Accenture Ransomware Case Study

Accenture/6 TB Employee & Partner computer systems & Data stolen!

Ransomware

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's personal data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system so that it is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.[1][2][3][4] In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem – and difficult to trace digital currencies such as paysafecard or Bitcoin and other cryptocurrencies are used for the ransoms, making tracing and prosecuting the perpetrators difficult.

https://en.wikipedia.org/wiki/Ransomware

According to the IBM X-Force Threat Intelligence Index,

The #1 threat was ransomware
Ransomware was the top threat type, comprising 23% of attacks. Sodinokibi (Revil) ransomware alone reaped a conservative profit estimate of USD 123 million.
https://www.ibm.com/security/data-breach/threat-intelligence

Here are some of the top ransomware stats relating to costs:
According to a 2020 market report by Marketsandmarkets, the global cybersecurity market is expected to grow from $183.2 billion in 2019 to $230 billion by 2021.
As per a 2019 Emsisoft report, the cost of ransomware attacks surpasses $7.5 billion in 2019.
According to a 2020 report from Coveware, the average cost of ransomware attacks in the fourth quarter of 2019 reflected a staggering 104% increase from $41,198 in Q4 2018.

Accenture plc is an Irish-based multinational company that provides consulting and professional services. A Fortune Global 500 company,[4] it reported revenues of $44.33 billion in 2020 and had 569,000 employees. In 2015, the company had about 150,000 employees in India,[5] 48,000 in the US,[6] and 50,000 in the Philippines.[7] Accenture's current clients include 91 of the Fortune Global 100 and more than three-quarters of the Fortune Global 500.[8]

https://en.wikipedia.org/wiki/Accenture

A ransomware group by the name of LockBit conducted a major ransomware attack on Accenture, one of the world's largest companies and requested a ransom of $50 million in return of the company's critical 6 TB of data.

This is a major compromise and a big trust concern that could be caused especially considering that Accenture does emphasise on Cybersecurity best strategies and practices which leads to a huge reputation downfall.

https://www.cshub.com/executive-decisions/articles/accenture-faces-50-million-ransom-demand

Timeline

Accenture Ransomware

July 30th 2021, Accenture found out that their data and systems have been breached. According to a report from cybersecurity news site CyberScoop, Accenture had spotted the LockBit ransomware attack on its systems on July 30.

August 4th 2021, Accenture releases its latest Global Incident Response Analysis Cybersecurity Report without disclosing the breach but instead highlighted ransomware as one of the top current threats in cybersecurity.

August 12th 2021, The news on the Accenture Ransomware attack starts surfacing and becomes known to the public. Accenture then makes a statement that the breached systems and data have been recovered.

Vulnerabilities

Overall Summary

Insiders are a very real threat. Of the total breaches that occur.
It is yet to be identified as to what sort of vulnerability has caused this, but the initial reports are all pointing towards a malicious insider.

Vulnerability #1
Malicious Insider

According to Forrester, 1 in 3 security breaches in 2021 will be caused by an insider threat, growing by eight percentage points from the previous year.

Vulnerability #2
Software

Code vulnerabilities creep in right at the time of software development. There might be logical errors that lead to security flaws – for example, creating an access privilege lifecycle that an attacker can hijack.

Vulnerability #3
Network

Incorrectly configured cloud systems, network misconfigurations, hurriedly set up Wi-Fi environments, and even the failure to restrict non-work device usage could exponentially multiply your risk exposure.

Vulnerability #4
Weak credentialing

This has emerged as one of the most common causes of vulnerabilities in both consumer and enterprise systems. Users tend to stick to convenient or comfortable credentialing practices, prioritizing ease of use over security.

Costs

- 6 TB of stolen data
- 2500 computers of employees and partners were compromised
- $50 million Ransom

Prevention

- Monitor the network, applications and users for unusual behavior.
- Make sure employees know that they are being monitored and provide them with notice of what the consequences of criminal behavior might include.
- Have endpoint protection in place.
- Have an anonymous method of reporting suspicious behavior available and/or provide the name of a security member to contact.
- Encrypt data at rest and in motion.
- Work with other organizational leaders to establish a cyber aware culture.