Ethan Schreiber

12/2/19

Comp 116: Cybersecurity

Data Breaches: The Clock is Ticking

Abstract

When a major company reports a data breach, it's often front-page news. Many times, these breaches have existed in the company's network for weeks or even months. This is due to the failure of the company's intrusion detection system, or IDS, and the time it takes companies to report breaches once discovered. The two major types of IDS are signature based (designed for known attacks) and anomaly based (designed for unknown attacks). Both types have varying levels of effectiveness. On the other side of the security war is the attackers: there are various strategies that can be employed to avoid IDSs. Once an attacker has created a breach, they work to maintain secrecy as they extract data. When a breach is discovered, companies can take even more time to report the breach to the affected users. Moving to a business view, effects of a breach on a company are rarely very significant. The paper concludes with a discussion of potential steps to speed the process from initial breach to user notification, via IDS improvement and affected user notification improvement.

Introduction

In recent years, the number of companies that have reported a large-scale data breach has skyrocketed. This is indicative of the constantly changing cybersecurity landscape and companies' unwillingness to keep up with the times – but significantly more alarming are the times attached to these breaches. Five months (GRA), two years, four years (Ye). Imagine finding out an account of yours that held sensitive information was stolen four years ago: what could an attacker have done with that information by now? Answers range in severity from no

affect to bank accounts drained and identity stolen. This leads to the guiding question of this paper: Why do companies take so long to report they've been breached? To answer this question, this paper provides an analysis of current types of intrusion detection systems, common reasons breaches occur, and covers the business side of the issue.

Why You Should Care

When users sign up for a service and give their information to a company, they have a reasonable expectation of privacy for that data. When a company gets breached, that sensitive personal data is immediately at risk, and the users should be informed so they can take the appropriate measures. The problem is twofold: first, security has always been a secondary concern for companies – the fallout of a breach is not as big as one might expect – and second, once a company has been breached, they tend to take lengthy periods of time to release that information. This paper's proposed solution to this problem is education. If more people are aware of the repercussions of breaches, companies are more likely to be held accountable and their business will see an impact. Once this happens, investing in security will be more appealing than it is currently, leading to less breaches.

What is an IDS?

An Intrusion Detection System, or IDS, is a blanket term for any software that aims to detect any foreign malicious intrusion into a system. Any company worth its salt has an IDS deployed to protect its systems – before diving into breaches, it's important to understand what protections against them are currently in place.

There are two major types of IDSs: The first is Signature Based Detection. These IDSs check incoming traffic against known attack signatures (bits of code, comparing hashes, etc) (Bricata). In other words, they check to see if the traffic matches an attack that has been seen

before. They are a reactive style of detection given that they only work on previously detected attacks, but they are very, very effective against these threats. However, they are somewhat vulnerable against new versions of the same attack, and completely fail against entirely new attacks (Bricata).

The second type of IDS is Anomaly Based Detection. It aims to compensate for the weaknesses of Signature Based detection by running an active search for suspicious activity on all traffic – trying to run as administrator, for example. Regardless of the operation, running as admin is something to investigate (Bricata). This allows the IDS to potentially identify previously unknown types of attacks, by flagging the behaviors it executes as suspicious. The problem with Anomaly Based Detection is that it can produce many false positives, as it is essentially shooting in the dark (Bricata). For example, if users are permitted to run as admin, all those reports wouldn't be real attacks. It can also be resource-intensive depending on the amount of traffic that needs to be scanned (Bricata).

The 80/20 Rule and Layered IDSs

No security is perfect – every IDS can be fooled or avoided, leading to a breach where the attacker gains access to a restricted system. Attacks tend follow the 80/20 rule: roughly 80% of all attacks on a system will be caught by a Signature Based IDS, and thus aren't significant threats. The remaining ~20% require an Anomaly Based IDS to catch them, and that 20% will cause 80% of the problems within the system (Bricata). Thus, in order to catch as many of the threats as possible, a layered IDS is necessary that includes Signature and Anomaly Based Detection. Failure to include both types can have catastrophic consequences: in 2015 the U.S. Office of Personnel Management (US OPM) announced a 4 million user breach which had occurred mainly because their IDS relies solely on Signature-Based Detection (GRA). One of the

big failures of companies currently is their unwillingness to devote resources to the proper operation of an effective Anomaly-Based IDS, since they are expensive and resource intensive.

Into the Breach(es)

An improperly maintained IDS means breaches can get into the system in a variety of ways. One of the most common is still phishing emails (Gallagher) – a worker clicks on a malicious link and suddenly the attackers have a foot in the network, just like they work there. Other attack vectors include still-prevalent vulnerabilities like SQL injection, Cross-Site Scripting, Cross-Site Request Forgery, and similar. When executed in a covert manner, a single injected script tag can be enough to bypass a low-budget IDS.

Current IDSs are often poorly implemented and maintained due to security's low priority, causing breaches to occur. But why do they take so long to close? There are two major steps between the occurrence of a breach and the public finding out about it: first, the company must discover it's been breached, and then they must decide to report it. Both steps take more time than they should.

As long as an intruder succeeds in avoiding the IDS as a result of their actions, it can be months or even years before the intrusion is even discovered. Because of the level of trust placed in IDSs, not enough human eyes check the system, and the intruder only has to worry about the IDS. For example, when the US OPM was breached, the intrusion took five months to detect and was only found during investigation of a separate breach (GRA, Gallagher). This makes it even more critical that companies inform affected users immediately to prevent more consequences from time lost.

However, it can take an unreasonably long time for companies to report their breaches. For instance, when Yahoo was breached, it took up to two months for Yahoo to come clean (Ye)

to mitigate business-related fallout. Another breach, Equifax, took forty days to disclose its breach of 143 million accounts (Armerding) for the same reason. This is valuable time where the affected users could have taken actions to prevent further negative effects – after Equifax announced its breach, many users executed credit freezes (Adams), a move that would have been much more effective had they been able to do it earlier.

Companies continue to take such long periods of time to disclose data breaches in major part due to lax regulations in this regard. Every state has laws about disclosure of breach knowledge, but almost all of them use a standard of 'as soon as reasonably possible' (Adams) or 'the most expedient time possible' (Hinnen). These terms are not well defined, which allows companies to use reasons like gathering information, waiting on law enforcement, or a whole host of others to delay announcing their breaches and thus harm the affected users.

The Business of Breaches

While there are often repercussions for companies that are breached, they are rarely more than a slap on the wrist. There are two main types of repercussions: direct monetary loss and decline in public opinion. The most severe example of direct monetary loss was Yahoo. Yahoo lost $350 million of its estimated value and ended up being acquired for only 4.48 billion (Armerding). That's a 7% loss in value, which is not insignificant, but when 3 billion accounts were stolen, making it the largest known data breach by 2.5 billion users (Armerding), it suddenly seems less significant. On the other hand, eBay is a good example of a public opinion backlash: their breach of 145 million users' data caused lower activity on their website, but no real effect on business: their revenue and earnings actually went up for that quarter (Armerding). So, none of the repercussions that businesses suffer cause lasting damage to the company.

Take Control of Your Data

So, what can be done to fix these problems? The first step is to demand better from the businesses who have access to our private information. Both steps of breach handling must be sped up – the discovery and the reporting.

For discovery, IDSs must be improved. To incentivize companies to see security as a good use of resources, there need to be significant consequences for failures. Companies should pay adequate damages for the information they lost, whether it be through lawsuits or boycotting services. For reporting, the best step is advocating for tighter security regulations - "as soon as reasonably possible" (Adams) is not an acceptable standard for reporting breaches.

Another way to personally avoid having information stolen is for the public to do their best with the information they control. There are two easy steps everyone should take: the first is to avoid giving services information they don't need to operate. Very few apps need to know your location while you aren't actively using them, for example. Checking permissions and not blindly clicking yes is an important step. The second step is to have no single point of failure. This means that if one account gets breached, other accounts should remain secure. This means using a different password for every service so no credentials can be used on multiple services, and 2-factor authentication so even if a password is broken, the account cannot be accessed.

Conclusion

There are two major areas that need to be improved in order to report breaches in a timely manner. The first is breach detection: an IDS is the best line of protection a company can have, and they need much more support and investment from companies. The second is breach reporting: regulations need to be tightened to ensure affected users are notified in a timely manner. We the people have the power to make these changes and keep our private data safe.

Works Cited

Adams, Kimberly. “Why Do Companies Wait So Long to Tell Us We've Been Hacked?” *Marketplace*, Minnesota Public Radio, 11 Sept. 2017, www.marketplace.org/2017/09/11/why-do-companies-wait-so-long-tell-us-weve-been-hacked/.

Armerding, Taylor. “The 18 Biggest Data Breaches of the 21st Century.” *CSO Online*, IDG Communications, 20 Dec. 2018, www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

Bricata. “Signature Detection vs. Network Behavioral Analysis.” *Bricata*, Bricata Inc, 13 Mar. 2019, bricata.com/blog/signature-detection-vs-network-behavior/.

Gallagher, Sean. “Why the ‘Biggest Government Hack Ever’ Got Past the Feds.” *Ars Technica*, Conde Nast, 8 June 2015, 11:00am, arstechnica.com/information-technology/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/.

GRA Quantum. “Failure of Intrusion Detection Systems.” *GRA Quantum*, GRA Quantum, 15 June 2015, graquantum.com/failure-of-intrusion-detection-systems-3/.

Hinnen, Todd, et al. “Security Breach Notification Chart.” *Perkins Coie*, Perkins Coie LLP, Sept. 2019, www.perkinscoie.com/en/news-insights/security-breach-notification-chart.html.

Ye, Yanfang. “Why Did Yahoo Take so Long to Disclose Its Massive Security Breach?” *The Conversation*, The Conversation US, 30 Sept. 2016, theconversation.com/why-did-yahoo-take-so-long-to-disclose-its-massive-security-breach-66014.