Why Everyone is Still Getting Hacked

John Tagliaferro
December 11, 2017

Abstract

Despite enormous sums of money being spent on corporate security, companies are more likely to be hacked than ever, and most companies feel as though they are blindly investing in cyber security tools. The reason for this is twofold. Firstly, security is not enough of a focus during the design process of software. Secondly, traditional cyber security tools are still in use despite being largely obsolete. This paper intends to explore and explain these two problems and propose a solution that will start to mitigate this growing problem.

1 Introduction

Huge companies are spending huge sums of money to prevent cyberattacks on their websites or servers. Despite this, companies still get hacked all the time. In 2017 alone, 41 large companies have been hacked leaking information ranging from emails and phone numbers to social security numbers [3]. These companies include multiple fast food chains, two universities, Uber, and Equifax. These companies are large and well-funded, but cannot secure their servers from individuals or groups with far less resources. Uber had to pay $100,000 so the hackers did not release the information they stole, and in the Equifax hack approximately information on 143 million people was leaked that potentially includes license plates and social security numbers. So how do these monoliths of companies get breached by small groups?

One factor is the problem of complexity. With so many lines of code in all these products, it only takes one bug to exploit the whole system. And also, there are many small groups that are trying to find bugs in the code so that evens the playing field there. But the real problem is in the entire mindset of the software engineering industry. This mindset can be broken into two distinct parts.

The first is the mindset of the software developers. The goal is to get a product working and to market as fast as possible. Security will come later, or a cybersecurity team will be relied upon to remove the vulnerabilities. The problem with this is that it is impossible to "fix" code's vulnerabilities if the design is fundamentally flawed. Once the product is released, rather than go and fix the security after the product has been released, the next update with the new features becomes the next priority with security always on the backburner.

Another problem is the use of cyber security tools that are outdated. Companies employ antivirus, firewalls, and intrusion detection systems, but have no metrics for their successfulness. They rely on these tools when they are becoming increasingly irrelevant due to changes in modern computing and changes in the malware that exist.

2 To the Community

Insecurities in software affect everybody who uses the Internet. So just about everybody. Every time you put in information about yourself on in forms for a company, you are relying on them to protect that information and keep out of an attacker's hands. The unfortunate reality is that this cannot be relied upon. Hacks are ever-present to point of barely being in the news unless they are especially big or damaging. The problem is that as a user there are not many options. It is not realistic that you can avoid these services. The IRS was hacked and taxpayers' information was stolen [3]. You still have to pay taxes. The only hope is that companies (and the government) stop the leaks from happening.

3 Design Process

The design process at most companies is currently all about pushing out working code as fast as possible. Companies have deadlines and need products to be sold as quickly as possible, with the

intention of being patched in the future. This leads to buggy and flawed code being put onto the market.

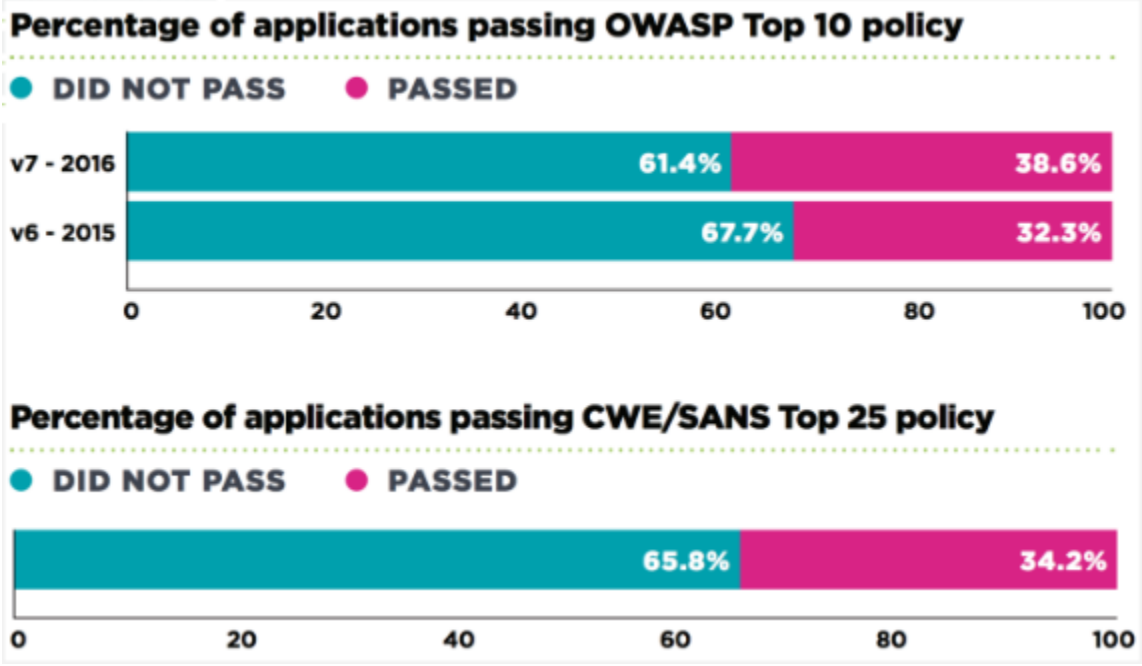
3.1 Patches

Patching code is a necessity, even if proper time and care is taken with the code in the first place. However, the constant barrage of patches causes cyber fatigue, which makes them less useful. WannaCry, a network ransomware worm that propagated in May 2017, exploited a vulnerability that had been patched two months earlier. Despite this, nearly 300,000 computers were infected due to people not updating their system.

According to hackers, approximately 10% of security breaches are due to unpatched software [1]. This is obviously a rough number, but is also something that should never happen. Patches can be easily automated so that they happen when the user is not actively using the computer, especially in a business setting. This is an extremely easy fix that will stop a lot of hacks from ever happening.

3.2 Old Vulnerabilities

The following graphic shows the data from a Veracode report of all web applications submitted to their vulnerability scanner.



[2]

Of course, this is not necessarily a terrible thing. The reason a company submits their code to Veracode is to find their vulnerabilities so that they can be fixed. However, in a presentation given by a representative of Veracode, it was revealed that by the third scan of a given application, 56% of applications either had more flaws, or the same amount [2]. And these are only the flaws Veracode can detect. If the flaws that Veracode can detect are so prevalent on a web application, the reality is there are likely many more flaws that Veracode cannot/does not even check for.

4 Cyber Security Tools

The two things that come to mind for cyber security tools are firewalls and antivirus software. In a survey of over 250 hackers, 43% said antivirus was the easiest to get past, and 30% said firewalls were the easiest to get past [1]. Multifactor authentication and encryption were considered some of the hardest tools to get past. This paper mostly deals with firewalls and antivirus software, hackers also identify intrusion detection systems as ineffective as they have access to the same tools. However, given the wide variance and complexity of intrusion detection systems, this paper does not go any deeper into the topic.

4.1 Firewalls

Firewalls are largely a relic of how networks used to work. They are a perimeter defense system that monitors and/or stops network traffic in and out of the internal network. In the past, access points into and out of a network were obvious and known by network administrators. Now that everyone has a smart phone, it is feasible to transfer data in and out of a network over a mobile hotspot without being monitored so the firewall in ineffective. Physical boundaries are no longer an obstacle to networks in general. The reality is that an attacker will be able to compromise one workers device somehow, be it because they connect their personal device to the network that is compromised due to old software or through a phishing scam. There are simply too many attack vectors passed a firewall that makes them an outdated and largely obsolete method of securing a network.

4.2 Antivirus Software

Antivirus software is relied upon to detect malware. Antivirus software detects malware by comparing files to blacklist of known malware. Modern antivirus also attempts to detect files that have been changed slightly or that exploit similar vulnerabilities. Changes to modern malware have made antivirus less effective. There has been an increase in the volume of malware. Keeping blacklist of all malware is becoming impossible because of the time required to research and keep up to date list of all malware [5].

Also, hacker test their own exploits against the common antivirus software, so they can keep changing their malware slightly so that it is not detectable by the antivirus in its current state. This allows hackers to ensure their exploits are undetectable by the antivirus on their own, and then exploit a victim's system very easily. Antivirus is good for catching the very basics, but cannot be relied upon to stop an attack of any sophistication.

5 What to Do

The solution to this is awareness, education, and vigilance. All software developers need to be educated on security, and constantly be aware of it as they are writing code so code is less buggy and more secure. Changing the culture of software development is also important. Security needs to be more important. More stringent review of code to ensure that it is bug free, at least of basic bugs. The fact that basic attacks like SQL injection and cross site scripting still exist in 2017 is a joke, never mind that they are present in 32 and 50% web applications respectively. This is a failure of the collegiate computer science programs.

Very few of the top college computer science require cybersecurity courses, and some do not even offer a cybersecurity source [6]. Not only that, but cybersecurity is seen by many as an annoying thing to deal with because it gets in the way of the fun development that they are doing. This attitude needs to be changed if the situation is ever going to get fixed. Until developers recognize security as an important and necessary part of the development process, these problems will never go away. The number one thing to do is change this mindset, and teach developers form early on in their education the importance of security, and what secure coding looks like.

6 Conclusion

Cyberattacks will happen. That comes with the territory. That does not mean basic attacks that have been known about for years and are detectable by static analysis tools should exist. As long as the only thing that matters to companies is pushing products to market this will always be a problem. The problem is in the software development mindset, and a reliance on outdated security tools. The solution is simple, yet extremely difficult to enforce. How does one make sure that developers are always thinking about the security of their products? Despite this tall task, all software developers have a responsibility to do their best to make their products as secure as possible.

References

1. Black Hat 2017 Hacker Survey Report. Rep. Thycotic, 15 Aug. 2017. Web. 11 Dec. 2017.

2. Chow, Ming. "The Hard Problems In Security." 2017. Presentation.

3. Datch, Heidi. "2017 Data Breaches - The Worst Breaches, So Far." *We Aren't Just Protecting You From Identity Theft. We Protect Who You Are.* Identity Force, 06 Dec. 2017. Web. 13 Dec. 2017.

4. Filkins, Barbara. "IT Security Spending Trends." SANS Institue, Feb. 2016. Web. 11 Dec. 2017.

5. Metivier, Becky. "Why Isn't Antivirus Software Enough for Malware Detection?" *Sage Advice - Cybersecurity Blog*. Sage Data Security, 10 Nov. 2015. Web. 11 Dec. 2017.

6. Higgins, Kelly Jackson. "Top US Undergraduate Computer Science Programs Skip Cybersecurity Classes." *Dark Reading*. 7 Apr. 2016. Web. 13 Dec. 2017.