CYBERSECURITY YEAR IN REVIEW

6 Noteworthy Data Breaches in 2019

VERACODE

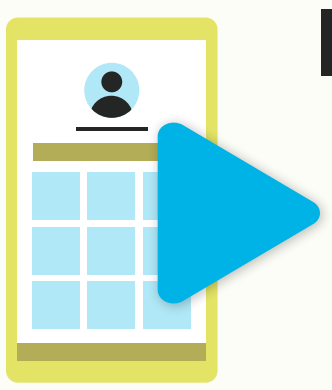
1 Capital One

Breaches can cost a pretty penny, as Capital One found out in March of 2019. A cyberattacker, who managed to infiltrate a third-party cloud computing company used by Capital One, successfully accessed its servers and 106 million customer records.

The attacker was able to do so by manipulating a misconfigured Web Application Firewall (WAF), an attack that Capital One later revealed in July. The data exposed included routinely collected information on credit card applications such as names, addresses, ZIP codes, emails, phone numbers, income, and birthdates. This involved about 140,000 Social Security Numbers and about 80,000 bank account numbers for American customers, alongside approximately 1 million Social Insurance Numbers for Canadian customers. After the damage was done, Capital One expected the breach to cost $100 million to $150 million in remediation.

SOURCE

2 TikTok



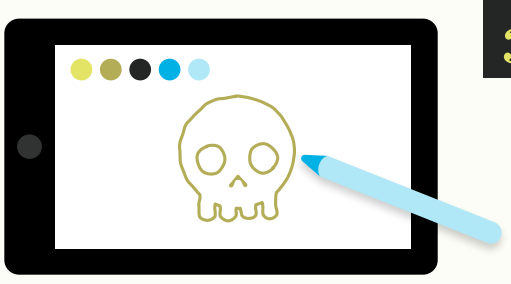
It was a close call for TikTok's 1 billion+ monthly users late last year. When Check Point Research uncovered potential threats, the popular video app made waves as a security risk that even the U.S. Navy and the U.S. Army deemed dangerous.

One of several vulnerabilities discovered by Check Point was the potential for Cross-Site Scripting (XSS) on TikTok's subdomain, which houses a help center for publishing ads on the platform. This opened cyberattackers to the possibility of Cross-Site Request Forgery (CSRF) through XSS and open redirection attacks, where a user is forwarded to a malicious website that executes JavaScript code. These and other vulnerabilities would have allowed potential attackers to access personal information, add or delete videos from user accounts, and change video settings from private to public. It's unclear if these flaws were exploited before discovery, though TikTok and Check Point since joined forces to patch the vulnerabilities.

SOURCE • SOURCE

Cross-Site Scripting is a particularly challenging vulnerability, as uncovered in Veracode's State of Software Security Volume 10 report. When we examined the makeup of security debt—defined as neglected flaws that accumulate over the lifespan of an application—we found that XSS vulnerabilities made up the lion's share.

3 Zynga



Zynga, the maker of popular mobile games Draw Something and Words with Friends, announced a data breach in September that impacted over 170 million players.

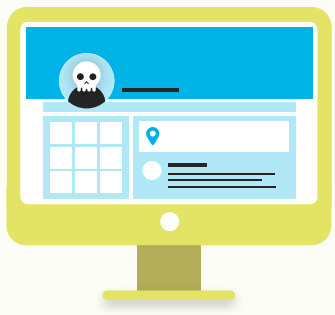
The breach occurred when an attacker accessed a database of information from iOS and Android users that included names, email addresses, and login IDs. It also contained some phone numbers, Facebook IDs, and Zynga account IDs that had been provided or connected by users. A Pakistani cyberattacker—who previously made the news for selling millions of user records from popular online services—ultimately claimed responsibility for the breach. While there was no financial information at risk from this breach, Zynga acted quickly and retained third-party forensics firms, taking necessary steps to protect user accounts from invalid logins.

SOURCE • SOURCE

4 Facebook

The world's largest social media network is a tempting target for attackers. In April, news broke that more than 540 million records of Facebook users were exposed through a third-party cloud computing service.

According to UpGuard, the cybersecurity research firm that discovered this stash of sensitive information, the records were leaked by media company Cultura Colectiva and two third-party Facebook app developers. Although UpGuard attempted to notify Cultura Colectiva earlier in the year, it wasn't until Bloomberg reached out for comment that the company finally secured the data in an Amazon cloud storage bucket. The information left vulnerable from this breach included unprotected Facebook passwords for 22,000 members as well as data on user IDs, location check-ins, friends, and photos.



SOURCE

5 People Data Labs

San Francisco-based People Data Labs (PDL) came under fire when an index with 622 million unique email addresses was discovered on an unprotected Elasticsearch server by security researchers Vinny Troia and Bob Diachenko.

While PDL said that it was responsible for aggregating the data, the company alleged that this was likely due to one of its customers failing to properly secure its database. In addition to email addresses, exposed information included phone numbers, social media profiles, employers, work history, and locations. The information seemed to be merged from four data sets, three of which were labeled as originating from PDL. Data on 1.2 billion people was exposed on the unprotected server, making this breach one of the largest data leaks ever from a single source.

SOURCE

6 Quest Diagnostics Inc.

Deficient security measures from third-party vendors can be detrimental to a company's health. Quest Diagnostics Inc. discovered this when a breach hit its billings collection vendor American Medical Collection Agency (AMCA) and exposed the private information of about 12 million customers.

AMCA notified Quest in May that an unidentified cyberattacker had gained access to its website to execute a man-in-the-middle attack (MITM), logging payment information and personal data entered by customers. This attack also impacted LabCorp, putting the personal and financial data of 7.7 million customers at risk. While there were no leaks of sensitive internal medical records according to Quest, the expensive fallout from the incident caused AMCA to file for bankruptcy citing "enormous expenses that were beyond the ability of the Debtor to bear."

SOURCE

Man-in-the-middle is a type of eavesdropping attack that occurs when malicious actors insert themselves as relays/proxies in a communication session between people or systems, exploiting the real-time processing of transactions, conversations, or transfer of other data. Dynamic Analysis testing checks for weaknesses and related vulnerabilities that can expose a user to MITM attacks, ensuring that your team is able to focus on remediating vulnerabilities.

GOALS FOR 2020 AND BEYOND

Less Security Debt

Big breaches are often the result of exploitable security flaws, which can accumulate in the security debt organizations carry by focusing on new vulnerabilities while not addressing older vulnerabilities. Data from our State of Software Security Volume 10 report shows that organizations with the highest scan frequencies carry about 5x less security debt than those with the lowest. Frequent scanning not only helps developers discover more vulnerabilities, but it can also significantly reduce the risk of breaches as flaws are found and fixed sooner.

LEARN MORE VERACODE.COM/SOSS

ABOUT VERACODE

Veracode is a leader in helping organizations secure the software that powers their world. Veracode's SaaS platform and integrated solutions help security teams and software developers find and fix security-related defects at all points in the software development lifecycle, before they can be exploited by hackers. Our complete set of offerings help customers reduce the risk of data breaches, increase the speed of secure software delivery, meet compliance requirements, and cost effectively secure their software assets—whether that's software they make, buy or sell.

Veracode serves more than 2,000 customers across a wide range of industries, including nearly one-third of the Fortune 100 and more than 20 of Forbes' 100 Most Valuable Brands.