Jaalen Cooper

CS462 Term Paper

The ICMR Data Breach

The cybersecurity world has something that inevitably will occur: cyberattacks. On October 9, 2023, this would further prove to be the case as the Indian Council of Medical Research (ICMR) was hit with a massive data breach that led to the personal information of 815 million Indian citizens being put up for sale on the dark web. The Indian Council of Medical Research (ICMR) is an institution in India that specializes in biomedical and an institution like that, of course has massive amounts of sensitive information belonging to citizens of the country. Here we will discuss the details of the breach as well as its effects and ways to prevent an attack like this from occurring again.

First, let's begin with what the ICMR is. The Indian Council of Medical Research is a biomedical research institute that was established in 1911 and has played a key role in advancing the medical research begin done in India. As you can imagine, an institution, such as the ICMR is home to a vast amount of sensitive health-related data belonging to the citizens in the country, which means that they must shoulder the responsibility of ensuring the confidentiality and integrity of the personal information it holds. However, on October 9th, 2023, reports emerged about a data breach at the ICMR after it being discovered by a security company known as Resecurity. They found that the personal information of 815 million Indian residents was compromised and put on sale on the dark web. To put this in perspective, the entire population of India is 1.486 billion people, which means this attack could've affected over half of the population in the country. This personal information included the name, age, gender, address, and passport number of Indian citizens as well as their Aadhaar number, which is a 12-digit government identification number and essentially is the country's version of a Social Security Number. This breach raised major concerns about the security of sensitive medical information that is held by the ICMR especially with the breach of their Aadhaar numbers as the functions they hold in Indian make a leak of them a potentially catastrophic incident that would affect hundreds of millions of the population. The concern has been raised even more as this is not the first time a data breach of the sort has occurred against the institution as there was a similar leak dealing with the Aadhaar of vaccinated citizens being leaked in June 2023 and with multiple breaches leaking highly sensitive data occurring the ICMR must do whatever to ensure public trust in them before things turn south very quickly.

The attack was reviewed by the Indian Computer Emergency Response Team (CERT-In). an office within the Indian government that specializes in cybersecurity, found that the attack was caused by “improper network segmentation.” This means that the network had not been properly segregated allowing for the personal information and data stored there to be accessed more easily. It was also found that the attack was carried out by a threat actor going by the alias “pwn0001”. People working Resecurity got in contact and found that the actor was only selling the information for $80,000 meaning that this is ransomware attack and there’s also the fact that the damage that leak would’ve done had someone with bad intentions had gotten a hold of the leaked data would have greatly surpassed a measly $80,000. The company was able to look at the information as the actor gave them samples with higher numbers of victims each time and every single name was verified to be a real Indian citizen. This leakage of PII (personal identifiable information) is possibly the largest data breach in Indian history.

Now that we know what the attack was and the potential damage of the attacks, what could be done to prevent this from occurring again. One thing is improving the thing that caused the breach, which is the network segmentation. Network segmentation is the method of dividing networks into multiple segments isolating the different parts of the network. By doing this, the chance of data breaches decreases, and the accessibility of the sensitive data has been lowered to a smaller number of people. This allows for the information to be monitored more easily since the information would be in its own separate space. The problem in this case was that the information was not properly segmented meaning that it was easier for the threat actor to access more information at once, which of course caused a massive breach. By properly segmenting the data and sensitive information, such as citizens Aadhaar number, the chances of attackers being able to access them decreases. This is especially important as India is one of the top countries targeted by attackers and attacks, such as the ICMR data breach have often occur due to the sheer number of people in India as well as its fast-growing economy. There also could be the implementation of strong encryption of the sensitive information that keeps getting targeted as well as keeping systems and security measures up-to-date especially with the rapid growth in the cyber world.

The ICMR data breach is just one example of the multitude of cybersecurity attacks that occur every day. This particular breach just puts into perspective the sheer number of innocent people that could be negatively affected by cyberattacks. It also highlights the importance of adequate, up-to-date cybersecurity to make sure that something like this doesn’t occur or at the very least doesn’t become such a large-scale thing. The ICMR is a cautionary tale and one that should be discussed more and by being discussed more and more governments and organizations will ensure that the data their citizens entrust them to keep is in good hands.

Cites:

- https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-2023#october-2023
- https://www.resecurity.com/blog/article/pii-belonging-to-indian-citizens-including-their-aadhaar-ids-offered-for-sale-on-the-dark-web
- https://health.economictimes.indiatimes.com/news/health-it/from-aiims-delhi-to-icmr-data-breaches-haunt-crores-of-indians/105173060#:~:text=The%20attack%20was%20analysed%20by,out%20by%20unknown%20threat%20actors.
- https://economictimes.indiatimes.com/tech/technology/opposition-security-experts-seek-answers-on-icmr-data-leak/articleshow/104865920.cms
- https://www.thehindu.com/news/national/us-cyber-security-form-indicates-data-breach-sourced-from-icmr/article67477424.ece
- https://www.securityweek.com/improving-security-proper-network-segmentation/