Data Breach vs. Data Hack

Devolutions

DO YOU REALLY KNOW THE DIFFERENCE BETWEEN A DATA BREACH AND A DATA HACK?

Some things in life have meaningful similarities, but they are not the same — to my fellow GOT fans out there, do you really know the difference between a white walker and a wight? Or the difference between a data breach and a data hack? I won't go into detail about the former pair, but I can definitely focus on the latter.

In this technological era where computer literacy is more important than ever, knowing the difference between a hack and a breach can mean the difference between your private data staying private and having it leaked all over the internet.

What Is a Data Breach?

A data breach is the unintentional release of secure or sensitive information from a trusted environment into an untrusted environment. A data breach occurs when information that is **unintentionally** left unsecured is viewed by someone who shouldn't have access to that information. The root cause of a data breach is typically negligence, incompetence, or human error (or sometimes a combination). There is no malicious intent — although the costs and consequences can be severe.

Example of a Data Breach

Probably the biggest and best-known data breach in recent years involved Facebook and Cambridge Analytica, through which millions of users had their confidential and private data exposed to a third party. While some mainstream media outlets referred to this as a hack, it was technically a breach. Cambridge Analytica didn't try and break through Facebook's security. Instead, they exploited a mistake in Facebook's API to get access.

What Is a Data Hack?

At its most basic level, a hack is any modification of computer hardware or software that is different from the original intent of the developer. In practical terms, though, hacking is usually carried out by cybercriminals in an attempt to steal private information and commit identity theft and fraud. In some cases, hackers lock a device and demand payment (i.e. ransomware).

A hack is the result of **malicious behaviour** and is carried out by a hacker or a group of hackers. The term "hacking" has taken on a number of negative meanings in the cybersecurity world, but it's important to note that not all hackers are criminals ("white hat" and "black hat" hackers, for example, are ethical hackers).

Example of a Data Hack

One of the most infamous hacks of all time was the attack on Yahoo! back in 2014. All of the company's 3 billion user accounts were compromised, exposing names, dates of birth, email addresses and passwords, and security questions/answers. A more recent example is from 2018, when Marriot International revealed that cybercriminals had stolen data from approximately 500 million customers, including passport numbers, travel information, loyalty club numbers, and other personal information. In the aftermath of this hack, former guests are screaming "Lawsuit!" instead of "Bonvoy!"

What's the Difference?

The key difference between a breach and a hack lies in the intent. A hack is the result of an **intentional** attack, while a breach is the result of an **unintentional** leak of information. Another way to look at this is to determine whether cybercriminals are part of the story — including internal rogue users. If so, then it's a hack. If not, it's a breach.

Knowledge is key to success and being able to clearly define if the attack was a breach or a hack will better your chances of reacting quickly and properly to the situation. Next week, I'll take a look at the best ways to avoid a data breach and the best ways to avoid a data hack, so stay tuned!

And by the way, if you're still wondering what the difference is between a White Walker and a wight, here's a little article to satisfy your curiosity!