Here are the five most serious cybersecurity breaches that have occurred in recent years:

1) Target data breach (2013): In 2013, retailer Target announced that hackers had accessed information personal credit card information, debit, and credit accounts of forty million customers, personal information of 70 million customers. Personal information of these 110 customers was also exposed.

2) Anthem Data Breach (2015): Anthem's data breach (cyber-attack) in 2015 resulted in the breach of Anthem, the largest US health insurance company, and was one of the biggest data breaches in history. Hackers gained access to the personal information of 78.8 million Anthem, Inc. customers. The breach led to numerous lawsuits and a settlement in which Anthem agreed to pay affected customers $115 million. It is unclear who carried out the attack, but state sponsored hackers were suspected.

3) Home Depot Data Breach (2014): The Home Depot data breach occurred from April to September 2 of 2014. It took place in Canada and the US. The malware was installed on self-service payment terminals, allowing criminals to steal the names and credit card information of more than 50 million customers.

4) Capital One Data Breach (2019): The Capital One data leak is notable not only for its size (more than one hundred million people affected) but also because a former Amazon Web Services (AWS) employee led it. This person accessed Capital One customer data through AWS, emphasizing the importance of security controls in the cloud. This breach also demonstrates how important it is for organizations to verify their internal operations, as the perpetrator was reported multiple times before carrying out his attack.

5) Twitter Data Breach (2020): In 2020, Twitter experienced a massive data breach, with hackers gaining access to over 130 million accounts. This was achieved by taking advantage of a vulnerability in Twitter’s system that allowed attackers to take control of user accounts and tweet on their behalf. This incident highlights the importance of strong authentication and tight control over what privileged users can do in the system.