Devolutions

7 Lessons Learned from the Biggest Data Breaches of 2020

HERE IS A RECAP OF SOME OF THE MOST NOTABLE INCIDENTS

Recently, we looked at some of the biggest data breaches of 2020. **Here is a recap of some of the most notable incidents:**

- 300,000 users were impacted by a mass account hijacking campaign at Nintendo.
- More than 500,000 Zoom accounts were breached and then offered on the dark web.
- A breach at the budget airline Easyjet exposed the data of 9 million customers, including some financial records.

- A security engineer at Cisco hacked his employer, which cost the company $2.4 million to fix (the rogue insider was later sentenced to two years in prison).
- Wattpad suffered a data breach that exposed nearly 271 million records.
- The Twitter accounts of some of the world's best-known personalities were compromised by hackers who used spear phishing attacks to drive traffic to Bitcoin scams.
- The hacker group ShinyHunters leaked the database belonging to Mashable.com, exposing more than 5.2GB worth of data.
- Hackers inserted malicious code into an update of the SolarWinds software, called Orion. This hack is called supply-chain attack, since it infects software as it's under assembly. SolarWinds said that around 18,000 customers installed the tainted update onto their systems. Supply-chain attacks are to be taken seriously and are very powerful. This attack had a huge impact, which continues to grow with the discovery of new information.

The Onslaught Continues

Just in case anyone hopes that hackers might take a break after a very busy and successful 2020, u**nfortunately that is not going to happen.** In fact, the onslaught is in full swing: in early January 2021, cybersecurity firm Safety Detectives discovered a leak at the Chinese social media startup Socialarks, which involved 400GB of scraped data exposing over 200 million Facebook, Instagram, and LinkedIn users. And so it begins…

Lessons Learned

To defend their data, customers, and reputations, **here are seven lessons learned from the biggest data breaches of 2020:**

1. It is not a question of if an SMB will be attacked — it is a question of when (or how many times).

Research has found that 66% of SMBs have experienced at least one cyberattack in the last 12 months. What's more, many SMBs have been attacked without even being aware of it. **What this all means is that SMBs**

should not speculate on "if" they will be attacked, but instead prepare for "when" they are attacked (or attacked again).

To that end, SMBs should have a comprehensive cybersecurity incident response plan (CSIRP), as well as a comprehensive disaster recovery (DR) plan. Without these fundamental plans in place, the impact of a cyberattack could be catastrophic. In 2020, the average total cost of a data breach in smaller organizations was $2.35 million.

2. Classifying, monitoring, and controlling access to privileged accounts is absolutely essential.

Although 80% of hacking incidents leverage compromised credentials, many SMBs are alarmingly vulnerable in this area. For example, a survey by cybersecurity company Varonis found that:

- **Only 5% of folders were properly protected.**
- **15% of companies had 1,000,000+ files open to every employee.**
- **17% of all sensitive files were accessible to all employees.**
- **60% of companies had over 500 accounts with non-expiring passwords.**

These findings align with insights from the **Devolutions State of Cybersecurity in SMBs in 2020 survey**, which found that while 78% of SMBs consider a Privileged Access Management (PAM) solution important, 76% of SMBs do not currently have a fully deployed PAM solution in place. Addressing this vulnerability should be the top priority in 2021. Our survey report contains practical and strategic recommendations to do this.

3. Vulnerability management must be active — not passive.

While patching vulnerabilities is obviously critical, SMBs cannot stop there. They must be proactive and continuously detect and address all potential threat vectors, including those that can emerge rapidly. Also as part of their comprehensive vulnerability management program, **SMBs must analyze any weaknesses that may exist with outside entities.** Several high-profile data breaches in 2020 (e.g. Blackbaud, Mailfire, Clearview AI, etc.) involved third parties.

4. All employees must have cybersecurity training.

One of the most troubling themes of 2020's biggest data breaches is that many could have been avoided with effective cybersecurity training. In fact, research has found that in recent years nearly half (47%) of all data breaches have been caused by employee negligence or carelessness. The bad news is that end users will always be the weakest link in the cybersecurity defense chain. But the good news is that SMBs can — and given the consequences, they absolutely must — **provide all of their employees with cybersecurity training.** For most SMBs, the most effective and affordable option is enrolling their workforce in an online cybersecurity training platform.

5. Insider threats are a growing problem.

Another worrisome trend we see in 2020's biggest data breaches is the number of attacks that involved rogue users (e.g., Postbank, Cisco, etc.). Yet despite the rise of insider threats, the Devolutions State of Cybersecurity in SMBs in 2020 survey found that **only 17% of SMBs think that the rise of insider threats will be a major concern in the next three years.** Closing this vulnerability involves **a mix of technical and non-technical controls**. The former includes elements like PAM and 2FA/MFA, while the latter includes aspects such as background checks, and implementing Segregation of Duties (SoD), the Principle of Least Privilege (POLP), and Zero Trust (which also leverages Defense in Depth).

6. SMBs need to partner with Managed Service Providers (MSPs).

Most SMBs do not have the in-house cybersecurity specialists they need to establish, monitor, and optimize the full range of technical and non-technical controls necessary to thwart hackers. And with the massive ongoing cybersecurity skills shortage, there is no expectation that this expertise will get more affordable in 2021. As such, SMBs need to partner with a good MSP that will give them **access to the experts, advice, and resources they need, but at an affordable price.**

7. Remote workers are a primary target.

Research by Malwarebytes found that 20% of businesses suffered a breach due to remote workers during the pandemic. The goal for hackers is to compromise endpoints, and then move laterally across the network without

being detected. **The massive increase in remote workers has triggered challenges for many SMBs:** the use of virtual private networks (VPNs), such as bandwidth bottlenecks that slow down productivity and frustrate end users and the use of their personal machines and devices that can "let down their guard" — and open the door for hackers to breach the corporate network. To address these challenges, **SMBs should strongly consider implementing a Zero Trust architecture.** By removing the assumption of trust and authenticating every action and device, Zero Trust helps SMBs establish a more robust and resilient security posture, while increasing efficiency and productivity. A survey by IBM found that the average time it took to identify a breach in 2020 was 207 days.

The Final Word

It has often been said: "Those who do not learn from history are doomed to repeat it." In light of this wisdom, all organizations — **but especially SMBs, a favorite target for hackers** — should heed the lessons described above, so they can avoid the costs and consequences of a cyberattack in 2021.