SailPoint

WHITE PAPER

The Anatomy of **a Data Breach**

The enterprise security landscape as we know it today has changed. Enterprises' applications and data are constantly under attack, breaches occur, and sensitive information is released every day. Successful data breaches are not only becoming more frequent, they're also becoming more destructive and pervasive, with source code, customer & employee information, and other sensitive data being released. The most frightening thought for enterprises about these data breaches may not be their consequences, but rather from the fact that often – 43% of the time – they're directly caused by insiders.

In 2016, there were at least 4100 data loss events that were recorded, releasing over 4.2 billion records. Perhaps the most memorable in recent years is Yahoo's "megabreach" with 1 billion compromised accounts. Others included the Office of Personnel Management, Morgan Stanley, and the IRS. All these high-profile breaches were caused by someone inside the company doing something they weren't supposed to do, from clicking on a phishing e-mail to using weak passwords.

Learning from the Past

An introduction from our CTO & CISO, Darran Rolls

In the early 80s, before I had entrenched myself in its culture and when the computer had just begun its entry into mainstream culture and media, the term hacking had not yet become a household term. There were no CTOs and I hadn't yet begun my foray into the world of technology, but I remember one of the pivotal moments in my decision to go into the field.

The show was Micro Live, and it was the reason I got up on those mornings each week. The episode that pertains particularly to the security world was when one of the earliest "hacks" caught live on television wasn't, in fact, due to coders breaking into a system through its network or cracking passwords; it was simple human error.

The show's hosts were in the midst of logging into a computer remotely for a demonstration. While the openly posted username clearly displayed on screen is an

obvious flag for the show to become a target of the more mischievous viewers, they did their due diligence and hid the keyboard as the host was typing his password. Nevertheless, seconds after he attempted to login, the screen changed to show instead a message from the show's successful hackers.

The cause of this breach? When prepping for the show ahead of time, the host asked the director to confirm the user's password over their lines of communication. What he didn't know is that one of the people in the control booth had accidentally crossed lines with those who were in the holding room: the subject matter experts that were speaking later in the program. Those experts were able to get the openly available username and its password and disrupt the demonstration all from a simple user error.

The moral of the story is that this same type of simple mistake in organizations today can, and have, caused some of the largest data breaches we have experienced. The consequences, however, are far more disastrous.

Common Process Pitfalls

Just as we can discern how to better protect ourselves from mistakes such as the one that happened on Micro Live, so too can we use the forensics on past data breaches to gain insight to what happens during a breach, as well as where the security processes in the organization failed. Five of these processes specifically fall under the realm of identity, and each could have delayed, if not prevented, a breach.

- **Poor account controls.** Once hackers gain entry into an enterprise's systems, they will usually create their own admin accounts. If proper account controls were in place, this could not occur.

- **Weak passwords.** Perhaps most famously found in the Hacking Team breach where an admin password was simply "P4ssword"[1], weak authentication credentials are easy points of entry for brute force attacks.

- **Orphan accounts.** After an employee leaves a company or moves to another role, accounts that should have had their access terminated are instead left active. This creates a massive gap, since if a malicious user were to gain access, no one would know the account had been compromised if no one was assigned to it and detective controls are not in place.

- **Weak inventory & cataloging.** Once a hacker has gained entry into the network and file shares, they will more than likely attempt to download all the information to which they can gain access.

- **Overentitled identities.** While an executive account is an obvious choice for spear phishing and attempting to gain credentials, any user is a valuable target

[1] *Hacking Team used shockingly bad passwords*, ZDNet

for hackers. Overentitled identities pose a particular threat: what may seem like a low-risk user may have inappropriate access into systems and data. If such an account is compromised, the hackers could potentially have access to sensitive information and systems if entitlements are not well-maintained.

The Anatomy of a Data Breach

It's obvious that there are some problems in security to be solved, but the question remains: how do we better protect ourselves? To best understand how, we must first learn from our collective past mistakes, and then go into "the belly of the beast." Taking from what we've learned, we can determine there are four general phases to a data breach: **Reconnaissance, Infiltration, Exploitation, and Exfiltration.**

Reconnaissance

The first phase of a data breach is all about the hackers learning about their target and how best to attack it. While hackers have begun to shy away from using network-based methods and SQL injections as their main method of infiltration, that doesn't mean it still isn't part of their retinue. As a starting tactic, the hackers will begin scanning all the externally-available resources the target enterprise uses.

This phase is also when social engineering begins. Anyone and everyone connected with the company – employees, customers, vendors, partners, etc. – will be researched and those with potential access into the enterprise will be sent blanket phishing e-mails. Executives and other high-value targets will be subject to spear-phishing campaigns.

Infiltration

With the number of employees an enterprise has, and the simple fact that humans make mistakes, it will only be a matter of time before someone clicks a link they shouldn't have, and the hackers gain entry. For instance, let's assume a spear-phishing attempt was successful and an executive clicked on a link that downloaded a piece of malware onto their computer. With that, the local admin account can be compromised, which then grants access to a number of the enterprise's resources. With that local admin access, the hackers can test their limits on the organization's servers, install exploitative software on the network, and begin scanning systems for any and all information that may be worth something.

Exploitation

At this point, the hackers have their way in and are looking for the best ways to gain full access to the "juiciest" information. They will start brute force attacks on all the administrative accounts. This method will crack the weakest passwords and grant them access into those systems. For instance, the internal company portal may be breached. From there, the intruders can request or create new admin accounts on the network, increase their permission levels on file shares, and further expand their reach into the organization's applications and data.

Phase 4

Exfiltration

Once all the systems that are necessary to download the information they want are breached, the last stage is for the hackers to download all the data they want. This includes financial documents, customer and employee information, sales data, product roadmaps, source codes and more. In many cases, the encryption information for the actual authentication credentials a company's identities use will also be downloaded. In the 2016 Market Pulse Survey SailPoint conducted, we found that 65% of employees reuse their passwords across multiple systems and applications. Once hackers get their hands on the actual authentication information en masse, they open the door to breaches in other companies and more information could be leaked.

Once the enterprise is aware of the breach and found the potential loss of information, the consequences begin. In many cases, this means a loss of business from dissatisfied customers, partners and other involved parties. For many businesses, a breach means repercussions and fines from regulations. The bottom line is that breaches cause a great deal of problems for both the breached entity and its constituents.

Lessons Learned from Identity

When we take the issues that were exploited to cause data breaches in the past with how we understand breaches occur in practice, we can better protect ourselves and the data we hold dear. First, consider the fact that an attempted attack – if not a successful infiltration – on an enterprise's systems is nearly certain, and combine that with the average time to even detect a breach is 229 days[2].

In these 7 months, countless attack methods have been made from both outside and within an enterprise's systems. A robust identity governance program could have helped to mitigate the risks before a breach occurred, and potentially slowed the progress once a breach had begun to be attempted.

Put Good Processes in Place

From the prior example, routine password resets and a strong password policy could have slowed both the infiltration and exploitation phases. We saw that the hackers' entry had succeeded through the use of malware and local admin accounts in the infiltration phase. If regular password resets had been enforced, access could have been lost. In the exploitation phase, weak passwords were the source that granted access into the internal company portal. If a strong password policy were in place, it would have taken longer for credentials to be cracked and allowed more time for detection of the hackers to occur.

Detect Suspicious Behavior

Good identity governance solutions are built to integrate with other systems in order to give your IT team a holistic view into all your systems and data – no matter where

[2] *2016 Cost of Data Breach Study: Global Analysis*, Ponemon Institute

they reside. By integrating your identity governance solution, you can integrate with SIEM and data access governance solutions to detect real-time threats. Having this type of arrangement in place could have detected the hackers in the situation above in the infiltration, exploitation and exfiltration phases, potentially discovering the breach and shutting it down before any information was stolen. Additionally, this collaboration of systems could detect when the rogue administrative accounts were created in the exploitation phase.

Set Traps for Intruders

While the hackers perform reconnaissance at the beginning of their project to breach your organization, they don't know your systems nearly as well as your IT team does. A good method of distracting the hackers and buying you and your team more time to detect and then shut down any breach is by leaving a "honey pots" of accounts and information that would be too valuable to not take advantage of.

After creating false admin accounts and other accounts with weak credentials, employ your identity governance system to raise flags whenever one of those accounts is accessed. This is an easy way to trap hackers into detection. Another tactic is to label documents with appealing names that entice the hacker into thinking they contain sensitive – that is, monetarily valuable – information. Just as your integrated systems can raise flags for access into the fake accounts, the data access governance portion can alert the appropriate parties when these false files are accessed to mitigate risk.

Conclusion

By utilizing a user-centric approach and integrating all the systems together (identity governance, data access governance, network security, user behavior analysis, etc.) into the Identity platform, IT would now have visibility into the entire security ecosystem. Only then can the organization truly put identity at the core of its security, mitigate the risks of a breach and protect the information that they need to succeed.

WP1042-1709