veracode, 10). Simply testing for vulnerabilities would easily reveal unconsidered vulnerabilities before they can be exploited.

Organizations should also have a set plan in place to deal with vulnerabilities and breaches if they should occur. For larger organizations, an incident response team can often be useful: in the past year, incident response teams reduced the cost of breaches to companies by approximately $19 per compromised record (Ponemon). Organizations should also use encryption wherever necessary, and store hashes instead of plaintext data when possible. In the past year, extensive use of encryption reduced the cost of breaches to companies by approximately $16 per compromised record (Ponemon).

Lastly, inform exposed users as soon as possible. Not only do they deserve to know about the security of their information, but they should update their credentials to minimize the chance of fraud.

II. Government

Field-specific legislation that helps to standardize security methods and breach disclosure is useful, especially in fields like healthcare that are disproportionately targeted. The United States federal government's policies on disclosing vulnerabilities should be formalized and publicized as well. According to White House Cyber Security Coordinator Michael Daniel, the Vulnerabilities Equity Process has "no hard and fast rules" (Schwartz et al). This is problematic because it leaves much of the decision to the discretion of the vulnerability discoverer and associated organizations. To avoid influence of individuals or organizations, the details of the process should be made clear and public.

III. Users

Only give away personal information where necessary, and only to organizations that have a good security history. If an account of yours is breached, change your credentials and follow instructions the breached organization provides. Periodically check that your accounts are secure: a good resource for this is https://www.haveibeenpwned.com.

Conclusion

Data breaches are a serious problem that isn't going away by itself. By displaying some of the reasons they still persist and what can be done both by organizations and individuals to minimize data breaches, hopefully improvement can be made. Knowledge of the issue alone is

worth something, given how few organizations scan their code before release, or how little the OWASP Top 10 have changed in the last few years. The responsibility for breach mitigation lies with everyone, organizations, developers, and users alike.

References

"Abbott Laboratories' Accent/Anthem, Accent MRI, Assurity/Allure, and Assurity MRI Pacemaker Vulnerabilities." Industrial Control Systems Cyber Emergency Response Team, 29 Aug. 2017, ics-cert.us-cert.gov/advisories/ICSMA-17-241-01. Accessed 13 Dec. 2017.

Givens, Beth. "An On-the-Ground Look at Consumer Impacts of Data Breaches." Privacy Rights Clearinghouse, 12 Jan. 2016, www.privacyrights.org/blog/ground-look-consumer-impacts-data-breaches. Accessed 13 Dec. 2017.

Identity Theft Resource Center. "Annual Number of Data Breaches and Exposed Records in The United States from 2005 to 2016 (in Millions)." *Statista - The Statistics Portal*, Statista, www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/, Accessed 13 Dec 2017

Office for Civil Rights. "Summary of the HIPAA Security Rule." US Department of Health and Human Services, 26 July 2013, www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html. Accessed 13 Dec. 2017.

Pascual, Al. "The Consumer Data Insecurity Report: Examining the Data Breach — Identity Fraud Paradigm in Four Major Metropolitan Areas." Javelin Strategy, June 2014, www.javelinstrategy.com/research. Accessed 13 Dec. 2017.

Ponemon Institute LLC. "2017 Cost of Data Breach Study." IBM, June 2017, www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN.

Schwartz, Ari, and Rob Knake. "Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerabilities Disclosure Process." Harvard Kennedy School for Science and International Affairs, June 2016. Manuscript.

"State of Software Security 2017." Veracode, 2017, www.veracode.com/resources/state-of-software-security. Accessed 13 Dec. 2017.