Kingdom of Saudi Arabia

Ministry of Education

Imam Abdurrahman bin Faisal University

Computer Science Department

College of Science and Humanities

Hacking of governmental system

# Students Names:	#Students ID:
May M. AlOtaibi	2200004606
Ghala M. Alkhaldi	2200003157
Razan A. Alqahtani	2200001391
Fida M. Alelou	2200003041

Date of submission : November 27, 2021

Submit to: Dr.Norah Alnaim

Contents

Abstract:

This report explains the study of the hacking and their impacts on the nation. The study specifically aims to provide the detailed analysis of the hacking in the government system and the precautionary measures and alternatives to reduce the risk of hacking the government system. The study also explains some of the examples from the past and present the conclusion of the research at the end of the report.

Introduction:

It has been seen in the past few decades that several advancements in the computer technology have made their way into the system standard improvements and also advancements in the technical aspects. Along with that, there are also negative points that produce a huge risk for such systems. Therefore, every system needs a proper setup of removing those hurdles and work as legitimate and under polices as much possible. Governments systems are the most confidential systems in any nation because they have to deal with various kind of information and data sets that allow them to negotiate in the interlinked way and also communicate with different authorities therefore a proper security system is required to keep things working and also making the work more steady and perfect.

The word hacking in informational technology refers to getting the data from different sources in non-ethical way and using it for self-interest. Hacking has been a common flaw of information technology sector due to the problem that people find the shortcuts and other possible ways to cut out the security factor and do their desired tasks.

Discussion:

In the recent years, Saudi Arabia has been deciding to implement the strategy for introducing the policies for the companies of the government to regulate the system in such a way that the system works for eliminating the hacking factor. The government files are mostly confidential and therefore the governmental departments must ensure to hire a team to secure the system from hacking attacks. The hacking attacks such as phishing, Trojan horses and the other kinds are the most viral factors that destroy the system and the hackers get access of the confidential files and therefore this is a great threat in such cases.

The governmental level policies have been changed and the educational system is also updated now with a technique that the institutions have new fields introduced such as ethical hacking, cyber security, artificial intelligence and the data sciences which ensure that the study of the such technology is more appreciated and then this way they serve the governmental departments and make it sure that the hacking is not considered as the threat because the technical staff is looking forward to protect the data of the companies. [1]

The very recent attack that got the attention of many people in the world was the Shamoom attack 1 and 2 and later on the Saudi Aramco company was also being hacked and the data was leaked which produced a very negative impact and the company went under a huge loss and therefore the company changed the strategy by introducing cyber-experts in the company to make sure that this kind of problem never happens again.

Objectives of the Project:

Some of the objectives that are covered in this brief report are listed below:

1. Meaning and definition of hacking
2. Controls and rules to protect government systems from hacking and cyber-attacks.
3. Damage caused by the penetration of government systems for users and officials.
4. Raising awareness, understanding problems and being able to develop solutions

Breaking down the objectives in steps, the information is explained below:

What is Hacking?

Hacking has multiple definitions based on the context of the situation but a very common definition is that the breaching of the computer network in such way that the desired information is lost from the authorizer and the some intruders get access of the computers information and use it as they desire. Based on the kind of the hackers there are different types of hacking such as black hat hacking, white hat hacking and the grey hat hacking most commonly used throughout the world. [1]

The white hat hackers are the ethical hackers therefore they work for the betterment and they are most of the time admired by the companies and the government institutions because they help in tracing the hacking approaches and also reduce the risk of hacking for any system. The black hat hackers are the worst among all because they are never welcomed and they work for money, self-interest or some other reasons and they use their capability of breaching the security barriers and try to get the information out of system to use it for different sinful purposes and this kind of hacking is considered as illegal and the government of Saudi Arabia strongly

condemns this and most of the time the black hat hackers have bounty over their head for making a disturbance in the system. [2]

Many think that "hacking person" alludes to some self-educated superstar or rebel developer talented at adjusting PC equipment or programming so it very well may be utilized in manners outside the first designers' purpose. However, this is a tight view that doesn't start to envelop the wide scope of motivations behind why somebody goes to hack. Hacking is ordinarily specialized in nature (like making breaching that stores malware in a drive-by assault requiring no client collaboration). In any case, programmers can likewise utilize brain research to fool the client into tapping on a pernicious connection or giving individual information. These strategies are alluded to as "social awareness."

Truth be told, it's precise to describe hacking as an all-encompassing umbrella term for movement behind most if not all of the malware and vindictive cyber-attacks on the figuring public, organizations, and state-run administrations.

How to overcome cyber-attacks?

In 2021 network safety is as significant as could be expected. With consistently developing dangers to organizations, having a hearty security arrangement is fundamental. It's all known about ventures paying enormous fines or in any event, leaving businesses given a straightforward hack to their frameworks. There are essentially very numerous dangers out there to disregard the dangers from ransom-ware to phishing, it could cost you your work. Counteraction is critical. Quite possibly the most widely recognized way cyber criminals gain admittance to government information is through their workers.

They'll send false messages mimicking somebody in the public authority association and will either request individual subtleties or access specific documents. Connections regularly appear to be real to an undeveloped eye and it's not difficult to fall into the snare. This is the reason worker mindfulness is crucial. One of the most effective methods for securing against

digital assaults and a wide range of information breaks is to prepare legislative workers on digital assault avoidance and advise those regarding current digital assaults. [3]

Government Policies:

With the critical speed increase of advanced change, the paces of digital assaults and the dangers of information breaks have expanded, making the Kingdom quicker to give a protected climate to information and computerized tasks through a vigorous security framework. Proper frameworks controls mean to help fundamental network protection controls.

It gives the base network safety necessities to delicate frameworks dependent on prescribed procedures and norms to meet current security needs and raises the preparation of elements inside the extent of these controls to ensure their touchy frameworks and forestall unapproved admittance to them. Whitecap programmers should be employed and a group of appropriate network safety staff ought to guarantee that the administrative associations are out of risk and is secured.

Effects of Hacking:

The world we are in today is about Information Technology (IT) since we are in the time of Information Technology and individuals with the right data, with the appropriate method of dispersing this data and handling them, is considered as the best. PCs have turned into the pillar of business and government processes. The business has been utilizing them for quite a long time and in many nations, there are drives towards the electronic or signed up government.

This is to permit individuals to get to taxpayer supported organizations from their work areas in their own homes. The quick development of PC wrongdoings and the arrangement of laws in various nations tends to the seriousness of the issue. Government hacking regularly relies upon taking advantage of weaknesses in frameworks to work with an observation objective. Government hacking may likewise include controlling individuals to meddle with their

frameworks. These methods go after client trust, the deficiency of which can subvert the security of frameworks and the web. [4]

Prevention Plan:

State legislatures ought to embrace government systems (NIST Cyber-security Framework) to help lay the basis for a solid, powerful state online protection strategy. The structure gives an undeniable level, vital perspective on the lifecycle of a network safety hazard to assist states with bettering comprehending their online protection hazard, and it empowers them to apply the standards and best acts of overseeing hazard to work on the security and versatility of basic framework and administrations. [5]

Much of the time, the most vulnerable reason behind security for an association including state legislatures, is its faculty. Turning around this peculiarity requires enabling representatives with the abilities they need to remain in front of and be ready to ensure against progressively complex dangers. In any case, just eighteen states today require network safety to prepare for their workers in general. We accept it is fundamental to create a proficient, digitally educated labor force to diminish digital dangers to the state. To make a culture of online protection and lessen the dangers from cyber-attacks, state legislatures should carry out a hearty network safety preparing a program for all state workers. [5]

As information is made and put away by states has expanded, so too have states' lawful and administrative commitments. It has become progressively significant that states look at their consistency and acquirement strategies, and guarantee that their sellers can show that they will empower consistency through their instruments and administrations.

Conclusion:

Policymakers today should constantly make smart, multidisciplinary choices to react to the difficulties of their developing populaces, expanded interconnectivity, changing assumptions for taxpayer-supported organizations, and the vulnerabilities of safety on the internet. Executing network safety and strategy structures to more readily ensure state legislatures can assist with

meeting those difficulties while empowering state workers to all the more likely secure their frameworks. Following the proposals and key methodology spread out in these seven standards can assist states with enhancing, advancing their security objectives, and better ensuring their data innovation frameworks and their residents.

Making public awareness and introducing professional training programs that can help in reduce the risk of hacking. Also, by making new rules and regulation and proper arrangement for the cyber security experts and making it possible that the people care about what they do in the governmental organization and making them understand their responsibilities is the proper way to prevent the hacking in KSA. [7]

References

[1] P. V. Nawaf Alhalafi, "Cybersecurity Policy Framework in Saudi Arabia: Literature Review," *Front. Comput. Sci.,* 2021 .

[2] E. E. Ryan Harkins, "GUARDING THE PUBLIC SECTOR: SEVEN WAYS STATE GOVERNMENTS CAN BOOST THEIR CYBERSECURITY," *marshmclennan ,* 2021.

[3] Chubb, "6 Ways to Protect Yourself From Hackers," 2020.

[4] F. S. a. F. A. Melissa Hathaway, "KINGDOM OF SAUDI ARABIA CYBER READINESS AT A GLANCE," *Potomac Institute for Policy Studies,* 2017.

[5] B. E. Bushra Mohamed, "Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future," *Journal of Information & Knowledge Management ,* vol. 3(12), 2013.

[6] R. Pfefferkorn, "Security Risks Of Government Hacking," 2018.

[7] E. F. Foundation., ""Government Hacking and Subversion of Digital Security".," 2018.

[8] J. Cox, ""The FBI Hacked Over 8,000 Computers In 120 Countries Based on One Warrant".," *Vice.com,* 2016.

[9] J. Granick, ""Challenging Government Hacking: What's at Stake".," 2018..

[10] M. Holloway, ""Stuxnet Worm Attack on Iranian Nuclear Facilities".," 2017.