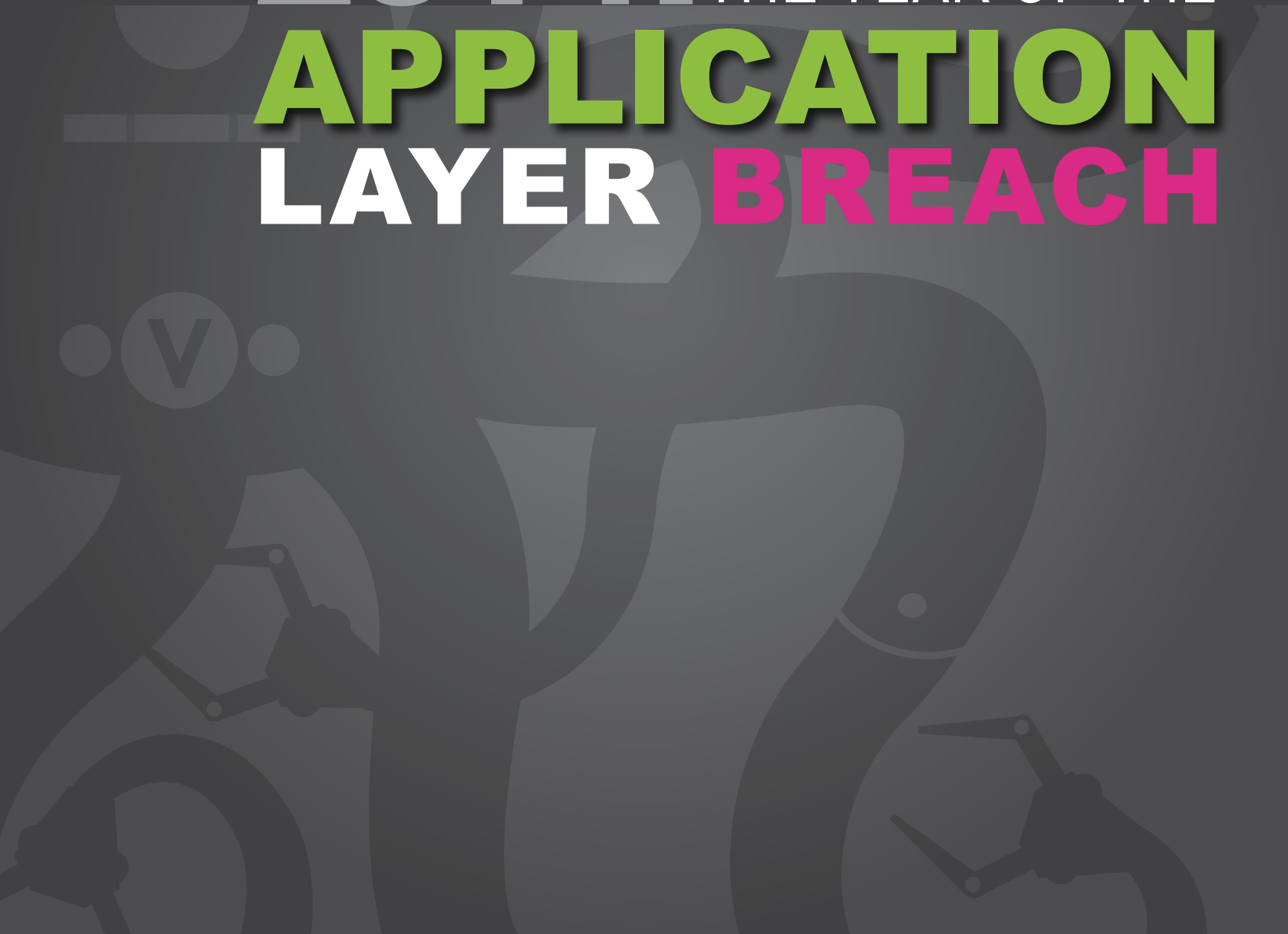
VERACODE

2014: THE YEAR OF THE APPLICATION LAYER BREACH



The rise of the digital economy means that the world runs on applications. As a result, every company is becoming a software company – regardless of what their primary business is. These enterprises are rapidly producing web, mobile and cloud applications in order to keep up with the pace of innovation. And in order to innovate even faster, they are using agile development processes, reusing open-source libraries and components, and purchasing software from third-party providers to augment their internal development efforts.

These programs have helped speed the pace of innovation. But the faster enterprises build, buy and borrow software, the more risk is introduced into the organization by that software. Ideally, every piece of software would be assessed for security risk, but that isn't the reality. Research done by IDG revealed that almost two-thirds of applications are not assessed for security. And this lack of assessment caused several costly and damaging breaches in 2014.

Target

HOW: Possibly the most widely talked about breach of 2014 was that of Target's credit card systems. Hackers used a sophisticated kill chain to steal the email addresses, phone numbers and mailing addresses of more than 70 million Target customers. This kill chain included the exploitation of a vulnerable web application, which Target's vendors used to process payments.

IMPACT: The theft of customers' personal information was later used for phishing attacks that caused an unknown number of credit card thefts.

Michaels

HOW: In 2014 Michaels suffered the second major application layer breach in the store's history.

IMPACT: Vulnerabilities in applications on the retailer's point-of-sale systems were targeted, resulting in the loss of credit card data for 2.6 million Michaels' customers.

Community Health

HOW: Community Health Systems was a victim of the infamous OpenSSL vulnerability CVE-2014-0160, popularly known as Heartbleed. The Heartbleed vulnerability was well publicized and patches were available. Yet, Community Health, like many other enterprises, was unable to identify all of the places where the vulnerable component was used.

IMPACT: As a result, hackers stole personal data, which could be used for insurance fraud, from over 4.5 million patients.

eBay

HOW: eBay has suffered several breaches over the years, but in 2014 security researchers found critical vulnerabilities in the company's web applications.

IMPACT: Evidence linking use of this vulnerability to a breach led to the loss of contact and login information for 233 million eBay customers.

JP Morgan Chase

HOW: Like many other enterprises, JPMorgan spends millions of dollars on securing the applications they produce. However, they assumed that the vendor developing a website for their annual charity road race took the same security precautions. Unfortunately, hackers found a vulnerability in this third-party website and used it to access the enterprise's network.

IMPACT: More than 76 million households and 7 million businesses were impacted by this breach.

Neiman Marcus

HOW: Using RAM scraper malware, cybercriminals were able to exploit vulnerabilities in the enterprise's internally developed applications. These vulnerabilities allowed an application to reach into another application's memory and grab the information stored there.

IMPACT: This resulted in the loss of credit card information for more than 350,000 individuals.

Home Depot

HOW: Home Depot fell victim to a hack that relied on credentials stolen from a third-party vendor and a vulnerability in Microsoft applications. This hack provided cybercriminals with access to the retailer's point-of-sale systems.

IMPACT: As a result, 56 million accounts were put at risk, and the company was forced to pay $62 million to cover the cost of the attack.

Sony

HOW: The Sony breach was a major news story at the end of 2014. Who breached Sony, how the company was breached, and why they were targeted is still under investigation. However, it is believed that the most likely path included a phishing attack, a web application vulnerability, or a combination of the two.

IMPACT: What we know for sure is that the breach resulted in hundreds of hard drives wiped, millions of emails stolen and leaked, and six previously unreleased films leaked in digital format.

Many of these enterprises spend millions of dollars on security and compliance, so why are they still being breached? Because the traditional, tools-based approach to application security does not scale to cover thousands of enterprise applications. It is not enough to secure just your business-critical applications, as cybercriminals will use any vulnerable application as the path of least resistance into an enterprise. These breaches are evidence that the traditional approach to securing applications isn't working – and now is the time to rethink this approach.

Learn how you can address the scalability challenge with cloud-based application security: **CLICK HERE >>**

SOURCE:

Target: www.cio.com/article/2600345/security0/11-steps-attackers-took-to-crack-target.html AND https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ#q5888

Michaels: www.nytimes.com/2014/04/19/business/michaels-stores-confirms-breach-involving-three-million-customers.html?_r=0 AND www.darkreading.com/attacks-breaches/michaels-data-breach-response-7-facts/d/d-id/1204630

Community Health: www.csoonline.com/article/2466726/data-protection/heartbleed-to-blame-for-community-health-systems-breach.html AND www.reuters.com/article/2014/08/18/us-community-health-cybersecurity-idUSKBN0GI16N20140818

eBay: http://securityaffairs.co/wordpress/25177/hacking/critical-ebay-vulnerabilities.html, http://thehackernews.com/2014/05/worst-day-for-ebay-multiple-flaws-leave.html AND http://www.cnet.com/news/ebay-hacked-requests-all-users-change-passwords/

Home Depot: http://krebsonsecurity.com/tag/home-depot-breach/ AND www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571

Neiman Marcus: www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html AND www.bloomberg.com/bw/articles/2014-02-21/neiman-marcus-hackers-set-off-60-000-alerts-while-bagging-credit-card-data

JPMorgan Chase: www.businessinsider.com/r-jp-morgan-found-hackers-through-breach-of-corporate-event-website-wsj-2014-10

Sony: www.wired.com/2014/12/sony-hack-what-we-know/

VERACODE