communications & digital technologies
Department:
Communications & Digital Technologies
REPUBLIC OF SOUTH AFRICA

Policy Brief # 1 / October 2021

Policy brief in response to ransomware attacks

POLICY RECOMMENDATIONS

For State Actors

- Invest in opportunities for security awareness campaigns. That specifically targets employees and individuals to be aware of ransomware attacks and how it is delivered.
- Develop an:
  - Incident response plan
  - Business continuity plan
  - Crisis management plan
- Regularly ensuring the implementation of some form of patch management
- Installing and maintaining anti-malware software.
- Implementing when possible application whitelisting which ensures that only select applications can be executed.
- Enable strong spam filters to help in the prevention of social engineering
- Ensure the principle of least privileges
- Implement network segmentation
- Implement strong access controls such as multi-factor Authentication

For Non – State Actors

- See above mentioned recommendations for state actors

Across all societies, the adoption of technology and is becoming the norm and as such it has become interwoven into our daily lives. But the scale brings with it an air of uncertainty and unforeseen risks and vulnerabilities. One such risk faced is the threat of ransomware.

As part of the **Cyber 9/12 Strategy Challenge: South Africa Regional Competition in 2021,** this brief focuses on recommendations for actors to follow, both non-state and state. It discusses the long and short impacts of these recommendations as well as which agencies are responsible for these recommendations. Furthermore, this policy will discuss whether an actor should attribute the threat and how to respond to these ransomware threats.

Long and short term impact of the recommendations

The high initial cost to implement the policy and provide appropriate training to employees and users that will ultimately remedy any further significant costs from incidents and reputation loss as a result. The short term impact will also enable the organisation to create a clear and comprehensive incident response plan and backups to recover if any further attacks are initiated. The inclusion of a report plan lets users and employees know exactly how and where to report suspicious activity that technicians can assess faster. Immediately removing/disconnecting the affected system to prevent the attack from propagating within the system will significantly improve the short term outcome. The restructuring of access to a least-privilege principle and segmentation of the network will make internal and external systems more inconvenient to compromise as a whole.

The long term impact of the recommendations will, over time, affect the organisational culture surrounding security and the responses to security violations. The shared goals of improving security in the organisation will vastly enhance the identification of attacks, responses, and restoration of systems and reporting incidents. The long term impact from additional security and response will make the system more resilient and inconvenient to attack due to faster and more appropriate reactions.

Vulnerabilities that may enable these form of attacks

The strength of your security is based on multiple perspectives. Vulnerabilities arise with the opportunity to exploit. Using access control in both physical and information security, it is possible to identify and limit access to places and resources. If unauthorised personnel are allowed access, vulnerabilities can arise because they may have the ability to make changes to the source code and install ransomware.

In accordance with the principle of least privilege, users, systems, and processes should only have access to resources such as networks, systems, and files. Specifically, these resources that are absolutely necessary for their assigned task. Accessing classified information only by a select few, both during development and during user administration.

Furthermore, vulnerabilities may occur if computer networks are not segmented into smaller pieces. Segmentation can improve the performance of the network and increase security. These terms are often used interchangeably: network segregation, partitioning, and isolation.

Collaboration between banks and e-commerce business

As e-commerce services almost always make use of electronic payment methods, such as electronic transfers. Therefore, both the e-commerce industry and the banking sector need to collaborate to ensure that the security surrounding the network communication between them is as sound as possible as well as providing warnings in the event of attacks. There needed to be security measures on both ends to ensure that the data that is being transferred between each other is what was intended to be sent and has not been intercepted and modified or replaced with ransomware – as an example.

Addressing these ransomware attacks both internally and externally.

Internally, these actors need to respond immediately to restore their website capabilities. As such, they need to rollback to an uninfected version of the site if possible – as such, offline back-ups are also a strong recommendation for the actors involved. It is also important that these actors make use of an incident response plan crisis management plan if they have ones already set up and if not should update internal policies to include these types of plans. As the e-commerce sites are infected with ransomware and are functionally defunct, they should be taken offline for the time being until they have been reinstated to a functioning version – which will also protect consumers if it is more than just a ransomware attack. Lastly, it is also important to not actually give in to the attackers' demands.

As for externally responding to the threat, the actors involved have several choices on how to handle the situation. They can either attribute the threat or not as well as publically disclosing this response or not. While attributing what type of attack has happened publically is not vital it should also be noted that the exact type of attack may not be known. However, these actors do have an ethical implication to inform their consumers of any attacks that would affect them in some form – either by disrupting transactions or involving their data.

Impact to South African's personal information and data

This scenario's impact on South Africans' personal information and data will result in a loss of part or all of the historical data stored on the affected systems if backups and responses are not in place.

The POPIA 2021, Cybercrime Act 2020, HITRUST CSF version 9 2017, ITIL V3 2011, NIST SP 800-53, NIST SP 800-37, ISO/IEC 20000-1:2011 are laws and regulations that exist to protect data and personal information in South Africa and policy development respectively.

Policy brief developed by: Wumpus Team

- Jumanah Al-Hazba
- Joshua Esterhuizen
- Affaan Muhammed
- Kelvin Popovic