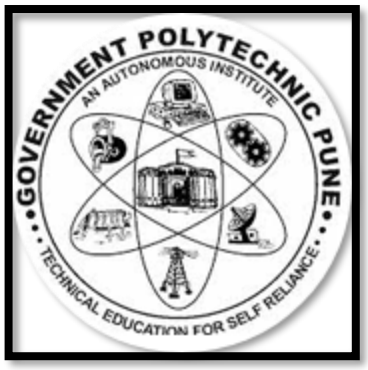
GOVERNMENT POLYTECHNIC PUNE,PUNE-16

(AN AUTONOMOUS INSTITUTE OF GOVERNMENT OF MAHARASHTRA)

.



Case Study report on

"NASA Cyber Attack"

Submitted by

Sakshi Sharad Kulkarni (1906070)

Janhavi Vijay Mali(1906083)

Vinayak Madan Shete(1906116)

Under the Guidance of

Prof. Bhagyashree Amrutkar Ma'am

GOVERNMENT POLYTECHNIC, PUNE

(An Autonomous Institute of Government of Maharashtra)

CERTIFICATE

This is to certify that,

1906070 KULKARNI SAKSHI SHARAD,

1906083 MALI JANHAVI VIJAY and

1906116 SHETE VINAYAK MADAN

of class Third Year (2021-22) have successfully completed Microproject on **"NASA CYBER ATTACK"** under the guidance of "**PROF. B. R. Amrutkar Ma'am**" in parallel fulfillment of requirement for the award of Diploma in Computer Engineering from Government Polytechnic, Pune.

PROF.B.R.Amrutkar	**Dr.S.B.Nikam**	**Dr.V.S.Bandal**
(Project Guide)	(H.O.D)	(Principal)

Acknowledgement

Apart from the efforts of myself, the success of any task depends largely on the support and encouragement of many others. First and foremost, I would like to thank to our Subject teacher, Mrs. Bhagyashree Amrutkar ma'am for the valuable guidance and advice and helping me throughout in the project. I would like to thank Prof. S.B.Nikam (HOD Computer Engineering Dept.), Dr. V.S. Bandal (Principal) and Government Polytechnic Pune for designing this curriculum for us and assigning such a useful task for us which helped us to increase our knowledge and think about the innovations.

I am expressing my gratitude toward other faculties as they also helped us in this micro project. I am thankful to my parents for helping me at each step, for encouraging me and providing me all the things I need. Last but not least for my friends I can't say thank you enough for the tremendous support and help, for solving my doubts whenever needed.

Table Of Contents

1) **Abstract**.....

2) **Introduction**.....

3) **Problem Definition** ….....

   a) **Case Study**

4) **Security Measures**.....

5) **Books/References/Websites**.....

6) **Conclusion**…..….

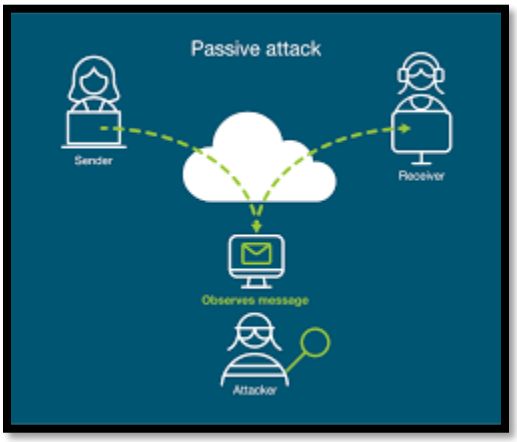
Abstract

This case study is based upon the Cyber security attack on NASA. In this world of digitalization every industry uses tremendous amount of digital data with digital devices. To protect the data is the main challenge. Malicious person always tries to hack device or system and steal data of professional organisations in order to steal information for malicious work or to demand money from organisations.

In this case study we have carried out observation about what factors are considered when an attack happens. Also what damage an organisation can have when attack happens. We have studied every detail of attack on NASA. And finally we tried to figure out what security measures they should have taken or any organisation should take in order to prevent these attacks.

Introduction

What is Cyber Attack?



A cyber attack is any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage. Cyber attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems.

A cyber attack can be launched from anywhere by any individual or group using one or more various attack strategies.

People who carry out cyber attacks are generally regarded as cybercriminals. Often referred to as bad actors, threat actors and hackers, they include individuals who act alone, drawing on their computer skills to design and execute malicious attacks. They can also belong to a criminal syndicate, working with other threat actors to find weaknesses or problems in the computer systems -- called vulnerabilities -- that can be exploited for criminal gain.

Government-sponsored groups of computer experts also launch cyber attacks. They're identified as nation-state attackers, and they have been accused of attacking the information technology (IT) infrastructure of other governments, as well as nongovernment entities, such as businesses, nonprofits and utilities

What is COMPUTER SECURITY?

Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system.

There are various types of computer security which is widely used to protect the valuable information of an organization.For example,

Information security is securing information from unauthorized access, modification & deletion

Application Security is securing an application by building security features to prevent from Cyber Threats such as SQL injection, DoS attacks, data breaches and etc.

Computer Security means securing a standalone machine by keeping it updated and patched

Network Security is by securing both the software and hardware technologies

Cybersecurity is defined as protecting computer systems, which communicate over the computer networks

It’s important to understand the distinction between these words, though there isn’t necessarily a clear consensus on the meanings and the degree to which they overlap or are interchangeable.

National Aeronautics and Space Administration(NASA):

National Aeronautics and Space Administration (NASA), independent U.S. governmental agency established in 1958 for the research and development of vehicles and activities for the exploration of space within and outside Earth's atmosphere.

The organization is composed of four mission directorates: Aeronautics Research, for the development of advanced aviation technologies; Science, dealing with programs for understanding the origin, structure, and evolution of the universe, the solar system, and Earth; Space Technology, for the development of space science and exploration technologies; and Human Exploration and Operations, concerning the management of crewed space missions, including those to the International Space Station, as well as operations related to launch services, space transportation, and space communications for both crewed and robotic exploration programs. A number of additional research centres are affiliated, including the Goddard Space Flight Center in Greenbelt, Maryland; the Jet Propulsion Laboratory in Pasadena, California; the Johnson Space Center in Houston, Texas; and the Langley Research Center in Hampton, Virginia. Headquarters of NASA are in Washington, D.C.

Problem Definition

- When most people think of hackers, they picture grizzled, bearded adults sitting in darkened rooms spotlit by the glow of multiple monitors. Or perhaps hardened foreign operatives covertly working for government agencies. If the movie "Wargames" has taught us anything, it's that hacking takes all kinds.

- In 1999, a 15-year-old north Floridian penetrated into Department of Defence and NASA computers, earning himself a spot in the hacker hall of fame. Jonathan James, who operated under the internet name "c0mrade," was a trailblazer in several respects. Not only was he recognized for his high-profile hack at such a tender age; he also became the first juvenile hacker sentenced to serve prison time.

- The majority of James' hacking exploits occurred between late August and October of 1999, when he breached various systems including telecommunications giant Bellsouth and the Miami-Dade school system.

- A 15-year-old computer hacker caused a 21-dayshutdown of NASA computers that support the international space station, and invaded a Pentagon weapons computer system to intercept3,300 e-mails, steal passwords and cruise around like an employee.

- In August and October 1999, c0mrade entered the computer network run by the Defense Threat Reduction Agency, whose mission is to reduce the threat from nuclear, biological, chemical, conventional and special weapons to the United States.

- By entering through a router in Dulles, and installing a back door for access, he intercepted DTRA e-mail, 19 user names and passwords of employees, including 10 on military computers.

  - James was able to enter 13 computers at the Marshall Space Flight Center in Huntsville, Alabama. While there, he stole data and downloaded $1.7 million in NASA proprietary software used to support the International Space Station's physical environment, including control of the temperature and humidity within the living quarters.

  - After the illegal entry was discovered, NASA was forced to shut down their computers for three weeks to check and repair the system at an estimated cost of $41,000.

  - "Breaking into someone else's property, whether it is a robbery or a computer intrusion, is a serious crime," said then-U.S. Attorney General Janet Reno at the time.

  - Discussing his arrest with "Frontline," James said he could have easily gotten away with his crimes if he had bothered to cover his tracks, but he took no measures to hide himself because he didn't think he was doing anything wrong. He said he was just "playing around" and didn't do anything to harm Department of Defense and NASA systems.

  - James' story came to a sad end in 2008, when he committed suicide after being accused of conspiring with other hackers to steal massive amounts of personal and credit card information from department store chain TJX and other prominent retailers. While he believed he would be prosecuted for this crime, he denied any involvement.

Security Measures:

- A 15 year old person was able to attack and steal information of a very important organisation like NASA, is the most serious thing to be considered.

- The organisations like NASA must have some serious security measures because they have very much sensitive data about user, government or organisation itself

- James himself told that, “I certainly learned that there’s a serious lack of computer security, if there’s a will, there’s a way, and if a computer enthusiast such as myself was determined to get into anywhere, be it the Pentagon or Microsoft, it’s been demonstrated that it’s possible and they will do it. And there’s next to nothing they can do about it, because there are people with skill out there, and they’ll get what they want.”

- The main aim is to stop the malicious activity in an organisations digital sector

- The person like James will always try to hack but providing stronger security is what an organisation can do to protect their systems

- The prosecution “shows that we take computer intrusion seriously and are working with our law enforcement agencies to aggressively fight this problem.

- The organisations like NASA should have a security team that will continuous look into protecting the systems. The data should have a proper encryption algorithm and the whole system should have serious security measures taken that will not let any unauthorized person enter into the organisation.

Conclusion

Thus by performing this Case study we understood how NASA got hacked and what adverse effects happened after this. Also what security measures NASA should have taken to stop the unauthorized access. Also we understood deeply the problem and that helped us understand the Cyber Security concepts we learned in the whole semester. This Case study helped us in several ways.

Books/References/Websites

- https://abcnews.go.com/Technology/story?id=119423&page=1
- https://www.industrialcybersecuritypulse.com/throwback-attack-a-florida-teen-hacks-the-department-of-defense-and-nasa/
- https://www.forbes.com/sites/simonchandler/2020/06/08/nasa-hit-by-366-rise-in-cybersecurity-incidents-after-budget-cuts/?sh=20a77675b31b